

**Report on the topic:**

**" Information threats "**

|  |  |
| --- | --- |
|  | **Maid by Pritykina Tatiana**  **Group: 2ИСП11-15**  **Supervisour Klimova I.V.**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

**Moscow, 2021**

**Content**

Introduction…………………..……………………......……… ……..3

**Chapter 1. Information security**................................................……4

* 1. Information threat………...………………………….................... 4
  2. The main components of information security...............................4

**Chapter 2. Objects of protection**………....…...................……….....8

2.1 The main objects of protection…........……………….…….…..... 8

Conclusion…………..…………………….…….….…………......... 11

References………………………….....…........……………………. 12

**Introduction**

This topic is very relevant today, because each of us interacts with information technology in one way or another. And more than using technology, we should understand how to protect our data, what to protect it from and what threats exist. This will be the topic of the study.  
 In the Information Security Doctrine of the Russian Federation, the term *information security* refers to the state of protection of national interests in the information sphere, determined by the totality of balanced interests of the individual, society and the state.

In a narrower sense, information security refers to the state of security of information and supporting infrastructure from accidental or intentional impacts of a natural or artificial nature (information threats, threats to information security), which can cause unacceptable damage to the subjects of information relations.

Information protection is a set of legal, organizational and technical measures and actions to prevent threats to information security and eliminate their consequences in the process of collecting, storing, processing and transmitting information in information systems.

Information security is one of the characteristics of an information system, i.e. an information system at a certain point in time has a certain state (level) of security, and information protection is a process that must be performed continuously throughout the life cycle of an information system.

The subjects of information relations are understood as both owners and users of information and supporting infrastructure. The supporting infrastructure includes not only computers, but also premises, electrical, water and heat supply systems, air conditioners, communications facilities and, of course, service personnel. The damage may be acceptable or unacceptable. Obviously, it is impossible to insure against all types of damage, especially since it is impossible to do it in an economically feasible way when the cost of protective equipment and measures does not exceed the amount of expected damage. So, you have to put up with something and you should protect yourself only from what you can not accept in any way. Sometimes such unacceptable damage is harm to human health or the state of the environment, but more often the threshold of unacceptability has a material (monetary) expression, and the purpose of information protection is to reduce the amount of damage to acceptable values.

**Chapter 1. Information security**

1.1 Information threat

Information threat is the potential for unlawful or accidental impact on the object of protection, leading to loss, distortion or disclosure of information.

Thus, the concept of information security, in general, should answer three questions:

- What to protect?

- From what (whom) to protect?

- How to protect?

The range of interests of subjects related to the use of information systems can be divided into the following components: ensuring the availability, integrity and confidentiality of information resources and supporting infrastructure. Sometimes the main components of information security include protection against unauthorized access (NSD) to information, which is understood as access to information that violates the rules of access differentiation using standard means. At the same time, ensuring confidentiality implies protection from NSD.

1.2 The main components of information security

In 1975, Jerry Salzer and Michael Schroeder in the article "Information protection in computer systems" for the first time proposed to divide security breaches into three main categories: unauthorized disclosure of information, unauthorized modification of information and unauthorized denial of access to information.

Later, these categories received short names and standardized definitions

• \* Confidentiality - the property of information to be inaccessible or closed to unauthorized persons, entities or processes;

\* Integrity - the property of preserving the correctness and completeness of assets;

\* Availability - the property of being available and ready for use at the request of an authorized entity.

Collectively, these three key principles of information security are referred to as the CIA triad. In 1992, the OECD published its own model of information security, consisting of nine principles: awareness, responsibility, counteraction, ethics, democracy, risk assessment, security development and implementation, security management, revision. In 1996, based on the 1992 OECD publication, the American National Institute of Standards and Technology (NIST) formulated eight basic principles that state that computer security "supports the mission of the organization", "is an integral component of rational management", "must be cost-effective", "requires a comprehensive and integrated approach", "is limited by social factors", "must be periodically reviewed", "responsibilities and responsibilities for computer security must be clearly formulated", and "system owners are responsible for security outside their organization." Based on this model, in 2004 NIST published 33 principles of engineering design of information security systems, for each of which practical guidelines and recommendations were developed, which are constantly being developed and maintained up to date.

In 1998, Donn Parker supplemented the classic CIA triad with three more aspects: ownership or control, authenticity and utility.

The advantages of this model, called the Parker hexada , are the subject of discussions among information security specialists.

In 2009, the US Department of Defense published the "Three Fundamental Principles of Computer Security": the system's exposure to risk, the availability of vulnerability and the ability to exploit vulnerability.

In 2011, The Open Group international consortium published the O-ISM3 information security management standard, in which it abandoned the conceptual definition of the components of the classical CIA triad in favor of their operational definition. According to O-ISM3, an individual set of security goals can be identified for each organization, belonging to one of five categories that correspond to one or another component of the triad: priority security goals (confidentiality), long-term security goals (integrity), information quality goals (integrity), access control goals (accessibility) and technical security goals.

Of all the information security models mentioned above, the classical CIA triad is still the most recognized and widespread in the international professional community. It is fixed in national and international standards and included in the main educational and certification programs on information security, such as CIS and CISM. Some Russian authors use tracing paper from it — "KCD triad". In the literature, all its three components: confidentiality, integrity and accessibility are synonymously referred to as principles, security attributes, properties, fundamental aspects, information criteria, essential characteristics or basic structural elements. Meanwhile, the professional community continues to debate about the compliance of the CIA triad with rapidly developing technologies and business requirements.As a result of these discussions, there are recommendations on the need to establish a relationship between security and privacy, as well as the approval of additional principles. Some of them are already included in the standards of the International Organization for Standardization (ISO):

✓ authenticity is a property that guarantees that the subject or

resource is identical to the declared one;

✓ accountability — the responsibility of the subject for his actions and

decisions;

✓ impossibility of refusal — the ability to certify the event or action that took

place and their subjects so that this event or action and

the subjects related to him could not be questioned;

✓ reliability is the property of compliance with the intended behavior and results.

Availability of information is the property of the system to ensure timely unhindered access of authorized (authorized) subjects to the information they are interested in or to carry out timely information exchange between them.

Information systems are created (acquired) to receive certain information services. If, for one reason or another, it becomes impossible to provide these services to users, this obviously damages all subjects of information relations. The leading role of accessibility is especially evident in various management systems – production, transport, etc. Outwardly less dramatic, but also very unpleasant consequences – both material and moral - can have a long-term unavailability of information services used by a large number of people (sale of railway and airline tickets, banking services, etc.).

Information integrity is a property of information that characterizes its resistance to accidental or intentional destruction or unauthorized modification. Integrity can be divided into static (understood as the immutability of information objects) and dynamic (related to the correct execution of complex actions (transactions)). Dynamic integrity controls are used, in particular, when analyzing the flow of financial messages in order to detect theft, reordering or duplication of individual messages.

Integrity turns out to be the most important aspect of information security in cases where information serves as a "guide to action". The prescription of medicines, prescribed medical procedures, the set and characteristics of components, the course of the technological process – all these are examples of information, the violation of the integrity of which can be literally fatal. Confidentiality of information is the property of information to be known and accessible only to authorized subjects of the system (users, programs, processes). Confidentiality is the most developed aspect of information security in our country.Unfortunately, the practical implementation of measures to ensure the confidentiality of modern information systems encounters serious difficulties in Russia. Firstly, information about the technical channels of information leakage is closed, so that most users are deprived of the opportunity to get an idea of the potential risks. Secondly, numerous legislative obstacles and technical problems stand in the way of user cryptography as the main means of ensuring confidentiality. If we return to the analysis of the interests of various categories of subjects of information relations, then accessibility is in the first place for almost everyone who actually uses IP. Integrity is practically not inferior to it in importance – what is the point of an information service if it contains distorted information? Finally, both organizations and individual users have confidential information. Two consequences follow from all of the above.

1. The interpretation of problems related to information security may differ significantly for different categories of subjects. To illustrate, it is enough to compare regime state organizations and educational institutions. In the first case, "let everything break down better than the enemy learns at least one secret", in the second – "yes, we don't have any secrets, as long as everything works."

2. Information security is not limited solely to protection from NSD to information, it is a fundamentally broader concept. The subject of information relations may suffer (incur losses and /or receive moral damage) not only from the NSD, but also from the breakdown of the system that caused a break in work.

**Chapter 2. Objects of protection**

2.1 The main objects of protection

The main objects of protection in ensuring information security are:

- all types of information resources. Information resources (documented information) - information recorded on a tangible medium with details that allow it to be identified;

- the rights of citizens, legal entities and the state to receive, distribute and use information;

- the system of formation, dissemination and use of information (information systems and technologies, libraries, archives, personnel, regulatory documents, etc.);

- the system of formation of public consciousness (mass media, social institutions, etc.). The Federal Law "On Information, information technologies and information protection". In Russian legislation, the basic law in the field of information protection is the Federal Law "On Information, Information Technologies and Information Protection" dated July 27, 2006, No. 149-FZ. Therefore, the basic concepts and solutions enshrined in the law require close consideration.

The law regulates relations arising under:

\* exercising the right to search, receive, transmit, produce and distribute information;

\* application of information technologies;

\* ensuring the protection of information.

The Law provides basic definitions in the field of information protection. Here are some of them:

\* information - information (messages, data) regardless of the form of their presentation;

\* information technology - processes, methods of search, collection, storage, processing, provision, dissemination of information and methods of implementation of such processes and methods;

\* information system - a set of information contained in databases and information technologies and technical means that ensure its processing;

\* information holder - a person who independently created the information or who, on the basis of a law or contract, has the right to allow or restrict access to information determined by any criteria;

\* information system operator - a citizen or a legal entity engaged in the operation of an information system, including the processing of information contained in its databases.

\* confidentiality of information is a mandatory requirement for a person who has access to certain information not to transfer such information to third parties without the consent of its owner.

Article 4 of the Law formulates the principles of legal regulation of relations in the field of information, information technology and information protection:

1. freedom to search, receive, transmit, produce and distribute information by any legal means;

2. the establishment of restrictions on access to information only by federal laws;

3. openness of information about the activities of state bodies and local self-government bodies and free access to such information, except in cases established by federal laws;

4. Equality of the languages of the peoples of the Russian Federation in the creation of information systems and their operation;

5. ensuring the security of the Russian Federation in the creation of information systems, their operation and protection of the information contained therein;

6. reliability of information and timeliness of its provision;

7. inviolability of private life, inadmissibility of collecting, storing, using and distributing information about a person's private life without his consent;

8. the inadmissibility of establishing by regulatory legal acts any advantages of the use of some information technologies over others, unless the mandatory use of certain information technologies for the creation and operation of state information systems is not established by federal laws.

All information is divided into public and restricted access. Publicly available information includes well-known information and other information, access to which is not restricted. The law defines information to which access cannot be restricted, for example, information about the environment or the activities of state bodies. It is also stipulated that the restriction of access to information is established by federal laws in order to protect the foundations of the constitutional system, morality, health, rights and legitimate interests of other persons, to ensure the defense of the country and the security of the state. It is mandatory to respect the confidentiality of information, access to which is restricted by federal laws. It is prohibited to require a citizen (individual) to provide information about his private life, including information constituting a personal or family secret, and to receive such information against the will of a citizen (individual), unless otherwise provided by federal laws.

The law distinguishes 4 categories of information depending on the order of its provision or dissemination:

1. information freely distributed;

2. information provided by agreement of the persons involved in the relevant relationship;

3. information that, in accordance with federal laws, is subject to provision or dissemination;

4. information whose dissemination in the Russian Federation is restricted or prohibited.

The Law establishes the equivalence of an electronic message signed with an electronic digital signature or other analogue of a handwritten signature and a document signed with his own hand.

The following definition of information protection is given - it is the adoption of legal, organizational and technical measures aimed at:

1. ensuring the protection of information from unauthorized access, destruction, modification, blocking, copying, provision, distribution, as well as from other illegal actions in relation to such information;

2. confidentiality of restricted access information;

3. realization of the right to access information.

The owner of the information, the operator of the information system, in cases established by the legislation of the Russian Federation, are obliged to ensure:

1. prevention of unauthorized access to information and (or) its transfer to persons who do not have the right to access information;

2. timely detection of unauthorized access to information;

3. prevention of the possibility of adverse consequences of violation of the order of access to information;

4. prevention of the impact on the technical means of information processing, as a result of which their functioning is disrupted;

5. the possibility of immediate recovery of information modified or destroyed due to unauthorized access to it;

6. constant monitoring of ensuring the level of information security.

Thus, the Federal Law "On Information, Information Technologies and Information Protection" creates the legal basis for information exchange in the Russian Federation and defines the rights and obligations of its subjects.

In December 2017, Russia adopted a new version of the Information Security Doctrine. The document defines information security as the state of protection of national interests in the information sphere. In this case, national interests are understood as the totality of the interests of society, the individual and the state, each group of interests is necessary for the stable functioning of society.

**Conclusion**

In this report, we have studied the basic concepts of information security. We also examined in detail the objects of protection.

In this work, a separate place was undoubtedly given to the analysis and examples with the laws of the Russian Federation, with the help of which we studied in detail the types of information objects, ways to protect them and the regulation of measures to prevent illegal actions.

First of all, the problem of information security is the problem of a person's choice - the choice of perceived information, behavior in society and the state, the choice of a circle of communication. It is necessary to accurately understand and identify oneself in the world, in society, awareness of goals and means to achieve them, consciously process information and broadcast only verified, accurate and objective information.

The problems associated with improving the security of the information sphere are complex, multifaceted and interrelated. They require constant, unflagging attention from the state and society. The development of information technologies encourages the constant application of joint efforts to improve methods and tools that allow us to reliably assess threats to the security of the information sphere and adequately respond to them.

**References:**

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2016. — 136 c.

2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 c.

3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 c.

4. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2016. — 239 c.