

УДК 004.056.53

Anita Zaytseva¹, Valentyna Kuzmenko²

¹student of group RT-819 National University “Zaporizhzhia Polytechnic”

²senior teacher National University “Zaporizhzhia Polytechnic”

INFORMATION SECURITY

Information is any data that is perceived by living organisms, electronic devices and other systems, about the outside world, processes, objects and phenomena.

Information security is the state of security of the information needs of individuals, society and the state, regardless of internal and external dangers.

Information protection is a certain system of measures directed to prevent illegal access to information, its modification, loss, destruction and so on.

The purpose of information security is to provide secret information support for the activities of the state, industry, enterprise and individual.

Security of information is the preservation of confidentiality, integrity, availability and reliability of information - the main properties of information.

There are information systems. They can be divided into three parts: software; hardware; communications.

Information security varies by application:

Information security of the individual is characterized by the protection of the individual, social groups or associations from impacts that are directed against them.

Information security of the organization ensures its normal functioning and dynamic development. It is often implemented by the Information Security Service.

Information security of a state is the protection of important interests of an individual, society and the state, under which harm is prevented through various factors.

The principles of ensuring information security contain: the law; systemicity; economic efficiency; the balance between the interests of the individual, society and the state.

It is impossible to create a system whose protection cannot be hacked. The basic principle can be the creation of such a protection mechanism, the cost of hacking which will be more expensive than the information that can be obtained. Therefore introduction of the software of safety which are built in structure of the software of system and are necessary for performance of functions of protection is necessary.

Thanks to human development and technology, information security has been modified. Nowadays, such security is called Cyber Security. In addition to protecting processes, information and activities in cyberspace, Cyber Security also protects against viruses, hacker attacks and data tampering.

Nowadays, Cyber Security is responsible for three factors: systems; processes; people.

The notion of information security does not correspond to the wide range of issues that arise in cyberspace today. But evolution has made it part of Cyber Security.

Cyber security is the processes and methods used to protect sensitive data, computer systems, networks and software applications from cyberattacks.

Types of dangers and attacks:

1. viruses and extortionists;
2. botnet attacks: spamming, confidential data theft, distributed denial of service attacks;
3. social engineering attacks;

4. cryptographic theft;

5. phishing - a fraudulent spamming activity that imitates messages from any legitimate source.

Cyber security in general is a very broad term, but it is based on three fundamental concepts known as "CIA" (confidentiality, integrity and accessibility).

This model is designed to guide the organization's cybersecurity policies in the area of information security.

Confidentiality takes measures to restrict access to confidential information to cyber attackers and hackers.

Integrity means that data must not be altered, deleted or illegally accessed, in a word compromised.

Accessibility will ensure uninterrupted operation and access to data without any disruption. It also ensures constant communication between components, ensuring sufficient bandwidth.

Within an organization, for an effective cybersecurity approach to be implemented, people, processes, computers, networks and technologies, large or small, must be held equally accountable.

If all components complement each other, then it is very possible to withstand severe cyber threats and attacks.