EJCBLT

ISSN:3031-7347

https://doi.org/10.61796/ejcblt.v1i7.872

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

**Toshboyeva Feruza To'lqin qizi**
Tashkent State University of Economics

**Bebutova Zulayxo Hamidovna**
Tashkent State University of Economics

***Received: Jun 22, 2024; Accepted: Jul 29, 2024; Published: Aug 27, 2024;***

**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

**Keywords:** 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.

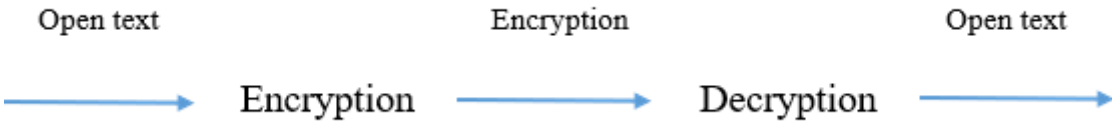
- Other obstacles. In addition, various doors, windows, gratings, mirrors, and window curtains are used in the organization of physical protection.


Figure 1. Protective equipment

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.

Figure 2. Surveillance cameras

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.




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.

## Methods

Uses a descriptive and analytical approach to explain the concept of information security, which is increasingly important in today's digital age. A descriptive approach is used to outline the basics of information security theory, including the different types of information that need to be protected and the importance of physical security measures in protecting devices, networks and data from threats. This method also includes a description of the various physical barriers, such as fences, walls and surveillance cameras, used to ensure security. In addition, an analysis of various encryption standards, such as AES, RSA, TLS/SSL, and others, shows how these technologies are used to protect data and address threats. The text also incorporates a historical element by reviewing the early development of cryptography, as well as how these principles have evolved over time. A practical implementation approach is included, providing concrete guidance for system administrators in implementing effective security measures. Overall, this statement combines theory, analysis, and practical application to provide a comprehensive overview of the application and importance of information security at various levels, both physical and digital.

## Result and Discussion

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].

Encryption standards are critical to the secure sharing, protection, and privacy of data. Encryption standards include:

1. AES (Advanced Encryption Standard): AES is a symmetric encryption standard. For example, when encrypting data with a 256-bit key according to the AES standard, it is possible to decrypt the data only when the key is known. AES is used to protect databases, networks, file encryption, and document collections. widely used.

2. RSA: RSA is the most popular standard for asymmetric encryption. It is used for standard encryption and electronic signature. The RSA standard consists of two keys, for security, one key is used to encrypt secure data, and the other key is used to de-encrypt encrypted data. RSA is used for several purposes, such as internet communication, authentication, electronic payment systems, etc.

3. TLS/SSL (Transport Layer Security/Secure Sockets Layer): TLS and SSL standards are used to ensure data protection on the Internet. They are used with encryption and authentication mechanisms implemented in alert protocols. TLS and SSL are used to ensure secure communication between browsers and web servers.

4. SHA (Secure Hash Algorithm): SHA standards are used to generate data hash values. Standards such as SHA-256, SHA-384, and SHA-512 are widely used to generate data hash values. Their purpose is to verify data integrity, create electronic signatures, and ensure data security.

5. PGP (Pretty Good Privacy): The PGP standard is used to encrypt private text and secure email. It uses a combination of asymmetric encryption, hashing functions, electronic signatures and key binding. The PGP standard is a must-see for individual users, corporate organizations, and email providers.

6. Diffie-Hellman Key Exchange: The Diffie-Hellman standard provides a key exchange protocol for asymmetric encryption. It is a two-way exchange protocol that prohibits any additional manipulation and implementation in the strictest of cases. The Diffie-Hellman protocol is used to provide confidentiality through key exchange, for example, a secure channel is created to implement a key in a relationship.

7. Blowfish: Blowfish is a standard used for symmetric encryption. It is used to encrypt words and files that are correct. Blowfish works with the standard, unique block-encryption algorithm and encrypts data using blocks and keys.

8. Triple DES (Data Encryption Standard): Triple DES is a standard used for symmetric encryption. It is a 3-times iteration variant of the DES algorithm. The Triple DES standard uses another layer and stronger keys to support DES.

9.ECC (Elliptic Curve Cryptography): ECC is a standard used for asymmetric encryption. It is based on elliptic curve lines and is used to convert key usage to short length keys in brightness. The ECC standard requires a small amount of storage space for keys and protection, so it consumes less resources.

10. Camellia: Camellia is the standard used for symmetric encryption. It provides the same

level of safety as AES. Camellia is a block-encryption algorithm that encrypts data using blocks[3].

At the same time, the representation of encryption algorithms consists of mathematical models. will be a source of possibilities. Such attempts are called crypto attacks.

## Conclusion

In conclusion, it is worth noting that due to the increasing threats to information security in today's world, improving knowledge and skills related to information security in the field of computer science positively impacts not only individuals but also entire nations. If we do not keep pace with the times, addressing existing shortcomings becomes increasingly difficult. This, in turn, demands continuous striving, being knowledgeable, proactive, and not negligent from us

## References

[1]. S. Bosworth, M. E. Kabay, and E. Whyne, *Computer Security Handbook*, 6th ed. Hoboken, NJ, USA: Wiley, 2014.
[2]. S. Harris, *All in One CISSP Exam Guide*, 6th ed. New York, NY, USA: McGraw-Hill, 2013.
[3]. S. K. Ganiev, M. M. Karimov, and K. A. Tashev, *Information Security*. Tashkent, Uzbekistan: Communicator, 2008.
[4]. S. I. Makarenko, *Information Security: Uchebnoe Posobie*. Stavropol, Russia: Stavropol State University, 2009.
[5]. M. Y. Whitman and H. J. Mattord, *Principles of Information Security*, 4th ed. Boston, MA, USA: Cengage Learning, 2012.
[6]. S. K. Ganiyev, M. M. Karimov, and K. A. Tashev, *Information Security*, 2nd ed. Tashkent, Uzbekistan: Communicator, 2017.
[7]. M. Aripov, B. Begalov, U. Begimkulov, and M. Mamarajabov, *Information Technology*. Tashkent, Uzbekistan: State Scientific Publishing House, 2009.
[8]. *National Encyclopedia of Uzbekistan*. Tashkent, Uzbekistan: State Scientific Publishing House, 2000.
[9]. G. Ghaffarova, "Philosophical-Methodological Problems of Information and Informationization Processes," Ph.D. dissertation, Tashkent State Technical University, Tashkent, Uzbekistan, 2008.
[10]. Internet sources: 10. "Introduction to Information Security," Intuit, [Online]. Available: www.intuit.ru. [Accessed: Aug. 25, 2024].
[11]. "Information Security Overview," SEC, [Online]. Available: www.sec.ru. [Accessed: Aug. 25, 2024].
[12]. "Open Security Training," Open Security Training, [Online]. Available: http://opensecuritytraining.info/. [Accessed: Aug. 25, 2024].