# CLASSIFICATION OF THREATS TO INFORMATION SECURITY

**Matchanov Bakhrombek Jumanazarovich**
Senior teacher at Urgench State University
*https://doi.org/10.5281/zenodo.8125140*

***Abstract.*** *This article discusses the classification of information security threats according to their level. The efficiency of information protection is determined by its timeliness, activity, continuity and complexity. Carrying out protective measures in a complex manner ensures the elimination of dangerous channels through which information can be spread. It is known that a single open channel of information dissemination drastically reduces the effectiveness of the entire protection system.*

***Keywords:*** *threat, information protection, protection object, information system, information carriers, threatening character, modes of action, protective measures, coding, encryption.*

The purpose of organizing any information computing systems is to simultaneously provide reliable information to users' requirements and maintain their confidentiality. In this case, the task of providing information must be solved on the basis of protection from external and internal unauthorized influences.

According to the level of threats to information security, they can be classified as follows:

➢ ***For an individual***:

- violation of the constitutional rights and freedoms of citizens to search, receive, transfer, develop, and distribute information.
- deprivation of citizens' right to privacy.
- violation of citizens' rights to protect their health from involuntary exposure to harmful information.
- threats to intellectual property.

➢ ***For society:***

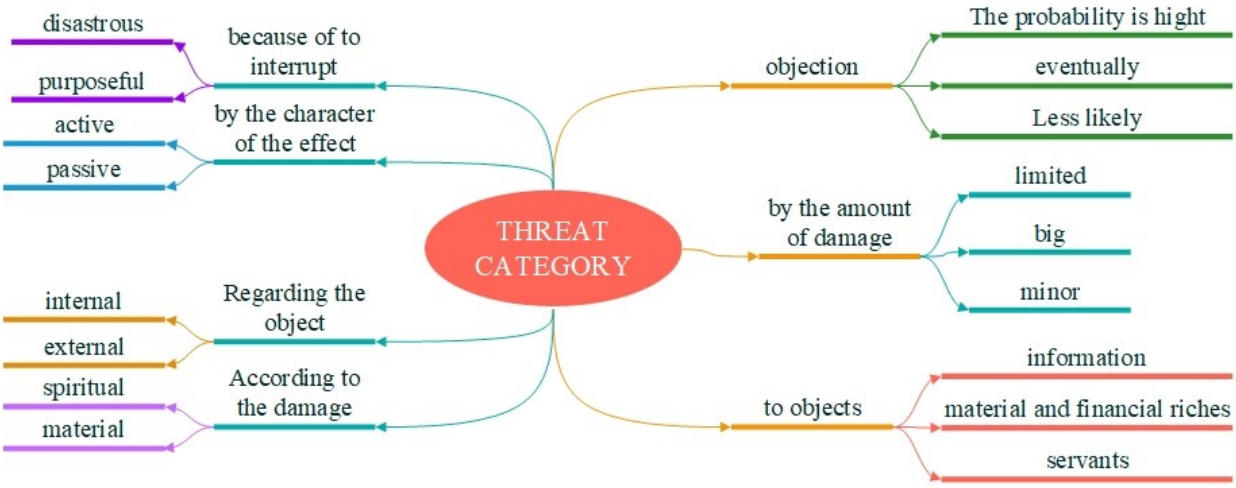
- obstacles to building an informed society.
- hindrance to the spiritual renewal of society, preservation of its spiritual wealth, dedication, impartiality, and the development of long-standing spiritual traditions of the country.
- impeding the promotion of national and cultural heritage and depriving society of moral standards.
- creating an environment that opposes the development of modern telecommunication technologies and hinders the advancement and preservation of the country's scientific and production potential.

➢ ***For the state:***

- actions against the protection of the interests of individuals and society.
- opposition to building a legal state.
- obstruction of the formation of institutions of public control over state management bodies.

- resistance to the establishment of a system for preparing, adopting, and implementing decisions by state management bodies that ensure the interests of individuals, society, and the state.
- obstacles to the protection of state information systems and state information resources.
- actions against the protection of the country's unified information environment.

A threat is an act committed by criminals with the aim of causing material or moral harm. We present to you the category of threats in the form of a scheme.




*The methodological approach* to information protection forms the basis for ideas and important recommendations to ensure the confidentiality of information at different stages. These principles are considered when creating normative frameworks for information protection and are applied as standards in the adoption of laws and regulations, with mandatory implementation.

The principles of information protection can be divided into three groups: *legal, organizational, and technical.* The practice of using information protection systems shows that only complex information protection systems can be effective. They encompass the following measures:

1. **Legislation:** The use of legal acts that strictly define the rights and obligations of legal entities, individuals, and the state in the field of information protection.
2. **Spiritual-ethical:** Creating and maintaining an environment where violations of established rules of conduct within the facility are strongly discouraged by most employees.
3. **Physical:** Creating physical barriers that prohibit unauthorized access to protected information.
4. **Administrative:** Establishing appropriate privacy, access, and internal control regimes.
5. **Technical:** Using electronic and other equipment for information protection.
6. **Cryptographic:** Implementing encryption and coding techniques that prevent illegal access to processed and transmitted information.
7. **Software:** Utilizing software tools to restrict usability.

All information carriers, including physical, hardware, software, and documentary means, are considered as complex *protection objects.*

In recent times, information is stored, transmitted, and processed in various forms of information systems. *An information system* is an application software, and sometimes a hardware-software system, designed to collect, store, search, and process textual or graphic information.

The material foundation for information availability in an information system consists of electronic and electromechanical devices, as well as information carriers. Information carriers can include paper, magnetic, and optical media, as well as electronic circuits.

Therefore, it is necessary to protect devices, systems, and information carriers. In various information systems, users can be service personnel, sources, and carriers of information. Thus, the concept of the object of protection is interpreted broadly. The protected object includes not only information resources, hardware and software tools, service personnel, and users, but also the building and the area where they are located.

*The main objects of information* protection include information resources related to state secrets and containing confidential information, tools and information systems (computing tools, networks and systems), software tools (operating systems, database management systems, application software), automated control systems, communication and data transmission systems, and technical means of processing access-limited information (such as recording, sound amplification, hearing, speech, television devices, document preparation, and reproduction tools, as well as other graphic, text, and alphanumeric data processing tools), as well as systems and tools for direct processing of confidential and state secrets. These systems and tools are often referred to as technical means of receiving, processing, and storing information.

There are also technical tools and systems located in the area where confidential information is processed, but they are not part of the main system. These auxiliary technical equipment and systems include telephones, communication sound amplification technical equipment, fire and security alarm systems, data transmission means in the radio communication system, control and measuring devices, household electrical appliances, etc., as well as the building in which they are located.

These components can be considered as a system that includes stationary equipment, peripheral devices, connection lines, distribution and communication devices, and power source systems. Technical means for processing confidential information, as well as the building in which they are located, constitute its protected object.

Protective actions aimed at ensuring information security can be characterized by various dimensions, including the nature of the threat, methods of action, distribution, and the scale of impact.

Depending on the nature of the threat, protective measures are aimed at protecting data from disclosure, leakage and illegal access. According to the methods of action, they can be divided into deficits or other damages: warning, detection, prevention and recovery. Protective actions on the enclosure can be directed to the area, building, structure, devices or their individual elements. The scale of protective measures is defined by object, group or individual protection.

***Types of information protection are classified into two main types:***

**firstly**, information privacy, more precisely, according to the type of protected secrets;

**secondly**, on groups of forces, means and methods used for information protection.

The first group can include the following main directions: protection of state secrets, protection of interstate confidential information, protection of business secrets, protection of service secrets, protection of professional secrets and protection of private information.

The second group includes the following main directions: legal protection of information, organizational protection of information and engineering and technical protection of information.

Legal protection is the special laws, other regulations, rules, processes and measures that ensure information protection on a legal basis.

Organizational protection is a strict determination of the mutual treatment and production activities of the performers on a regulatory and legal basis, which eliminates or alleviates the voluntary damage that can be caused to the performers.

Engineering-technical protection is the use of various technical means that resist damage caused to the activity.

***Classification of information protection tools and methods.***

The main methods used in information protection are *hiding, layering, disinformation, information fragmentation, insurance, spiritual and educational, accounting, coding and encryption*.

***Hiding*** - as a method of information protection is one of the main organizational methods of data protection in practice, it limits the number of individuals authorized to confidential information. Encryption is one of the most widely used methods of information protection.

***Layering*** - as a method of information protection, firstly, distributes confidential information according to the level of confidentiality, and secondly, limits access to protected information.

***Disinformation*** is one of the methods of information protection, which means spreading false information instead of real information about an object.

The method of ***information fragmentation*** means that the information is divided into pieces, and the complete information cannot be obtained through any part of it.

***Insurance*** is just now being recognized as a way to protect information. Its meaning is to protect the rights and interests of the information owner or information media from traditional threats and information security threats. This method is more likely to be used to protect trade secrets. When securing information, it is required to first undergo an audit and have a conclusion.

The method of ***spiritual and educational*** protection of information plays a very important role in the protection of information. It is a person, who is an employee of an enterprise or an organization, who is aware of confidential information, accumulates a lot of information in his memory, and in some cases can become a source of information leakage, and because of his fault, others get this information illegally.

The method of spiritual and educational protection of information implies the following:

- training the employee, carrying out special work aimed at forming certain qualities and views with him (patriotism and information protection are not only important on a broader societal level but also hold personal significance for individuals);
- training the employee in the rules and methods of information protection, and formation of practical working skills with confidential information carriers;

***Accounting*** is one of the important methods of information protection, which allows to obtain information about the location of confidential information carriers and their users at any time. It is very difficult to solve the problem of protection without this method. Principles of accounting for confidential information:

- an obligation to register all carriers of the protected information;
- to ensure that the registration of a specific information carrier is one time (not repeated);
- indicate the current address of the confidential information carrier in the list;

- the sole responsibility for the preservation of each protected information carrier and the reflection of information about the user who used this information in the account.

***Coding*** is a method of converting plain text into conditional information using the coding method, in order to hide the protected information from the adversary when there is a risk of being intercepted by others during the transmission of information through the channel. For encoding, a set of characters (symbols, numbers, etc.) is usually used, as well as a certain system of rules that allows information to be transformed into an unintelligible set of characters. And in order to read this information, it is necessary to bring it back to its original state, that is, to open the code (key). Coding of information can be done using technical means or manually.

***Encryption*** is a method of information protection, which is often used when transmitting information by means of radio devices when there is a risk of interception by an adversary. Encrypting information means making it unintelligible without the key even if intercepted by others.

*Information protection tools* are a set of engineering and technical, electrical, electronic, optical and other devices used to solve information protection issues.

Information protection, like other areas, should be provided with material, economic and informational resources in addition to personnel training.

*Material resources are* of special importance in information protection. A specially allocated building, special devices, certified computer and office equipment based on accepted standards, hardware, software, information protection tools, etc.

*Information resources are* information on which optimal management solutions for information protection are adopted at the organization level.

It includes:

- legal information (normative base on security issues);
- commercial information (information about the manufactured product and information protection services provided in it);
- scientific and technical information (information about the security policies of the country and foreign countries);
- information on production technology processes;
- analytical information obtained as a result of information-analytical activities regarding the state of information security of the organization, and threats to it.

*Material resources.* It is impossible to design and implement information protection without material support. This work is carried out in complex conditions: competition in the field of security, the desire of the service provider to get more profit for less cost, implementation of poor quality security work, etc.

Information security represents complex measures aimed at preventing the dissemination, destruction, destruction and modification of protected information by its owners.

*The information protection system* should be understood as the state information protection system and the protection systems of specific objects.

The state information protection system includes:

- state regulatory documents, standards, management documents and requirements;
- development of information protection concepts, requirements, normative-technical documents and scientific-methodical recommendations;

- the order of organization, implementation and implementation of measures aimed at the protection of state-owned information, as well as recommendations on the protection of information owned by individuals and legal entities;

- organization of testing and certification of information protection tools;

- establishment of organizations and sectoral coordination structures for information protection;

- control of work on the organization of information protection;

- to determine the procedure for legal and natural persons who are foreign citizens to use state-owned information or the information of legal and natural persons whose distribution of information is restricted by the state.

The objectives of information protection in certain objects of information are determined by the list of possible threats.

Any information protection system, while having its own characteristics, must meet general requirements. The more common data protection requirements are:

Information protection system

- to be in unity;

- ensuring the safety of information, information media and the protection of the interests of those related to information;

- ensuring information communication between its elements within the system;

- covers the technological complex of information activities;

- different means of use, multi-level hierarchical view of information accessibility;

- be open to changing and supplementing information security measures;

- non-standard;

- simple maintenance and ease of use;

- it should be reliable (intentional failure of technical means can become a channel of information dissemination).

An information security system, like any other system, must have certain types of support. Therefore, this system can have:

– *legal support* (this includes mandatory regulatory documents, instructions, guidelines, and requirements);

– *organizational support* (it is assumed that information protection is applied through certain structural units: document protection service; guarding, access authorization service; information protection service using technical means; information-analytical activities, etc.);

– *hardware supply* (this includes the large-scale use of technical means to ensure information protection and the operation of the protection system);

– *information supply* (this supply includes data, information, indicators, and values that solve the tasks that ensure the system's operation. It also includes indicators of a different nature related to the activity of the security service: authorization, registration, storage, etc.);

– *software* (this includes various information, accounting, statistical and calculation programs that assess the existence of illegal access to confidential information sources and information leakage channels);

– *mathematical security* (this implies the use of mathematical methods that assess the norms, and areas by the risk of technical means of intruders in the implementation of various calculations necessary for protection);

– *linguistic support* (set of special language tools used by experts and users in the field of information protection);

– *normative-methodological support* (this encompasses the norms, regulations of the bodies, services, and tools that ensure information protection, also includes various methods that facilitate the activities of users when performing tasks in situations where information protection is of paramount importance, provides a framework for establishing and implementing effective security measures, ensuring compliance with established standards, and promoting secure practices within organizations and industries).

**REFERENCES**

1. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: Учебное пособие. – Брянск, 2007.
2. Безбогов А.А. Методы и средства защиты компьютерной информации. Учебное пособие. – Тамбов, 2006.
3. Зайцев А.П., Голубятников И.В., Мещеряков Р.В. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие. – М., 2006.
4. Казиев В.М. Введение в правовую информатику. – http://www. intuit.ru.
5. Мельников В.П. Информационная безопасность. Учебное пособие. – М., 2005.
6. Миродова Ш. Проблемы обеспечения информационной безопасности Республике Узбекистан в условиях глоболизации. – Т., 2008.
7. Muhammadiev J.O‘. Axborot xavfsizligi: muammo va yechimlar: Monografiya. – T., 2011.
8. Партыка Т. Л., Попов И. И. Информационная безопасность: Учебное пособие. – М., 2002.
9. Семененко В.А. Информационная безопасность: Учебное пособие. – М., 2008.
10. G`aniyev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Axborot – kommunikatsion tizimlari xavfsizligi. – T., 2008.
11. Ярочкин В.И. Информационная безопасность. – М.: 2004.