TECHNOLOGIES OF INFORMATION SECURITY

Pesotsky V. A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Maksimchuk R. T. – Senior Lecture

Annotation. The role of information security is described in the thesis. The main types of InfoSec are disclosed. The importance of spreading knowledge about relevant InfoSec technologies are emphasized. The main principles of important technologies are observed. Recommendations on the best quality methods of security protection are presented in the paper.

Keywords. Information security, hackers, cyber threats, artificial intelligence, types of InfoSec, cyber warfare, behavior analytics.

In the modern world there are many facilities where confidential information is stored, but they also have some vulnerabilities, so there are a lot of people who want to steal this information for their own benefit. Such people are called black-hat hackers. People who want to get someone else's confidential information find some new loopholes every day, so information security technologies are constantly developing to counter them. To begin with, it is necessary to find out what information security is in general and how it works.

Information security or InfoSec is the protection of information and all confidential data by eliminating security holes and different threats. It monitors information risks and manages them. It usually helps reduce an unauthorized access to information, unlawful use of personal data, removing, damaging, copying or corrupting it. Information security also provides data encapsulation, which helps reduce the negative impact of such intrusions. InfoSec protects information of any type, such as tangible and intangible, electronic and physical [1]. The main purpose of information security is to optimize the work with data, provide balanced protection of confidentiality, integrity and availability for the user without sacrificing system performance.

The need to constantly maintain information security may be incomprehensible to an ordinary user. And this is the norm, so let's highlight the most basic reasons. The targets of attacks are changing. All critical infrastructures at present such as utility services, nuclear power plants, healthcare facilities, airports are connected to a network and their number is growing. Consequently, there are more targets and opportunities for hackers to steal information or harm it for personal gain. Cyber threats are becoming more advanced because of the growth of different technologies, innovations in programming and just increase of the number of black-hat hackers.

All information is stored on servers, storage devices and other multiple resources and everywhere it can be stolen. Therefore, to protect confidential information on different resources, various methods and technologies are used, which are developing constantly. Here is a description of the existing types of information security, the current technologies and the most relevant and useful information security methods. There are six types of information security:

- The first type is application security. It is a broad sphere that includes two concepts. One of them is software testing and verification by the developer and the second one is a set of applications that scan software and web technologies for their vulnerabilities. These concepts also apply to mobile applications and websites.
- The second group is cloud security, which is used for storing information and working with data on a third-party isolated platform in a secure environment that can even be disconnected from the Internet. Often, such cloud storage is connected to multiple devices, so the user can transfer information between them [3].
- The third type is cryptography - the science of encrypting information based on a secret algorithm. Encrypting data helps protect data confidentiality and integrity. Usually cryptography uses digital signatures to confirm data and identity.
- The fourth type is infrastructure security. It works with the protection of the intranet and extranet and different resources that store information such as mobile phones, laboratories, desktops, data centers and servers.
- Incident response. It is a method of dealing with the consequences of a cyberattack. The goal is to eliminate malicious software behavior with the least damage and recovery cost. It often consists of hiding the fundamental files and blocking access to software.
- The last group is vulnerability management. It is a process that scans an application or a website for weak points such as unsecured hosting or out-of-date software that conflicts with antivirus software. It also suggests fixing or blocking the environment based on risk.

Some words about the most relevant technologies of InfoSec. Cyberwarfare continues and new techniques to hack systems and networks appear. Nowadays there are many technologies for protecting information. Here is a list of the most advanced ones, that are worth paying attention to:

- Artificial intelligence. It is also used to protect information and even to create a space to store it. Often, on large projects, artificial intelligence plays the role of advanced two-factor authentication, which works on the basis of two parameters to verify identity, most often the user's password and a code that is generated randomly and sent to the user on the second device. AI analyzes data, transactions and other sources, asks for confirmation of the operation if it is unjustified.
- User and Entity Behavioral Analytics. It provides user-centric analytics alongside information about networks, endpoint and applications. The correlation of these analytics offers more effective, accurate threat detection.
- Nowadays, PIN codes and passwords no longer provide reliable equipment protection. Built-in authenticators are now more secure. Today Intel Corporation is the leader in this segment. They developed the sixth generation vPro chips. These microcircuits are built into the equipment. Designed to change the security of authentication, they use a layered authentication system that includes many methods and steps that work together.
- Also one of the types of information security is a pervasive trust service. It can monitor user’s devices and manage many requests, track malware, but with a limited processing speed. A trust service works with the Internet resource and checks for its safety, and only then provides access to the user. More importantly, trust services can offer secure storage of data on a site by checking the reliability of the resource. It also preserves data integrity and confidentiality.
- The last in this list of relevant technologies is Zero-Trust model. The term "Zero-Trust" means that information security method assumes that the network has already been hacked, which strengthens internal defenses, monitors and encrypts valuable data. To avoid potential hacking, the Zero-Trust method identifies business-critical data and its integrity, displays its logical and physical segmentation and imposes additional authentication methods. In this case, the user himself will have to go through this encryption every time [2].

So, if you want to protect your business resources or just keep your personal information private, it is worth delving into the technologies described above. Nowadays all users have to be aware of hacking techniques and of relevant information protection technologies in order to securely store their information in any digital form. After all, information is the most valuable resource in our world. By protecting your confidential information, you can save not only money, but also your time, reputation and intellectual property from intruders and from unfair spread of it to other people.

References:

1. Cisco secure products and solutions. Cisco Systems – multinational technology conglomerate [Electronic resource] – Access mode: cisco.com/c/en/us/products/security – Date of access: 26.03.2021.

2. Gartners top technologies of InfoSec. Gartner – research company connected with IT [Electronic resource] – Access mode: blogs.gartner.com/smarterwithgartner/category/it/security - Date of access: 27.03.2021.

3. John P. Mello, emerging security technologies set to level the battlefield. Tech Beacon – digital hub [Electronic resource] – Access mode: techbeacon.com/security - Date of access: 26.03.2021