# CYBERSECURITY: AN IMPORTANT PART OF THE IT WORLD

*Sayfiyeva Gulnigor Negmurod kizi*

*Teacher of Bukhara City Technical School*

**Abstract:** This article provides information about the problem of cybersecurity and its aspects related to modern information technologies (IT). Cybersecurity is the protection of computer systems, networks, and data from unauthorized access or theft.

**Keywords:** cybersecurity, problem, modern information technologies, computer systems, networks, data, unauthorized access, protection against theft.

In today's rapidly developing information technologies, cybersecurity has become one of the main issues. Along with the expansion of the Internet, modern technologies, the emergence of artificial intelligence and IT (Internet of Things) devices, the number of cyberattacks is also increasing. Cybersecurity means taking measures to protect computer systems, networks and data from unauthorized access or theft. IT has become an integral part of the infrastructure. To fully understand the meaning of the term cybersecurity, let's divide the word into two parts: "cyber" and "security". The term "cyber" usually refers to anything related to computers, information technology or the Internet. To understand this better, it should be imagined as a special word related to computers and the Internet. Security, on the other hand, refers to the state of being free from danger or threat and being safe. So, putting the two words together, "cybersecurity" refers to keeping computers, networks, and any device connected to the internet safe from any risk or threat.

Why is cybersecurity so important today? Cybersecurity is closely related to all the technological advances that are taking place in our time, especially. The development of modern methods of processing, transmitting and collecting information leads to an increase in threats associated with the loss, corruption and disclosure of user information. Therefore, ensuring information security in computer

systems and networks is one of the leading directions in the development of information technologies.

Cybersecurity consists of several important components:

- Confidentiality – ensuring that only authorized persons have access to information.

- Integrity – ensuring that information remains unchanged and accurate.

- Availability – ensuring that the system and information are accessible as needed.

This trio (the CIA triad) constitutes the emergence of cybersecurity. Modern IT systems face a variety of situations. The most common are:

- Malware. Malicious software such as viruses, Trojans, spyware, and ransomware that damage or steal user data.

- Phishing. A method of obtaining personal information by deceptively selling products. Often done through email or fake websites.

- DDoS attacks. Distributed Denial of Service (DDoS) attacks cause servers to fail by overloading them.

- Social engineering. Attacks that target human factors rather than technical factors, such as tricking users into logging into a system.

Types of protection methods:

- Cryptography. A method of protecting data by encrypting it. Algorithms such as AES and RSA are widely used in modern systems.

- Antivirus and software. Programs designed to detect and eliminate malicious programs.

- Network security. Monitoring network traffic through firewalls, IDS/IPS systems.

- Multi-factor authentication (MFA). Taking into account the removal of benefits by transferring them from one to another when necessary.

The global importance of cybersecurity. Today, it is important not only at the security level, but also at the state level. Cybercrime is causing great damage to the economy. For example:

- Attacks on banking systems lead to losses.
- Attacks on government systems pose a threat to the national system.
- Theft of personal information leads to social movements.

That is why many countries are developing cybersecurity strategies.

Today, modern digital technologies introduced in our country are opening the door to a number of conveniences and opportunities for our citizens. Along with this process, there is, of course, the problem of ensuring the security of digital technologies and information systems being created. In the fight against cybercrime, which is improving day by day, we can protect ourselves from them, that is, ensure cybersecurity, by fulfilling the following basic requirements:

- educate citizens on the basics of information security;
- regularly test the vulnerabilities of the software used;
- use reliable antivirus software;
- use official licensed programs;
- use multi-factor authentication to protect information systems;
- adhere to a strong password policy when using passwords;
- regularly encrypt data on computer hard drives, etc.

In Uzbekistan, great attention is also being paid to cybersecurity. A "Cybersecurity Center" has been established, which is engaged in protecting systems, securing information and obtaining it safely. In addition, special attention is being paid to cybersecurity in IT through training young people through in-depth knowledge and developing education.

Cybersecurity is an integral part of modern IT infrastructure. It is connected to technologies and works in a complex way. Therefore, it is necessary to use effective

resources, ensure user safety and implement modern technologies. In the future, cybersecurity is expected to develop with artificial intelligence, blockchain and other innovative technologies.

**References:**

1. Alahmadi, A., & Altuwaijri, M. (2019). Cybersecurity challenges in healthcare information systems. Journal of Healthcare Informatics Research, 3(2), 123-140.
2. Bärcanescu, E. (2021). Cybersecurity for medical data: Risks, challenges, and solutions. Health Policy and Technology, 10(3), 100-118.
3. European Union. (2018). General Data Protection Regulation (GDPR). Official Journal of the European Union.
4. Fernandez-Aleman, J. L., Senor, I. C., Lozoya, P. Ä. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3), 541-562.
5. Xolmirzaev, R. M. (2018). Axborot xavfsizligi va kiberxavfsizlik. Tashkent: “Fan” nashriyoti.
6. Jumayev, A. T. (2020). Sun’iy intellekt va kiberxavfsizlik: Yangi imkoniyatlar va xatarlar. Tashkent: O‘zbekiston Milliy Universiteti nashriyoti.