

DEVELOP A TRAINING PROGRAM FOR YOUNG PROFESSIONALS IN EDUCATIONAL INSTITUTIONS, WHICH IS THE CORE OF CYBERSECURITY

Davronjon Shokirjon oqli Abdullajonov

Kokand University, teacher of business department

abdavron94@gmail.com

Gulmira Kahramon qizi Kasimova

Kokand University, Department of Economics

qosimovagulmira342@gmail.com

ABSTRACT

This article focuses on cybersecurity, one of the key drivers of the digital economy. The article discusses the work being done in Uzbekistan on cyber security. It also briefly describes the role of our country in the international global ranking of cybersecurity.

Keywords: Digital data, information security, e-government, cybersecurity, network security, software security, operational security, information systems and resources.

INTRODUCTION

As we live in this age of technology, we are witnessing significant changes in every area. Today, we know that cybersecurity has also become a topical issue in international politics, which is due to the fact that the development of the digital economy and the formation of the information society depend on certain aspects. In particular, raising the position of Uzbekistan in global rankings has risen to the level of public policy. Therefore, the study of international and national rankings for determining the level of cybersecurity, according to the assessment criteria set out in them, is one of the most pressing issues in the important information infrastructure in government agencies and

organizations. It is known that the head of our state Shavkat Mirziyoyev declared 2020 the Year of Science, Enlightenment and Development of the Digital Economy. On March 2, 2020, the Presidential Decree "On the State Program for the implementation of the Action Strategy for the five priority areas of development of the Republic of Uzbekistan in 2017-2021 in the "Year of Science, Enlightenment and Digital Economy "" The State Program "Year of Science, Enlightenment and Development of the Digital Economy" was adopted.¹

The state program consists of five main directions, the fifth direction of which is the development of the National Cyber Security Strategy for 2020-2023 and the draft law "On Cyber Security". Ensuring information security is an important factor in digital data management. Emphasis should be placed on ensuring unauthorized access to digital data, ensuring their security by protecting them from the media, and ensuring the simplicity of data transmission. So what is cybersecurity and how serious are cybersecurity threats today?

Cybersecurity is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from unauthorized attacks, also known as information technology security. The term is used in a variety of contexts, from business to mobile computing, and cybersecurity falls into several categories:

1) Network security is the practice of protecting a computer network from intruders, regardless of targeted attackers or malware.

2) Software Security - This is to protect software and devices from threats.

3) Operational security - includes information asset management, protection processes and decisions. The permissions that users have when accessing the network are how and where the data is stored.

¹ Decree of the President of the Republic of Uzbekistan "On the State Program for the implementation of the Action Strategy for the five priority areas of development of the Republic of Uzbekistan in 2017-2021 in the "Year of Science, Enlightenment and Digital Economy ", March 2, 2020, No. PF-5953

LITERATURE ANALYSIS AND METHODS

In writing this article, the President of the Republic of Uzbekistan "On the State Program for the implementation of the Action Strategy for the five priority areas of development of the Republic of Uzbekistan in 2017-2021 in the" Year of Science, Enlightenment and Digital Economy "and Decrees "On measures to further improve the field of information technology and communications" in the Presidential Decree "On measures to improve the system of control over the introduction of information technology and communications, their protection" and the Strategy "Digital Uzbekistan - 2030" The data provided were the basis. The analysis of statistical data in the article used data from the official website of the International Association of Electronic Communications (www.itu.int) and SUE "Cyber Security Center" (State Unitary Enterprise) and statistical analysis methods in the analysis of data in the article.

DISCUSSION AND RESULTS

In today's age of technology, our daily lives are more dependent on technology than ever before. The benefits of these trends range from close access to data on the Internet to the modern conveniences offered by smart home automation technology, while the convenience of these technologies can be hard to believe that there are potential threats hidden behind every device and platform.

Nevertheless, the cybersecurity threats posed by the modern technologies of society are a real threat. The steady rise in cybercrime highlights the shortcomings of the devices and services we are connected to. While some components of cybersecurity are primarily designed to strike, most experts today believe that the best way to protect all assets from attacks, from computers and smartphones to networks and databases, is to protect the privacy of the media. is the process of protecting against every type of cybercrime, from theft to international digital weapons. However, cybercrime is defined as any unauthorized activity involving a computer, device, or network, and

there are 3 classifications: computer-assisted crimes, computer-targeted crimes, and computer-directed crimes. are crimes that are not related but are random to the offender.

Today's cybersecurity industry focuses on protecting devices and systems from intruders, and cybersecurity professionals are constantly refusing services from many websites without constantly working. It should be noted that the threat of "Internet of Things" in the field of cybersecurity is a matter of serious concern. The concepts of digitalization and cybersecurity always come side by side. Because along with the digitization of all systems and processes, it is important to ensure their technically perfect and flawless operation and security. The more attention is paid to the development of the digital economy in our country, the more attention is paid to cyber security. A clear example of this is the fact that our country ranks high in the International Global Cybersecurity Rankings, published annually by the International Telecommunication Union. The International Global Cybersecurity Rating is a joint project of ABI Research and the International Telecommunication Union (ITU), which provides an assessment of the level of participation of countries in the field of cybersecurity. The level of commitment is assessed in five areas: legal measures, technical measures, organizational measures, capacity building and international cooperation. Cybersecurity, in the broadest sense, is a set of measures to protect information technology, such as devices, applications, information systems and data. This means maintaining the confidentiality of data, protecting its integrity, and ensuring that software and information systems function properly without compromise. This will increase production efficiency. In addition, monitoring of the national segment of the Internet has identified more than 130,000 cyber security threats. Of these, 106,508 cases belong to hosts who have become participants in botnet networks. 13,882 cases are related to the blocking of blacklisted IP addresses by various services due to spam e-mail or

password breaches. 8,457 cases are related to the use of the TFTP (Trivial File Transfer Protocol) protocol and its respective ports, which can lead to the download of third-

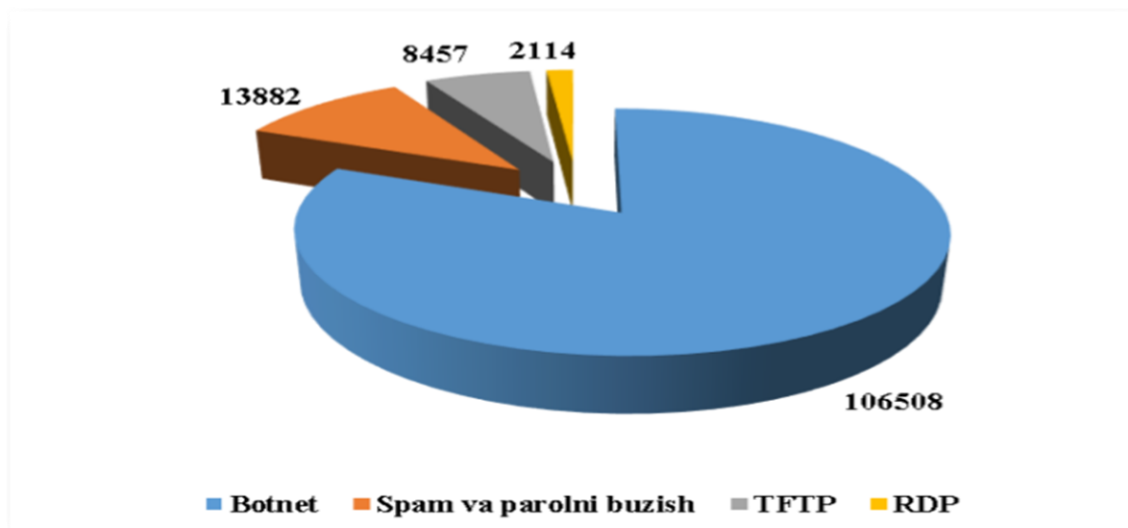


Figure.1 Hypersecurity threats in the national segment

party content due to the lack of authentication mechanisms. 2,114 cases are related to the use of the vulnerable protocol RDP (Remote Desktop Protocol). In 1,042 cases, the lack of authentication mechanism in software and database management systems is due to expired or invalid signed SSL certificates. (Figure 1)

These analyzes once again confirm the urgency of the issue of cybersecurity, as software vulnerabilities can lead to intruders accessing information systems or websites, files and data remotely, and leaking personal data of citizens. Cybersecurity measures prevent such cases.

There is an urgent need to strengthen the legal framework for cybersecurity. The digital world has not yet been able to clearly define its legal status. New types and forms of threats are emerging every day, and they need to be reflected in the legislation. The development of a national cybersecurity strategy will regulate the activities in the field of combating crime in the national cyberspace. After all, the harm and risk of crime in the virtual world is no less than in the real world. According to the National Cyber Security Strategy for 2020-2023, a unified system of cyber security and a legal

framework for the protection of critical infrastructure from cyberattacks will be formed. The Law on Cyber Security reflects the protection of information and communication technologies from modern cyber threats, the introduction of modern mechanisms for cyber security for various levels of systems, the definition of the rights and obligations of government agencies, enterprises and organizations in this area, coordination of their activities. is expected to reach. At the heart of all the reforms being carried out in our country is the goal of creating conveniences for our people. The emphasis on cybersecurity has led to the reliable and secure use of digital capabilities.

CONCLUSION

In short, the digitalization of all sectors of the economy will allow us to integrate into the world community, to gain a foothold in the world market, to achieve economic development, to create conveniences for the population. Fortunately, this is the main issue on the agenda in our country. Uzbekistan is taking bold steps towards digitalization. Our country is taking comprehensive measures to actively develop the digital economy, the widespread introduction of modern information and communication technologies in all sectors and industries, especially in public administration, education, health and agriculture.

More than 220 priority projects have been launched to improve the e-government system, further develop the local market of software products and information technologies, establish IT parks in all regions of the country and provide the industry with qualified personnel. In addition, a comprehensive program "Digital Tashkent" is being implemented, which provides for the launch of an integrated geoportal with more than 40 information systems, the creation of an information system for public transport and utility infrastructure management, digitalization of the social sphere and subsequent introduction of this practice in other regions. Special attention should be paid to data security in the implementation of the tasks listed above. Ensuring the

accuracy, reliability and confidentiality of statistics on economic, social and cultural development of the country is one of the most pressing issues today.

REFERENCES

1. Decree of the President of the Republic of Uzbekistan "On the State Program for the implementation of the Action Strategy for the five priority areas of development of the Republic of Uzbekistan in 2017-2021 in the" Year of Science, Enlightenment and Digital Economy ", March 2, 2020, No. PF-5953
2. Decree of the President of the Republic of Uzbekistan "On measures to further improve the field of information technology and communications", February 19, 2018, No. PF-5349
3. Annex 1 to the Decree of the President of the Republic of Uzbekistan "On approval of the Strategy" Digital Uzbekistan - 2030 "and measures for its effective implementation" Strategy "Digital Uzbekistan - 2030". October 5, 2020, No. PF-6079.
4. Mulaydinov, F., & Nishonqulov, S. (2021). The role of information technologies in the development of the digital economy. The role of information technologies in the development of the digital economy.
5. Abdullajonov, D. (2022). IMPROVING THE SOCIO-ECONOMIC MECHANISMS OF STRENGTHENING LABOR MOTIVATION IN THE ENTERPRISE: labor motivation, foreign experience, efficiency, corporate systems, innovative economy. Kokand University Scientific Materials Database, 1 (000005).
6. G.Q. Qosimova, F.M. Mulaydinov. Problems of innovative development in the economy and business. Science and culture in the eyes of young scientists and leaders: International scientific-practical online conference, June 26, 2020. "Kokand." Pages 172-174.
7. <https://www.itu.int> - Official website of the International Telecommunication Union



8. <https://ncsi.ega.ee/country/uz/> - National Cyber Security Index
9. <https://tace.uz> - Official site of the State Unitary Enterprise Cyber Security Center

