INFORMATION TECHNOLOGIES IN INFORMATION SECURITY

Fundovna M.L., *agrey3605@gmail.com*
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute»
Institute of Special Communication and Information Protection

The widespread computerization of society and the introduction of information technologies in all areas of human activity have led to an acute issue of ensuring the safety of information. Information security is not only the protection of information from unauthorized access, but also prevent the use, disclosure, violations, modifications, checks, records or destruction of information. To date, information security is the main element of the information system in which information is processed and stored. The safety factor also plays a primary role in many data processing systems e.g., in the banking information system. Providing and maintaining personal data protection implies, first of all, the security and confidentiality of the transmitted data, as well as user authentication.

Information security programs are built around 3 main components:

Confidentiality means that the information is not disclosed to unauthorized persons, organizations and third-party processes.

Integrity - preservation of accuracy and completeness of data. This means that the data cannot be edited by an unauthorized way.

Availability - means that the information must be available if necessary. The refusal of service is one of the factors that can prevent the availability of information [1].

Information support is based on information security, which ensures that the information will not be compromised in any way if critical problems and threats occur. Thus, in recent years, the selection of information security has been significantly improved and modernized, affecting more and more areas and specializations. The existence of information security is due to the factor in the negative impact of a natural or artificial threat, in other words, a combination of factors that violate the work of the information protection mechanism. It is extremely important to analyze all the risks using various methods of diagnosis, and already on the basis of the analyzed detailed indicators, it is possible to build a system of protection against threats in the information space [2].

Sources of the threat of information security

There are natural threats and artificial threats. Artificial threats are divided into artificial intentional threats and artificial unintentional threats.

Sources of natural threat include natural disasters and natural phenomena, independent of humans; failures in computer systems.

Artificial threats make more harm to the subsequent work of the entire information system.

Artificial deliberate threats: copying and stealing of documents; destruction of information; interception of information; sabotage; hacker attack; violation of accessibility to information; fraud; disclosure of information; violation of information integrity; unauthorized access.

Artificial unintentional threats: negligence; curiosity; software errors; user error etc.

To protect digital materials, several methods of information protection can be applied:

Encryption.

Encryption is a cryptographic method that protects the digital material, turning it into an encrypted form. Encryption can be applied at many levels, from one file to a whole disk. There are many encryption algorithms, each of which scrambles information in its own way, and also requires the use of a key to decrypt data and convert them to its original form. The reliability of the encryption method depends on the key size. For example, 256-bit encryption will be safer than 128-bit.

Access control.

Access control allows the administrator to specify which access to digital materials is allowed, and the type of permitted access (for example, read only). Access control is a fundamental security concept that minimizes business risks or organization, providing security technologies and access control policies to protect confidential information (customer data). Most organizations have infrastructure and procedures that limit access to networks, computer systems, applications, files and confidential data, such as personal information and intellectual property.

Editing.

Editing is understood as the process of analyzing of a digital resource, identifying confidential information, as well as its removal or replacement. General methods used include anonymization and pseudonyimization to remove the identifying identity of information, as well as cleaning information about the authorship [3].

In the Internet era, the protection of personal information has become as important as the protection of property. Information security is the practice of protecting both physical and digital information from destruction or unauthorized access. Our world quickly turns out of the industrial into a digital society, in which cyberattacks have become a serious threat to business, individuals and governments. Therefore, in order to avoid possible losses, it is necessary to know the types of possible threats, as well as topical methods of information protection.

References

1. Nesterov S. Fundamentals of information security. St. Petersburg, 2017. 324.
2. Gafner V. Information security: A textbook. Rostov-on-Don, 2010. 324.
3. Bondarev V. Introduction to information security of automated systems. Moscow, 2016. 252.

Language adviser: *Buha S.Yu, English Teacher, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»*