BASIC PRINCIPLES AND NECESSITY OF CYBER SECURITY AS AN EXAMPLE OF FOREIGN EXPERIENCE

Jalolov Lazizbek Jasur ugli
University of Business and Science
1st year student of information systems and technologies

Abstract:
Cyber security is an important issue for every organization and country today. Along with the development of digital technologies, the widespread use of the Internet and the increasing role of information systems in our lives, the need to fight against cyber threats is also increasing. The basic principles of cyber security and its necessity will be considered on the example of foreign experiences, which will help to understand what achievements have been made in this field and what problems exist.

Key words: cyber security, privacy, information, state, society, foreign experiences.

The main principles of cyber security are as follows: Confidentiality should ensure that information is used and viewed only by authorized persons. Encryption, authentication and authorization mechanisms are used to ensure confidentiality. For example, in the US, government organizations and corporations use advanced encryption technologies to protect their data. In ensuring privacy, it is important to implement mechanisms to protect personal data, identify users and authorize data. Integrity is necessary to ensure the correctness and immutability of information. This is important to prevent data from being improperly modified or destroyed. Abroad, for example, European Union countries have implemented strong control and monitoring systems to ensure data integrity.To ensure integrity, it is necessary to create backup copies of the database and update them regularly. Availability means ensuring that information and systems are always accessible by authorized users. To ensure availability, it is necessary to develop and implement backups, rapid recovery plans in critical situations. In China, for example, government institutions are constantly focusing on strengthening cyber security to maintain the availability of their systems in the event of cyber attacks. Analyzing and monitoring processes are important in combating cyber threats. It is necessary to use modern analytical tools and artificial intelligence to detect cyber attacks and threats. Cyber security agencies in the US are using advanced analytics to detect and counter cyber threats.

Monitoring systems allow quick response to cyber threats and increase the level of security of organizations. The need for cyber security depends on several factors. First, as the digital economy grows, so does the number of cyber attacks. Cybercriminals act to steal, blackmail, or harm organizations' financial and informational resources. Therefore, organizations need to strengthen their cyber security strategies. Organizations suffer huge financial losses as a result of cyber-attacks, as well as their reputation and credibility. Second, competition between states and cyber wars make cyber security even more important.
In order to ensure their national security, foreign countries have established cyber security as their strategic goals and established special units to combat cyber threats. For example, countries such as Russia and China view cyber security as an important factor in ensuring their national security. Third, the importance of cyber security is that it plays an important role in protecting personal information and ensuring the privacy of citizens. Theft of personal information and its illegal use are on the rise. Therefore, countries and organizations are obliged to strengthen legislative and technological measures to protect personal data. The European Union, for example, has developed strict laws on the protection of personal data and established strict controls in their implementation.
Foreign experiences show that many achievements have been made in the field of cyber security. For example, the European Union passed the General Data Protection Regulation (GDPR) in 2018. This law sets high standards for the protection of personal data and imposes strict requirements on how organizations collect, store and use data. This law is important in strengthening cyber security and protecting the rights of citizens. Also, the Cybersecurity and Infrastructure Security Agency (CISA) was established in the US to strengthen cooperation between federal agencies and the private sector on cyber security.This agency plays an important role in countering cyber threats, sharing information and developing strategies for cyber security. CISA also runs a variety of programs in partnership with the private sector to identify and counter cyber threats. Canada has developed a "Cyber Security Strategy" to ensure cyber security. This strategy aims to strengthen cooperation between the government, the private sector and citizens. There is a strong focus on education and awareness to ensure cyber security in Canada. Cyber security education programs and seminars are organized to prepare citizens to deal with cyber threats. A number of measures should be implemented to strengthen cyber security. Organizations must constantly update their cyber security strategies. Cyber threats

and technology are constantly changing, so organizations need to keep their security measures up to date. This, in turn, ensures that it is effective in combating cyber threats. Cyber security education and awareness is important. Organizations need to conduct training and workshops to prepare their employees to deal with cyber threats. Employees should be educated on how to respond to cyber threats, how to protect personal information, and how to use the internet safely. This, in turn, increases the overall security level of the organization. It is necessary to strengthen the cooperation between the states and the private sector. In the field of cyber security, it is important to cooperate, share experiences and fight cyber threats together. Building mutual trust between governments and the private sector will help develop effective strategies to combat cyber threats.

Modern technologies play an important role in ensuring cyber security. Artificial intelligence, machine learning and big data are effective tools in combating cyber threats. With the help of artificial intelligence, the processes of identifying cyber threats and taking measures against them can be automated. This saves time and increases productivity for cybersecurity professionals. Legislation and regulations are important in ensuring cyber security. States need to develop laws and regulations to ensure cyber security in their territories. These laws provide guidance to organizations in combating cybercrime, protecting personal information, and combating cyber threats. The future of cyber security depends on digital technologies and cyber threats. As the digital economy grows, cyber attacks are becoming more complex and dangerous. Therefore, it is necessary to develop new technologies and strategies in the field of cyber security. Artificial intelligence, blockchain and other advanced technologies play an important role in cyber security.

Conclusion:

In conclusion, the basic principles of cyber security – confidentiality, integrity, availability, analysis and monitoring – are important in today's digital world. Foreign experiences show the need to strengthen cyber security and develop effective strategies to combat threats.To ensure cyber security, it is necessary to strengthen cooperation between states, organizations and individuals, introduce modern technologies and improve legislation. This, in turn, helps ensure the stability of the digital economy and the safety of citizens. Issues and threats in the field of cyber security are constantly changing, so it is necessary to constantly be prepared for innovations and changes in this field. By ensuring cyber security, we can create a safe and sustainable environment in the digital world.

References:

1. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
2. Stallings, W. (2018). Network Security: Principles and Practice. Pearson.
3. Kizza, J. M. (2017). Guide to Computer Network Security. Springer.
4. European Union. (2018). General Data Protection Regulation (GDPR). [Online] Available at: https://gdpr.eu/
5. U.S. Department of Homeland Security. (2020). Cybersecurity Strategy. [Online] Available at: https://www.dhs.gov/cybersecurity-strategy
6. Canadian Centre for Cyber Security. (2019). Cyber Security Strategy. [Online] Available at: https://cyber.gc.ca/en/guidance/cyber-security-strategy