OVERVIEW OF INFORMATION SYSTEMS AND THEIR CYBER SECURITY REQUIREMENTS ON THE EXAMPLE OF FOREIGN EXPERIENCE

Jalolov Lazizbek Jasur ugli
University of Business and Science
1st Year Student of information Systems and Technologies

Abstract: Modern information systems play an important role in every field, including business, health, education, and government. They help to automate the processes of data collection, storage and processing. However, the effective operation and security of information systems depends on cyber security. Cyber security, in turn, is a set of measures necessary to ensure the protection of information systems, the confidentiality and integrity of information. This article provides an overview of information systems and their cyber security requirements on the example of foreign experiences.

Keywords: modern information systems, cyber security, automation, data integrity, foreign experiences, data processing.

Information systems are used for a variety of purposes and their cyber security requirements include: Information stored in information systems should only be viewed and used by authorized users. Authentication and authorization mechanisms are used to ensure confidentiality. In order to ensure the integrity of data, it is necessary to prevent their change or loss. Data backup and control mechanisms are used to achieve this goal. Information systems and data must be continuously available. To ensure availability, it is necessary to ensure the stability and continuous operation of systems. Foreign experiences show different approaches to ensuring information systems and cyber security requirements. These include public-private partnerships, the use of modern technology, and cybersecurity education and training.

In the US, the Cybersecurity and Infrastructure Security Agency (CISA) focuses on promoting collaboration between the public and private sectors in cyber security. CISA works with private companies to combat cybersecurity threats and helps them set security standards. This cooperation will be effective in ensuring cyber security. The European Union has developed a number of laws and regulations to ensure cyber security. For example, the General Data Protection Regulation (GDPR) aims to ensure data privacy. The EU develops and implements cybersecurity education programs that help train cybersecurity professionals. The Australian Government has developed a 'Cyber Security Strategy' to help ensure cyber security. This strategy aims to strengthen cooperation between the public and private sectors in combating cyber security threats. Australia focuses on training professionals through cyber security education and training. Singapore has developed a "Cyber Security Strategy" for cyber security, which aims to strengthen the country's cyber security infrastructure. Cyber security education and training is being held in Singapore, and collaboration between the public and private sectors is developing.

There are a number of challenges to cyber security. Among them are factors such as technological changes, the human factor and the development of cyber security threats.

The rapid development of technologies creates challenges in ensuring cyber security. New technologies create new opportunities for cyber attacks, which require constant updating for cyber security professionals. The human factor plays an important role in ensuring cyber security. Failure of users to comply with cyber security rules or carelessness can be a reason for cyber attacks. Therefore, it is necessary to educate users about cyber security. The development of cyber security threats creates challenges in cyber security. Malware, phishing attacks, and other cyberattacks are constantly evolving, requiring cybersecurity professionals to develop new strategies.

Conclusion:

An overview of information systems and their cyber security requirements is illustrated by examples of foreign experiences. Cyber security is essential for the protection of information systems and the security of data. Foreign experiences show approaches such as cooperation between the public and private sectors, the use of modern technologies and the provision of education and training on cyber security. Requirements such as confidentiality, integrity and availability are important in ensuring cyber security.However, there are challenges in ensuring cyber security, such as technological changes, the human factor and the evolution of cyber security threats. It is necessary to develop and implement effective strategies to solve these problems. Staying abreast of developments and news in the field of cybersecurity, as well as educating users, is essential to maintaining cybersecurity.

References:

1. NIST (2018). "Framework for Improving Critical Infrastructure Cybersecurity". National Institute of Standards and Technology. https://www.nist.gov/cyberframework

2. ISO/IEC (2013). "ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements". International Organization for Standardization.

3. European Commission (2016). "General Data Protection Regulation (GDPR)". https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

4. Australian Government (2020). "Australia's Cyber Security Strategy 2020". Department of Home Affairs. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security

5. Ponemon Institute (2020). "Cost of a Data Breach Report 2020". Ponemon Institute LLC. https://www.ibm.com/security/data-breach

6. ENISA (2020). "Threat Landscape for 2020". European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020