Information Security

Middle East Technical University

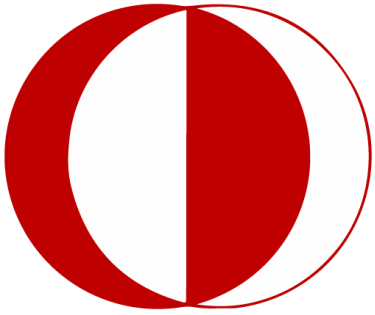
CEIT 207

Instructor:

Prof. Dr. Zahide YILDIRIM

Student:

Akran Abykeev



12 November 2023

Department of Computer Education and Instructional Technologies

Summary

In the contemporary digital landscape, the protection of information stands as a critical imperative. This comprehensive chapter addresses the multifaceted nature of information, recognizing it as a valuable asset necessitating effective safeguards.

The exploration begins by establishing the foundational concept of information as an object of protection. It defines information as more than a byproduct of operations, emphasizing its strategic importance across diverse domains. The discussion further encompasses the various levels at which information is presented within organizational contexts, acknowledging its nuanced forms and complexities. The chapter concludes by outlining the fundamental properties that characterize protected information—confidentiality, integrity, and availability—forming the basis of robust information security practices.

The exploration continues with an examination of specific information security measures. This section covers risk assessment, incident response, and security policies, offering practical insights into how organizations can proactively address and mitigate security threats to their information assets.

In essence, this chapter provides a holistic and in-depth exploration of information protection and security, combining conceptual frameworks with practical considerations. It equips readers with the knowledge needed to navigate the complexities of safeguarding valuable information in the ever-evolving digital age.

Glossary

Information: organized and meaningful data.

Information security: involves protecting information from unauthorized access.

Information protection: encompasses measures to safeguard data.

Threats in the Internet: refer to potential risks to information integrity and security online.

CONTENT

Objectives

- Students will define the Concept of Information Protection
- Students will identify Basic Properties of Protected Information
- Students will categorize Information Security Measures
- Students will describe approaches to protect Information
- Students will state techniques available for safeguarding information
- Students will present Comprehensive Security Policies

1. Information as an object of protection

1.1 The concept of information as an object of protection

In general, information is knowledge in the broad sense of the word. Not only educational or scientific knowledge, but information and data that are present in any object and are necessary for the functioning of any information systems (living beings or human data).

Information as an object of cognition has a number of features:

· immaterial in nature, displayed as symbols on media

· after recording to the media, the information acquires certain parameters and can be measured in volume

· information recorded on a tangible medium can be stored, processed, transmitted via various communication channels

· moving along communication lines, information creates physical fields that reflect its content.

During processing, storage, and transmission, information circulates in the information system. The simplest information system consists of an information source, a communication channel and the recipient of the information (Fig. 1.1). It follows from this that it is impossible to put an equal sign between the protection of information and the protection of an information system.

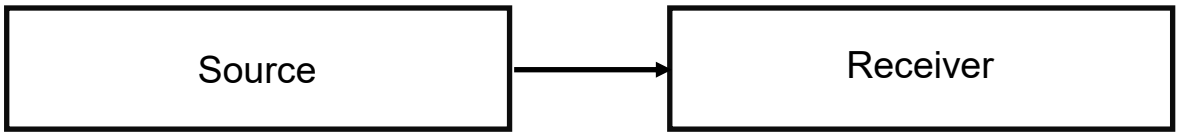


Figure 1.1. The simplest information system

1.2. Levels of information presentation

There are several levels of information presentation:

· media level

· the level of means of interaction with the carrier

· logic level

· syntactic level

· semantic level

Let's characterize each of them.

1) The level of media

By its nature, information is not material and pure the video is not available to a person. In order for a person to perceive information, there must be a material carrier: another person, substance (material carrier), energy (energy carrier). Information, being the subject of protection, requires the protection of those objects in which it is present in one or another material form.

All carriers have two categories of information:

· characteristic information: information of the carrier "about itself", about specific features: shape, size, structure, chemical and physical properties, energy parameters

· semantic information: something that does not depend on the type of carrier, the product of abstract thinking in the language of symbols.

The role of a person in relation to information is that a person can be not only a carrier of information, but also a generator of new information, a source of information, a businessman, a user. In relation to protection issues ,a person can act both as a violator and as a defender.

Many defense should be protected from damage, premature wear, theft, loss. Protection is also necessary when copying information. Copying is the process of transferring information to a similar or other medium without changing the quantity and quality. Copying is easily provided by using modern technologies. For documents on paper, copying is carried out using a copier, scanner, camera. For electronic media operation copying is provided by a standard software.

As a result of copying, the same information is placed at different points in space on different carriers, therefore, protection of all carriers in all locations is needed. Energy carriers are electromagnetic and acoustic fields.

Features of energy carriers:

· used mainly for information transmission

· do not age

· spread uncontrollably in space

· capable of mutual transformation

· recording of information is associated with changing the parameters

of the field (various types of modulation).

The main ways to protect information on an energy carrier are: ensuring noise immunity when choosing coding (modulation), ensuring the required energy of the signal, protection against leakage, including through side electromagnetic radiation and interference (PEMIN), protection against interception in the main channel.

2) The level of means of interaction with the carrier

Direct interaction with the carrier is not always it is possible and often carried out through complex technical devices. For protection at this level, it is necessary to monitor the serviceability of information reading devices, for the absence of technical means of unauthorized access to information (so-called "bookmarks"), whose task is to intercept or redirect the flow of read information.

3) Logic level

At the logical level in an information system, information can be represented in the form of logical disks, reels, files, sectors, clusters. In modern operational systems, the levels of individual bytes, clusters, and sectors are not visible, so

so they are often forgotten. It should be remembered that the removal of information at a high logical level (for example, at the file level) does not lead to the removal of information at lower levels from where it can be read.

4) Syntactic level

The syntactic level of information representation is related to coding. Information is recorded and transmitted using symbols. A symbol is a certain sign that is given a certain meaning. A linear set of symbols forms an alphabet. During the encoding process, one alphabet can be converted into another.

Depending on the goals, the following types of coding differ:

· in order to eliminate redundancy — archiving, linear coding

· in order to eliminate errors — noise-resistant coding;

· for the purpose of inaccessibility of information — cryptographic coding.

5) Semantic level

The semantic level is related to the meaning of the transmitted information. The same lexical constructions can have different meanings in different contexts. The use of professionalism, polysemous words and words whose meaning has changed over time can distort the meaning of information (Rahanov & Rahanova, 2021)

1.3. Basic properties of protected information

Information as an object of cognition and an object of protection has many properties. Let's list the most important of them.

Value. As an object of property, information has a certain value. Precisely because information has value, it needs to be protected.

The secrecy (confidentiality) of information is a subjectively determined characteristic of information, indicating the need to impose restrictions on the range of subjects, having access to this information. This characteristics provided by the ability of the system to maintain the specified information is kept secret from subjects who do not have the authority to access it. The objective prerequisites for such a restriction of the availability of information for some subjects are the need to protect the legitimate interests of other subjects of information relations.

The integrity of information is the property of information to exist in an undistorted form. Usually, we are interested in ensuring a broader property — the reliability of information, which consists of the adequacy (completeness and accuracy) of displaying the state of the subject area and directly the integrity of the information, that is, its undistorted. The issues of ensuring the adequacy of the display go beyond the scope of the information security problem.

Accessibility of information is a property of the system in which information circulates, to ensure timely and uninterrupted access of subjects to the information they are interested in and readiness to service requests from subjects whenever there is a need to address them.

Concentration. The total amount of information may turn out to be secret, summary data is usually more secret than single.

Pragmatic properties:

· importance

· completeness (degree of reduction of a priori uncertainty);

· reliability

· timeliness

· expediency

· correlation with facts, phenomena.

In order to satisfy the legitimate rights and interests of information owners, it is first of all necessary to constantly maintain the secrecy, integrity and availability of information. If at least one of these properties is violated, the value of information is reduced or lost altogether:

· if the value is lost when it is disclosed, then it is said that there is a danger of violating the secrecy of information

· if the value of the information is lost when the information is changed or destroyed, then it is said that there is a danger to the integrity of the information

· if the value of information is lost during its non-operational use, then it is said that there is a danger of violating the availability of information. The value of information changes over time. The dissemination of information and its use lead to a change in the value of information. The nature of the change in value the time depends on the type of information. For most types, it is possible to present a general scheme of the information life cycle (Fig. 1.2).

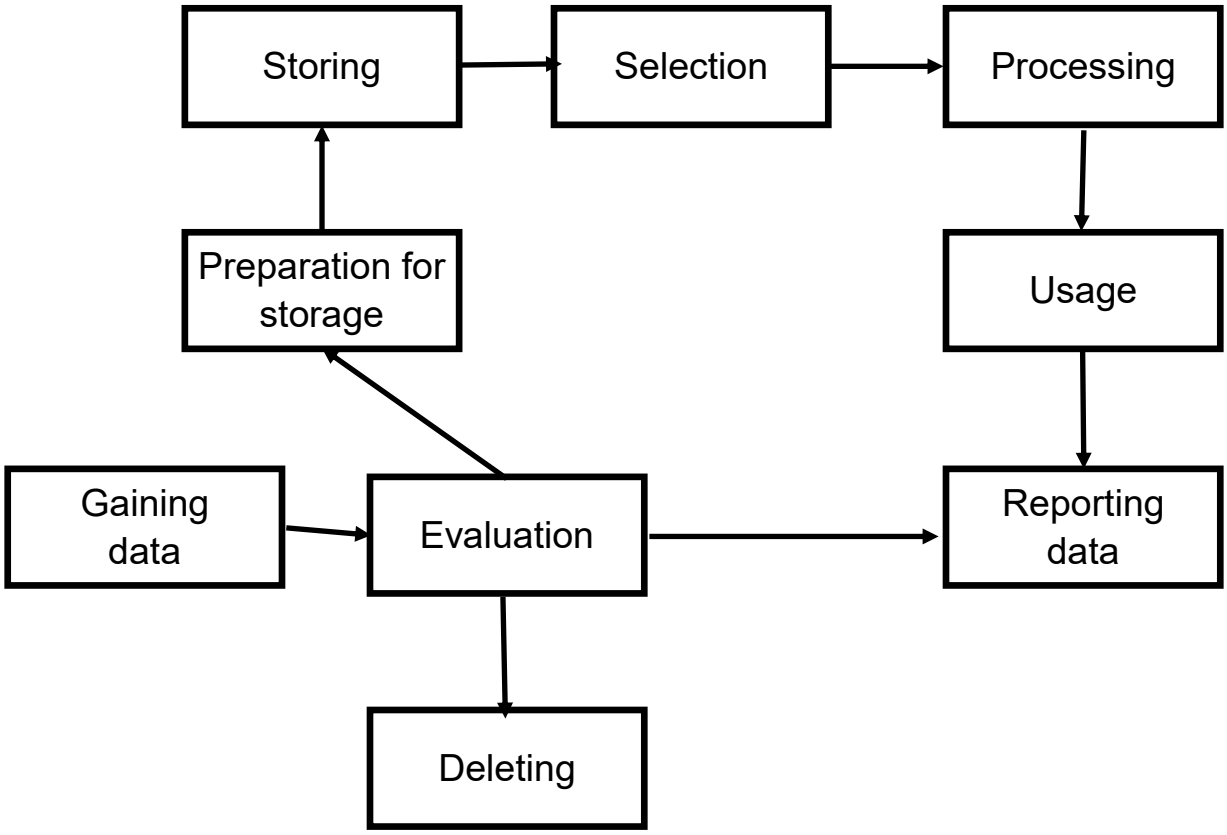


Figure 1.2. Information life cycle

2. Information protection.

Information (information system) illegal actions in respect of which may cause harm to its owner, user or other person, is subject to protection. Harm here is understood as damage to life or health, property or moral damage, subject to monetary measurement.

Information protection is a set of legal, organizational and technical measures aimed at ensuring confidentiality, integrity, authenticity, accessibility and preservation of information.

Provision of information – actions aimed at familiarization with the information of a certain circle of persons.

Dissemination of information – actions aimed at communicating information to an indefinite circle of people.

Information integrity is the state of information security from modification, substitution, destruction by unauthorized means.

The reliability (authenticity, authenticity) of information is a property expressed in the strict belonging of information to the subject who is its source, or to the subject from whom it is received.

Accessibility is the state of information technology that provides timely and reliable access to information and (or) functional capabilities of information technology in a competent manner.

If the information, the distribution and/or provision of which is restricted, is not contained in the information system, its protection is organized by the owner of the information. The owner of information is a person who has two types of powers: the right to use information and determine the conditions for its processing, use it in information systems and networks, and the right to dispose of property rights to information.

Literally: the owner of the information is the copyright holder in relation to the information. It is important to understand that the concepts of "owner of information" and "owner of information" are legally incorrect and cannot be used, since the right of ownership (as well as ownership as an element property rights) can be established only on a material (bodily) thing, and information is an immaterial object. It follows from this that civil transactions are unacceptable in relation to information (in other words, it is impossible, for example, to "sell information"). The property of turnover is possessed only by material information carriers, as well as property rights to information when the information has an economic (commercial) value.

The owner of the information should be distinguished from the user of the information – a person who has the right to receive, provide (distribute) and use the information, but does not have the authority to exercise rights in relation to such information.

Restricted access information contained in information systems, as a general rule, is protected by the owner or operator of the information system. In information relations related to the protection of information, other entities may also be included: owners of software and technical means, information resources, information systems and information networks; owners of software and technical means, information resources, information networks. Technical protection of information is an activity aimed at ensuring the confidentiality, integrity, availability and safety of information by technical measures without the use of cryptographic protection of information. Cryptographic information protection is an activity aimed at ensuring confidentiality, monitoring the integrity and reliability of information using cryptographic information protection tools. Means of technical protection of information – technical, programmatic, software and hardware mean of information protection intended to protect information from unauthorized access and unauthorized impacts on it, blocking lawful access to it, other unlawful impacts on information, as well as to control its security.

Means of cryptographic protection of information – technical, software, software and hardware mean of information protection that implement one or more cryptographic algorithms (encryption, generation and verification of electronic digital signature, hashing) and cryptographic protocols, as well as cryptographic key management functions and functionality without danger.

Licensing is provided for cases when information protection activities of limited distribution are carried out by external organizations. If the work on technical and (or) cryptographic protection of information is carried out for their own needs by the owner of information, the distribution and (or) provision of which is restricted, by the owner (owner) of information systems and critically important objects of informatization, then obtaining a license for such activity is not required. A separate license is provided for activities in relation to cryptographic means of protecting state secrets. Information security is the state of protection of the balanced interests of the individual, society and the state from external and internal threats in the information sphere. The threat to information security is a factor (a set of factors) that creates a danger to the individual, society, state in the information space. In fact, this is a potentially possible action can harm the interests of subjects.

A separate license is provided for activities in relation to cryptographic means of protecting state secrets. In this area, licensing is carried out by the State Security Committee of the Republic of Belarus. The list of activities subject to licensing is established by paragraph 107 of the Regulation on the procedure for licensing activities related to specific goods. "On the procedure for licensing activities related to specific goods (works, services)". Information security is the state of protection of the balanced interests of the individual, society and the state from external and internal threats in the information sphere. The threat to information security is a factor (a set of factors) that creates (creates) a danger to the individual, society, state in the information space. In fact, this is a potentially possible action, event or process that, by affecting information and other components of the information system, can harm the interests of subjects.
Let's consider a detailed classification of information security threats proposed in Figure 2.1. (Vostretsova, 2019)

Depending on the results of exposure, threats can be passive and active. The information system is exposed to an active threat, i.e., targeted impact on its components in order to disrupt the normal functioning (for example, disabling a device, operating system, software destruction, network disruption, destruction or distortion of data). Passive threats are aimed at unauthorized use of the information system without disrupting its functioning and changing the information content. Active security threats can be natural and artificial. Natural ones are caused by the impact on information systems of objective physical processes or natural phenomena.

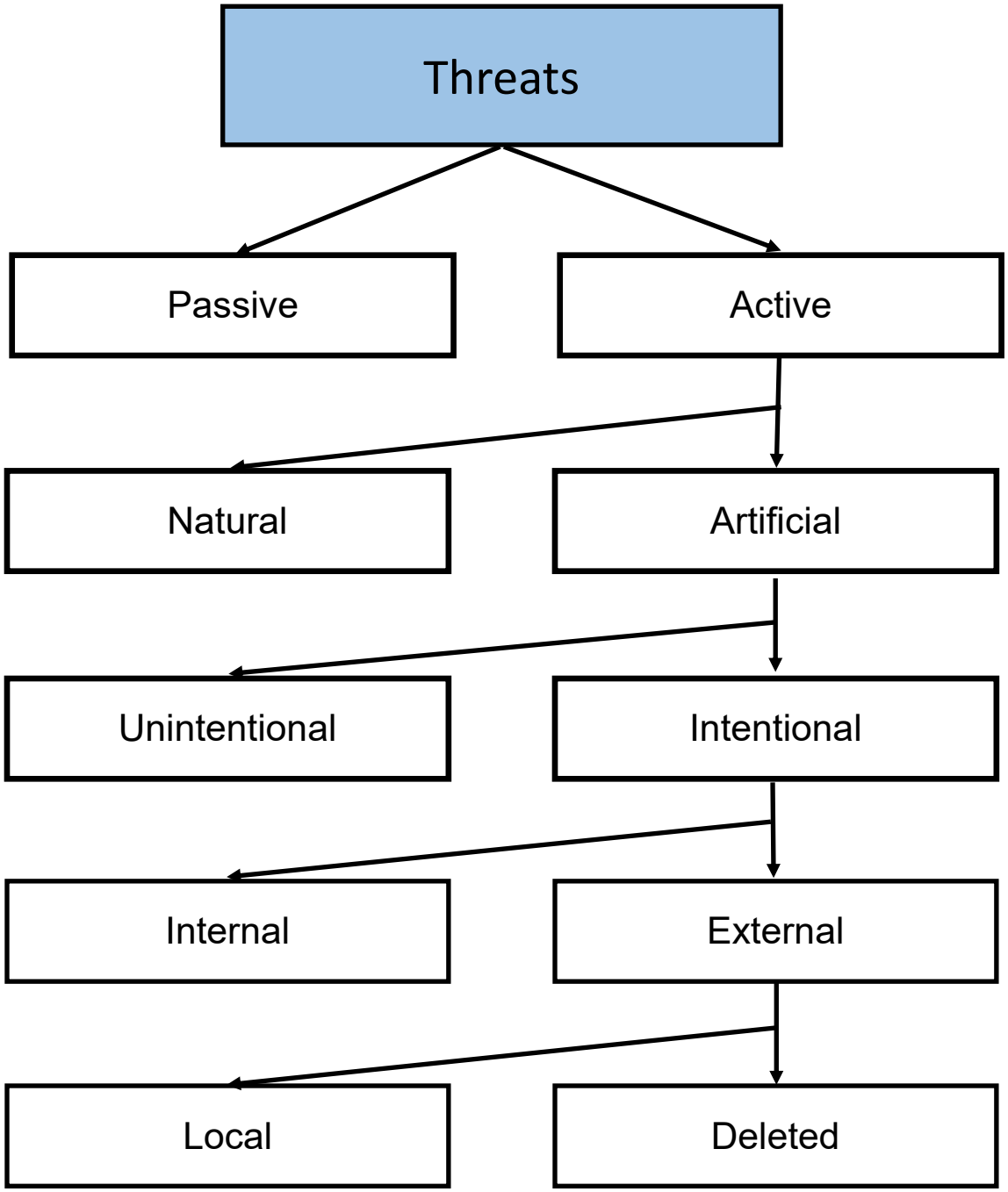


Figure 2.1. – Threats to information security

Artificial threats are caused by human actions (anthropogenic) and are divided into unintentional (accidental) and intentional. Methods of countering these threats are manageable and, as a rule, depend on the organization of the information security system, since the actions of the subject can always be evaluated, predicted, and then take appropriate measures.

Unintended threats are associated with people directly working with the information system. As a rule, these are actions committed by people accidentally, out of ignorance, inattention or negligence, but without direct intent. Often such threats are the result of non-compliance by personnel with organizational and technological rules and requirements of internal regulatory documents. Deliberate artificial threats are divided into internal (from the organization's staff) and external (from outsiders and organizations). The violator model is assumptions about the capabilities (limitations of capabilities) of violators whose actions can lead to potential damage.

The formation of the violator model is provided as follows:

1) the zones surrounding confidential information are determined
2) all means of protection between and within the zones are determined
3) possible threats and probabilities of their occurrence are determined
4) describes the state of the environment
5) classification and description of probable violators

of information security is being formed.

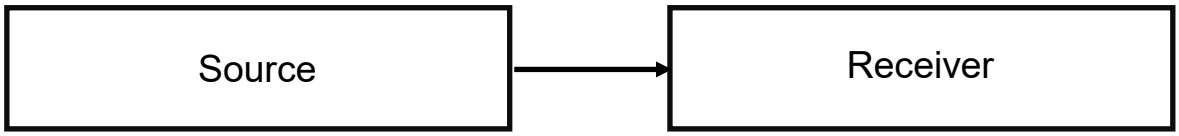
The allocation of classes of violators can be performed according to various methods. Each category of violators is tied to certain threats and the amount of potential damage.

The manual will not pay attention to issues of legal liability for offenses related to the protection of the confidentiality of information on the Internet.

PRACTICE QUESTIONS

1. What is the concept of information as an object of protection?

2. Does the graph below represents the simplest information system? Select True or False.



3. Which of the following shows, in order, levels of information presentation?

A. Media — Interaction with the carrier — Logic — Syntactic — Semantic levels

B. Media — Semantic — Logic — Syntactic — Semantic — Interaction with the carrier levels.

C. Media — Semantic — Syntactic — Logic — Semantic — Interaction with the carrier levels.

D. Media — Semantic — Syntactic — Logic — Interaction with the carrier — Semantic levels.

4. Which of the following is not a basic property of protected information?

A. Value

B. The secrecy (confidentiality) of information

C. Accessibility

D. Source

5. _____ is a set of legal, organizational and technical measures aimed at ensuring confidentiality, integrity, authenticity, accessibility and preservation of information.

PRACTICE QUESTIONS

6. Give the definition of the accessibility of information?

7. _____ of information is a property expressed in the strict belonging of information to the subject who is its source, or to the subject from whom it is received.

8. What are the two main types of information threats?

A. Active and Passive

B. Local and Active

C. Natural and Unintentional

D. Artificial and Intentional

9. Person is working with information system directly. Because of his inattention he couldn't protect data. What type of threat is described in this situation?

A. Natural

B. Unintended

C. Artificial

D. Deleted

10. What is the violator model?

ANSWER SHEET

1. Information, as an object of protection, refers to the immaterial nature of knowledge represented as symbols on media. Recorded information can be measured, stored, processed, and transmitted through communication channels, creating physical fields that reflect its content. This concept forms the basis for safeguarding information in various systems (p. 7).
2. True, the graph represents the simplest information system (p. 7).
3. Levels of information presentation are media, interaction with the carrier, logic, syntactic, and semantic levels (p. 8).
4. Source is not a basic property of protected information (p. 12).
5. *Information protection* is a set of legal, organizational and technical measures aimed at ensuring confidentiality, integrity, authenticity, accessibility and preservation of information (p. 15).
6. Accessibility is the state of information technology that provides timely and reliable access to information and (or) functional capabilities of information technology in a competent manner (p. 15).
7. *The reliability of information* is a property expressed in the strict belonging of information to the subject who is its source, or to the subject from whom it is received (p. 15).
8. Active and passive are two main types of information threats (p. 19).
9. Unintended threat is described in the situation. Unintended threats are associated with people directly working with the information system. As a rule, these are actions committed by people accidentally, out of ignorance, inattention or negligence, but without direct intent (p. 20).
10. The violator model is assumptions about the capabilities (limitations of capabilities) of violators whose actions can lead to potential damage (p. 20).

References

Rahanov K. Y. & Rahanova N. A. (2021), “Confidentiality of information on the internet”, Publishing House of Polotsky university (Novopolsk)

Vostretsova E. V., (2019), “The basics of information security”, Publishing House of Ural University (Yekaterinburg)

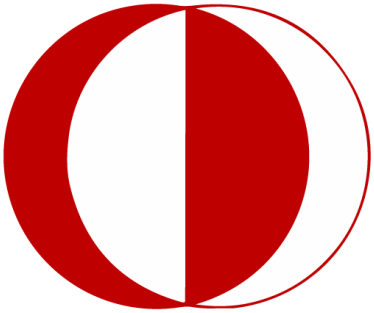
References

Pictures:

- https://www.dreamstime.com/photos-images/cyber-security.html
- https://www.pexels.com/search/cyber%20security/
- https://www.shutterstock.com/ru/search/computer-security
- https://www.freepik.com/free-photos-vectors/information-security
- https://pixabay.com/illustrations/cyber-security-information-security-7960243/

Middle East Technical University

Computer Education and Instructional Technologies



Ankara, Turkey