

MODERN METHODS AND ESSENCE OF ENSURING INFORMATION SECURITY IN THE INFORMATION SOCIETY

Toshboyeva Feruza To'lqin qizi

Tashkent State University of Economics

Abstract: *In today's information society, the problem of information security is extremely important. In this article, the concept of information security and its tasks, threats to information security, the concept of encryption and types of encryptions, encryption standards, cryptography goals are given in-depth information. Issues of reliable protection of information were studied.*

Key words: *information, security, physical security, encryption, cryptography, algorithm, decryption, asymmetric encryption, authentication, natural environment, artificial environment.*

INTRODUCTION

Today, the demand for information security is increasing and it is evident that all aspects of computer technology have entered. Information security is protection against accidental and intentional attacks. Information security is a multifaceted field of activity, and only a systematic and comprehensive approach to it can bring success.

In fact, information about persons, objects, facts, events, events and processes, regardless of their sources and form of presentation. Information is called information, and information protection means measures to prevent threats to information security and eliminate their consequences.

Body. There are several views of the information, which are as follows:

- ❑ Public information
- ❑ Documented information
- ❑ Confidential information
- ❑ Confidential information

As threats to information, intrusions, and effects by malicious persons have increased, the demand for its protection has also increased. One of the first measures to ensure information security is physical security.

In order to prevent unauthorized physical control, threats carried out by a person, and threats related to the environment, organizations, relevant bodies, and individuals must implement appropriate physical security controls and measures. A system administrator must ensure that physical security measures are in place and functioning properly to protect against physical security threats.

Physical security deals with the protection of physical devices, people, network and information from attacks. We can say that physical security is one of the important parts of an organization's information security program. Physical security does not perform the same actions as network, application, or database security domains. That is, physical security deals with protection at the physical level of the OSI model.

The physical level includes:

- all cable and network systems;
- physical control of the system and cables;
- power source for system and cable;
- system support environment.

Factors affecting physical security violations can be divided into two groups: natural/environmental threats and man-made (artificial) threats [1].

Physical barriers separate the physical boundary from the general area to the restricted area. These barriers can be divided into external, middle and internal barriers according to their location. External barriers usually include fences, walls, etc. Middle fences are usually used to block individuals. Internal barriers are made up of doors, windows, lattices, mirrors, curtains, etc.

There are the following types of physical barriers used inside the building:

- Fences/ electric fences/ metal fences. These barriers are commonly used to define restricted areas, controlled areas, and protection against unauthorized access.

The main purpose of implementing physical barriers:

- block and hold the attacker;
- defining the boundaries of the organization;
- protection of the safe area from external attacks;
- protection against the entry of vehicles;
- protection against explosive attacks.
- Tumba. This barrier is in the form of a small vertical mound and is used to protect cars from entering.

- Turnstiles. Turnstiles allow one person to enter or exit at a time. In this case, the system allows access when a person presents a suitable coin, ticket, fingerprint or token.

- Other obstacles. In addition, various doors, windows, gratings, mirrors, and window curtains are used in the organization of physical protection.

In addition, surveillance cameras are also useful for physical security. Today's video surveillance tools are very modern and effective, allowing not only to record actions, but also to identify ongoing actions. Video surveillance devices are usually installed at the entrance doors, halls and working areas of the organization, protected place or area. These tools are a very useful aid in tracking movement in and out of an organization.

What we discussed above was the physical protection of data. Now the proposal to use special algorithms to hide information has come in. Encrypting the content of a secret message, that is, creating a new encrypted text by changing the data according to special algorithms. with 'li' refers to the method of blocking unauthorized access to information.

Open text
Encryption

Encryption
Decryption

Open text

Above, the clear text (the real meaning of which has not been changed with the help of symbols) has been changed to another form with the help of special symbols, algorithms, that is, encrypted and decrypted with the necessary keys and returned to its original state. In general, encryption is understood as the transfer of information into a form of symbols that cannot be understood by humans. We know that one of our most valuable things today is information, and we must protect it as much as possible, safely and from outside hands (malicious or aware). This is why this science is getting better and entering our lives more and more.

The term "Cryptography" is translated from the Greek language and means "to hide, cover the writing". The meaning of the term means that cryptography is used to hide and protect the necessary information. 20th century BC. During excavations in Mesopotamia, the oldest encrypted texts were found. The text, written in pegs on a clay tablet, is a recipe for a paint used to cover artisans' pottery and is considered a trade secret. Ancient Egyptian religious writings and medical recipes are also known. Usually, the following two types of reflection are used in data encryption (decryption) in cryptography. One of them is substitution reflection, and the second is permutation reflection [2].

Summary

In conclusion, it should be said that as our current life progresses, the demand and need for information is increasing in society and in every aspect, especially the daily development of information technologies is serving to increase the volume of information. security requires protection, confidentiality and secrecy in a certain sense, because such situations as the disclosure, theft or destruction of this information, cyber-attacks are dangerous for the state and citizens, organizations can cause losses, financial and moral damage.

In order to prevent such situations, no matter what the field or direction, it is necessary to implement information security, its protection and protection.

Every manager of information security and experts, responsible persons should take practical measures and measures to properly organize the organization's activities and ensure sufficient information security in the organization.

REFERENCES:

1. 5. Seymour Bosworth, Michel Ye. Kabay, Eric Whyne. Computer security handbook. Wiley. 2014.
2. 6. Sean Harris. ALL IN ONE CISSP. McGraw-Hill 2013.
3. 7. Ganiev S. K., Karimov M. M., Tashev K. A. —Information security||. Communicator. 2008.
4. 8. Makarenko S. I., Information security. Uchebnoe posobie. Stavropol, 2009.
5. 9. Michael Ye. Whitman. Herbert J. Mattord. Principles of Information Security, Fourth Edition. Course Technology, Cengage Learning. 2012.

6. S. K. Ganiyev, M. M. Karimov, K.A. Tashev. Information security. T., 2017. 2. S. S. Kasimov. Cryptographic methods of ensuring information security and their application.
 7. M. Aripov, B. Begalov, U. Begimkulov, M. Mamarajabov. Information Technology. T. 2009.
 8. National Encyclopedia of Uzbekistan. - T.: State Scientific Publishing House, 2000.
 9. GhaffarovaG. Philosophical-methodological problems of information and informationization processes. False. science. name ...dis. -Tashkent, 2008.
- Internet sites
1. www.intuit.ru
 2. www.sec.ru
 3. [http7/opensecuritytraining.info/](http://7/opensecuritytraining.info/)