BRIDGING THE GAP: INTERDISCIPLINARY INSIGHTS IN SOCIAL SCIENCE
2025
Conference
JANUARY 30TH, 2025
FLORIDA USA

MEANS AND METHODS OF INFORMATION PROTECTION ACCORDING TO THE LEVEL OF THREAT

Matchanov B.J.
Senior teacher at Urgench State University, independent researcher of Tashkent State Pedagogical University, Uzbekistan

ABSTRACT

Information security threats are categorized based on their level in this thesis. The timeliness, activity, continuity, and complexity of information protection all affect how effective it is. Complex protection procedures are implemented to guarantee that harmful routes for information dissemination are eliminated.

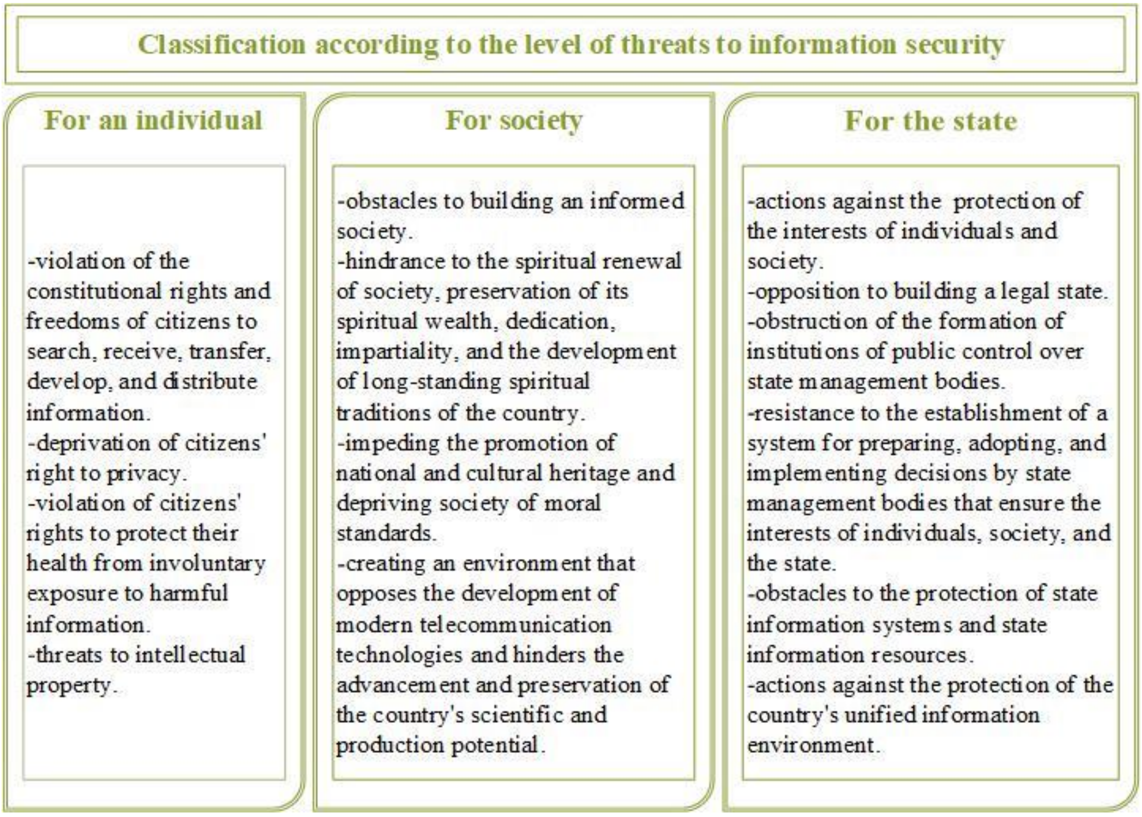
KEY WORDS

Threat, information protection, protection object, information system, threatening character, modes of action, protective measures, coding, encryption.

INTRODUCTION

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.

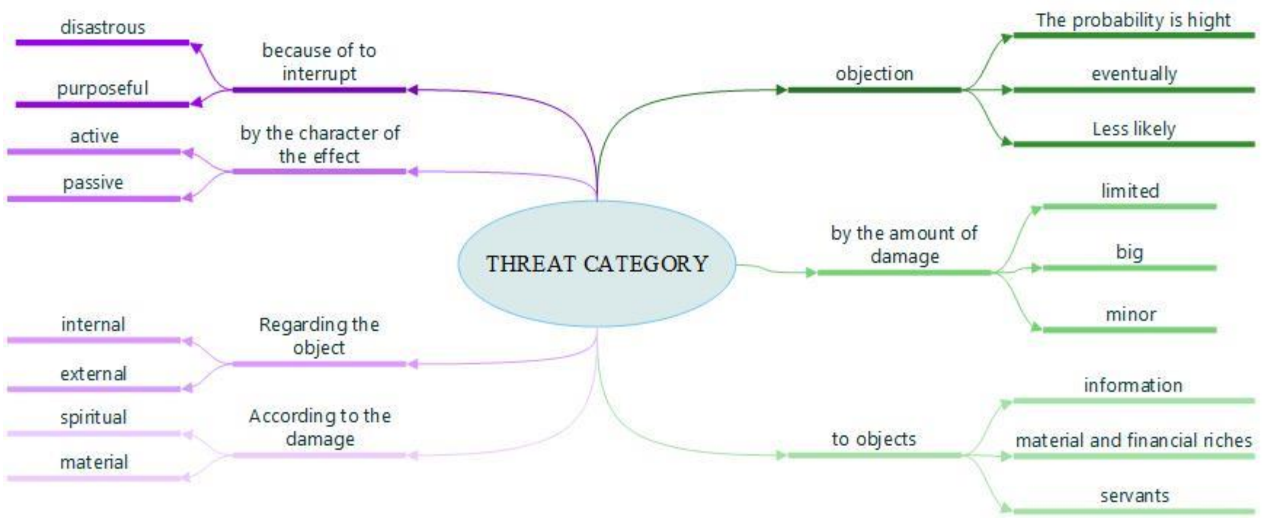
According to the level of threats to information security, they can be classified as follows:



Classification according to the level of threats to information security

For an individual	For society	For the state
-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.	-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.	-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. The categories of threats are presented in the form of a diagram below.

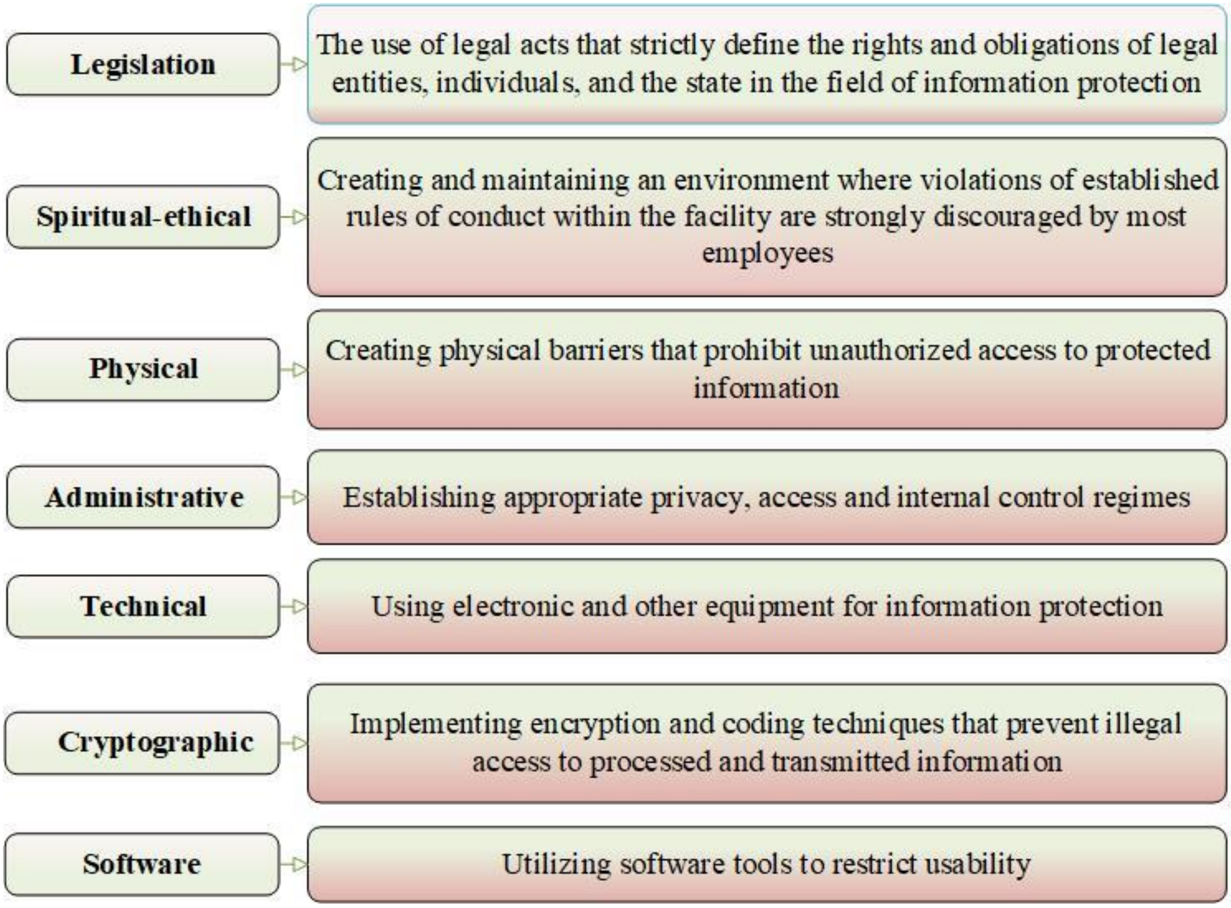


The methodological approach to information protection forms the basis for ideas and important recommendations to ensure the confidentiality of information at different stages. These principles are considered when creating normative frameworks for information protection and are applied as standards in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

The principles of information protection can be divided into three groups:

legal	*organizational*	*technical*

The practice of using information protection systems shows that only complex information protection systems can be effective. They encompass the following measures:



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
Spiritual-ethical	Creating and maintaining an environment where violations of established rules of conduct within the facility are strongly discouraged by most employees
Physical	Creating physical barriers that prohibit unauthorized access to protected information
Administrative	Establishing appropriate privacy, access and internal control regimes
Technical	Using electronic and other equipment for information protection
Cryptographic	Implementing encryption and coding techniques that prevent illegal access to processed and transmitted information
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.

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.

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.
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.

Information fragmentation	- the method of means that the information is divided into pieces, and the complete information cannot be obtained through any part of it.
Insurance	- its meaning is to protect the rights and interests of the information owner or information media from traditional threats and information security threats.
spiritual and educational	- 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.
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.
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.
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.

REFERENCES

1. Matchanov B.J., Classification of threats to information security, SCIENCE AND INNOVATION, international scientific journal volume 2 issue 7 july 2023, UIF-2022: 8.2|ISSN: 2181-3337| scientist.uz, 23-30 p
2. Muhammadiev J.O‘. Axborot xavfsizligi: muammo va yechimlar: Monografiya. – T., 2011.
3. Семененко В.А. Информационная безопасность: Учебное пособие. – М., 2008.
4. Миродова Ш. Проблемы обеспечения информационной безопасности Республике Узбекистан в условиях глоболизации. – Т., 2008.
5. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: Учебное пособие. – Брянск, 2007.
6. Безбогов А.А. Методы и средства защиты компьютерной информации. Учебное пособие. – Тамбов, 2006.
7. Зайцев А.П., Голубятников И.В., Мещеряков Р.В. Программно- аппаратные средства обеспечения информационной безопасности: Учебное пособие. – М., 2006.

8. Казиев В.М. Введение в правовую информатику. – http://www. intuit.ru.
9. Мельников В.П. Информационная безопасность. Учебное пособие. – М., 2005.
10. Ярочкин В.И. Информационная безопасность. – М.: 2004.