

MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE RUSSIAN
FEDERATION FEDERAL STATE AUTONOMOUS EDUCATIONAL
INSTITUTION OF HIGHER EDUCATION
NORTH CAUCASIAN FEDERAL UNIVERSITY

Methodological guidelines

for the completion of practical work
by discipline

" Organization of protection of confidential information / Организация защиты
конфиденциальной информации"

for students in the field of study

02.04.01 Mathematics And computer science
profile Training Program for Electronic Information

INTRODUCTION

The purpose and objectives of mastering the discipline

The purpose of mastering the discipline "Organization of protection of confidential information / Организация защиты конфиденциальной информации" is to form a future master's degree in the field of training 02.04.01 Mathematics and computer science profile " Training Program for Electronic Information » improving the knowledge, skills and abilities of specialists.

List of competencies to be mastered:

Code	Formulation
ОПК-1	Able to assess the role of information, information technology and information security in modern society, their importance for meeting the objective needs of the individual, society and the state

A list of planned learning outcomes for the discipline, correlated with the planned learning outcomes of the higher education program

Code, formulation of competence	Code, indicator formulation	Planned learning outcomes for the discipline, characterizing the stages of formation of competencies, indicators
ОПК-1 Capable of assessing the role of information, information technology and information security in modern society, their importance for meeting the objective needs of the individual, society and the state	ID-1 understands the role of information security in the Russian Federation's national security system and the forms of information warfare in the modern world	is familiar with the basic concepts associated with ensuring information and psychological security of the individual, society and the state, the concepts of information warfare, information warfare and the forms of their manifestation in the modern world
	ID-2 identifies and classifies information security threats to modern automated systems	analyzes sources and provides classification and assessment of information security threats

EDUCATIONAL AND METHODOLOGICAL MATERIALS

PRACTICAL CLASSES

Section 1. Concept, organization and legal basis for ensuring information security

Topic 1.1. History and modern trends in the development of information security

Plan.

1. History of the development of means and methods of information protection.
2. The main stages of solving information security problems.
3. Protection from information influence.
4. Information war.
5. The concept of information security.

We live in a world of information. Possession of information has always provided an advantage to the opposing side that possesses more accurate and comprehensive information about its rivals. State and commercial secrets emerged at the dawn of human society, along with states and trade between them. Intelligence activities aimed at obtaining this information emerged and developed in parallel. The entire history of state development testifies to the widespread use of intelligence to obtain information about their economies, weapons, military readiness, and other matters.

During the Renaissance, the great Italian thinker of the 16th century, Niccolo Machiavelli, who considered it acceptable in political struggle in the name of great goals to neglect the laws of morality and to use any means, justifying the cruelty and treachery of rulers in their struggle for power, pointed out: "In order to unravel the secrets of the enemy, some commanders sent ambassadors to him, sending with them, under the guise of servants, experienced warriors who observed the structure of the enemy army, learned its weaknesses and strengths, and with their reports facilitated victory"¹.

The topic of intelligence was first developed in detail at the level of a real theory back in the 4th century BC by the Chinese strategist and thinker Sun Tzu, who said: "It is inhumane not to have spies, for one spy will save an entire army"².

In his book, "Treatise on the Art of War," Sun Tzu explores issues of intelligence and counterintelligence, psychological warfare, the use of false rumors and falsifications, and security, which are still relevant today. Specifically, he states:

"Great commanders achieve success by uncovering the enemy's secret game, ruining his plans, sowing discord in his army... The art of a general should consist in keeping the enemy completely ignorant of the battlefield and in concealing from him the points being secured, the smallest measures... If you can do anything, pretend you can't. In other words, keep all your military preparations, the state of your weapons, etc., secret." ³

It's clear that these words remain relevant today and can be applied with justification not only to military conflict but also to intelligence, economic, and

political activities. They are also applicable to law enforcement activities related to combat operations and investigative operations.

Along with military secrets, the opposing sides have always hunted for technological secrets, especially those related to weapons production. In particular, in the 7th century, the Greeks began using "Greek fire" to set enemy ships and fortresses on fire. Greece's enemies, especially the Persians, long and unsuccessfully hunted for the secret of this weapon. Then, in the 13th century, gunpowder appeared in Europe, which marked the beginning of a scientific and technological revolution in the field of armament. *The history of industrial espionage dates back to ancient times. In contrast, owners of industrial and commercial secrets have always carefully guarded them from competitors.* For example, the European hunt for the secret of Chinese porcelain, discovered as early as the 4th century, continued for a long time and yielded no positive results until the invention of a method for porcelain production in Europe itself in the early 18th century. Silk was an even more ancient target for industrial spies.

In the Middle Ages, industrial espionage developed widely in Europe, aimed at obtaining the secrets of guild associations of artisans who monopolized the production and sale of certain products. Considering the importance of preserving technological secrets to ensure economic superiority over other countries, many states adopted special legislation protecting the interests of guild organizations.

The desire to obtain confidential information has always been accompanied by an equally strong desire on the part of the opposing side to protect that information. Therefore, the history of the development of intelligence tools and methods is also the history of the development of information security tools and methods. Moreover, the methods of information security that emerged in ancient times have essentially remained unchanged to this day; only the techniques for their implementation have improved. For example, the method of masking information content has undergone several stages of development.

The most intensive development of these methods occurred during the period of mass informatization of society. Therefore, the history of the most intensive development of the problem of information security is associated with the introduction of automated information processing systems and is measured over a period of more than three decades.

In the 1960s, a large number of open publications on various aspects of information security began to appear in the West. This attention to this issue was primarily driven by the ever-increasing financial losses of companies and government organizations from cybercrime. For example, the FBI's annual report stated that in 1997, American intellectual property owners suffered losses exceeding \$300 billion from the illegal activities of foreign intelligence agencies.

Our country has also long and successfully addressed information security issues—it's no coincidence that the Soviet cryptographic school is still considered the best in the world. However, the excessive secrecy of all information security work, concentrated primarily in law enforcement agencies, and the lack of a regular system for training professionals in this field and opportunities for the broad exchange of experience have led to a certain lag in certain areas of information security, particularly in computer security.

Nevertheless, by the late 1980s, a rapid growth in interest in information security issues had not bypassed our country. Currently, there is every reason to

believe that a national school of information security has emerged in Russia. Its distinctive feature is that, in addition to addressing purely practical information security issues, it places considerable emphasis on developing a well-developed scientific and methodological foundation that creates the objective preconditions for addressing the entire range of relevant tasks on a regular basis.

Naturally, over time, both the understanding of the essence of the information security problem and the methodological approaches to its solution have changed. These changes have occurred gradually and continuously, so Any attempt to divide this process into distinct periods and stages would be artificial. Nevertheless, the entire period of active work on the problem under consideration, depending on the methodological approaches to its solution, can be quite clearly divided into three stages.

The initial phase of addressing information security issues (the 1960s and early 1970s) was characterized by the idea that this activity was meant to prevent unauthorized access to protected information. Formal (i.e., operating without human intervention) means were used for this purpose. The most common methods used in automated data processing systems (ADPS) were password-based access rights to computers and access control to data arrays. These mechanisms provided a certain level of protection, but they did not solve the overall problem, as experienced attackers could easily find ways to overcome them. For objects processing confidential information, protection tasks were primarily addressed by establishing a so-called secrecy regime, which defined a strict access control regime and strict rules for maintaining classified records.

The development stage (seventies, early eighties) is distinguished by intensive searches, development and implementation of methods and means of protection and is determined by the following features:

1. The gradual recognition of the need for comprehensive information protection—the first result of this work—was the joint solution to the problems of ensuring the integrity of information and preventing unauthorized access to it.
2. Expansion of the arsenal of used security tools – the comprehensive use of technical, software and organizational tools and methods has become widespread , and cryptographic protection of information has become widely practiced. The targeted unification of all applied information security tools into functional independent systems.

However, the mechanical growth of security tools and measures ultimately led to the problem of assessing the effectiveness of an information security system, taking into account the ratio of the resources spent on creating it to the probable losses from a possible leak of protected information. To conduct such an assessment, it is necessary to apply the fundamental principles of the theory of assessing complex systems. In other words , successfully addressing the problem of comprehensive information security requires not only scientifically sound concepts of comprehensive protection but also a robust toolkit of methods and tools for solving the relevant problems. The development of such tools, in turn, can only be accomplished on the basis of a sufficiently developed scientific and methodological foundation for information security.

Therefore, the first characteristic feature of the third, *modern stage of* comprehensive information security (from the mid-1980s to the present) is the attempt to analytically and synthetically process data from all available theoretical

research and practical solutions to security problems, as well as the development of a scientific and methodological basis for information security on this basis. The primary objective of the third stage is to transfer the information security process to a strictly scientific basis.

By now, the foundations of a comprehensive theory of information security have already been developed. The formation of these foundations can be considered the beginning of the third stage in the development of information security. It is fundamentally important that Russian specialists and scientists, for objective reasons lagging behind in the development of some specialized methods and means of protection (especially in the field of computer security), At this stage, they made a significant contribution to the development of the fundamentals of information security theory.

An analysis of the stages in the development of information security revealed that the prevailing notion of information security as preventing unauthorized access, until recently, is overly narrow. Moreover, the very concept of "secret" was until recently associated primarily with state secrets, whereas in modern conditions, concepts such as

Industrial, commercial, banking, personal, and other types of secrets .

Therefore, even within the traditional understanding of information security, its scope must be significantly expanded. Based on this, the problem of information security has recently been viewed as a problem *of information security* , which requires a comprehensive solution in two main areas.

The first area includes the traditionally established concept of "protecting state secrets and confidential information," which primarily ensures the impossibility of unauthorized access to this information. Confidential information, in this context, refers to confidential information of a public nature (commercial, banking, professional, party secrets, etc.), as well as personal confidential information (personal data, intellectual property, etc.).

However, recently, the issue of information security has been examined more broadly. It has been discovered that modern technical, technological, and organizational systems, as well as individuals, groups, and society as a whole, are highly susceptible to external information influences, and the consequences of negative impacts can be extremely severe.

Thus, information security is determined by the ability of the state, society, and individuals to:

- ensure, with a certain probability, the security of information resources and information flows necessary to maintain its vital activity and viability, sustainable functioning and development;
- to counter information dangers and threats, negative information impacts on individual and public consciousness and the psyche of people, as well as on computer networks and other technical sources of information;
- develop personal and group skills and abilities for safe behavior;
- maintain constant readiness for adequate measures in information warfare, no matter who imposes it.

Based on the listed objectives, information security can be defined as a state of protection of the information needs of individuals, society and the state, which ensures their existence and progressive development regardless of the presence of internal and external information threats.

In the current circumstances, it is important to consider information security as an integral part of the national security of the Russian Federation. Clearly, ensuring information security is closely linked not only to solving scientific and technical problems, but also to issues of legal regulation of information technology relations and the development of a legislative framework for information protection.

Topic 1.2. The system of organizational and legal support for information security

Plan

Information security system.

1. Structure of the state information security system.
2. The main subjects of the state information security system.
3. State system of organizational and legal support for information security.

An information security system is a set of interconnected means, methods, and measures aimed at preventing the destruction, distortion, and unauthorized acquisition of confidential information displayed by physical fields, electromagnetic, light, and sound waves, or material carriers in the form of signals, images, symbols, technical solutions, and projects.

An information security system consists of two parts: structural and functional. The structural part comprises a set of elements whose interrelations constitute the internal organization and architecture of the information security system. The elements of this system also have external connections that specifically influence the external environment and achieve the system's objectives. These external connections constitute the functional part of the system. Clearly, these two parts are inseparable, representing the internal (organizational) and external (executive) aspects of the information security system.

The structural component of an information security system comprises its internal organization, which enables the system to function effectively and creates conditions for ensuring the security of classified information and its circulation only through the channels established by the system. This includes:

- The system of laws and other state legal acts establishing: the procedure and rules for protecting information, as well as liability for an attempt on protected information or the established procedure for its protection;
- protection of the rights of citizens whose service involves information constituting a state or other secret;
- rights and obligations of government agencies, enterprises and officials in the field of information protection.

2. An information classification system that includes:

- legislative or other definition of categories of information that may be classified as a state secret;
- legislative definition of categories of information that cannot be classified as a state secret;
- delegating authority to classify information as a state secret to the relevant government bodies and their officials;
- compiling lists of information classified as state secrets.

3. A system of security services that ensure the functioning of the entire information security system.

The functional part of the information security system is more adaptive, flexible, and flexible. It strives to best accommodate the needs of the external environment when handling protected information and providing it to consumers, and is also aimed at blocking information leakage channels and preventing its disclosure.

The main elements of the functional part of the information security

system are:

- the procedure and rules for determining the level of secrecy of information, indicating the secrecy classification on information carriers, as well as declassifying information or reducing its level of secrecy;
- internal regime and security regime maintained at the facility, corresponding to the level of secrecy of the information accumulated and used at the facility;
- system of processing, storage, accounting, issuance, dispatch and receipt of media containing protected information, rules for secret office work;
- a permitting system regulating the procedure for consumer access to protected information carriers, to restricted facilities and to their individual premises;
- a system for identifying possible channels for leakage of protected information and measures to block them;
- a system for monitoring the presence of protected information carriers at a facility and identifying attempts to remove them from the facility.

No area of modern society can function without a developed information structure. National information resources are becoming one of the main foundations of any state's economic and military power. Information, permeating all spheres of state activity, acquires specific political, material, and monetary expressions determined by a number of factors, including the extent of damage caused by a decline in its quality.

One indicator of information quality is its security. The issue of information security from a state perspective has become increasingly pressing in recent years and is considered a priority state task and an important element of national security.

The problem identified is so complex, multifaceted, and specific that it can only be addressed through dynamic development—from traditional information protection in processing, transmission, and storage systems to ensuring comprehensive security for protected objects. Such objects These may include not only specialized military and defense facilities, law enforcement units, enterprises, and organizations, but also entire economic sectors, regions, and other state entities. As an integral element of statehood, information security exists in every state and undergoes numerous stages of development, determining its qualitative growth depending on the state's information security needs, capabilities, methods, and means of obtaining it, the state's legal regime, and its actual efforts to ensure information security. The state information security system is understood as a system of legal, organizational, technical, and other measures implemented by federal authorities, local governments, enterprises, organizations, and institutions aimed at ensuring the security of the Russian Federation, preserving its state, official, commercial, and other secrets and restricted information, information resources, systems, technologies, and the means to support them.

Information security is viewed as an activity aimed at preventing the leakage of restricted information, as well as preventing various types of unauthorized and unwanted unintentional impacts on information and its storage media. The pressing need for information security stems from a number of objective factors that play a significant role in modern society. Among these factors, the following are particularly noteworthy:

- the steady increase in the role of information in ensuring the functioning of society and the state;
- ever-increasing intensification of the processes of informatization of various spheres of activity;
- stable
- the tendency of organic fusion of traditional (paper) and automated (paperless) information processing technologies; a sharp decentralization of the use of modern electronic computing equipment, etc.

Despite the overall positive impact, objective appropriateness, and inevitability of these circumstances, they also give rise to a number of negative phenomena, one of which is a sharp increase in the vulnerability of accumulated, stored, and processed information. These phenomena can be both accidental and intentional.

All of the above highlights the urgent need to develop a state information security system, improve its regulatory framework, and create effective methods for ensuring information security. Let's consider the structure of the existing state information security system and the main functions of its constituent bodies.

The main body coordinating the actions of government agencies on information security issues is *the Interdepartmental Commission for the Protection of State Secrets*, established by Decree of the President of the Russian Federation No. 71 of January 20, 1996. The Interdepartmental Commission

– a collegial body whose main function is to coordinate the activities of federal government bodies of the constituent entities of the Russian Federation to protect state secrets in the interests of the development and implementation of state programs, regulatory and methodological documents that ensure the implementation of federal legislation on state secrets.

It operates within the framework of the State System for the Protection of Information from Leakage through Technical Channels, the provisions of which were put into effect by RF Government Resolution No. 912-51 of September 15, 1993. This resolution defines the structure, tasks, and functions, as well as the organization of information protection work in relation to information, Constituting a state secret. The primary objective of the State System for Protecting Information from Leaks through Technical Channels is to implement a unified technical policy, organize, and coordinate information protection efforts in the country's defense, economic, political, scientific, technical, and other areas of activity.

In carrying out its activities, the Interdepartmental Commission has the right to prepare and submit, in accordance with the established procedure, proposals to the President and the Government of the Russian Federation:

- on organizing the development and implementation of state programs, regulatory and methodological documents that ensure the implementation of federal legislation on state secrets;
- on legal regulation of issues of protection of state secrets, improvement of the system of protection of state secrets,
- on the procedure for determining the amount of damage that may be caused to the security of Russia as a result of the unauthorized dissemination of classified information or the classification of information owned by enterprises;
- according to the rules for classifying information constituting a state secret into various levels of secrecy.

The state information security system in our country was officially established in December 1973. It was headed by the USSR State Commission for Countering Foreign Technical Intelligence, which included the heads of all defense industries. The creation of this body and the state information security system it headed was a necessary response to the actions of the United States and its allies in creating a global intelligence system and their rapid development and widespread use of technical intelligence assets. The objects of protection included weapons and military equipment, military and military-industrial facilities, troop and weapons command and control systems, and defense operations.

In the 1980s, Russia's foreign and domestic policies underwent dramatic changes, resulting in radical economic reforms, the conversion of the defense industry, the introduction of open regimes, the development of joint ventures and production facilities with foreign companies, and the development of information processes. These changes created additional conditions and preconditions for foreign intelligence operations, leading to the widespread collection of various sensitive information in all areas of government activity.

– defense, economic, scientific and technical, political, law enforcement, etc. The leakage of information constituting state and official secrets was particularly alarming. It became clear that the information security system established in the USSR, which focused solely on defense matters, no longer met the needs and objectives of our state under the new legal conditions.

By a decree of the President of the Russian Federation dated January 5, 1992, for the purpose of overall coordination of work on protecting information processed by technical means, the State Technical Commission under the President of the Russian Federation— *the State Technical Commission of Russia (now transformed into the Federal Service for Technical and Export Control—FSTEC)*—was established on the basis of the USSR State Technical Commission. The state information security system was reborn, and its scope of interests significantly expanded. It should be noted that the basic principles and forms of information security organization, proven over many years of practical work, were preserved—collegiality in decision-making on the most important areas of information security, in the approval of regulatory and methodological documents, on the one hand, and complete independence and personal responsibility, on the other. managers at all levels for the implementation of decisions taken and the effectiveness of information – on the other.

IN The FSTEC is composed of the heads of federal government agencies that determine scientific, technical, and financial policy for information protection in the political, economic, and military spheres, or their first deputies. Within its purview, the FSTEC performs the following functions:

- forms a general strategy and determines priority areas for information protection in vital areas of state activity in order to prevent damage to the interests of the country;
- determines the main directions of research, reviews and approves concepts, requirements, standards and other regulatory, technical and methodological documents;
- reviews and submits draft state programs for information protection to the government for approval;
- hears the heads of ministries and departments, state enterprises and

associations, and chief designers on issues related to information security.

The Federal Security Service of Russia exercises control over the implementation of organizational and security measures in government agencies and at enterprises conducting work on defense and other classified topics.

Rosstandart acts as a national body for product standardization and certification.

Other government bodies (ministries, departments) within their competence:

- determine the list of protected information; ensure the development and implementation of technically and economically sound measures to protect information at subordinate enterprises;
- organize and coordinate the implementation of research and development (R&D) in the field of information security in accordance with state (industry) programs;
- develop industry documents on information protection in agreement with FSTEC;
- monitor compliance with established standards and requirements for information protection at industry enterprises;
- create industry centers for information protection and monitoring the effectiveness of measures taken;
- organize training and advanced training for information security specialists.

To carry out the specified functions, scientific and technical divisions (centers) for information protection and control operate within government bodies.

At enterprises performing defense and other classified work, there are scientific and technical divisions for information protection and control that coordinate the activities of the scientific and production structural divisions of the enterprise in this area, participate in the development and implementation of information protection measures, and monitor the effectiveness of these measures.

In addition, licensing centers are being created and operating in the industries and regions of the country, which organize and control activities in the field of providing information security services, certification bodies for computer equipment and communications equipment, testing centers for certifying specific types of products according to information security requirements, and certification bodies for information technology objects.

The state information security system implies the need to divide rights and responsibilities between the entities ensuring information security: the state, enterprises, their associations, institutions and organizations, as well as individual officials.

The state, as the main entity ensuring the protection of information, through its legislative, executive and judicial authorities, in order to create conditions for the implementation of protection and coordination of actions to protect information, organizes:

- creation of a system of legal norms regulating relations in the field of information protection;
- implementation of a unified technical policy in this area, development of state programs for the protection of information, requirements, norms and recommendations;
- creation of technical systems and means of protection and control;

- coordination of work carried out to protect information, general and methodological guidance thereof;
- General control over the state of information security in the country, individual regions, and at critical security sites.

Enterprises and their associations, institutions and organizations, regardless of their organizational and legal form and form of ownership, as well as individual officials performing work related to the use of information classified as state and official secrets, must ensure their protection.

In accordance with the stated objectives of the state information security system, five main categories of information security bodies can be distinguished in its organizational structure, implementing the following functions:

1. *Administrative* – form the general strategy of information security, carry out the general organization and They coordinate work, resolve funding issues, and organize industrial production of protective equipment. At the national level, these functions are implemented by bodies such as the Security Council of the Russian Federation, the Interdepartmental Commission for the Protection of State Secrets, and the Federal Service for Technical and Export Control (FSTEC) of the Russian Federation. At the regional level, similar bodies may be created under the governing bodies of the constituent entities of the Russian Federation. Almost all agencies, especially law enforcement agencies (the FSB, the Ministry of Internal Affairs, the Federal Protective Service, etc.), have permanent commissions on information security.

2. *Research and development agencies* organize research and development work and coordinate research and development in the field of information security. At the state level, these agencies include all-Russian research institutes and centers operating under the direct supervision of the Federal Service for Technical and Export Control (FSTEC) of Russia. Many law enforcement agencies have their own research institutes, such as the Research Institute of Special Equipment within the Ministry of Internal Affairs.

3. *Educational and methodological* – carry out preparation and increase qualifications specialists V areas ensure information security, conduct research in this area, develop educational And educational and methodological base teaching information security disciplines. At the state level, these functions are performed by educational and methodological associations that develop a unified policy for training specialists, guiding regulatory documents (educational standards, programs) etc.), coordinating this activity in Russia. In addition, there are many universities of national significance, as well as departmental and regional ones. educational establishments, cooking specialists on information security.

Specialized information security centers conduct research and development in the field of information security and provide a wide range of services to enterprises, institutions, and firms in this field. Such centers, at both the national and regional levels, can certify facilities processing information containing state secrets or personal data; conduct special inspections of premises, special studies of technical equipment; develop and install information security systems at facilities, and perform other work. Moreover, centers can be established on both a government and commercial basis. For example, the largest non-governmental information security centers in Russia are the firms "NOVO" and "Nelk ."

"Confident" and others.

4. *Information security services* address a full range of issues related to direct information security. Such services are required to be established at facilities processing information constituting state secrets and at defense industry enterprises. Banks, large state-owned enterprises, and commercial firms may also establish their own information security services.

The existing composition of information security agencies covers all levels of government and all areas of state activity related to the use of classified and official information, and ensures the implementation of information security measures on a continuous basis throughout the country. The main forms of organizing information security activities are:

- implementation of state orders for the relevant work; licensing of the activities of enterprises and organizations on issues of information protection and admission of enterprises to work with information constituting a state secret;
- certification of systems and means of receiving, processing, storing and transmitting information in terms of information security from leakage through technical channels, as well as protection and control means;
- certification of facilities for compliance with information security requirements;
- Conducting control measures to assess the effectiveness of information protection.

The bodies of the state information security system in their activities are guided by the decisions of the highest federal authorities on the following issues:

- appointment of a special regime for the closure of administrative-territorial entities;
- regulated visits by foreign representatives to individual sites and territories;
- selection of priority areas of information protection in vital areas of state activity;
- implementation of a unified technical policy, legal regulation of information protection and examination of the most important information.

The main government agencies responsible for organizing information security in various fields are the Federal Security Service (FSB), the Federal Protective Service (FSO), the Ministry of Internal Affairs (MVD), the Ministry of Defense (Ministry of Defense), the Ministry of Atomic Energy (Ministry of Atomic Energy), and their respective information security departments. These agencies, within their respective jurisdictions, have specific goals and objects of protection and possess specific protection methods. Their rights and functions in the area of information security are defined by the relevant laws and regulations governing these agencies. Information security departments are either independent structural units or part of one of the main scientific, technical, or specialized departments of a government agency. Specialized companies and organizations licensed to carry out information security work may be contracted to perform information security work.

A significant role in the state information security system is assigned to research, scientific and technical, design and engineering organizations, which are called upon to contribute not only to the development of the entire set of regulatory and methodological documents on information security, but also to actually implement in practice the development and implementation of methods, techniques and means of information security.

With the recent adoption by the Government of the Russian Federation of a number of regulatory documents on the issue of protecting state secrets, regional information protection structures in the constituent entities of the Russian Federation have begun to develop more actively.

An important place in the state information security system belongs to higher education institutions and institutes for advanced training in the training and retraining of personnel in the field of information security, which carry out:

- primary training of specialists in comprehensive information security;
- retraining (advanced training) of information security specialists from government agencies and enterprises;
- Improving the knowledge of heads of government agencies and enterprises in the field of information security.

Thus, the organizational period for the creation of the state information security system has now been largely completed. During its development, extensive experience has been accumulated in its functioning during the transition period. a period characterized by the formation of a new legislative and legal framework in the field of information protection, clarification of the powers and functions of the elements of this system.

The next stage in the development of the state information security system involves the development and practical implementation by specialists of methodological support adequate to the goals and objectives of this system. Scientific research is needed on the comprehensive assessment of potential information security threats and the effectiveness of the information security system, as well as licensing of information security activities, certification of security tools, determining damage from unauthorized dissemination of information, and regulating the legal and financial liability of officials and specialists for information leakage through technical communication channels, its destruction, distortion, and loss.

The organizational and legal framework for information security is a set of decisions, laws, and regulations governing both the overall organization of information security activities and the operation of information security systems at specific sites. Therefore, the organizational and legal framework for information security must ensure the following key functions:

- 1) development of basic principles for classifying information of a confidential nature as protected information;
- 2) determination of the system of bodies and officials responsible for ensuring information security in the country and the procedure for regulating the activities of enterprises and organizations in this area;
- 3) creation of a complete set of regulatory, legal, guiding and methodological documents governing issues of ensuring information security both in the country as a whole and at a specific facility;
- 4) determination of measures of responsibility for violations of protection rules;
- 5) determination of the procedure for resolving controversial and conflict situations on information security issues.

Developing a legislative framework for information security is a necessary measure to address the fundamental need for information protection in the context of the socio-economic, political, and military development of the state. Particular

attention to the formation of such a framework is necessitated by the steadily increasing costs of combating "information" crimes.

The basis for the creation of a state system of organizational and legal support for information security is the state information protection system discussed above, which is understood as a set of federal and other governing bodies and interrelated legal, organizational and technical measures implemented at various levels of governance and aimed at ensuring the security of information resources.

The state system of organizational and legal support for information security is being created to address the following issues requiring legislative support:

- protection of state secrets;
- protection of commercial secrets and provision of favorable conditions for entrepreneurial activity;
- creation of a system of mutual financial settlements in electronic form with elements of digital signature;
- the fight against computer crime, primarily in financial sector;
- protection of personal data;
- insurance of information and information systems;
- certification and licensing in the field of information security, control of information systems security;
- organization of interaction in the field of information security with CIS countries and other states.

An analysis of the current state of information security in Russia shows that its current level does not meet the vital needs of individuals, society, and the state. Negative factors complicating information security include:

- the aggravation of contradictions between the needs of society to expand the free exchange of information and the need to maintain certain restrictions on its dissemination;
- imperfection of the regulatory framework, lack of effective mechanisms for regulating information relations in society and the state;
- poor provision of government authorities and administration with complete and reliable information, underdevelopment of information relations in the field of entrepreneurship;
- insufficient protection of state information resources and the weakness of measures to ensure the safety of state secrets in government bodies and administration;
- Lack of protection of citizens' rights to information, manipulation of information, causing an inadequate reaction from the population and leading to political instability in society.

This situation in the field of information security requires an immediate solution to a number of key organizational and legal problems:

1. Development of the concept of information security, which is the basis of state policy in this area.
2. Formation of a legislative and regulatory framework for ensuring information security.
3. Development of mechanisms for implementing citizens' rights to information.
4. Formation of an information security system that ensures the

implementation of state policy in this area.

5. Improving methods and technical means to provide a comprehensive solution to information security problems.
6. Development of criteria and methods for assessing the effectiveness of information security systems and tools.
7. A study of the forms and methods of civilized influence of the state on the formation of public consciousness.
8. A comprehensive study of the activities of information systems personnel, including methods for increasing motivation, moral and psychological stability, and social security of people working with classified and confidential information.

Practical Lesson No. 1: The System of Organizational and Legal Support for Information Security

At behavior classes necessary consider next questions:

Information security system. Structure of the state information security system. Key entities within the state information security system. State system of organizational and legal support for information security.

Recommended reading:

1. Goncharenko, L. P. Security Management: a textbook / L. P. Goncharenko, E. S. Kutsenko. - M.: KnoRus, 2005 - 272 p.
2. Starostenko, K.V. National security: a teaching aid / K.V. Starostin - Orel: ORAGS, 2003 - 124 p.
3. Malyuk A.A. Information security: conceptual and methodological foundations of information protection: textbook for universities / A.A. Malyuk - M.: Hotline -Telecom, 2004 - 280 p.
4. Grinberg, A.S. Protection of information resources of public administration: textbook / A.S. Grinberg, N.N. Gorbachev, A.A. Teplyakov - M.: UNITY. 2003. - 327 p.

Topic 1.3 Legal basis for information security

Plan

1. Requirements for legislation in the field of information security
2. Legal basis for ensuring information security in Russia.
3. The Constitution and legislative acts of the Russian Federation on information protection.
4. Regulation of information security issues in departmental regulations.
5. Liability for Violating Information Security Requirements. An analysis of international experience in developing legislative frameworks in the field of information security shows that the development of legal frameworks for information security is proceeding in three directions:

1. Protection of individual rights to privacy.

This aspect is not new to the global community. The basic principles for establishing limits on interference in private life by the state and other entities are defined by fundamental norms: the Declaration of Human Rights, the UN Convention on Human Rights, and the Council of Europe Convention on Human Rights.

The development of information technology in Western countries and the associated increase in the threat of violation of individual rights (uncontrolled distribution and access to personal information) required the development of special acts that take into account the factor of information security.

By the end of the 1970s, three basic principles of information security had been formulated, which were subsequently reflected in national legislation on information technology:

- establishing limits on interference with privacy using computer systems;
- the introduction of administrative mechanisms to protect citizens from such interference;
- protection of an individual's intellectual property.

The European Parliament Resolution on the Protection of Individual Rights in Connection with the Progress of Information Technology (1979) and the EU Convention can be attributed to this area.

"On the Protection of Individuals with regard to Automatic Processing of Personal Data" (1980).

2. Protection of state interests.

This problem is addressed through well-developed national legislation defining national priorities in this area. The integration of EU member states necessitated coordinated efforts in this area, resulting in the general principles of information classification being reflected in the EU Convention on the Protection of Secrets. This protection mechanism encompasses the following aspects:

- setting protection priorities;
- definition of executive mechanisms and regulatory support for protection mechanisms.

3. Protection of business and financial activities.

This line of activity is carried out through the creation of a legislative mechanism that ensures the protection of commercial secrets and creates conditions for the

implementation of “fair” competition. When creating a legal basis for information security in our country, it is necessary to take into account:

- the state and composition of international norms in the field of informatization;
- the state of domestic legislation in this and related areas;
- the formation of a legislative system covering all its levels, ensuring the continuity and compatibility of norms in laws at different levels - constitutional, general, special;
- consistent development of departmental and local regulations based on the legislative framework;
- creation of mechanisms that ensure the organization, application, and effectiveness of the legislative framework for informatization.

The directions for creating a legal framework in the field of information security should affect all levels of Russian legislation:

- constitutional legislation;
- fundamental general laws;
- laws on the organization of the state administration system;
- special laws.

For example, the rights of citizens, organizations, and the state to information must be constitutionally enshrined and formalized and consistently ensured in all fundamental laws—on property, citizens' rights, citizenship, entrepreneurship, etc.

Issues of information support must be included in laws on the division of powers and the legal status of various state systems, bodies and organizations of the state structure vertically and horizontally.

Special laws in the field of informatization should be aimed at creating conditions for the organization and ordering of information itself, the management of state information resources, and ensuring the process of incorporating modern technologies into all areas of informatization, creation of an information security system, establishment of guarantees, etc.

In addition to federal legislation, information security issues must be taken into account in the legislation of the republics within the Russian Federation.

Subordinate regulatory acts reflecting information protection processes should occupy an important place in the legal framework for informatization.

This hierarchical structure of the legislative system must be completed by law enforcement legislation, which includes provisions on liability for offenses committed when working with information.

At the level of administrative state regulation in the order of execution specified laws corresponding Government agencies must develop state standards establishing information security standards, as well as organizational and technical requirements and rules. These standards must take into account the vulnerability of information and define a set of comprehensive security measures necessary for the secure processing of information, depending on its value or the public danger posed by disruptions to information systems.

An analysis of the legislative framework for information security, as discussed above, allows us to conclude that a transition is currently underway from the principle of "integrated protection" of information to the principle of "differential protection," ensuring equal protection for various types of protected information. It should be noted, however, that the task of creating a coherent legislative system

that simultaneously satisfies all the stated requirements for comprehensive information protection is proving to be extremely complex and currently lacks adequate solutions. The basic act of the information legislation of the Russian Federation is the Federal Law “*On Information*”, adopted in 2006.

Information Technology and Information Security .” It establishes, for the first time, the legal rights and obligations of citizens, organizations, and the state in the information sphere, establishing a legal framework for the processing and use of information, and a procedure for protecting the rights of subjects of information relations. This Law specifies the following key areas of state policy related to ensuring national security in the field of information technology:

- обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;
- формирование и защита государственных информационных ресурсов;
- обеспечение национальной безопасности в сфере информатизации
- обеспечение реализации прав граждан и организаций в условиях информатизации;
- развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

The said law formulates the following objectives for protecting information and ensuring the rights of subjects in the field of information processes and informatization:

- предотвращение утечки, хищения, утраты, искажения и подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы;

- обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах;
- сохранение государственной тайны и конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

The Law " On Information, Information Technologies, and Information Protection" is the first in Russian legislative practice to regulate the following issues:

- закрепил права граждан, организаций и государства на информацию;
- установил правовой режим информации на основе применения в этой области института собственности, правил документирования, деления информации на открытую и закрытую (с ограниченным доступом), методов формирования информационных ресурсов и пользования ими;
- установил основные права и обязанности граждан, организаций и государства в процессе создания информационных систем, развития научно-технической базы информатизации, формирования рынка информационной продукции и информационных услуг;
- установил гарантии безопасности субъектов в процессе реализации их права на информацию;
- определил порядок включения страны в международные информационные системы.

The said Law recognizes information as an object of property rights of citizens, organizations, public associations, and the state. It emphasizes that information resources can be a commodity and, as material assets, they can be included in the property of organizations. The owner of the information has the right to establish access regimes and protection rules for the information. Access regimes to information resources are determined by the division of information into open and restricted access categories. Restricted information, in accordance with the terms of its legal status, can be classified or confidential.

The Federal Law "On Participation in International Information Exchange" adopted by the State Duma on June 5, 1996

Establishes the procedure for the exchange of confidential and mass information between states. In accordance with this Law, government bodies are obligated to:

- создавать условия для обеспечения, своевременного и достаточного пополнения государственных информационных ресурсов Российской Федерации иностранными информационными продуктами и услугами;
- содействовать внедрению современных информационных технологий для участия в международном информационном обмене;
- обеспечивать защиту государственных ☐ informational resources and compliance with the legal regime of information;

- стимулировать расширение взаимовыгодного международного информационного обмена документированной информацией;
- создавать условия для защиты от некачественной и недостоверной иностранной информации, недобросовестной конкуренции со стороны физических и юридических лиц иностранных государств в информационной сфере;
- способствовать развитию товарных отношений при международном информационном обмене.

□

In accordance with Article 8 of the said law, restrictions have been introduced on the movement of documentary information from the Russian Federation, classified as a state secret or other confidential information, all-Russian national heritage, archival fund and other categories of documented information, the export of which may be limited by Russian legislation.

The protection of state secrets is also regulated by international regulations. For example, in January 1993, the Agreement between the CIS countries on the Mutual Protection of Interstate Secrets was signed in Minsk. It established the general principles for ensuring secrecy in political, economic, scientific, technical, and military cooperation between the states parties to the agreement. The legal framework for information protection also includes a number of other laws, decrees, resolutions, and bylaws that indirectly regulate legal relations in the field of information security. We will list and briefly describe the most important of these.

of the Russian Federation "On

"Law on the Protection of Mass Media" establishes the right to freedom of information: Article 1 states that the search for, receipt, production, and dissemination of mass media information are not subject to restrictions except in cases stipulated by law. Specifically, in accordance with Article 40 of the said Law, mass media may be denied access to requested information if it contains information constituting a state, commercial, or other specially protected secret.

Article 41 of the Law limits the rights of mass media to disseminate confidential information: editors are not entitled to disclose information provided by a citizen under the condition of keeping it confidential in the messages and materials they distribute. The editors are obligated to keep the source of the information confidential and are not entitled to name the person who provided the information under the condition of non-disclosure, except except in cases where the relevant request was received from the court in connection with a case pending before it.

Article 4 of the Law stipulates that it is prohibited to use the media for the purpose of committing criminal offenses, for disclosing information constituting a state or other secret specifically protected by law, for calling for the seizure of power, the violent change of the constitutional order and the integrity of the state, for inciting national, class, social, or religious intolerance or hatred, or for war propaganda. Due to the danger of using neurolinguistic psychology (NLP) techniques, such as "The 25th frame effect" is a law that prohibits the use of hidden inserts in television, video, and newsreel programs that affect only the subconscious of people.

The Federal Laws *"On the Bodies of the Federal Security Service of the Russian Federation"* of April 10, 1995 and *"On Foreign Intelligence"* of January 10, 1996

have much in common in terms of obtaining, processing and using intelligence information, as well as in matters of protecting state secrets.

Article 20 of the Law "On the Federal Security Service of the Russian Federation" states that storing information about individuals and legal entities in information systems does not constitute grounds for taking measures restricting the rights of these individuals. In accordance with Article 6 of the said Law, information about a private life obtained during the activities of the Federal Security Service (FSB) of the Russian Federation that affects a citizen's honor and dignity or could harm their legitimate interests may not be disclosed by the FSB to anyone without the voluntary consent of that citizen, except in cases stipulated by federal laws. The Law "On Foreign Intelligence" prohibits the use of intelligence methods and means by foreign intelligence agencies against Russian citizens within the Russian Federation. Along with the activities of the Foreign Intelligence Service (SVR), this law also regulates the activities of FAPSI radio intelligence units and subdivisions that conduct intelligence activities in the area of encrypted, classified, and other types of special communications.

The Federal Law "On State Security", adopted on May 27, 1996, obliges the bodies of the Federal Security Service (FSO) of the Russian Federation to carry out the following activities:

- организовывать и проводить в пределах своих полномочий мероприятия по развитию и совершенствованию системы президентской связи, обеспечению ее надежности, информационной безопасности и оперативности при предоставлении объектам государственной охраны
- производить шифровальные работы;
- организовывать и проводить на охраняемых объектах, а также в местах постоянного и временного пребывания объектов государственной охраны оперативно-технический контроль;
- осуществлять во взаимодействии с федеральными органами правительственной связи и информации меры по противодействию утечке информации по техническим каналам.

In accordance with *the Law of the RSFSR "On the Police,"* adopted on April 18, 1991, internal affairs agencies have broad powers to conduct work in the information sphere. Specifically, the police are obligated to "receive and register statements, reports, and other incoming information about crimes, administrative offenses, and events threatening personal or public safety" (Clause 3, Article 10).

In accordance with Article 11, the police are granted the right to "receive from citizens and officials the necessary explanations, information, certificates, documents and copies thereof" (clause 4). In addition, they are permitted to "conduct registration, "photographing, sound recording, filming and video recording, fingerprinting of persons taken into custody, detained on suspicion of committing crimes or vagrancy, accused of committing intentional crimes, subjected to administrative arrest, as well as persons suspected of committing an administrative offence when it is impossible to establish their identity..." (paragraph 15).

Information centers and forensic units, in cooperation with other units of the internal affairs agencies and services of other law enforcement agencies (including foreign ones), perform the functions of forming and maintaining national reference and information funds (paragraph 15).

The Regulation on the Ministry of Internal Affairs of the Russian Federation, approved by Decree of the President of the Russian Federation of July 18, 1996 No. 1039, establishes the right of the Ministry of Internal Affairs to form, maintain and use federal records, banks of operational reference, investigative, forensic, statistical and other information, to provide reference and information services to internal affairs agencies, internal troops and other interested government agencies, to organize state statistics and statistics in the system of the Ministry.

The Civil Code of the Russian Federation considers information an object of civil law, along with intellectual property and assets (Article 128). It also defines information constituting official and commercial secrets. Article 139 of the Civil Code sets forth the essence of special formalities that allow for the application of sanctions against those who violate information confidentiality:

- Firstly, this confidential information must have actual or potential commercial value and it cannot be known to third parties; secondly, the institution in possession of confidential information has lawfully taken certain measures to prevent free access to this information and protect its confidentiality;
- Thirdly, all employees familiar with this information were officially warned about its confidentiality.

Adopted on May 24, 1996, the Criminal Code of the Russian Federation enshrines fundamentally new approaches to certain criminal law issues for domestic legislation. In particular, Chapter 28

"Crimes in the Sphere of Computer Information" defines which socially dangerous acts involving the use of computer information are criminal. Article 272 of the Russian Criminal Code establishes criminal liability for "unauthorized access to legally protected computer information, that is, information on a computer storage medium, in an electronic computer (ECM), in a computer system, or in their network, if this act results in the destruction, blocking, modification, or copying of information, or the disruption of the operation of the computer, computer system, or their network." Article 273 of the Russian Criminal Code, for the first time in Russian legislation, establishes criminal liability for the creation, use, and distribution of malicious computer programs or "modifications to existing programs that knowingly lead to the unauthorized destruction, blocking, modification, or copying of information, or the disruption of the operation of the computer, computer system, or their network." In accordance with Article 274 of the Criminal Code of the Russian Federation, the violation of the rules for the operation of a computer, computer system or their network by a person with access to them, resulting in the destruction, blocking or modification of information protected by law, is now considered a criminal offense.

The category of crimes against the constitutional rights and freedoms of man and citizen, of an informational nature, in the Criminal

The following acts are classified in the code: – нарушение неприкосновенности частной жизни, то есть «незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстных или иной личной заинтересованности и причинили вред правам и законным интересам

граждан» (статья 137 УК);

– нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 138 УК), отказ в предоставлении гражданину информации, то есть «неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан» (статья 140 УК);

– воспрепятствование законной профессиональной деятельности журналистов путем принуждения их к распространению либо к отказу от распространения информации (статья 144 УК);

– нарушение авторских и смежных прав (статья 146 УК);

– нарушение изобретательских и патентных прав (статья 147 УК). Среди преступлений против основ конституционного строя и безопасности государства следует выделить такие «информационные» противоправные деяния, как государственная измена (статья 275), шпионаж (статья 276 УК), разглашение государственной тайны (статья 283 УК) и утрата документов, содержащих государственную тайну (статья 284 УК).

Practical Lesson #2: Legal Framework for Information Security

When conducting a lesson, it is necessary to consider the following:

questions:

Information security legislation requirements. The legal basis for ensuring information security in Russia. The Constitution and legislative acts of the Russian Federation on information protection. Information security regulations in departmental regulations. Liability for violating information security requirements.

Recommended reading:

1. Fatyanov, A.A. Legal support for information security in the Russian Federation: a textbook for universities / A.A. Fatyanov. Moscow: Jurist , 2001. - 412 p.
2. Melnikov, V.P. Information security and information protection: a textbook for universities / V.P. Melnikov, S.A. Kleymenova, A.M. Petrakov. - M.: Academy, 2007. - 336 p.
3. Snytnikov , A.A. Ensuring and protecting the right to information / A.A. Snytnikov . - M .: Gorodets- publishing house , 2001. - 344 p.
4. Partyka , T.L. Information security: textbook / T.L. Partyka , I.I. Popov. - M.: Forum-Infra-M, 2004 - 368 p.
5. Yarochkin , V.I. Information security: textbook for universities / V.I. Yarochkin . -M.: Triksa : Acad.proekt , 2005.- 544 p.
6. Rastorguev S.P. Fundamentals of Information Security: a textbook for universities / S.P. Rastorguev. - M.: Academy, 2007. - 192 p.

Section 2. Principles, methods and means of information protection

Topic 2.1. Sources of threats to protected information.

Plan

1. Classification and content of possible information threats.
2. Causes and conditions of leakage of protected information.
3. Methods of illegally obtaining protected information. Let's return to the concept of "information security" discussed above, which was defined as "a state of protection of the information needs of individuals, society, and the state, ensuring their existence and progressive development, regardless of internal and external threats." Based on this concept, **a threat to protected information can be defined as the potential impact of destabilizing factors on the state of information, jeopardizing the vital interests of individuals, society, and the state** . A threat to information in processing systems is understood as the possibility of a phenomenon or event occurring at any stage of the system's lifecycle that could result in undesirable impacts on the information.

Currently, many different *types of information threats are known* , the main ones of which are threats that may lead to violations:

- physical integrity (destruction, destruction of elements);
 - logical integrity (destruction of logical connections);
 - content (change of information blocks, external imposition of false information);
 - confidentiality (destruction of protection, reduction in the level of information security);
 - property rights to information (unauthorized copying, use).
- The most dangerous threats to information processing systems are:
- susceptibility to physical distortion or destruction;

- the possibility of unauthorized modification of data;
- the danger of unauthorized acquisition of information by persons who do not have official access to it.

by their origins as intentional (deliberate threats) and natural (unintentional threats). These threats include destructive and distorting effects of the external environment, the reliability of information processing systems, and the deliberate, selfish actions of unauthorized users whose goal is the theft, destruction, disruption, unauthorized modification, and use of processed information. Intentional (deliberate) threats are those caused by malicious human actions. Accidental (natural) threats are those beyond the control of humans.

Sources of threats to protected information are:

- People;
- technical devices;
- models, algorithms, programs;
- technological processing schemes;
- external environment.

The following are the main *reasons for the emergence of information threats* :

- quantitative insufficiency – a physical shortage of information processing means, causing disruptions in the technological processing process;
- qualitative deficiency – imperfection of the design (organization) of elements of an information system, due to which the possibility of accidental or intentional negative impact on the information being processed or stored may arise;
- activities of intelligence agencies of foreign states - specially organized activities of state intelligence agencies, professionally oriented towards obtaining the necessary information by all available means and methods;
- industrial espionage is the covert activity of domestic and foreign enterprises (firms) aimed at illegally obtaining confidential information used to achieve industrial, commercial, political or subversive goals;
- malicious actions of criminal elements - the theft of information, means of processing it or computer programs for the purpose of profit or their destruction in the interests of competitors;
- poor psychophysiological state – a permanent or temporary uncomfortable psychophysiological state of employees, which, under certain non-standard external influences, leads to an increase in errors and failures in the maintenance of information processing systems or directly to the disclosure of confidential information;
- Insufficient quality training of employees – the level of theoretical and practical training of personnel to perform information security tasks, the insufficient degree of which may lead to a disruption in the functioning of the information security system.

During the course of a company's or organization's operations, protected information may, for various reasons, leave the possession of those who own it, or to whom it was entrusted, or to whom it became known through service or work. When this happens, protected information moves beyond the established scope of circulation, protected by special security measures, and control over its distribution is lost—an information leak occurs.

A leak of protected information is an unauthorized disclosure, the transfer of information beyond the circle of persons to whom this information was entrusted. In other words, a leak of protected information is an unlawful the opponent gains possession of this information and thereby gains the opportunity to use it for his own interests.

An information leak can generally be viewed as the uncontrolled and unauthorized release of confidential information outside an organization or the circle of individuals to whom it was entrusted. An information leak, by its very nature, involves the unlawful (covert or overt, deliberate or accidental) acquisition of confidential information, regardless of the means by which it is achieved.

Along with information leakage, it is necessary to highlight such closely related concepts as disclosure, disclosure and dissemination of protected information, and unauthorized access to it.

Disclosure of protected information is the unauthorized disclosure of such information to individuals without legal access to it, committed by an individual who has been entrusted with the information or who has become aware of it through official duties. Disclosure may include disclosure to colleagues who do not have access to the information, as well as to relatives, acquaintances, and other individuals.

Disclosure of protected information is its publication in the media or use in speeches at public conferences or symposiums by individuals who have become aware of this information in the course of their professional activities. As a result of such actions, protected information becomes publicly known to an indefinite number of people and loses its confidentiality.

Dissemination of protected information is the open use of restricted information.

Unauthorized access is the circumvention of a security system using software, hardware, or other means, as well as due to random circumstances, of access to protected information. One of the most important issues in information security is protecting the storage media itself, as the information being protected cannot exist separately from it. However, not all storage media can be hidden in a safe or behind strong walls, as information may be in the possession of people, and it may be contained in various types of radiation, communication channels, and so on. An adversary typically seeks access to these media, creating a path to the information they seek.

Thus, the source of leakage of protected information is any carrier of classified information to which an adversary has managed to gain unauthorized access, possessing the necessary knowledge and technical means to “remove,” extract information from the carrier, decrypt it and use it for their own purposes to the detriment of the interests of the owner of the information.

The most common causes of information leakage are :

- imperfection of regulatory acts governing information protection;
- insufficient resources and resources to block information leakage channels;
- violation by persons authorized to work with protected information of the established rules for its protection.

The above reasons lead to information leakage if this is facilitated by the corresponding subjective or objective conditions . Subjective conditions for information leakage include :

- ignorance of regulatory acts on information security issues by performers;
- weak educational and preventive work in the team;
- insufficient attention on the part of management to issues of ensuring secrecy;
- weak control over the state of the secrets storage system; decision-making by managers without regard to the requirements of the secrecy regime.

Objective conditions for information leakage include :

- imperfection or absence of regulations governing the rules for protecting information on specific issues;
- imperfection of the list of information subject to classification;
- staff turnover in sensitive units;
- non-compliance of the premises with the requirements necessary for carrying out work with classified documents and products.

These causes and conditions create the preconditions and opportunities for the formation of a leakage channel for protected information. This concept should not be confused with a communication channel, which is a channel (physical medium) for transmitting information from one system (the transmitter) to another (the receiver).

Channel for leakage of protected information - is a social phenomenon reflecting the confrontation between the defender (owner) of information and their opponents. Depending on the forces and means used by the opponent to gain unauthorized access to the protected information, information leakage channels are classified as intelligence, technical, legal, and other.

Agent-led information leakage is the use of covert agents by the enemy to gain unauthorized access to protected information.

Technical channels for information leakage are a set of technical reconnaissance means, unmasking signs of a protected object and signals carrying information about these signs.

Legal channels for leaking information are the use of open sources of information by an opponent, and the extraction of information from persons entrusted with it by virtue of their service under a plausible pretext. Other channels for information leakage include voluntary (initiative) disclosure of protected information to an adversary, export deliveries of secret products abroad, etc.

Methods and means of obtaining protected information can be overt or covert. To obtain protected information that is not readily accessible, covert forces, means, and methods are more often used. The sources of the information obtained can be overt or covert. Accessing sources of protected information may involve overriding security measures. Such activity is typically illegal and punishable by law.

Currently, intelligence can be roughly divided into human intelligence and technical intelligence. The distinction is that human intelligence is obtained using technical means, while technical intelligence is conducted by humans. Therefore, the differences lie only in the predominance of human or technical factors.

The most effective way to obtain protected information is **human intelligence** , which relies on recruited or embedded secret agents. One type of human intelligence is espionage—the deliberate collection, theft, storage, and transfer to a foreign state of information constituting a state secret. The danger of espionage lies in the fact that these actions pave the way for other crimes aimed at harming national security, threatening the territorial integrity, military power, and economic

interests of the state.

Methods of human intelligence have been known since ancient times. For example, as early as the 4th century BC, the famous Chinese commander Sun Tzu wrote in his chapter

" The Use of Secret Agents" in his book "A Treatise on Military "Art" revealed espionage methods, many of which are still used today. The author discusses five types of agents: individuals with access to classified information ("inside spies"), local residents ("local spies"), doubles ("reverse spies"), defectors ("death spies"), and active agents ("life spies").

The agents, consisting of local residents and people with access to secrets, are undercover officers, whom we would now call agents, embedded in the facility being developed.

A double is an agent who has infiltrated the enemy's camp, been exposed by his counterintelligence, re-recruited and used in the "reverse" direction.

Defector agents are a unique Chinese ploy used to mislead the enemy. By defecting, these agents become willing hostages: they risk execution if the information they convey is found to be false. However, their willingness to sacrifice themselves ensures that the enemy will readily accept the disinformation as truth. Historically, such agents were often ambassadors or influential figures within the state, who sought to mislead the enemy through their actions or the information they conveyed, persuading them to take harmful actions. When the enemy relaxed their guard and became lax, the opposing side would launch a military operation.

The agents the Chinese military commander called "active agents" later became known as infiltrators. They infiltrate enemy lines, gather information, and manage to return alive.

The danger of human intelligence lies in the fact that the agent has direct access to classified information. He is among those who work with classified information and protect it. Therefore, Intelligence agencies of all countries do not skimp, trying to recruit precisely such secret bearers .

To obtain protected information through agents, the following methods are used: access to classified information, espionage, and surveillance. Using espionage access to classified documents and documents, an intelligence agent can memorize them, make extracts from them, copy them by hand or on a photocopier, photograph them, and so on, in order to gather the information of interest. When espionage, agents rely on people's talkativeness, thirst for publicity, lapses in vigilance, and simply their own insensitivity. Surveillance can be physical, electronic, or complex, combining elements of both. Physical surveillance is carried out directly by the agent or another person interested in obtaining the protected information. Electronic surveillance is based on the use of specialized technical means and can be accompanied by the recording of audio and video information.

Technical reconnaissance is a type of intelligence activity aimed at identifying and recording data on objects of interest using technical means. The diversity of information carriers has given rise to a variety of technical reconnaissance types. When classified by the physical nature of the storage medium, technical reconnaissance is divided into the following types:

- optical (carrier - light radiation in the visible and infrared parts of the

spectrum);

- radio-electronic (carrier - radio waves and electric current);
- acoustic (carrier - sound vibrations);
- chemical (carrier - particles of substance);
- radiation (carrier - radioactive radiation);
- magnetometric (carrier - magnetic field).

The presented types of technical intelligence provide for the extraction, removal, interception, and copying of information from any known media.

When discussing the dangers of any given type of intelligence, it should be noted that, despite the advances of the scientific and technological revolution, which have led to the widespread use of technical means for obtaining, processing, and storing protected information for intelligence purposes, human intelligence remains the most dangerous. It can solve any task, including those addressed by technical and other types of intelligence. Human intelligence can operate selectively, obtaining the most sensitive information: documents, product samples, the data itself, etc. Therefore, information security measures should be aimed primarily at blocking this particular channel of information leakage.

Topic 2.2. Forensic characteristics of methods for illegally obtaining protected information

Plan.

1. Theft of documents containing protected information.
 2. Illegal acquisition of confidential information Forensics distinguishes two main methods of illegally obtaining protected information:
 - 1) obtaining information by taking possession of a document (or other information carrier, technical means) in which it is contained;
 - 2) Obtaining information without taking possession of the document. The first method includes:
 - a) theft of documents in the possession of the person responsible for them (including “contract thefts” with the participation of specially embedded agents or representatives of criminal structures);
 - b) taking possession of documents that have left legal possession as a result of their loss and are unguarded. The second method covers:
 - a) obtaining information orally from persons aware of it; b) obtaining unaccounted copies of documents made by photocopying, scanning, copying magnetic media; c) obtaining information as a result of interception of information circulating in technical means, premises, and means of transport.
- As a rule, the following are used to illegally obtain information:
- 1) theft of documents and other information carriers;
 - 2) obtaining protected information from individuals who are aware of it from among the organization’s employees (including former ones) through bribery, threats, persuasion, and disguised extortion of information;
 - 3) the introduction of agents into positions that allow them to gain direct access to protected information and documents, or to covertly collect confidential information in the course of official (production) activities;
 - 4) interception of information circulating in technical means and premises (office, residential and others);

5) Unauthorized access to information contained in computers and electronic databases. The criminal's behavior during the implementation of illegal intentions consists of active and varied actions, which may involve various psychological techniques, technical, and other means. Disguise measures are taken.

Crimes are typically logically consistent with the criminal's previous behavior during the preparation and commission of the crime. All this leaves characteristic traces that allow us to obtain information about the nature of the offense (crime), its circumstances, and the perpetrator. Let's consider the forensic characteristics of each of the above-mentioned methods for obtaining protected information. ***Theft of documents containing protected information.***

The choice of method for stealing a document is often determined by the presence of certain deviations from the rules of confidential office work, which reduce the degree of protection of the object of attack.

In the vast majority of cases, documents are stolen secretly. Secret theft consists of the following elements:

1. Preparation for committing a crime.
2. Taking possession of a document.
3. Camouflage actions.

Obtaining sensitive information often requires extensive, multi-stage preparatory operations. The most time-consuming and time-consuming preparation for document theft typically involves infiltrating the organization with special agents. Sometimes these "moles" are infiltrated in stages, through intermediary firms or government agencies.

In such cases, agents' preparatory actions are aimed at gaining official access to confidential records or securing a position that allows them to maintain business contacts with individuals working with classified materials. Agents establish informal relationships with individuals with access to confidential records. They identify persistent violations of confidential document handling regulations in order to create a favorable situation for their secret acquisition. They seek unsupervised access to premises where confidential information is stored or processed, attempting to obtain a key from the authorized personnel to the designated premises or safe. They also prepare hiding places in advance for short-term or long-term storage of stolen confidential materials.

The above actions may be supplemented by: finding accomplices to the crime; manufacturing, finding the instrument of commission crimes; eliminating circumstances that prevent the theft. Some of the above elements of preparation for the theft of documents are also characteristic of the illegal actions of a bribed employee of an organization, as well as of an individual stealing documents on their own initiative for the purpose of selling them.

In some cases, the preparatory stage and cover-up actions may be absent entirely, or present in a very limited form. Such cases typically involve the situational development of criminal intent, particularly among individuals with authorized access to documents.

Preparatory actions for document theft include various types of surveillance to identify circumstances conducive to the commission of a crime. According to one former DGSE executive, each of its representatives abroad must be aware of major contracts currently being signed, closely monitor the travel routes of representatives of competing firms, and anticipate potential topics for trade

negotiations and plan operations to obtain the necessary documentation in advance. A number of foreign commercial firms have units dedicated to cracking safes, secretly entering hotel rooms, and installing listening devices in the homes of competitors and potential future partners for the purpose of economic espionage. Representatives of Russian businesses have already encountered such activities. Units with covert surveillance, eavesdropping, interception of information from technical communication channels, and the like are also currently part of some Russian commercial entities.

Depending on the method of obtaining a document, theft is divided into two main types:

1. Taking possession of a document in the custody of a responsible person without adequate security
2. Taking possession of a document that has left the custody of the responsible person as a result of loss.

Experience shows that the first type of kidnapping is the most common. Actions committed in this manner yield more extensive forensic information, and the aggregated data on them reflects consistent characteristics.

criminal attempts to seize documents⁴.

It was established, in particular, that more than half of the document thefts were committed from locked storage rooms located in official buildings.

In secure rooms, using the standard key. Thieves used the main or spare keys stored in an inappropriate location, stole them from the responsible person, and appropriated them when transferring the storage facility to other employees. Cases of using a non-standard key (by guessing or adjusting the keys) in thefts were sporadic.

The next most common method of obtaining documents is by temporarily leaving them outside the safe in an office (sometimes in an apartment or hotel room) by entering through an unlocked door; through a locked door using a key or master key or other devices; sometimes through an unlocked window. Relatively less common are cases where the criminal exploits the fact that the document was issued without proper documentation (issued without proper registration) or conceals the receipt to obtain it illegally. In accordance with the established procedure, the document after illegal changes have been made into the records of the responsible person (forged entry, theft of a receipt, register, card).

The least common method involves acquiring documents left unguarded during authorized destruction. However, this method is the most dangerous, as the theft and illegal use of documents is most effectively concealed.

A specific type of theft involves the illegal seizure of documents that are not properly secured, during their unauthorized movement in vehicles (planes and trains), or storage in hotel rooms and safes and other places of residence. Typically, these thefts are

These are "custom" thefts, carried out by specially trained employees of government intelligence agencies, private organizations, or criminal elements. The document routes are tracked in advance, and the thieves' actions are carefully planned and disguised as ordinary theft.

It's also possible that in some cases, the thief's intent was genuinely aimed at stealing property (a personal computer, suitcase, or briefcase), and the documents

contained within were disregarded. According to available data, confidential documents were often stolen during attacks on the property of responsible individuals through theft, robbery, or armed assault. Significantly, in many of the cases studied, the responsible individuals were intoxicated.

It should be noted that mistaken possession of a document does not at all eliminate the possibility of harm to the interests of the owner of the protected information. Moreover, the risk of the stolen document falling into the hands of an adversary potentially increases due to improper handling. The possibility of the thief has a new purpose, which involves using the document to the detriment of the owner's interests.

Taking possession of a document that has been lost or lost is less common. Experience shows that in most cases, lost documents are discovered by law-abiding citizens, who return them to their proper owners or hand them over to law enforcement agencies. However, some individuals, having discovered a lost document, take possession of it for illegal purposes, including disclosing or illegally using the information contained within.

The lack of a predetermined motive and goal for such individuals, as well as their consistent personality traits, complicates the selection of a search target. However, it should be noted that the lack of a stable motive in this case increases the likelihood of persuading the perpetrator to return the stolen document. In this case, positive results can be achieved by appealing through the media or by other means of announcing the loss. Motivations to return the document may include the desire to receive official approval of their actions from an organization or agency, sympathy for the responsible party, pity, or the hope of receiving a financial reward.

At the same time, one should not lose sight of the fact that accidental loss can be exploited by an intruder who, for a more or less long period of time, had been nurturing the intention of taking possession of documents containing confidential information and was going to carry it out in one of the ways under favorable circumstances.

The main directions of camouflage actions used by document thieves can be summarized as follows:

1. Concealment of the fact of kidnapping. Typically, such actions involve the use of a specific method of extracting confidential information. Materials that prevent the detection of missing materials based on documentary records. Most often, this involves the theft of a document during authorized destruction. There are known instances of theft of items and products listed as expended or used for their intended purpose. Because this method allows concealing not only participation in a crime but also the fact of the crime itself, it is often used by individuals seeking to obtain a document for the purpose of transferring it to competing organizations.
2. Concealing participation in the theft of a document. This method is the most common method of camouflage employed by thieves. Criminals actively conceal and destroy evidence of entry into a safe deposit box or presence at the crime scene, falsifying physical and physical evidence that could lead to suspicion of other individuals committing the crime, or creating the appearance of a document being lost, mistakenly destroyed, or transferred to other individuals, etc. Miscalculations by those conducting the investigation, inquiry, or preliminary investigation in assessing falsified evidence can significantly expand the number

of leads to be investigated, lead to unfounded suspicions against innocent individuals, and lead to the unjustified termination of the search. On the other hand, identifying traces of concealment is often essential for identifying the method of crime and obtaining other information that can help determine the correct direction for the search for the thief.

A study of practice shows that in some cases, it is advisable to begin the investigation of a loss by searching for traces of concealment. Their discovery in a significant number of cases facilitated the acquisition of the data necessary to uncover the nature of the incident and predetermined the success of the search. Concealing the true motives for acquiring confidential information materials This occurs when documents are found in the thief's possession or when they are caught red-handed. Some thieves develop false explanations for the incident. These explanations are typically aimed at concealing the criminal nature of the events. The seizure of the document, depending on the circumstances, is explained by official necessity, error, carelessness, a desire to make a joke, "teach a lesson in vigilance," or to draw attention to violations of confidential office procedures.

Signs of intentional acts aimed at document theft are characterized by the following indicators. Document theft, occurring under unclear circumstances, is initially considered a loss event. It is impossible to determine the exact nature of this event without verifying the theory that the perpetrator may have attempted to steal the documents, and if this is confirmed, without establishing the severity of the thief's actions. Therefore, signs of intentional acts aimed at the theft of confidential materials are of particular interest to those investigating the disappearance of a document under unclear circumstances. These signs include:

1. The absence of a document from a storage location when its release from possession by other means is excluded.
2. The simultaneous or sequential disappearance of several documents stored in one or different places (safes), or used in work.
3. The disappearance, along with the lost document, of money, valuables, and personal belongings stored in a safe or in an office where the safe was located.
4. Disabling or disabling the security alarm system of the room in which the document was stored. The presence of circumstances indicating an intent to disrupt the work of an institution or individual in order to cover up evidence of another crime. The disappearance of a document on the eve of an investigation into a report of abuse by individuals, etc.
5. The presence of circumstances that could cause bitterness, envy and other base feelings of the kidnapper: the announcement of a penalty, unwanted transfer at work, etc.
6. Threats to steal a document or attempts to illegally take possession of it in the period preceding the event.
7. Unusual awareness by individuals of the absence of a document, coupled with a hidden interest in discovering the loss: an anonymous report of loss, a request to provide a document for work that is not necessary, etc.
8. Receipt of a document or part of it to higher organizations or to persons entrusted with control functions in a non-traditional manner.

Of course, these signs, taken individually, do not always indicate document theft. They may be explained by other factors. To avoid misinterpretations, one should

rely on a combination of interrelated circumstances, the most important of which are traces of document theft.

From a forensic perspective, intentional document thefts are characterized by the presence of specific material traces at the location where the document is stored. These traces include:

- traces of unauthorized opening of the safe - traces of a non-standard key or master key, metal filings on the parts and the lock box;
- damage to the integrity of the seal, or traces of its temporary removal (with subsequent restoration) by cutting or separating it from the body

storage after freezing, turning out the lugs that secure the sealing device;

- traces of use of a spare key stored in a designated place (opening of a package or case in one of the ways);
- traces of damage to the safe body - breaking in, squeezing, cutting;
- fingerprints and clothing marks on the safe body, as well as on documents and items left in the vault after the theft, including skin particles and traces of blood on sharp edges
- traces of document extraction through the opening of the damaged storage facility;
- traces of an outsider entering a protected facility and staying in the premises where the absence of confidential materials was discovered;
- failure or disabling of security alarms
- signs of unlocking the door of the room with a non-standard key or master key, forcing the door or the lock bolt, locking the door in an unusual way;
- signs of entry into the premises through a window or in some other way;
- traces of hands and feet of a stranger in the room, objects thrown out or dropped by him.

Characteristic material traces left by breaching security measures, opening a safe, and handling stolen confidential materials remain on the thief and their clothing. These include abrasions, scratches, and microparticles from a document or object.

Furthermore, the illegal acquisition of confidential materials implies their use (and in some cases, destruction) by the perpetrators. This, in turn, creates the preconditions for the discovery of traces of theft and the exposure of the perpetrators. Traces of use The stolen confidential materials include: material traces on the stolen document - fingerprints, layering of micro-objects, etc. traces of destruction of the stolen document

- scraps of a document, charred parts of it, unburned fragments, paper clips, parts of the product, remnants of the product's substance or products of its combustion.

In a broad sense, evidence of the use of stolen confidential materials may include the use of documents by competing enterprises or private individuals for the purpose of disclosure or illegal use for selfish motives, for educational and scientific purposes, as well as evidence that a person suspected of stealing confidential materials has received significant sums of money or valuables.

International and Russian practice recognizes a wide variety of other methods used to illegally obtain confidential information.

Illegal acquisition of confidential information by theft The theft of small personal computers and magnetic media is generally not significantly different from the document theft cases described above. The following circumstances should be noted as specific features in this case:

- technical means containing information, unlike documents, are most often stolen outside of secure office premises (in air or rail transport, hotels, temporary office premises of exhibition complexes, in apartments at the place of permanent residence of the owners);
- People from the criminal world who specialize in illegally entering premises and opening safes and other storage facilities are often involved in committing this crime (the French DGSE uses employees of the so-called "plumbers" service for these purposes);
- Often, service personnel from hotels, airlines and railway companies are

involved in committing crimes;

- assisting thieves in breaking into premises and opening safes;
- The commission of a crime with the aim of illegally obtaining confidential information is usually disguised as ordinary theft of property.

Illegally obtaining confidential information through espionage. Typical methods of obtaining protected information (hereinafter referred to as espionage or espionage) are characterized by the following characteristics.

Open survey. An individual is induced to disclose information entrusted to them through bribery, threats, or persuasion. Circumstances related to family, ethnic, or racial proximity, as well as the desire to avenge a grievance over unfair treatment by management or dismissal, may also be exploited. Information may be disclosed through oral retelling, by allowing the individual to view the text of a document or text displayed on a computer monitor, or by transmitting information copied to an unaccounted hard drive (paper, diskette).

Disguised acquisition of information (intelligence survey). In this case, we're talking about the use of special techniques to obtain information from informed individuals who unknowingly disclose protected information. For example, information is gathered from scattered statements and slips of the tongue by informed individuals, initiated by the offender. This technique is typically supplemented by the accumulation of relevant information from accidentally overheard or intentionally eavesdropped (without the use of technical means) on official conversations, speeches at meetings, or viewing text on a computer screen. The person collecting the information can exploit inadequate soundproofing of walls and partitions, the design of ventilation ducts and air conditioners, and the lack of visual protection of screens from unsecured areas. These methods of illegally obtaining information are used during collaboration or informal communications, as well as during trade shows, presentations, and seminars with experts and businesspeople.

Cases of covert information gathering using special questionnaires and surveys sent to organizations by mail, fax, and other means have become widespread . Typically, such operations are conducted under the guise of well-known consulting and other firms and are motivated by a desire to establish cooperation. "Intelligence" questions are fragmented and carefully disguised among other questions. The security of this method and the relatively low cost of its implementation allow such operations to be carried out on a large scale.

Various symposiums and conferences are organized specifically to ferret out confidential information. In some cases, shell companies are established to enter into false contracts and sham commercial deals. There are known instances of joint ventures being created specifically to obtain information constituting a trade secret. Typically, contract execution and joint activities are first delayed and then cancelled entirely under trumped-up pretexts.

Due to the difficulties in proving the illegality of such acts, individuals collecting information usually remain unpunished.

Illegally obtaining confidential information through the infiltration of agents.

This method involves obtaining protected information by placing special employees—"moles"—in positions that allow direct access to information and documents, or by covertly collecting confidential information during official (work) activities. The actions of such individuals aimed at collecting information

may include:

- in the theft of documents, defective or unaccounted copies, copying of documents using photographic equipment, a copier, a scanner, a fax machine;
- in the production of additional copies of documents during their replication; in copying magnetic media;
- in recording information on a voice recorder or on paper, memorizing information.

Personal meetings with the "customer" of the obtained information (or another person on their behalf), as well as postal, technical, and other communication channels, may be used to transfer (disclose) the collected information. Preparation for the introduction of a "mole" includes actions to obtain information about the owner and types of protected information, its storage locations, the procedure for obtaining, processing, accumulation, familiarization rules, and the possibility of removing documents and other media outside the territory. The organization's established procedure for familiarization with confidential information, the structure and effectiveness of the security service, and technical security equipment are clarified. Requirements for individuals applying for a job and sources of recruitment are carefully studied. A legend is developed that convincingly justifies the fact of the person's employment with the organization, characterizing him positively from the business and personal sides. Actions are taken to disguise his connections with competitors and criminal elements, certain biographical

data, facts of unseemly behavior or conflicts with the law, creditors, tax and other law enforcement agencies.

Signs indicating a person's possible involvement in the category

"moles" may be identified during the verification process related to the decision on access to work with protected information.

The most effective way to improve the security of Russian business entities' trade and industrial secrets from penetration by individuals infiltrated by foreign intelligence agencies and organizations, as well as domestic criminal organizations, is through business cooperation with domestic intelligence agencies and law enforcement agencies. A successful example of such collaboration is the joint work of units of the Russian Ministry of Internal Affairs and the security services of the Association of Russian Banks under cooperation agreements on banking security.

Illegally obtaining confidential information by intercepting information circulating in technical means and premises. Actions aimed at illegally obtaining information circulating in technical means and premises vary significantly depending on the objects from which the information is obtained and the method used, whether the offender used technical means and devices to intercept information (specifically), or obtained the information through direct perception without the use of technical means.

The objects from which information is removed are divided into the main technical means and systems (and their communications) used for processing, storing and transmitting confidential information, and auxiliary technical means and systems not intended for transmitting, processing and storing confidential information, installed together with the main technical means or in Protected premises. These include various types of telephone equipment, radio communications, security and fire alarms, air conditioning systems, wired radio broadcasting systems, and electronic office equipment.

The specifics of intercepting information using technical means vary depending on the signal from which information technology object they are picking up, the method by which the information is picked up and transmitted, whether the device is stationary or portable, and whether it is located within the protected area or outside it.

Commonly used devices for intercepting information include autonomous automatic devices and electronic devices (bookmarks); devices for intercepting information connected to communication channels; portable devices for intercepting electronic signals and accumulating information, carried by the subject under clothing (covertly worn), or disguised in things he has on him or

"neutral" devices when visiting service residential and other premises.

Electronic devices for intercepting information are divided into the following types:

- built into the main technical means of processing and transmitting information (as a rule, before they are acquired by the organization - the owner of the protected information);
- removing information through secondary electromagnetic radiation;

- Capturing information in the form of an acoustic (speech) signal. The introduction of Type II and Type III interception devices into building enclosures, heating and ventilation systems, furniture and other interior items, as well as lines and fittings of communication, power, lighting, and alarm systems, typically requires entry into the protected premises (or protected area). Vibroacoustic interception equipment is installed using mechanical or optical contact with the enclosing structures of the premises.

The above-mentioned differences in technical equipment are directly related to the method of installation and use and determine the characteristics of the perpetrator. Thus, the person installing a "bug" in a protected area must possess certain technical skills and be able to remain in the area temporarily or permanently without supervision. These individuals are typically employees of the organization or representatives of technical and other services involved in the setup and repair of the equipment.

Information interception devices covertly installed outside the protected premises (area) may be devices that do not require mechanical contact with the monitored object, or they may be connected to lines and communications extending beyond the protected area. These devices may be installed by individuals not affiliated with the specific organization.

Interception of information circulating in a protected area or information technology facilities without the use of special technical means is usually carried out by listening in (eavesdropping) on conversations.

The above-mentioned methods of intercepting information include listening to telephone conversations using monitoring equipment under the guise of carrying out preventive maintenance on telephone exchanges, crosses, cable communications, viewing information from display screens and other means of displaying it through doors and windows.

Obtaining information without the use of technical means, as a rule, is associated with the presence of the person collecting it directly in the protected premises. This person is usually an employee of the organization.

Traces of an offense may include:

- the presence of radio emissions indicating the operation of electronic "bugs" and vibroacoustic interception equipment located in technical equipment, building structures, and furniture and other interior items, in mechanical or optical contact with window frames, glass and other structures of the room, or connected to communication channels;
- mechanical changes in the structure of the premises, heating and ventilation systems, furniture and other interior items, as well as on the lines and fittings of communication, power supply, lighting and signaling systems, which occurred as a result of the installation of the said bookmarks and equipment;
- the presence of damage on the door of the protected premises; the absence of a stamp on the seal with which it is sealed;
- signs of unlocking the lock with a non-standard key;
- signs of unauthorized entry of a person into the protected premises;

- damage to cable insulation and communication wires;
- the occurrence of an unauthorized break in the communication line (and restoration);
- violation of the integrity of the seal or seal of cable wells and distribution cabinets (boxes);
- damage to the insulation of the cords in the switchboard consoles.

Illegal acquisition of confidential information contained in computing equipment and automated systems. Actions of persons illegally acquiring confidential information contained in computing equipment and automated systems. computing technology and automated systems are determined by the type and characteristics of the information carrier.

In some cases, an attack may be committed on technical or software means of computing equipment, means and communication lines intended for movement and copying information.

In others, the attacker attacks the computer's memory storage devices, which may contain information, or magnetic or paper storage media.

A typical method for implementing this intent is the introduction of software or hardware into an IT facility, allowing for bypassing security measures and gaining unauthorized access to information. Equally common is the interception of information contained in computing equipment using electronic devices.

In addition, the theft of machine or other originals of information carriers, software or hardware keys and cryptographic information protection tools may be used to illegally acquire protected information.

It's important to remember that attackers may not only attempt to overcome technical and software security measures. They may also illegally obtain information by influencing employees with official access through bribery, threats, or blackmail. Unauthorized access to protected information may result in the information being read, copied, seized, modified, or destroyed.

Traces of illegal acquisition of information contained in computing equipment and automated systems are Information about unauthorized access attempts recorded by computers (date, time, use of specific hardware and software). Illegal actions may be evidenced by the discovery of non-standard software or hardware in the information technology facility.

Signs of illegal acquisition of information may include traces of theft of machine or other original storage media, software or hardware keys, and cryptographic information protection tools. The methods for detecting and recording these traces are not fundamentally different from those for the theft of confidential documents, as described above.

To obtain the most complete information about the event of illegal seizure of protected information, a criminological characterization of the personality of the offender, that is, the subject of the attack, is required.

First of all, this concerns her attitude towards

The organization is the owner of the information. Thus, the organization's full-time employees who maintain computer equipment, communications, and

operational printing are generally cleared for confidential records and have access to the premises where the information is processed. They must, first and foremost, be checked for involvement in the leak of confidential information.

Other potential victims of data loss include private specialists, employees of related and service organizations, programmers and cryptographers, developers of information processing systems, and equipment adjusters. Without official access to the protected premises or territory, they can obtain information using arbitrary communication channels with databases or specially developed programs. The possibility of involvement in the illegal acquisition of information should also be considered. criminal elements. The latter may or may not be employees of the organization.

Practical lesson: Forensic characteristics of methods for illegally obtaining protected information

When conducting a lesson, it is necessary to consider the following:

questions:

Methods for investigating the loss of confidential documents. Theft of documents containing protected information. Typical personality traits of document theft perpetrators. Main methods of concealment employed by document thieves. Signs of intentional actions aimed at the theft of confidential materials. Illegal acquisition of confidential information through espionage. Illegal acquisition of confidential information through the infiltration of agents. Illegal acquisition of confidential information by intercepting information circulating in technical equipment and premises. Illegal acquisition of confidential information contained in computing equipment and automated systems.

Recommended reading:

1. Konev, I. Information security of the enterprise / I. Koneev, A. Belyaev. - St. Petersburg: BHV-Petersburg, 2003. - 752 p.
2. Informatization of business: concepts, technologies, system / A.M. Karminsky, S.A. Karminsky, V.P. Nesteov, B.V. Chernikov. - M.: Finance and Statistics. 2004. - 624 p.

Topic 2.3. Principles of information protection .

Plan.

1. Legal principles of information protection.
2. Organizational principles of information security.
3. Specific principles of information protection.

The principles of protecting classified or confidential information encompass fundamental theoretical ideas and key practical recommendations for organizing and implementing this activity. They are considered when creating the regulatory framework for information protection and are incorporated as legal norms into legislative and bylaws, thereby becoming mandatory regulatory requirements for information protection entities. These principles have been developed through extensive practice by sensitive organizations and departments in our country and also take into account international experience in protecting state and other secrets. Most current regulatory documents embodying these principles govern the protection of state secrets. However, due to the universality of these principles, they can and should be used when organizing the protection of commercial, professional, personal, and other types of secrets. Information protection principles can be divided into legal and organizational.

Legal principles of information protection guarantee compliance with the law when classifying information and ensuring its protection from unauthorized acquisition and use.

The principle of the legality of information protection lies in the need for normative and legal regulation of this important area of public relations within the state. Legislative and subordinate regulations must clearly and unambiguously define the rights and responsibilities of those subject to information protection, detail the criteria for classifying information as state, commercial, and other types of legally protected secrets, thoroughly regulate the procedure for classifying information and the rules for its protection, and establish criminal, administrative, financial, and other liability for illegal attacks on protected information. Officials and other employees of institutions and enterprises who are entrusted with secrets in their line of work or employment must, in accordance with laws and regulations, be granted the rights necessary to ensure the reliable protection of the classified or confidential information entrusted to them. They are also obligated to comply with the requirements of the relevant regime, the fulfillment of which ensures the security of the information.

The principle of the primacy of international law over domestic law stipulates that information subject to public disclosure under international agreements cannot be classified. Our country has committed to aligning its domestic legislation with the provisions of the conventions and agreements of the European Union, the International Monetary Fund, and other international economic organizations to which it is a party. One of the conditions of membership in these organizations is the provision of information on the actual state of affairs in the national economy.

The principle of equal rights to classify information means the right of a sovereign state, on an equal basis with other countries, to protect and classify information in areas that ensure its national security. Each state has the right to decide for itself

what it will classify and what it will disclose. Reciprocity and equality between states or coalitions of states in protecting national secrets will foster trust in international relations and help eliminate the asymmetry of security restrictions that have developed in different countries. Excessive secrecy by a state always arouses suspicion in other countries, as such actions are usually associated with malicious intent. The principle of information ownership determines the right of information owners (possessors) to take measures to protect it. This may involve copyright and patent law, intellectual property protection mechanisms, commercial or banking secrecy, and other means. Only the information owner has the right to determine what information should be classified, what classification level (classification) to assign, who is allowed access to it, what resources to spend on its protection, and what methods and means to use to ensure the protection of their information. In this regard, Russian legislation has adopted legal acts regulating property relations in the areas of intellectual property, information resources, and commercial secrets, as well as regulating the rights of owners to own, manage, and protect information.

The principle of economic feasibility for information security is that the costs of protecting information must be economically justified. Secrecy must be valued as a consumer property, and its cost must be included in the price of the manufactured product. The profit from using classified information must offset the costs of implementing security measures to protect it. Secrecy is also an economic category, so its observance in a market economy is the responsibility of secret owners, who must determine the duration of secrecy, taking into account the potential benefits of its use or the possible losses from its leakage. In the area of protecting state secrets, other factors (political, military, etc.) also come into play when addressing information security issues.

Organizational principles of information security reflect general rules and approaches to protecting secrets, so they have undergone significantly fewer changes in recent years compared to legal principles. They are used in any socio-political and economic system, being equally effective in protecting state, commercial, banking, professional or other secrets.

The principle of a systems approach to organizing information security involves, on the one hand, identifying possible leakage channels for protected information, and on the other, studying the adversary's (competitor's) capabilities for obtaining protected information. This analysis is carried out taking into account the operating conditions of a specific enterprise, institution, industry, or problem. A systems approach enables the creation of an organically interconnected set of forces, means, and specialized methods to optimally limit the circulation of protected information and prevent unauthorized access. When creating an information security system, a set of protective measures is implemented aimed at preventing the loss and leakage of information.

The principle of maximum limitation of the number of persons admitted to The concept of "secret information" is widely used in all areas of government and commercial activity to protect information. The basic idea behind this measure is that the security of classified information is directly related to the number of

individuals authorized to handle it. The narrower this circle, the higher the likelihood of maintaining the information's secrecy. Organizationally, this protective measure is implemented as follows: only those individuals who have permission (clearance) to review information with the appropriate classification level and the right to access specific information with which they are directly involved in their work are allowed access to classified work and documents.

The principle of personal responsibility for the safety of entrusted secrets is effective when each employee with access to protected information understands their personal interest in maintaining the confidentiality of the information entrusted to them. If an employee sees, If someone believes that keeping certain information secret is only beneficial to the company or the government, but provides no personal benefit, they will approach information protection perfunctorily, complying with relevant requirements solely out of fear of liability. However, an effective way to increase employees' responsibility for maintaining the confidentiality of information entrusted to them is to train them in information security and handling confidential documents.

The principle of continuous information security means that protective measures must be implemented continuously from the moment information is generated, through all stages of its processing, transmission, use, and storage, right up to its destruction or declassification. At the same time, officials involved in working with protected information must not lose sight of related security issues when addressing production, financial, marketing, and other tasks.

The organizational and legal principles of information protection discussed above are fairly general and universal in nature, and therefore are equally applicable across various fields. However, when protecting various types of information and information processes, specific principles are also used, conditioned by the specifics of the subject matter being protected, as well as the forces, means, and methods employed for security purposes.

Topic 2.4. Activities, methods and means of information protection .

Plan.

1. The concept of information security.
2. Information security measures.
3. Methods of information protection.
4. Methods of information protection.
5. Information security tools

Protected information may constitute state, official, commercial, or other types of legally protected secrets, each with its own specific requirements for the regulation, organization, and implementation of such protection. The most common characteristics of protection for any type of protected information are the following:

- protection of information is carried out by its owner or persons authorized to do so;

- information protection is aimed at preserving the owner's rights to own and manage information;

- Information protection is achieved by implementing a set of measures to restrict access to protected information and create conditions that exclude or significantly hinder unauthorized access to classified information.

Protected information isn't usually simply stored in safes—it's constantly being used, accessed, updated, and updated. To prevent this information from becoming known to unauthorized persons, its owner establishes a specific regime that limits its circulation. Any release of classified information outside the designated regime would pose a risk to those from whom it is being protected.

Nowadays, information security is not limited to protecting classified information from possible leakage or loss. The widespread use of computer technology in processing, accumulating, and storing information requires protecting information arrays from destruction, distortion, forgery, blocking, and other interference with information and information systems. Thus, information security - this is an activity owner of the information or persons authorized by him to ensure his rights of ownership, disposal and management of protected information, prevention leakage and loss of information, maintaining its completeness, reliability and integrity, ensuring the secrecy of protected information in accordance with legislative and other regulatory acts.

Information security is closely linked to maintaining a secrecy regime, which is a set of measures to protect information at a specific facility (in a ministry, department, or organization) or during the performance of a specific task (for example, when developing a new type of product). The main objective of a secrecy regime is to establish a level of information security at a sensitive facility that corresponds to the level of secrecy of the information being protected there. Thus, a secrecy regime is the implementation of existing regulations at a specific facility. norms and rules for the protection of information constituting state information, commercial or other secret protected by law.

The secrecy regime requires the implementation of various protective measures:

- implementation of a permitting system that determines the procedure for employee access to protected information or to certain premises where classified work is being conducted;

- compliance with the rules of secret office work regarding the reproduction, handling, and forwarding of secret documents;

- establishment of access control and internal facility regime corresponding to the level of secrecy of the information available at the facility;

- Conducting educational and preventive work with employees working with protected information.

It should be noted that maintaining a confidentiality regime at a facility creates certain difficulties for those working with protected information. Firstly, the security requirements lead to some delays in solving management, official, scientific, and production tasks. This is caused by the need to complete various formalities associated with The receipt, registration, and timely submission of

classified documents. Secondly, the permit system limits employees' ability to use information outside their immediate area of expertise. The system of access to protected information is designed so that each specialist can access only the information they need for their job.

The directions of information protection are determined by the measures used to ensure the protection of classified and confidential information.

Legal measures regulating information protection issues can be divided into two main groups:

- laws and by-laws, decrees of the President and resolutions of the Government of Russia, departmental regulations governing the rules of information protection;

- The criminal, civil, and administrative codes of Russia, as well as other legal acts, establish liability for attempts to access information constituting a state or other secret, and for crimes against the established procedure for maintaining classified information. Criminal law norms, on the one hand, prohibit citizens from committing crimes against protected information under penalty of criminal punishment, and on the other, oblige internal affairs agencies, the Federal Security Service, the courts, and the prosecutor's office to prosecute those guilty of such crimes. Furthermore, violations of secrecy regulations and rules for maintaining state and other secrets may entail financial, disciplinary, or administrative penalties, such as dismissal from service, removal from classified work, demotion in rank or position, or loss of access to classified work and documents. Organizational measures for information security are aimed at ensuring compliance with rules, procedures, and requirements for protecting state or other secrets based on the rules established by laws and regulations. These measures include careful selection and placement of personnel, employee training in information security rules, and monitoring compliance with the secrecy regime. Organizational measures are aimed at preventing leaks of protected information in the press, during employee contacts with foreigners, and in other circumstances that create objective preconditions for the emergence of information leakage channels. Their primary purpose is to prevent unauthorized access to protected information, its disclosure, or exposure.

Engineering and technical measures for information security are a set of organizational and technical measures aimed at preventing or significantly hindering the acquisition of protected information using technical intelligence equipment (TIE). The entire set of engineering and technical measures can be divided into three groups: general preventive measures, organizational and technical measures, and technical measures. *General preventive measures* include legal regulation of the use of technical means during classified work, and the establishment and maintenance of an appropriate secrecy regime to prevent the leakage of protected information.

Organizational and technical measures include the analysis and generalization of information on new developments in technical means, determining their capabilities and making forecasts for their development, and developing methods for protecting information from technical means.

Technical measures include a set of engineering and technical means and measures used to conceal protected information from the enemy's tactical and technical means and to disinformation the enemy technically. They are implemented through the use of specialized vehicles and equipment. Classification. To mask various emissions, reduce their intensity and change their spectrum, electronic noise suppression devices, natural and industrial interference, equivalent and directional antennas are used, as well as the introduction of radio silence and compliance with established rules for the use of communications equipment and computing equipment.

Software and mathematical activities provide for the implementation of the following set of measures to protect information in computer equipment (CET):

- *organizational and security measures* : ensuring the established regime for premises where computer processing and accumulation of protected information is carried out, compliance with the rules of confidential office work during computer typing of documents;
- *engineering and technical measures* : shielding of premises, electronic noise reduction, use of certified computers, etc.;
- *software and hardware measures* that restrict access of information network users to the corresponding categories of protected information, antivirus programs, etc.;
- *cryptographic measures* for coding and encrypting information in computer systems.

The following main methods are used to protect information: concealment, ranking, disinformation, fragmentation, moral and ethical measures, accounting, coding and encryption.

Hiding protected information is one of the most widely used methods. It involves the following steps:

- classification of information, establishment of a corresponding secrecy classification on the media and, in connection with this, delimitation of access to it by users in accordance with the clearance they have; elimination or weakening of technical unmasking signs of protected objects and technical channels of information leakage.

Protected information is classified by categorizing it according to its level of secrecy, restricting access to it according to the user's security clearance, and granting individual users individual rights to use classified documents and perform classified work. Access to information can be restricted by subject matter or by the information's secrecy. This method is a special case of the concealment method, as the information is hidden from users who do not have security clearance.

Disinformation involves the dissemination of deliberately false information regarding the true purpose of certain objects or the content of protected information. It is typically carried out by disseminating false information through various channels, imitation

or distortion of the characteristics and properties of individual elements of protected objects, the implementation of false actions that are similar in their characteristics to the actions of interest to the opponent, etc.

A special case of disinformation is legend-making – supplying the enemy with distorted information about the nature and purpose of the protected information or object, when their presence is not completely hidden, but the actual purpose and nature of the actions are masked.

In practice, given the highly sophisticated nature of modern reconnaissance, completely concealing information about targets is extremely difficult. Modern photo reconnaissance equipment, for example, allows for the capture of images from space with a resolution of several tens of centimeters.

The fragmentation (dismemberment) of information into parts is carried out so that knowledge of one part of it does not allow the restoration of the whole picture. This method is widely used in the production of weapons, but can also be used to protect technological secrets that constitute commercial secrets .

Moral and ethical methods of information protection involve educational work with employees authorized to handle classified work and documents, aimed at developing certain moral principles, views, and beliefs, such as patriotism and an understanding of the importance of information protection for them personally, their work, the organization, the agency, and the state as a whole. Educational work can be supplemented by preventative and control methods and other ways to instill positive qualities in employees.

Accounting is one of the most important methods of information security, allowing for the monitoring of the availability and location of protected information media, as well as the data of the individuals who used them. The main principles of accounting are:

- mandatory registration of all carriers of protected information;
- one-time registration of a specific carrier of such information;
- indication in the records of the address where the given carrier of classified information was sent or where it is currently located;
- sole responsibility for the safety of each carrier of protected information.

Encoding involves converting plaintext into conventional text using codes when transmitting information over communication channels, sending written messages, and also when processing and storing information in computer systems. Encoding typically uses a set of characters (symbols, numbers, etc.) and a system of specific rules, with the help of which information can be encoded in such a way that it can only be read by those with the appropriate key (code) for it. Decoding. Information encoding can be performed using technical means or manually.

encryption is commonly used when transmitting messages over technical communication channels (radio, wires, computer networks). Encryption involves converting information into a form that prevents its contents from being understood unless the interceptor has the appropriate decryption key. Encryption can be either preliminary, where the text of a document is encrypted before transmission via teletype, email, or other means of communication, or linear, where information (conversation, text, graphic images, computer files) is encrypted directly during transmission. Encryption typically utilizes specialized encryption equipment (cipher machines), analog, and digital scramblers.

The importance and effectiveness of such a measure of information protection is

evidenced by the fact that state ciphers, codes and corresponding classified equipment are usually assigned the highest secrecy classification, since they provide the key to declassifying intercepted radiograms .

Numerous methods and tools for information security have been developed. Their diversity is driven by the multitude of known methods for influencing destabilizing factors that pose threats to protected information. Let's examine the content of these methods.

An obstacle consists of creating a barrier to the emergence or spread of a destabilizing factor, preventing it from reaching dangerous proportions. Typical examples of obstacles include blocking devices or programs that prevent unauthorized actions, creating physical barriers to attackers, shielding premises and technical equipment, and so on.

Management involves determining, at each stage of an information processing system's operation, the control actions on system elements that will ultimately address information security issues. For example, access control to a facility includes the following security functions:

- identification of persons seeking access, personnel and system resources (assigning a personal identifier to each object);
- identification (establishment of authenticity) of an object or subject based on the identifier presented by it;
- verification of authority (checking that the day of the week, time of day, requested resources and procedures comply with the established regulations);
- registration (logging) of requests to protected resources;
- response (alarm, shutdown, work delay, request denial) in case of unauthorized actions.

Masking involves transforming information so that it becomes inaccessible to attackers or significantly hinders access. Masking includes cryptographic methods of information transformation, concealment, disinformation, and legending , as well as measures to create noise fields that mask information signals.

Regulation consists of developing and implementing such rules for handling confidential information and the means of processing it that will make it as difficult as possible for an intruder to obtain this information.

Coercion is the creation of conditions in which employees are forced to comply with the rules for processing, transferring, and using protected information under threat of financial, administrative, or criminal liability.

Motivation is a method of protecting information that consists of stimulating personnel with material, moral, ethical, psychological and other motives to comply with established rules for information protection.

An attack can be identified as a separate method used by opposing sides during active operations . This involves both the use of information weapons in information warfare and the direct physical elimination of the enemy (during combat) or their reconnaissance assets.

The above-mentioned methods of ensuring information security are implemented through the use of various means.

Information security tools are a set of engineering, electrical, electronic,

optical and other devices and accessories, instruments and technical systems, computer programs used to solve various information security problems.

Information security tools are divided into physical, hardware and software.

Physical means – mechanical, electrical, electronic-mechanical and other devices and systems that function autonomously, creating various kinds of obstacles in the path of destabilizing factors.

Hardware – various electronic and electromechanical devices integrated into data processing system hardware or interfaced with it specifically to address information security issues. For example, noise generators are used to protect against leaks through technical channels.

Software – special software packages or individual programs included in the software Automated systems for information security purposes. These may include various programs for cryptographic data transformation, access control, virus protection, and more.

Physical and hardware means are combined into a class of *technical means of information protection*. The following requirements apply to them :

- state of constant readiness for use;
- high probability of detecting attempts at unauthorized entry into a secure facility or to protected information carriers;
- high hardware reliability;
- low power consumption and the possibility of autonomous power supply of equipment;
- small dimensions, ensuring low visibility of technical means of information protection;
- minimal maintenance costs.

tasks are solved with the help of technical means of information protection :

1. Creation of physical (mechanical) barriers to accessing information carriers (bars, safes, armored doors and glass, locks, etc.).
2. Detection of attempts to penetrate a protected facility, to places where protected information carriers are concentrated (security alarm systems).
3. Warning of emergency situations (fire, flood, etc.) and their elimination (fire alarm, fire extinguishing equipment, warning equipment, etc.).
4. Maintaining communication with various organizations, departments, premises and other security facilities (radio and wire communications, signaling devices, etc.). Neutralization, absorption or reflection of radiation from used radio-technical devices (screens, protective filters, separating devices in power supply networks, electromagnetic noise suppression devices, etc.).
5. Misleading technical intelligence (disinformation) regarding the true content of protected information.
6. A comprehensive inspection of restricted areas, communication channels and information processing equipment used for compliance with information security requirements, preventive measures to protect the information used there (means of acoustic noise reduction of areas, “burners” of telephone eavesdropping

devices, indicators of electromagnetic radiation, software and hardware means of monitoring radio broadcasts, etc.).

7. Comprehensive information protection in automated data processing systems using filters, electronic locks and keys, and access control systems to protect information to prevent unauthorized copying, distortion, or modification.

The undoubted advantages of technical means include:

- a wide range of tasks to be solved;
- fairly high reliability;
- the possibility of creating advanced integrated security systems;
- flexible response to attempts at unauthorized actions;
- traditional nature of the methods used to implement protective functions.

The main disadvantages of technical means are as follows:

- high cost of many products;
- the need for regular maintenance and control;
- possibility of false alarms.

Practical Lesson #3: Information Security Measures, Methods, and Tools

Questions for discussion:

The concept of information security. Information security measures. Information security methods. Information security tools.

Recommended reading:

1. Shlykov, V.V. Comprehensive provision of economic security of the enterprise / V.V. Shlykov. - St. Petersburg: Aleteya, 1999. - 138 p.
2. Kupriyanov, A.I. Fundamentals of Information Security: A Textbook for Universities / A.I. Kupriyanov, A.V. Sakharov, V.A. Shevtsov. - M.: Academy, 2007. - 256 p.

Topic 2.5. The concept of protected information .

Plan.

1. Features of protected information
2. Carriers of protected information
3. Classification of protected information

Information is the foundation of any human activity. Information becomes one of the primary tools for solving problems in government, production, research, commercial, and other fields. However, in some cases, this information is only valuable when it is known to a limited number of people.

Information as a category that has actual or potential value, like any other type of value, is protected and defended by its owner or possessor. The owner of the protected information owner is a legal entity or individual who, at his own discretion, owns, uses, and disposes of the information belonging to him. protected information is a natural or legal person who has the authority to own, use and dispose of this information information under an agreement with the owner, by virtue of law or decision of administrative authorities.

Every state protects its information resources. State information resources can generally be divided into three broad groups:

- open information, the distribution and use of which are not subject to any restrictions;
- patented information that is protected by national legislation or international agreements as an object of intellectual property;
- classified information that is protected by mechanisms to protect government, commercial, or other protected information.

The concept of protected information includes two categories: classified and confidential. Classified information is currently defined as information containing state secrets. Confidential information typically includes information containing commercial, professional, and industrial secrets, as well as secrets related to the personal (non-official) life and activities of individuals.

When applied to government bodies and administrative bodies, a secret is understood to mean something that is hidden from others and known only to a strictly defined circle of people. The primary use of this concept is for the state to classify certain information, the concealment of which from rivals or potential adversaries enables it to successfully address vital defense issues, as well as political, economic, scientific, technical, and other problems, with less expenditure of effort and resources and without compromising the country's national security. The protected information has the following distinctive features :

- Only the owner (holder) of information or persons authorized by him to do so may classify information, that is, restrict access to it;
- the more important the information is for the owner, the more carefully he protects it in accordance with the level of secrecy assigned to it;
- The information being protected must have a certain value and bring benefit to its owner, justifying the efforts and resources expended on its protection.

The emergence of new protected information is the result of the activity of the subject—the information owner—or their authorized representatives who classified

the information. Once created, it is, as it were, alienated from the subject-author, independently dictating the rules for its use to all who encounter it. The level of information protection is determined by the secrecy or confidentiality classification established by its author or owner.

Once created, protected information (like unclassified information) can be reused over an unlimited period of time by any number of users. It has the ability to withstand destruction, not diminish over time, and even grow with use, generating new information. This property of information growth creates objective preconditions for its vulnerability: if someone borrows classified information without compromising the physical integrity of the medium (an information leak, as they say), the owner may not know about it at all, or may only learn about it from other sources. Classified information also possesses a certain genetic property: data, documents, and products created from it are also, as a rule, classified.

There is also such a feature as the dissemination of information. For open information it is random in nature, whereas the distribution of protected information occurs in a deterministic manner: the possible number of consumers of classified information is determined in advance, in accordance with which a certain number of copies of the relevant document are reproduced, which are then sent to pre-determined recipients.

Information can be displayed on or in material objects that can preserve it relatively unchanged for a long time or transfer it from one location to another. Material objects used to receive, record, accumulate, store, transmit, and subsequently use information are called information carriers.

As a rule, carriers of protected information are protected by their owner. This is because if the person from whom they are protected gains access to them, the carrier may become a source of information from which that person can illegally obtain the information they seek. Article 2 of the Law of the Russian Federation "On State Secrets" defines the term "carriers of information constituting a state secret," according to which this category includes "material objects, including physical fields in which information constituting a state secret is reflected in the form of symbols, images, signals, technical solutions, and processes." Carriers of protected information may include documents, products, substances and materials, electromagnetic, thermal, radiation, and other emissions, hydroacoustic, seismic, and other fields, geometric shapes and dimensions of objects, etc.

A document is information recorded on a tangible medium with identifying characteristics. Documents can take a wide variety of forms: paper, film, photographic film, magnetic tapes and disks, topographic maps, and so on.

Documents are the most informative media, as they usually contain reliable information in a processed form.

and in a compressed form. Signed and approved documents are especially valuable to the enemy, confirming their authenticity.

A document containing protected information is marked with a security classification, which allows consumers to determine who can access this information and how. A weakness of this document is that an unscrupulous

consumer who gains access to it can use the information contained therein for their own purposes, as well as copy, steal, damage, or destroy the document.

A classified document may also be in electronic form, which in no way diminishes its importance as a source of classified information.

Products Items such as military and other equipment, including technical means, materials, and substances secretly used in investigative operations, can also be carriers of protected information. Waste from sensitive facilities, as well as samples of water, air, sediment, soil, and plants taken in the immediate vicinity, allow foreign intelligence agencies to obtain information about the nature of these facilities' activities. Even typing on a typewriter leaves traces of the text on carbon paper, which an inexperienced or careless employee discards in the wastepaper basket after use, potentially leading to the leak of classified information. There are also psychological prerequisites for this possibility, as employees often do not perceive waste as a source of classified information.

Electromagnetic radiation of varying frequencies carries information from the source (radio transmitter, emitter) to the receiver. Their propagation is generally uncontrolled, making them susceptible to interception by appropriate devices. For more information, see The content of the transmitted information must be decoded by the intercepted signals.

Humans are sometimes considered information carriers, with their brains being exceptionally complex systems that store and process information coming from the outside world. The brain's ability to reflect and perceive the outside world and accumulate colossal amounts of information, including sensitive information, naturally places humans in prime position as carriers (or rather, sources) of confidential information. Humans not only have the ability to receive and store information, but also to analyze and process it to create new information.

A person holding protected information can have both positive and negative qualities. The positive aspect is that, as a rule, no information can be extracted from their memory without their consent. They can assess the sensitivity of information and handle it accordingly, knowing to whom and what information can be entrusted.

At the same time, the secret bearer may be mistaken about the authenticity of the consumer of the protected information, through negligence or other reasons lose classified documents, having lost vigilance, blab secrets to his friends and relatives, out of base motives commit treason (collecting, stealing, storing for the purpose of transferring to a foreign state information constituting a state secret, issuing classified information to the enemy, etc.).

Typically, employees with access to state secrets possess a volume of classified information that exceeds what is necessary to perform their official duties. It should be kept in mind that, as a result of informal interpersonal relationships, classified information may be leaked to unauthorized persons. Those who are less responsible about keeping "other people's" secrets than about their own. Vain people often inadvertently reveal confidential information in public speeches and conversations, seeking to demonstrate their knowledge and engage their interlocutor.

Practical lesson #4 : Programming arithmetic algorithms

Introduction

As the means, methods and forms of automation of information processing processes develop and become more complex, society's dependence on the degree of security of the information technologies it uses increases, which is determined by the degree of protection and stability of both computer systems as a whole and individual programs.

The purpose of the work

Research and development of basic methods of symmetric cryptosystems.

Brief information from the theory

Cryptography – ensures the concealment of the meaning of a message by means of encryption and its opening /decryption , which are performed using special algorithms and keys.

A **key** is a specific secret state of some parameters of a cryptographic data transformation algorithm, which ensures the selection of only one option from all possible ones for a given algorithm. **Cryptanalysis** – is engaged in cracking a cipher without knowing the key (checking the cipher's stability).

Coding (not related to cryptography) is a system of symbols used in the transmission of information. It is used to improve the quality of information transmission, compress information, and reduce the cost of storage and transmission.

Cryptosystems are divided into **symmetric** and **public key** .

In **symmetric cryptosystems** , **the same key** is used for both encryption and decryption .

Public-key systems use two keys— **a public key** and **a private key** —that are mathematically related to each other. Information is encrypted using the public key, which is accessible to everyone, and decrypted using the private key, known only to the recipient of the message.

Cryptographic transformations are intended to ensure that information is inaccessible to persons without the key and to maintain the required level of reliability in detecting unauthorized corruption. Most information security tools are based on the use of cryptographic ciphers and encryption/ decryption procedures . According to GOST 28147-89, **a cipher** is defined as a set of reversible transformations of a set of open data into a set of encrypted data, defined by a key and a transformation algorithm.

The following main encryption algorithms are used in cryptography: – алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;

- алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
- гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
- аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Encryption and decryption processes are carried out within a cryptosystem. **Symmetric** cryptosystems typically use the same key for both encryption and decryption . **Asymmetric cryptosystems** use one (public) key for encryption and another (private) key for decryption .

Symmetric cryptosystems.

Transposition ciphers. Medieval ciphers often used tables to perform simple encryption procedures based on the permutation of letters in a message. The key in this case is the size of the table. For example, the message "Today is a new day" is written in a table of 4 rows and 4 columns.

WITH	D	ABOUT	D
E	N	IN	E
G	I	Y	N
ABOUT	N	Y	Ь

To obtain an encrypted message, the text is read line by line and grouped into 4 letters: СДОД_ЕНВЕ_ГЯЫН_ОНЙЬ

The single key permutation method is somewhat more resistant to attack . It differs from the previous method in that the table columns are permuted using a keyword, phrase, or set of numbers the length of a table row. Using the word "Vase" as the key, we obtain the following table.

IN	A	Z	A					A	A	IN	Z
3	1	4	2					1	2	3	4
WI TH	D	AB OU T	D					D	D	WI TH	A B O U T
E	N	IN	E					N	E	E	IN

G	I	Y	N					I	N	G	Y
AB OU T	N	Y	Ь					N	Ь	AB OU T	Y

Before the rearrangement. After the rearrangement.

The top row of the left table contains the key, and the numbers beneath the letters of the key are determined according to the natural order of the corresponding letters in the alphabet. If the key contained identical letters, they would be numbered from left to right. The resulting encryption is: ДДСО_НЕЕВ_ЯНГЫ_НЬОЙ.

To ensure additional security, a message that has already been encrypted can be re-encrypted. To do this, the size of the second table is chosen so that the lengths of its rows and columns differ from the lengths of the rows and columns of the first table. It is best if they are relatively prime.

In addition to single permutation algorithms, **double permutation algorithms are used**. First, the message text is written to the table, then the columns are permuted one by one, followed by the rows. During decryption, the order of permutations is reversed. The number of double permutation variants increases rapidly with the table size: for a 3 x 3 table, there are 36, for a 4 x 4 table, there are 576, and for a 5 x 5 table, there are 14,400.

An example of this encryption method is shown in the following tables. The key to the cipher is column numbers 2413 and row numbers 4123 of the original table:

	2	4	1	3			1	2	3	4			1	2	3	4
4	W I T H	E	G	A B O U T		4	G	W I T H	A B O U T	E		1	I	D	N	N
1	D	N	I	N		1	I	D	N	N		2	Y	A B O U T	Y	IN
2	A B O U T	IN	Y	Y		2	Y	A B O U T	Y	IN		3	N	D	Ь	E

3	D	E	N	Ь		3	N	D	Ь	E		4	G	WI	A	E
														T	B	
														H	O	
															U	
															T	

Double permutation of columns and rows

The resulting encryption was: YADNNOYVND'EGSOYE. In the Middle Ages, **magic squares were also used for encryption** . Magic squares are square tables with consecutive natural numbers inscribed in their cells, starting with one, which add up to the sum of each column, each row, and each The diagonals contain the same number. To encrypt, you need to enter the original text according to the numbering in the square and then rewrite the table contents row by row. The result is a ciphertext formed by rearranging the letters of the original message.

16	3	2	13			A	AN	R	T
						B	D		
						O			
						U			
						T			
5	10	11	8			Z	Sh	E	Yu
9	6	7	12			–	A	A	WI
							N		T
							D		H
4	15	14	1			E	G	A	P
								B	
								O	
								U	
								T	

A R I V I N G O N T H E 6 T H

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

The number of magic squares increases very sharply with the increase in the size of its sides: for a 3*3 table there are 1 such square; for a 4*4 table - 880; and for a 5*5 table - 250,000.

Procedure for performing work

In DELPHI, VBA C++ or C#, write a program to encrypt and decrypt a text file using the method specified by the teacher.

Contents of the report

1. Title of the work.
2. Purpose of the work.
3. Block diagram of the encryption algorithm.
4. Program texts.

Self-test questions

1. The purpose and objectives of cryptography.
2. Single permutation and keyword permutation ciphers.
3. Double transposition ciphers. Magic square encryption.

Recommended reading

1. Zhelnikov V. Cryptography from papyrus to computer. Moscow: ABF, 1997. – 336 p.
2. Nils Ferguson , Bruce Schneier "Practical Cryptography", Moscow: Williams Publishing House, 2005. - 424 pages.
3. Petrov A.A. "Computer security. Cryptographic methods of protection", Moscow: DMK, 2000. - 448 p.
4. Koblitz N. Course of number theory in cryptography. – Moscow, Scientific Publishing House TVP, 2001.
5. Maslennikov A. Practical cryptography BHV – St. Petersburg 2003.
6. Schneier, Bruce, Applied Cryptography. Protocols, Algorithms, and C Source Code. Triumph, 2002.
7. Barichev S. Fundamentals of Modern Cryptography. Training Course. Telecom Hotline, 2002.

Additionally

8. <ftp://ftp.kiae.su/msdos/crypto/pgp>
9. <http://drago.centerline.com:8080/franl/pgp/...>
10. Yahoo - Computers, Security-and-Encryption

Practical Lesson #5: Programming Algebraic Algorithms

Introduction

There is currently no single technical method or means for ensuring information security, but the common solution to many security problems is the use of cryptography and cryptographic transformations of information.

The purpose of the work

Research and development of classical methods of symmetric cryptosystems

Brief information from the theory

Simple substitution ciphers. The Caesar cipher is a special case of a simple substitution cipher. The method is based on replacing each letter of the message with another letter of the same alphabet, by shifting K letters from the original letter.

The famous phrase of Julius Caesar VENI VINI VICI - I came, I saw, I conquered, encrypted using this method, is transformed into SBKF SFAF SFZF (when shifted by 4 symbols).

the Greek writer Polybius invented the so-called **Polybian square**, a 5x5 grid filled with randomly ordered alphabets. The Greek alphabet has 24 letters, with the space as the 25th symbol. To encrypt the grid, a letter was found in the grid and the letter below it in the same column was written into the ciphertext. If the letter was in the bottom row of the grid, the top letter from the same column was used.

Complex substitution ciphers. The Gronsfeld cipher The Caesar cipher is modified with a numerical key. To do this, the digits of the numerical key are written under the letters of the message. If the key is shorter than the message, its entry is repeated cyclically. The ciphertext is obtained in much the same way as in the Caesar cipher, but instead of counting the third letter alphabetically (as in the Caesar cipher), the ciphertext is counted from the letter that is shifted alphabetically by the corresponding digit of the key.

Let's say the key is a group of three numbers - 314, then the message is

TOP SECRET

Key 3143143143143143143

Encryption FPISIOSSAHILFIUSS

In **polyalphabetic substitution ciphers**, a different simple substitution cipher (its own alphabet) is used to encrypt each character of the original message.

	ABVGDEYZHZIKLMNOPRSTUFHCHSHSHSHYYY YUYA_
A	ABVGDEYZHZIKLMNOPRSTUFHCHSHSHSHYYY YUYA_

B	_ABVGDEYZHZIKLMNOPRSTUFHCHSHSHSHYYY YAY
IN	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЫЬЭЮ
G	YUYA_ABVGDEYZHZIKLMNOPRSTUFHCHSHSHS HCHYYE
.	
I	VGDEЁZHZIKLMNOPRSTUFHCHSHSHSHCHYYY YYUYA_AB
_	BVGDEYZHZIKLMNOPRSTUFHCHSHSHSHYYY YUYA_A

Each row in this table corresponds to a single substitution cipher, similar to the Caesar cipher for a space-padded alphabet. When encrypting a message, it is written in a row, followed by the key. If the key is shorter than the message, it is repeated cyclically. The ciphertext is obtained by finding the symbol in the table column for the letter of the text and the row corresponding to the letter of the key. For example, using the key AGAVA, the following ciphertext is obtained from the message ARRIVING ON THE SIXTH:

Message	I'M ARRIVING ON THE 6TH
Key	AGAWAAGAVAAGAWAA
Encryption	ПНИГЗЖЮЮУАЭОТМГО

In a computer, such an operation corresponds to adding the ASCII codes of the message characters and the key modulo 256.

Gaming

encryption process involves generating a cipher suite and superimposing this suite on the original plaintext. Before encryption, the plaintext is split into blocks $T(0)_i$ of the same length (64 bits each). The cipher gamma is generated as a sequence of blocks $G(sh)_i$ of similar length $T(w)_i = G(w)_i + T(0)_i$, where $+$ is bitwise addition, $i = 1 - m$).

decryption process comes down to re-generating the text cipher and overlaying this gamma on the encrypted data $T(0)_i = \Gamma(w)_i + T(w)_i$.

Procedure for performing work

Basic steps of encrypting a text file using the gamma method . Get the key, input and output file name from the user.

1. Initialize the random number generator using the key. Open the specified files.

2. Read a line from a file.
3. Get a random number.
4. Get the ASCII code of the next character in the string and increase it by the random number obtained in step 4.
5. Check the validity (valid range) of the new ASCII code.
6. Write the next character corresponding to the ASCII code obtained in step 6 to the output string.
7. If you have not reached the end of the input string, then go to step 4.
8. Write the resulting string to the output file.
9. If the end of the file has not been reached, go to step 3.
10. Close files.

The decryption algorithm is similar to the encryption algorithm, except that we subtract 256 from the ASCII code and check whether it is greater than zero or not.
 Open Filename For Input As # FileNumber – opening file For readings . Out
 Put – for output.

In ASCII code, characters 10 and 13 (carriage return).

You need to open the files as binary, the keyword is Binary . Line
 Input # FileNumber , A\$ is a string variable.
 Print – for recording.

To read and write a binary file, we declare a variable of type Variant .
 Put # NF ,, VA Get # NF,, VA
 Close – closes the file.

In VBA, C++, or C#, write a program to encrypt and decrypt a text file using the method specified by the teacher.

Contents of the report

1. Title of the work.
2. Purpose of the work.
3. Block diagram of the encryption algorithm.
4. Program texts.

Self-test questions

1. Gronsfeld cipher .
2. Double transposition ciphers. Magic square encryption.
3. Polyalphabetic substitution cipher and its implementation algorithm.

Recommended reading

1. Zhelnikov V. Cryptography from papyrus to computer. Moscow: ABF,

1997. – 336 p.

2. Nils Ferguson , Bruce Schneier "Practical Cryptography", Moscow: Williams Publishing House, 2005. - 424 pages.

3. Petrov A.A. "Computer security. Cryptographic methods of protection", Moscow: DMK, 2000. - 448 p.

4. Koblitz N. Course of number theory in cryptography. – Moscow, Scientific Publishing House TVP, 2001.

5. Maslennikov A. Practical cryptography BHV – St. Petersburg 2003.

6. Schneier, Bruce, Applied Cryptography. Protocols, Algorithms, and C Source Code. Triumph, 2002.

7. Barichev S. Fundamentals of Modern Cryptography. Training Course. Telecom Hotline, 2002.

Practical Lesson #6: Protecting Against Backdoors in Program Development

The purpose of the work

Research and analysis of Windows XP utilities to improve computer performance .

Brief information from the theory

A firewall is a security system that acts as a protective barrier between a network and the outside world. Internet Connection Firewall (Internet Connection Firewall (ICF) is a software tool used to configure restrictions governing data exchange between the Internet and a home or small office network. You can use the Network Setup Wizard to configure network connection settings. When sharing computer resources, never share the entire C: drive, as your passwords are stored in the Windows directory.

Procedure for performing work

Task 1. Set up authentication for access to computer resources from the local network. Block access to your computer's resources from the Internet.

1. To verify authenticated access to computer resources from the local network, follow these steps.

Open Control Panel by selecting Start > Settings > Control Panel from the Windows Start menu . **Double** - click the **Network Connections icon** and in the *Network Connections Properties window* , select the **Authentication tab**. Check the boxes for "**Manage network access using IEEE 802.1X,**" "**Authenticate as the computer when computer information is available,**" and "**Authenticate as a guest when computer or user information is not available.**"

2. To enable Internet Connection Firewall, check the box and open the **Advanced tab**. and check the "**Secure my connection to the Internet**" box. Click "OK" to complete the network connection settings.

Task 2. Allow remote access to your computer's resources.

1. Right-click the My Computer icon to open *the System Properties window* and select the Remote tab. Check the box next to Allow remote access to this computer

and click the button.

"OK" to close *the System Properties window*.

2. To share a printer installed on this computer from the network, open the Printers and Faxes window by selecting Settings - **Printers and Faxes** from the Windows main menu. Select the desired printer in the window and open the printer properties window. On the Sharing tab, click the link "If you know the security risk but want to share the printer without running the wizard, click here." In the *Printer Sharing window*, enable the "Allow" option. "Sharing" and click the "OK" button. After that, in the printer properties window, on the Sharing tab, check the "Share this printer" box, and in the *Share name field*, specify the printer name. By clicking the button

Click "Apply" to apply the changes you've made to the printer properties, and close the printer properties window by clicking "OK." In the *Printers and Faxes window*, a hand icon will appear under the printer icon, indicating that the printer is shared. Close *the Printers and Faxes window*.

3. To view the access and security settings for a drive or a specific folder, select the object (drive or folder) and select Sharing and Security from the context menu. In the *Properties window*, open the Sharing tab and select the Share this folder check box. Specify the name under which this resource will be visible to network users. If you allow network users to modify files in this folder, select the Allow network users to modify files check box. Click Apply to apply the changes to the folder properties, and close the properties window by clicking OK.

Task 3. Using remote access to network resources.

1. Windows Explorer and select **Map Network Drive** from the **Tools** menu. In the *Map Network Drive window*, specify the drive letter and network folder you want to connect to. If you don't know the exact folder name, click the Browse button, select it in the *Browse for Folder window*, and click OK. If you want to reconnect to this network folder every time you log on, select the **Reconnect at logon** check box. Click Finish to complete the connection to the network resource.

2. Settings - **Printers and Faxes** from the Windows Start menu. In the *Printers and Faxes window*, select Add Printer from the File menu. **In the Wizard window** *When installing printers*, select the type of printer you want to install by checking the box next to "A network printer connected to another computer." Click "Next," select "Connect to a printer," and enter a name for the printer in the *Name field*. Click "Finish" to complete the connection to the network printer. Close the *"Printers and Faxes" window*.

Task 4. Protecting and restoring data on a computer

1. **Backup** utility, back up the data from the C:\Program Files \ Microsoft folder. Office \ Templates to an archive named Templates on drive D:.

To launch the Data Backup application, select **Programs - Accessories - System Tools - Data Backup** from the **Start** menu. If the backup application starts in Wizard mode, click the "Advanced" button in the Backup Wizard window to switch to Advanced mode.

To archive the selected files and folders on your hard drive, go to the **Archive tab** and select the check box in the Select the check boxes for the C:\Program Files \ Microsoft folder list. Office \ Templates , the data from which you want to archive. Specify drive D: as the drive and the file name for the archive Templates , click the Archive button, and then in the *Archive Task Details window* , select the option **Overwrite the drive with this archive.**

Click the "Archive" button to start the archiving process. Then, in the *Archiving Progress window* , monitor the archiving process. Once completed, a completion message window with brief information will appear. To view the detailed report, click the "Report" button.

Backup utility , create a backup of your system files and an emergency repair diskette that can be used to restore your system in the event of a system failure. Prepare a blank 1.44 MB diskette to save your system settings, then run the Backup utility in **Advanced mode. From the Tools** menu , select Emergency Repair **Wizard** . Follow the on-screen instructions. Click Next to proceed to the next step of the wizard. After selecting the system backup media type and the name of the backup media, for example, D:\Arxiv\Backup.bkf , click "Next" to create the archive. After this, the archive will be executed. system files required to boot the system and create a rescue diskette.

Once the backup process is complete, when prompted to insert a floppy disk, insert a blank floppy disk. This will create a rescue diskette. To view a detailed report, click the button.

"Report." Close the **Data Archiving program window.**

Assignment for work

1. Using the System Information program, determine the following computer system parameters: information about the ports available on the computer, the sound device, system drivers, and automatically loaded programs.
2. Using a standard Windows program **Check disk**, check drive A: for bad sectors and file system errors. If errors are found, enable the disk's bad sector recovery mode to automatically fix system errors.
3. Using the standard **Disk Cleanup program, clean up drive D:**
4. Using the standard **Disk Defragmenter program**, run assess the fragmentation of files on drive D: and, if necessary, defragment this drive.
5. **Backup** utility , back up the data from the C:\Program Files \ Microsoft folder. Office\Templates to an archive named Templates on drive D:.
6. **Backup & Recovery** utility to create an archive of system files and a rescue diskette that can be used to restore the system in the event of a system failure.

Self-test questions

1. Why is it important to know the parameters of a computer system when operating it?
2. What standard Windows XP tools allow the user to determine computer system parameters?
3. Why is ensuring the smooth operation of a computer's disk system one of the

most important measures to ensure information security?

4. Describe the causes of malfunctions in magnetic disks.
5. Why is the disk cleanup procedure necessary?
6. What is file fragmentation? Why does it occur, and how does it affect disk read speed?
7. When is disk defragmentation recommended?
8. What is the purpose of archiving computer data?
9. What is a rescue diskette? What program creates it?
10. What programs do you know for recovering information from magnetic disks?

Recommended reading

1. Guk M. IBM PC Hardware. Encyclopedia. - St. Petersburg: Piter, 2002, - 928 p.
2. The pages of this book provide a systematic description
The hardware component of the most common personal computer family. This book provides in-depth knowledge of both individual electronic subsystems (memory, processors, disks, etc.) and their interconnection into a single unit. Hardware is examined in conjunction with software, providing a comprehensive picture of computer operation.
3. Miiasi M. Modernization and maintenance of a personal computer. Basic course. - M.; Vek, 2000. - 592 p.

Practical Lesson #7: Programming Public-Key Cryptographic Algorithms

Introduction

No matter how complex and reliable cryptographic systems are, their weak point in practical implementation is the problem of *key distribution*. For the exchange of confidential information between two information system entities to be possible, a key must be generated by one of them and then somehow confidentially transmitted to the other. In other words, in general, key transmission requires the use of some kind of cryptosystem.

public key systems were proposed based on the results obtained in classical and modern algebra.

The essence of these systems is that each recipient of an information system generates two keys, linked according to a specific rule. One key is declared *public*, and the other *private*. The public key is published and accessible to anyone who wishes to send a message to the recipient. The private key is kept secret.

The original text is encrypted with the recipient's public key and transmitted to them. The encrypted text cannot, in principle, be decrypted with the same public key. Decryption of the message is only possible using the private key, which is known only to the recipient.

The purpose of the work

Research and analysis of the main methods of asymmetric cryptosystems

Brief information from the theory

The very definition of irreversibility contains an ambiguity. *Irreversibility* refers not to theoretical irreversibility, but to the practical impossibility of calculating the reciprocal value using modern computing tools within a reasonable timeframe.

Therefore, to ensure reliable information protection, public key systems (PKS) are subject to two important and obvious requirements:

1. The transformation of the original text must be irreversible and exclude its recovery based on the public key.
2. Determining the private key from the public key should also be impossible with current technology. A precise lower bound on the complexity (number of operations) of cracking the cipher is desirable.

ElGamal encryption scheme. The ElGamal encryption algorithm is based on the use of large numbers to generate public and private keys, and its cryptographic strength is due to the difficulty of calculating discrete logarithms.

Sequence of user actions:

1. The recipient of the message chooses two large numbers P and G , where $P > G$.
2. The recipient chooses a secret key - a random integer $X < P$.
3. The public key $Y = G^{x \text{ is calculated}} \bmod P$.
4. The recipient chooses an integer K , $1 < K < P - 1$.
5. Message encryption (M): $a = G^K \bmod P$, $b = Y^K M \bmod P$, where the

pair of numbers (a, b) is the ciphertext .

The RSA data encryption cryptosystem was proposed in 1978 by Rivest , Shamir , and Aldeman and is based on the difficulty of factoring large integers into prime factors. They exploited the fact that finding large prime numbers is computationally easy, but factoring the product of two such numbers is practically impossible. It has been proven (Rabin's theorem) that breaking the RSA cipher is equivalent to such a factorization. Therefore, for any key length, a lower bound can be given for the number of operations required to break the cipher, and, given the performance of modern computers, the time required can also be estimated.

The ability to reliably assess the security of the RSA algorithm has become one of the reasons for its popularity among dozens of other cryptographic schemes. Therefore, the RSA algorithm is used in banking computer networks, especially for remote client interactions (such as credit card processing).

Currently, the RSA algorithm is used in many standards, including SSL, S-HHT P , S-MIME, S/WAN, STT and PCT .

Sequence of user actions:

6. The receiver chooses two large prime integers p and q , based on which he calculates $N = pq$; $M = (p - 1)(q - 1)$.
7. The recipient chooses a random integer d that is coprime to the value of M and calculates the value of e from the condition $ed = 1 \pmod{M}$.
8. d and N are published as the public key, e and M are the private key.
9. If S is a message and its length is: $1 < \text{Len}(S) < N$, then this text can be encrypted as $S' = S^d \pmod{N}$, that is, it is encrypted with the public key.
10. The recipient decrypts using the private key:
 $S = S'^e \pmod{N}$.

Example: Let's encrypt the message "SAB." For simplicity, we'll use small numbers (in practice, much larger ones are used).

1. Let's choose $p = 3$ and $q = 11$.
2. Let's define $n = 3 \cdot 11 = 33$.
3. We find $(p - 1)(q - 1) = 20$. Therefore, as d , relatively prime to 20, for example, $d = 3$.
4. Let us choose the number e . This number can be any number for which the relation $(e \cdot 3) \pmod{20} = 1$ is satisfied, for example 7.
5. Let's represent the encrypted message as a sequence of integers using the mapping: A1, B2, C3. Then the message takes the form (3,1,2). Let's encrypt the message using the key $\{7, 33\}$.
 $\text{IIT1} = (3^7) \pmod{33} = 2187 \pmod{33} = 9,$
 $\text{IIT2} = (1^7) \pmod{33} = 1 \pmod{33} = 1,$
 $\text{IIT3} = (2^7) \pmod{33} = 128 \pmod{33} = 29.$
6. let's decrypt the received encrypted message (9,1,29) based on the private key $\{3, 33\}$:
 $\text{IT 1} = (9^3) \pmod{33} = 729 \pmod{33} = 3,$
 $\text{IT 2} = (1^3) \pmod{33} = 1 \pmod{33} = 1,$
 $\text{IT3} = (29^3) \pmod{33} = 24389 \pmod{33} = 2.$

So, in real systems, the RSA algorithm is implemented as follows: each user chooses two large prime numbers and, in accordance with the algorithm described above, selects two prime numbers e and d . The result of multiplying the first two numbers (p and q) is determined by n .

$\{e, n\}$ forms the public key, and $\{d, n\}$ forms the private key (although it can be done the other way around).

The public key is published and accessible to anyone who wishes to send the key's owner a message encrypted with the specified algorithm. Once encrypted, the message cannot be decrypted using the public key. The owner of the private key, however, can easily decrypt the received message.

Procedure for performing work

Basic steps of encrypting a text file using the gamma method .

1. Get the key, input and output file name from the user.
2. Initialize the random number generator using the key. Open the specified files.
3. Read a line from a file.
4. Get a random number.
5. Get the ASCII code of the next character in the string and increase it by the random number obtained in step 4.
6. Check the validity (valid range) of the new ASCII code.
7. Write the next character corresponding to the ASCII code obtained in step 6 to the output string.
8. If you have not reached the end of the input string, then go to step 4.
9. Write the resulting string to the output file.
10. If the end of the file has not been reached, go to step 3.
11. Close files.

Assignment for work

In VBA, C++, or C#, write a program to encrypt and decrypt a text file using the method specified by the teacher.

Contents of the report

1. Title of the work.
2. Purpose of the work.
3. Block diagram of the encryption algorithm.
4. Program texts.

Self-test questions

1. Double square encryption algorithm. Enigma cipher .
2. DES encryption algorithm.
3. Encryption algorithm GOST 28147-89.
4. RSA encryption algorithm.

5. Gamal encryption algorithm .
6. Tasks and algorithms of electronic signature.
7. Key distribution problems.

Recommended reading

1. Zhelnikov V. Cryptography from papyrus to computer. Moscow: ABF, 1997. – 336 p.
2. Nils Ferguson , Bruce Schneier "Practical Cryptography", Moscow: Williams Publishing House, 2005. - 424 pages.
3. Petrov A.A. "Computer security. Cryptographic methods of protection", Moscow: DMK, 2000. - 448 p.
4. Koblitz N. Course of number theory in cryptography. – Moscow, Scientific Publishing House TVP, 2001.
5. Maslennikov A. Practical cryptography BHV – St. Petersburg 2003.
6. Schneier, Bruce, Applied Cryptography. Protocols, Algorithms, and C Source Code. Triumph, 2002.
7. Barichev S. Fundamentals of Modern Cryptography. Training Course. Telecom Hotline, 2002.
- 8.

Additionally

9. <ftp://ftp.kiae.su/msdos/crypto/pgp>
10. <http://drago.centerline.com:8080/franl/pgp/...>
11. Yahoo - Computers, Security-and-Encryption

Practical Lessons #8-9: Preventing Computer System Virus Infections

The purpose of the work

Analysis and research of antivirus programs.

Brief information from the theory

Kaspersky Anti-Virus 7.0 represents a fundamentally new approach to information security. Kaspersky Anti-Virus 7.0 is a new generation of information security solutions.

The main difference between Kaspersky Anti-Virus 7.0 and existing products, including those from Kaspersky Lab, is its comprehensive approach to protecting information on the user's computer.

Kaspersky Anti-Virus 7.0 represents a fundamentally new approach to information security. The key feature of the application is the unification and significant improvement of the current functionality of all the company's products into a single, comprehensive security solution. The application provides not only antivirus protection but also protection against unknown threats.

You no longer need to install multiple products on your computer to ensure comprehensive protection. Simply install Kaspersky Anti-Virus 7.0.

Comprehensive protection is provided across all data entry and transmission channels. Flexible configuration of any application component allows for maximum customization of Kaspersky Anti-Virus to meet the needs of each individual user. Unified configuration of all protection components is also available.

You can work with Kaspersky Anti-Virus via the command line. This allows you to perform the following operations:

- starting, stopping, pausing and resuming application components;
- start, stop, pause and resume virus scanning tasks;
- obtaining information about the current status of components and tasks and their statistics;
- checking selected objects;
- updating application databases and modules;
- call help on command line syntax;
- Calling up command syntax help.

Command line syntax:

avp.com <command> [parameters]

The following are used as <commands>:

ACTIVATE	Activate the application online using an activation code
-----------------	--

ADDKEY	Activating the application using a key file (executing the command is only possible with the password specified via application interface)
START	running a component or task
PAUSE	suspend the operation of a component or task (executing the command is only possible with the password specified via application interface)
RESUME	resume the operation of a component or task
STOP	stopping the operation of a component or task (executing the command is only possible with the password specified through application interface)
STATUS	display the current status of a component or task
STATISTICS	display statistics on the operation of a component or task
HELP	Help with command syntax, list of commands

SCAN	checking objects for viruses
UPDATE	launching an application update
ROLLBACK	rollback of the last application update (the command can only be executed by entering the password specified through the application interface)
EXIT	exiting the application (executing the command is only possible with the password specified through the application interface)
IMPORT	Importing Kaspersky Anti-Virus protection settings (the command can only be executed by entering a password specified through the application interface)
EXPORT	Exporting Kaspersky Anti-Virus protection settings

Kaspersky Anti-Virus protection is built based on threat sources. Each source has its own dedicated program component, ensuring control and implementing the necessary measures to prevent malicious impacts on user data. This design of the protection system allows for flexible customization of the application to meet the

needs of a specific user or the entire enterprise.

Kaspersky Anti-Virus includes:

- Real-time protection components that ensure protection of your computer on all channels of information receipt and transmission.
- Virus scan tasks that search for viruses in individual files, directories, disks, or areas, or perform a full computer scan.
- An update that ensures that the application's internal modules, as well as the databases used to scan for malware, are up to date.

- Service functions that provide information support for working with the application and allow you to expand its functionality.

Kaspersky Anti-Virus includes a special component that protects your computer's file system from infection: File Anti-Virus. It launches at operating system startup, resides permanently in your computer's RAM, and scans all files opened, saved, and executed.

Microsoft taskbar . Windows , which takes the form every time a file is checked.

By default, File Anti-Virus scans only new or modified files—that is, files that have been added or modified since they were last accessed. The file scanning process follows the following algorithm:

1. Each user's or program's access to each file is intercepted by the component.
2. [the iChecker](#)™ and [iSwift](#)™ databases for information about the intercepted file . Based on this information, a decision is made on whether to scan the file.

The verification process includes the following steps:

1. The file is analyzed for viruses. Malicious objects are detected using the application's databases. These databases contain descriptions of all currently known malware, threats, network attacks, and methods for neutralizing them.
2. As a result of the analysis, the following application behavior options are possible:
 - a. If malicious code is detected in a file, File Anti-Virus blocks the file and attempts to repair it. If the repair is successful, the file becomes available for use. If the repair fails,

The file is deleted. When a file is repaired or deleted, a copy of the file is placed in backup storage.

b. If code resembling malware is detected in a file, although there's no 100% guarantee, the file is placed in a special quarantine storage area. An attempt to disinfect it can be made later using updated databases.

c. If no malicious code is detected in the file, it immediately becomes available for work.

Procedure for performing work

Task 1.1. Review the encyclopedia of computer viruses on the Kaspersky Lab website at [http:// www.viruslist.com/viruslist.asp](http://www.viruslist.com/viruslist.asp), To do this, open a web browser, enter the encyclopedia address, and explore the sections. What is a computer virus? Classification of computer viruses. View a description of one of the most popular viruses of the week on the Kaspersky Lab website. In the "Methods of Detecting and Removing Computer Viruses" section, explore the topic "Methods of Using Antivirus Software."



2. Launch Kaspersky Anti-Virus 7.0 and examine the main program window.



Fig. 5.1. Main window of Kaspersky Anti-Virus 7.0

3. One of the key components of computer antivirus protection is virus scanning in user-defined areas. Kaspersky Anti-Virus 7.0 scans individual objects (files, folders, disks, removable devices) and the entire computer for viruses. Virus scanning eliminates the possibility of malicious code spreading that is undetected by real-time protection components for various reasons.

Kaspersky Anti-Virus 7.0 includes the following virus scan tasks by default:

Critical areas

Scans all critical areas of the computer for viruses. These include system memory, objects executed during system startup, disk boot sectors, Windows system directories, and system32. The goal is to quickly detect active viruses in the system without running a full computer scan.

My Computer

Search for viruses on your computer with a thorough check of all connected drives, memory, and files.

Startup objects Checking for viruses in objects that are loaded when the operating system starts.

Search for rootkits

Searching for rootkits on your computer, which conceal malware within the operating system. These utilities infiltrate the system, masking their presence, as well as the presence of processes, directories, and registry keys of any malware described in the rootkit's configuration.

By default, these tasks are run with recommended parameters. You can [change these parameters](#) and [set a schedule, running tasks](#).

It is also possible [to create your own tasks](#). Virus scans and schedule their execution. For example, you can create a task to scan mailboxes once a week or a task to scan My Documents for viruses.

In addition, you can [scan any object for viruses](#). (for example, one of the hard drives containing programs and games, email databases brought from work, an archive received by email, etc.) without creating a special scan task. You can select an object for scanning from the Kaspersky Anti-Virus 7.0 interface or using standard Microsoft operating system tools. Windows (for example, in the Explorer window or on the Desktop, etc.).

You can view a full list of virus scan tasks created for your computer in the Virus Scan section on the left side of the main application window.

You can create [a rescue disk](#), which is designed to restore the system after a virus attack that has damaged the operating system files and prevented it from booting. To do this, use the [Create Disk link](#). [disaster recovery](#).

4. To check the functionality of File Antivirus;

1. Enable logging of all events to ensure that the report file contains information about corrupted objects or objects not scanned due to a failure. To do this, select the "Log non-critical events" checkbox in the "Reports and data files" section of the application settings window.

2. Create a folder on the disk, copy into it the test "virus" downloaded from [the organization's official website](#), as well as the modifications of the test "virus" you created.

File Anti-Virus will intercept the file access, scan it, and notify you if a dangerous object is detected:

By selecting different options for actions on a detected object, you can test File Anti-Virus's reaction to detecting objects of different types.

The full results of File Antivirus operation can be viewed in [the report](#). on the operation of the component.

5.To check the Virus Scan task;

1. Create a folder on the disk, copy into it the test "virus" downloaded from [the organization's official website](#), as well as the modifications of the test "virus" you created.

2. [Create a new task virus scan and select the folder](#) containing the set of test "viruses" as the scan object .

3. Enable logging of all events to ensure that the report file contains information about corrupted objects or objects not scanned due to a failure. To do this, select the "Log non-critical events" checkbox in the "Reports and data files" section of the application settings window.

4. [Run the task](#) virus search for execution.

During the scan, as suspicious or infected objects are detected, notifications will be displayed on the screen with information about the object and a request for further action from the user:

Thus, by selecting different action options, you can test Kaspersky Anti-Virus's reaction when detecting objects of different types.

The full result of the virus scan task can be viewed in [the report](#). on the operation of the component.

7. To learn about the program's features and how to manage it, select Contents from the **Help menu** . In the Help window : *Kaspersky Anti-Virus Scanner* Review the section " **Working with the Antivirus Scanner,**" including the topics "**Program Interface,**" "**Configuring Scan Settings,**" "**Finding and Removing Viruses,**" and "**Running the Antivirus Database Updater.**" After reviewing the help information, close the help window.

8. To view information about viruses in the Interactive Virus Encyclopedia, click on the View task Online Virus Encyclopedia . This will open the web page of the online virus encyclopedia on the Symantec website.

(h t t p://securityresponse.Symantec.com/avcenter/virfodb.html?prodid = nav2007). On this page, you can see what a particular file is infected with and how

to remove it.

9. To view the program's execution log, click on the View task Activity log . This will open a program log with three parameters: detected virus threats, scans, and errors. **Task 2:** Explore additional features of Norton AntiVirus for data protection (recovery of mistakenly deleted files and guaranteed deletion of files and folders).

For Norton data protection AntiVirus has UnErase Wizard (Wizard for restoring mistakenly deleted files) and Wipe Info (tool for guaranteed file deletion). By calling the UnErase wizard Wizard , simply specify the name (or part) of the file, its extension, and its location on your computer's drives. After searching for UnErase The Wizard will display all files found according to the specified criteria and prompt you to select which one to recover.

If you frequently have to delete files and want to be sure that they cannot be recovered, the Wipe tool will help. Info . But it is recommended to use Wipe in the settings. Info , install protection against deleting system files so that after an ill-considered action, the operating system does not fail to boot.

1. Advanced button in the main window. Tools ". Then in the *Advanced window Tools* select the UnErase option Wizard and click on the " Start " button. Tool ". In the next step of the recovery wizard, select the option to search for deleted files, enable the **Find flag Norton Protected Users files** (Search for all protected files) and click Next. The recovery wizard will then search for the file category you selected. In the next step of the recovery wizard, after specifying the files to recover, click Next.

" Recover ." Click "Next" to proceed to the recovery results message. Review the message and click "Finish" to complete the recovery wizard.

2. To ensure file deletion, select *Advanced in the window. Tools* Wipe option Info and click on the " Start " button. Tool ". In the next step of the removal wizard, drag it into the *Wipe window Info* files and folders that you want to be sure to delete. Then click the " Wipe" button. All » (Delete all).

Assignment for work

1. Using a virus demonstration software package, study the effects of different types of viruses. Run the programs from the demonstration software package one by one to study the manifestations of a virus. infection. After monitoring is complete, restart the computer.

2. Launch Dr.Web and scan your computer's RAM for viruses. Test drives A and C for viruses. If viruses are detected, disinfect the infected files.

3. Download and install the ADInf32 trial version on your computer. Schedule ADInf to run weekly on Saturdays at 6:00 PM.

4. Download and install a trial version of Kaspersky antivirus software on your computer. Anti-Virus . Create a new task to scan your computer's disks for viruses.

5. Download and install a trial version of Norton antivirus software on your computer. AntiVirus . Update your antivirus database and scan your computer for viruses.

6. Visit the Symantec website [at http://www.sarc.eom//avcenter/vinfodb.html](http://www.sarc.eom//avcenter/vinfodb.html) for an online virus search . On this page, you can see what a particular file is infected with and how to remove it.

Self-test questions

1. What is a computer virus? What properties do computer viruses have?
2. How are computer viruses classified? List the types of viruses.
3. What viruses are called resident and what is special about such viruses?
4. What are the differences between replicator viruses, stealth viruses, mutants and Trojan programs?
5. Describe the operating scheme of a boot virus.
6. Describe the operating scheme of a file virus.
7. Describe the operating scheme of boot file viruses.
8. What is a polymorphic virus? Why is this type of virus considered the most dangerous?
9. What causes computer viruses? Give examples of well-known viruses.
10. Is there criminal liability for the creation and distribution of computer viruses in the world and in the Russian Federation?
11. What are the ways in which viruses penetrate a computer and what are the signs of a computer infection with a virus?
99763008. What are the methods of virus detection and antiviral prevention?
99763009. List the basic measures to protect against computer viruses.
99763010. Describe the purpose of different types of antivirus programs.
15. Name examples of modern antivirus programs and describe their features.

Recommended reading

1. **Kozlov D.A., Parandovsky A.A., Parandovsky A.K.** Encyclopedia of computer viruses. - M.: SOLON -R, 2001. - 461 p.

This encyclopedia contains comprehensive information on computer viruses, from their creation to their detection and destruction. Examples of creating and destroying COM , EXE , Boot , Internet , and macro viruses, including both non-resident and resident viruses, are provided. The book's main advantage lies in its practical application.

2. **<http://www.avp.ru>** - Eugene Kaspersky Lab's antivirus server 6.0, which allows you to quickly and freely scan files for viruses. In the " Trial Versions" section, you can preview Kaspersky Lab antivirus products before purchasing.
3. **<http://www.viruslist.com/virusHst.asp>** - a section of the server of the antivirus laboratory of Evgeny Kaspersky, containing a huge number of descriptions of viruses and demonstrations of the effects caused by viruses, classification of viruses, general methods of detection and removal of computer viruses.
4. **<http://www.dials.ru>** - antivirus laboratory server " DanilovaLaboratory " and " DialogScience ." On this server , you can find information about the Doctor scanner programs. Web ; resident guard SpIDer Guard ; ADinf disk auditor and ADinf universal healer Cure Module , perform a free remote scan of your files for viruses over the Internet using the latest version of the Doctor antivirus scanner Web , and also get non-commercial versions of antivirus products, add-ons for the Doctor program Web and documentation.
5. **<http://www.adinf.ru>** - Website of ADinf antivirus developers .
6. **<http://www.symantec.ru>** - Russian Internet representative of Symantec , the manufacturer of the Norton antivirus package Anti Virus .

MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE RUSSIAN FEDERATION
FEDERAL STATE AUTONOMOUS EDUCATIONAL INSTITUTION OF HIGHER
EDUCATION
NORTH CAUCASIAN FEDERAL UNIVERSITY

Methodological guidelines

for students on organizing and conducting independent work
on the subject " Organization of Confidential Information Protection "
for students majoring in
02.04.01 Mathematics and Computer Science

**Stavropol
2026**

1. General Provisions

Independent work is the planned educational, educational and research, or scientific research work of students, carried out outside of class (in class) time, as assigned and under the methodological guidance of the teacher, but without his or her direct participation (with partial direct participation of the teacher, leaving the leading role to the students' work). To Vladislav Vyacheslavovich

Student independent work (SIW) at a university is an important form of student learning and research activity. Student independent work plays a significant role in the rating system of learning.

The main types of independent work for students include:

- formation and assimilation of the content of lecture notes based on the educational literature recommended by the lecturer, including information educational resources (electronic textbooks, electronic libraries, etc.);
- writing reports;
- preparation for seminars, practical and laboratory work, their design;
- compilation of an annotated list of articles from relevant journals in the fields of knowledge (pedagogical, psychological, methodological, etc.);
- implementation of educational and research work, project activities;
- preparation of practical developments and recommendations for solving problematic situations;
- completing homework assignments in the form of solving individual problems, performing typical calculations, computer calculations and individual work on individual sections of the content of disciplines, etc.;
- computer-based current self-monitoring and progress monitoring based on electronic training and assessment tests;
- completion of coursework (projects) within the framework of disciplines;
- completion of final qualifying work, etc.

The methodology for organizing students' independent work depends on the structure, nature, and characteristics of the discipline being studied, the number of hours for its study, the type of assignments for students' independent work, the individual qualities of students, and the conditions of educational activities.

The process of organizing students' independent work includes the following stages:

- preparatory (defining goals, drawing up a program, preparing methodological support, preparing equipment);
- basic (implementation of the program, use of techniques for searching for information, assimilation, processing, application, transfer of knowledge, recording of results, self-organization of the work process);
- final (assessment of significance and analysis of results, their systematization, assessment of the effectiveness of the program and work methods, conclusions on areas of labor optimization).

Independent work on the course "Information technologies for teamwork and project activities" is aimed at developing the following **competencies** :

Code	Formulation
OPK-1	Able to assess the role of information, information technology and information security in modern society, their importance for meeting the objective needs of the individual, society and the state

2. The purpose and objectives of independent work

The main goal of organizing and implementing independent work coincides with the goal of student education – the formation of a set of general scientific, professional and universal competencies of the future bachelor.

When organizing independent work, developing the ability to work independently to acquire knowledge, skills, and the ability to organize educational and research activities is an important and essential condition. The goal of students' independent work is to master fundamental knowledge, professional skills, and relevant professional activities, as well as experience in creative and research activities. Students' independent work promotes the development of independence, responsibility, self-discipline, and a creative approach to solving academic and professional problems.

The objectives of the SRS are:

- systematization and consolidation of the acquired theoretical knowledge and practical skills of students;
- deepening and expanding theoretical knowledge;
- development of skills in using regulatory, legal, reference documentation and specialized literature;
- development of students' cognitive abilities and activity: creative initiative, independence, responsibility and organization;
- development of independent thinking, abilities for self-development, self-improvement and self-realization;
- development of research skills;
- use of material collected and obtained during independent work and laboratory classes.

3. Technological map of independent student work

Technological map of independent student work						
Code s of imple mented compet encies	Type of student activity	The final product of independen t work	Assessme nt tools and technologie s	Volume of hours, including (astr.)		
				SRS	Contact work with the teacher	Tot al
3rd semester						
OPK-1	Preparing for lectures	Lecture notes	Interview	9.0	9.0	18.0
OPK-1	Preparation for practical classes	Electronic report	Interview	9.0	9.0	18.0
OPK-1	Independent study of literature	Abstract	Interview	9.0	9.0	18.0

OPK-1	Self-testing, preparation for testing	Testing	Test tasks	9.0	9.0	18.0
Total for 3rd semester				36.0	36.0	72.0
Total				36.0	36.0	72.0

4. Control points and types of reporting on them

Quality control and deadlines for independent work are assessed in accordance with the academic schedule and are formatted according to the assignment. The following knowledge rating is provided:

Description of the rating scale

Within the framework of the rating system, students' academic performance in each discipline is assessed during ongoing monitoring and midterm assessment.

Current control

5. Procedure for completing independent work by a student

5.1 . Methodological recommendations for working with educational literature

When working with books, you need to select literature, learn to read it correctly, and keep records. To select literature, the library uses alphabetical and systematic catalogs.

It is important to remember that rational skills in working with a book always mean great savings of time and effort.

The instructor teaching the course recommends the appropriate selection of textbooks. Required literature may also be listed in the course's teaching materials.

When studying the material in a textbook, you should move on to the next question only after correctly understanding the previous one, describing on paper all the calculations and computations (including those that are omitted from the textbook or given in the lecture for independent derivation).

When studying any discipline, independent individual work plays a large and important role.

Particular attention should be paid to defining the course's key concepts. Students should thoroughly analyze examples that illustrate these definitions and be able to construct similar examples independently. It's important to develop a clear understanding of what you're learning. Taking supporting notes is helpful. When studying the material from the textbook, it's helpful to supplement your lecture notes in the designated margins in your notebook. You should also note any questions you've identified for consultation with the instructor.

It is recommended to highlight the conclusions obtained as a result of the study in the notes so that they are better remembered when rereading the notes.

Experience shows that many students find it helpful to create a reference sheet containing the most important and frequently used formulas and concepts. Such a sheet helps students remember formulas and key points of the lecture, and can also serve as a constant reference for them.

Reading scientific text is part of cognitive activity. Its goal is to extract the necessary information from the text. The effectiveness of the action largely depends on how consciously the reader approaches the printed word (finding the necessary information, assimilating it in whole or in part, critically analyzing the material, etc.).

There are **four main attitudes towards reading scientific text** :

information retrieval (the task is to find and highlight the desired information)

assimilative (the reader's efforts are aimed at fully comprehending and remembering both the information presented by the author and the entire logic of his reasoning)

analytical-critical (the reader strives to critically comprehend the material, having analyzed it, and determined his attitude toward it)

creative (creates in the reader a readiness in one form or another - as a starting point for his own reasoning, as an image for action by analogy, etc. - to use the author's judgments, his train of thought, the result of observation, the developed methodology, to supplement them, to subject them

to new testing).

The main types of systematic recording of what has been read:

Annotation is an extremely brief, coherent description of a book (article) viewed or read, its content, sources, nature and purpose;

Planning is a brief logical organization of the text, revealing the content and structure of the material being studied;

Thesis is a concise reproduction of the author's main assertions without using factual material;

Quoting is the verbatim copying of excerpts and extracts from the text that most significantly reflect a particular idea of the author;

Note-taking is a brief and sequential presentation of the content of what has been read.

A summary is a complex way of presenting the contents of a book or article in a logical sequence. A summary integrates previous notes and allows for a comprehensive understanding of the book or article's content. Therefore, the ability to create an outline, make notes, take excerpts, and other notes determines the technique of summary writing.

5.2. Methodological recommendations for compiling lecture notes:

1. Read the text carefully. Look up any unfamiliar words in reference books. When taking notes, be sure to include reference information in the margins.

2. Highlight the main points and make a plan.

3. Briefly formulate the main points of the text, note the author's argumentation.

4. Take notes on the material, strictly following the outline. When taking notes, try to express your thoughts in your own words. Keep your notes clear and concise.

5. Write quotes correctly. When quoting, keep in mind the brevity and significance of the idea.

In the summary, it is advisable to present not only thesis statements but also their evidence. When formatting the summary, strive for the conciseness of each sentence. The author's thoughts should be presented concisely, with care taken to maintain style and expressiveness. The number of additional elements in the summary should be logically justified, and entries should be arranged in a specific sequence consistent with the logical structure of the work. Leave margins for clarification and addition.

Mastering note-taking skills requires a student to be determined and to work independently on a daily basis.

5.3. Methodological recommendations for preparation for practical classes

To maximize the benefit of practical classes, it's important to remember that exercises and problem solving are based on lecture material and typically involve a detailed analysis of specific topics covered in the lecture course. It's important to emphasize that only after the lecture material has been mastered from a specific perspective (namely, the perspective from which it is presented in lectures) will it be reinforced in laboratory classes, both through discussion and analysis of the lecture material and through solving problem situations and tasks. Under these conditions, students will not only master the material well but also learn to apply it in practice, and will also receive additional incentive (and this is very important) to actively engage with the lecture.

When independently solving problems, it's important to justify each step of the solution based on the theoretical principles of the course. If a student sees several possible solutions to a problem (problem), they should be compared and the most efficient one selected. It's helpful to create a brief plan for solving the problem (problem) before beginning calculations. Solutions to problematic problems or examples should be presented in detail, with calculations arranged in strict order, separating auxiliary calculations from the main ones. Solutions should be accompanied by comments, diagrams, drawings, and illustrations, if necessary.

It's important to remember that the solution to each learning problem should be followed through to the final logical answer required by the conditions, and, if possible, with a conclusion. The resulting answer should be verified using methods specific to the nature of the problem. It's also helpful (if possible) to solve the problem in several ways and compare the results. Problem solving of this type should be continued until solid solving skills are acquired.

Practical work No. 1-9 is completed by students of correspondence and part-time education independently.

5.4. Guidelines for self-assessment of knowledge

After studying a specific topic using notes in the notes and textbook, as well as solving a sufficient number of relevant problems in practical classes and independently, the student is advised to conduct a self-assessment of the acquired knowledge by answering test questions on the topic studied.

If necessary, you need to carefully review the material again.

Sometimes, a lack of understanding of a particular question only becomes apparent upon further study. In this case, it's necessary to go back and review the poorly understood material. An important criterion for mastering theoretical material is the ability to answer interview questions.

Evaluation criteria:

An "excellent" grade is awarded to a student if he/she is fully versed in the basic concepts related to ensuring the information and psychological security of the individual, society and the state, the concepts of information confrontation, information warfare and the forms of their manifestation in the modern world, fully analyzes sources and provides a classification and assessment of threats to information security.

A "good" grade is given to a student if he or she is familiar with the basic concepts related to ensuring the information and psychological security of the individual, society and the state, the concepts of information confrontation, information warfare and the forms of their manifestation in the modern world, analyzes sources and classifies and assesses threats to information security .

A "satisfactory" grade is given to a student if he or she is generally oriented in the basic concepts related to ensuring the information and psychological security of the individual, society and the state, the concepts of information confrontation, information warfare and the forms of their manifestations in the modern world, generally analyzes sources and provides a classification and assessment of threats to information security.

A student is given a grade of "unsatisfactory" if they have difficulty understanding the basic concepts related to ensuring information and psychological security of individuals, society, and the state, the concepts of information warfare, information confrontation, and their manifestations in the modern world, and if they have difficulty analyzing sources and classifying and assessing information security threats . The OPK-1 competency has not been mastered.

Description of the rating scale

The maximum possible score for the entire ongoing assessment is set at 55. A current assessment is considered passed if the student receives at least 60% of the maximum score established for that assessment. The rating score assigned to a student for a current assessment completed within the deadlines set in the assessment schedule is determined as follows:

Level of completion of the control task	Rating score (as a percentage of the maximum score for the test task)
Great	100
Good	80
Satisfactory	60
Unsatisfactory	0

5.6. Methodological recommendations for preparation for tests

Monitoring students' independent work

Independent work is monitored by the teacher in the classroom.

The following types of control are provided: interview, assessment of the report and its presentation.

Detailed criteria for assessing competencies are provided in the Fund of Assessment Tools for Conducting Current and Interim Assessments.

6. List of literature for completing independent work

List of key literature

1. Electronic warfare. Force defeat of radio-electronic systems / V.D. Dobykin , A.I. Kupriyanov, V.G. Ponomarev, L.N. Shustov; under. ed. A.I. Kupriyanova. - M.: University Book, 2007.
2. Methods and means of protecting computer information: a textbook, manual / I.V. Anikin, V.I. Glova. - Kazan, Publishing house of KSTU named after A.N. Tupolev, 2008.
3. Fundamentals of Information Security: a textbook, manual / N.V. Medvedev, V.V. Badanin , O.A. Akulov - M.: Publishing house of the Moscow State University named after N.E. Bauman, 2008.
4. Powerful electromagnetic pulse impact on electronic means and methods of protection / N.V. Balyuk . L.N. Kechiev , P.V. Stepanov - K IDT Group, 2008.
5. Shielding of technical means and shielding systems L.N. Kechiev , B.B. Akbashev , P.V. Stepanov. - M. IDT Group, 2010;
6. Belov E.B., Los V.P., Meshcheryakov R.V., Shelupanov A.A. Fundamentals of Information Security. - M.: Hotline - Telecom, 2006.
7. Zaitsev A.P., Shelupanov A.A., Meshcheryakov R.V. et al. Technical means and methods of information protection: textbook, manual for university students.
8. Under the editorship of A.P. Zaitsev and A.A. Shelupanov . 4th edition , corr . and add. - M.: Goryachaliniya -Telecom, 2009. A.A. Khorev . Technical information security: Textbook, manual for students of higher education institutions. In 3 volumes. - M.: Scientific and Production Center "Analytics", 2010;

List of additional literature

1. Powerful ultra-short-pulse and ultra-wideband electromagnetic radiation and their interference: in: e and damaging effects on electronic equipment for transmitting, receiving, processing and storing information: monograph / edited by V. G. Gerasimenko, V. B. Avdeev, A. Berdyshev. - Voronezh: Nauchnaya kniga, 2008.
2. Sakharov K. Yu. Emitters of ultrashort electromagnetic pulses and methods for measuring their parameters. – M MGIEI, 2006.
3. EMC and information security in telecommunication systems / L.N. Kechiev , P.V. Stepanov. - M.: Publishing house of Technology, 2005.
4. Special requirements and recommendations for the protection of confidential information (STR-K. Approved by the order of the State Technical Commission of Russia dated March 2, 2001, No. 282
5. Requirements for the protection of information that does not constitute a state secret, contained in state information systems Approved by order of the FSTEC of Russia dated February 11, 2013, No. 17.
6. GOST R 50922-2006. Information Security. Basic Terms and Definitions. Rostekhnregulirovanie , 2006.
7. GOST 51624-2000 Information Security. Automated Systems in Secure Design. General Requirements. Moscow: Gosstandart of Russia, 2000.
8. GOST R 51275-2006. Information Security. Informatization Objects. Factors Affecting Information. General Provisions. – Moscow: Rostekhnregulirovanie , 2006.
9. GOST R 56093-2014. Information Security. Automated Systems in Protected Design. Means of Detecting Intentional Electromagnetic Impacts. General Requirements. Rosstandart 2014.
10. GOST R 56103-2014 Information Security. Automated Systems in Protected Design. Organization and Contents of Work on Protection from Intentional Electromagnetic Impacts. General Provisions. Rosstandart , 2014.
11. GOST R 56115-2014. Information Security. Automated Systems in Protected Design. Means of Protection against Intentional Electromagnetic Impacts. General Requirements. Rosstandart , 2014.

List of educational and methodological support for independent work of students in the discipline

1. Methodological guidelines for organizing independent work of students in the discipline " Organization of protection of confidential information ". Stavropol: SKFU, 2025 .
2. Methodological guidelines for practical classes on the discipline " Organization of confidential information protection ". Stavropol: SKFU, 202 5 .

List of resources of the information and telecommunications network "Internet" necessary for mastering the discipline

1. <http://biblioclub.ru/> – University online library " Biblioclub "
2. <https://4brain.ru/liderstvo/> – Leadership: Lessons from an Effective Manager
3. <https://spravochnick.ru/psihologiya/> – Psychology Handbook