CYBERSECURITY AND PERSONAL DATA PROTECTION

SAODAT RAKHMATOVA AMRAKULOVNA
Scientific supervisor: Associate Professor of the Department of Languages
Samarkand branch of Tashkent University of Information Technologies
Samarkand, Uzbekistan
Email: saodatraxmatova67@gmail.com
XASANOV DIYORBEK MUZAFFAROVICH
Student of group KI 25-01, Samarkand branch of Tashkent University of Information Technologies. Samarkand, Uzbekistan
Email: xasanovdiyorbek4007@gmail.com

Abstract: This scientific article examines the theoretical foundations of cybersecurity, its role in society and the economy, and the issues of personal data protection. In the context of digital transformation, the value of information resources is increasing, making their protection a critical task. The article analyzes types of cyber threats, their classification, modern protection technologies, and the need to improve users' information literacy. It also highlights the importance of cybersecurity policies at both global and national levels.

Keywords: cybersecurity, information security, personal data, cyber attack.

Introduction

The 21st century is the century of information technologies, and almost all spheres of human life are being digitized at a rapid pace. Today, e-government systems, online banking services, distance learning, social networks, and cloud technologies are widely used. As a result of the formation of the digital economy, information has become one of the most important resources. As a result, the speed of information exchange is increasing, the quality of services is improving, and people's lives are becoming much easier.

At the same time, the expansion of the digital environment is also causing various risks. In particular, the increasing number and complexity of cybercrime is becoming a global problem. Modern cyberattacks can cause serious damage not only to individual users, but also to large organizations, financial institutions, and even state systems. This makes the issue of ensuring cybersecurity one of the priority areas.

Cybersecurity is a complex set of measures aimed at protecting information systems, computer networks and data from unauthorized access,

modification, destruction or dissemination. It includes not only technical means, but also organizational, legal and human factors measures. The main goal of cybersecurity is to ensure the confidentiality, integrity and availability of information.

The protection of personal data is especially relevant today. As a result of the growing number of Internet users, active participation in social networks and the use of various online services, the volume of personal data is increasing dramatically. Misuse or theft of this data can lead to financial losses, violation of privacy and other negative consequences.

In addition, the issue of cybersecurity on a global scale also requires international cooperation. Each state, along with developing its own national cybersecurity strategy, must also study international experience. Because cyberattacks do not recognize borders and their prevention is possible only through an integrated approach.

Therefore, ensuring cybersecurity and protecting personal data is becoming an important task not only for specialists, but also for every user. By improving information literacy, adhering to security rules and using modern technologies correctly, cyber risks can be significantly reduced.

Theoretical foundations of cybersecurity

Cybersecurity is an important component of information security, which includes a set of theoretical and practical approaches aimed at protecting computer systems, networks and digital data from various threats. Since information has become a strategic resource in the modern information society, its protection requires a systematic and comprehensive approach.

The most important model that forms the theoretical basis of cybersecurity is the CIA model (Confidentiality, Integrity, Availability), which defines three basic principles of information security:

Confidentiality - information should be accessible only to authorized users. To ensure this principle, mechanisms such as authentication, authorization and cryptography are used. For example, unauthorized access is prevented by passwords, biometric systems and data encryption.

Integrity - information should not be changed, corrupted and remain in its original state. This principle is aimed at preventing unauthorized changes to data. To ensure integrity, hash functions, digital signatures and control mechanisms are used.

Availability – the system and data must be available to users when needed. This principle is aimed at ensuring the uninterrupted operation of services and includes measures to protect servers, create backups and combat DDoS attacks.

These three principles are closely interconnected, and the violation of one

of them negatively affects the overall level of security. Therefore, cybersecurity systems are developed in a comprehensive manner based on these principles.

In addition, modern cybersecurity theory also includes additional principles. Including:

Authentication – determining the user's identity

Authorization – determining the user's rights in the system

Audit and monitoring – monitoring and analyzing system activity

Accountability – recording actions and determining responsibility

The theoretical foundations of cybersecurity cover not only technical aspects, but also the human factor. Because many cyberattacks are carried out due to the negligence or lack of sufficient knowledge of users. Therefore, in ensuring information security, along with technologies, it is also important to increase the information culture of users.

Cybersecurity threats and their classification

Modern cyber threats are becoming increasingly complex with the development of technology. Cybercriminals are using new methods to gain access to information systems, steal data, or disrupt system operations. Therefore, the correct classification and analysis of threats is of great importance in ensuring cybersecurity.

Cybersecurity threats are usually divided into the following main groups:. Technical threats

Technical threats are threats that arise at the software or hardware level and are based on the exploitation of system vulnerabilities.

Viruses and malware – programs created to damage a computer system, steal data, or control the system (virus, trojan, ransomware, etc.).

Network attacks (DDoS, MITM) – attacks aimed at disabling services or controlling information exchange. For example, DDoS attacks cause the server to fail by overloading it.

Exploits – illegal access to a system using software errors and vulnerabilities.

Technical threats are often carried out using automated means and can cause significant damage.

Social engineering attacks

Social engineering is a set of methods aimed at obtaining confidential information by influencing the human factor. This type of attack is based on a psychological approach, not a technical one.

Phishing – forcing a user to enter their login, password or bank details through fake messages or sites.

Spear phishing – a more carefully prepared type of attack aimed at a specific person or organization.

Pretexting – obtaining information by creating a fake situation or identity and deceiving the user.

The success of these attacks is often associated with the carelessness and low information literacy of users.

Internal Threats

Internal threats are related to individuals within the organization and are often overlooked.

Disclosure by employees – intentional or accidental disclosure of confidential information.

Misuse or negligence – damage to systems due to non-compliance with security rules.

Internal threats are particularly dangerous and are carried out by individuals who already have access to the system.

The importance of protecting personal data

Personal data is any information that can directly or indirectly identify an individual. This includes name, phone number, address, passport data, biometric data and online identifiers. The volume of this data is increasing dramatically as a result of the widespread use of digital technologies.

Personal data protection is important for the following reasons:

Financial security - theft of bank cards and financial information can cause significant damage

Privacy - disclosure of personal data leads to violation of human rights

Fraud prevention - illegal use of data can lead to various crimes

In addition, the protection of personal data is associated with ensuring the constitutional rights of citizens. Therefore, in many countries, including Uzbekistan, special laws have been adopted in this direction and their implementation is monitored.

Modern methods of protection

To ensure cybersecurity, various technical, organizational and individual measures are used in a comprehensive manner.

Technical means serve to automatically protect information systems:

Cryptography - protects data from unauthorized reading by encrypting it

Firewall - controls traffic between external and internal networks

Antivirus programs - detect and destroy malicious programs

IDS/IPS systems - detect and prevent attacks in real time

In modern systems, security tools based on artificial intelligence are also widely used.

Organizational measures

Organizational measures are aimed at reducing risks associated with the

human factor:

Regular training and education of employees

Development and implementation of an information security policy

Minimum allocation of access rights (least privilege principle)

Perform security audits and monitoring

Personal security rules

Each user can protect their data by following the following simple rules:

Create strong and complex passwords (various character combinations)

Use two-factor authentication (2FA)

Do not open suspicious links and files

Use public Wi-Fi networks with caution

Regularly back up important data

The relevance of cybersecurity in the digital age

Today, as a new stage in human development, the process of digital transformation continues at a rapid pace. Modern technologies such as artificial intelligence (AI), the Internet of Things (IoT), blockchain, cloud computing and big data are penetrating all areas of life. While these technologies increase economic efficiency, improve the quality of services and increase the level of automation, they also create new types of cyber threats.

In particular, the following threats are becoming increasingly relevant:

Data theft through smart devices (IoT) - home appliances, cameras and sensors can monitor users' lives or steal data

Sophisticated cyberattacks using artificial intelligence - automated and difficult-to-detect attacks are being developed using AI technologies

Big Data security issues - breaches of large databases can lead to the leakage of a huge amount of user data

Therefore, cybersecurity strategies must be constantly updated, adapted to new technologies and developed based on a proactive approach. Today, cybersecurity is becoming not only a protection, but also a system for identifying and preventing threats in advance.

Cybersecurity in the conditions of Uzbekistan

In Uzbekistan, in recent years, the process of digitization has become one of the important directions of state policy. The introduction of the e-government system, the development of online payment systems, and the digitalization of public services are leading to the widespread use of information technologies.

At the same time, a number of important works are being carried out in the country to ensure cybersecurity:

National cybersecurity systems and centers are being developed, the protection of state information systems is being strengthened

The legislative framework for information security is being improved, including the development of regulatory documents on the protection of personal data

A system for training cybersecurity specialists is being established, special directions are being opened in universities and training centers

Attention is being paid to increasing digital literacy, training and programs are being organized for the population and youth

These measures will strengthen information security in the country, ensure the stability of the digital economy, and effectively combat cybercrime.

Conclusion

Cybersecurity and personal data protection are one of the most important and integral components of a modern digital society. Along with the rapid development of information technologies, cyber threats are also becoming more complex and becoming a serious problem on a global scale.

Every user, organization and state should approach this issue systematically and responsibly. Along with the introduction of technological protection tools, it is important to take into account the human factor, improve information literacy and strictly adhere to security rules. In conclusion, ensuring cybersecurity is a continuous process that requires constant updating, innovation and cooperation. Only through an integrated approach can we ensure safe and sustainable development in the digital environment.

REFERENCES

1. Law of the Republic of Uzbekistan “On Informatization”
2. Law of the Republic of Uzbekistan “On Personal Data”
3. ISO/IEC 27001: Information Security Management Systems
4. Stallings W. Cryptography and Network Security, Pearson Education, 2017
5. Schneier B. Secrets and Lies: Digital Security in a Networked World, Wiley, 2015
6. Official materials of Kaspersky Lab
7. Cisco Networking Academy – Cybersecurity Essentials
8. ENISA (European Union Agency for Cybersecurity) reports