CYBERSECURITY IS AN ESSENTIAL CONDITION OF THE DIGITAL ECONOMY

Student of TATU Fergana branch
M.I.Abdurahimova

All systems are being digitized in Uzbekistan. Especially in the quarantine regime introduced due to the coronavirus, the demand for online goods and services has increased, and the range of digital functions has expanded in all areas. Today, it is possible to make payments without leaving home, get distance education without any problems, use the world's largest libraries and even work. Digital services have a number of advantages over the traditional type, such as lack of paperwork, formalities, and time savings. For example, if you receive government services digitally, you will receive a discount of 10 percent of the fixed fee.

All this is a sign of the active transition to the digital economy in our country. Another factor in the development of the digital economy is the provision of cyber security. In quarantine conditions, there have been cases of distribution of viruses that crash software systems on the global network under the label of instructions for avoiding the coronavirus. Financial fraudsters have been using fake online stores, websites, social media accounts and email addresses to trick unsuspecting people by promising online sales and delivery of medicines overseas and asking for money upfront. . This once again confirms the need to ensure information security.

The concepts of digitization and cyber security always go hand in hand. Because along with the digitization of all systems and processes, it is important to ensure their technically perfect and error-free operation and safety. The more attention is paid to the development of the digital economy in our country, the more urgent it is to ensure cyber security. Uzbekistan is strengthening its position in the global cyber security index. In 2017, our country took 93rd place in this rating, and in 2018, it rose to 52nd place.

Cybersecurity, being a form of information security, is a different concept than high spirituality that serves to sort out information. It refers to more technical processes, and for the average user it means setting up reliable and strong passwords in mail, social networks, payment systems, protecting their personal computer and smartphone from viruses. In a broader sense, cyber security is a set of measures aimed at protecting networks, mobile applications and devices. This means maintaining the confidentiality of data, protecting their integrity, and the full operation of this or that site, application, or program.

According to the analysis of the "Cybersecurity Center" SUK, in 2019, 268 cyber security incidents were detected on the websites of the national segment of the Internet.

This means that the number of crimes in the digital world has decreased by 44% compared to the previous year. Of these, 222 were related to unauthorized uploading of content, 45 to deface (a hacking attack that means a website page is replaced with another, such as an ad page), and one to stealth mining (hidden activity on a cryptocurrency platform).

69 percent of the incidents were detected on websites hosted by hosting providers in Uzbekistan, and the remaining 31 percent related to sites hosted by hosting providers in foreign countries. In relation to 80 cases, investigations were carried out and practical recommendations were given to eliminate the identified vulnerabilities, and the remaining 188 cases were independently resolved by the website owners. Security issues in cyberspace include managing content with security flaws in the code, working with outdated versions, easy access passwords, templates downloaded from insecure sources, and managing websites on virus-infected computers. .

As a result of monitoring the national segment of the Internet, more than 130,000 threats to cyber security have been identified. Of these, 106,508 cases relate to hosts that became participants in botnet networks. 13,882 cases are related to blocking IP addresses blacklisted by various services due to spam e-mail or password cracking. 8,457 cases are related to the use of the TFTP (Trivial File Transfer Protocol) protocol and related ports, which can lead to the download of extraneous content due to the lack of authentication mechanisms. 2,114 cases are related to the use of a vulnerable RDP (Remote Desktop Protocol) protocol. 1,042 cases were related to software and database management systems not having an authentication mechanism, as well as SSL certificates with expired or invalid signatures.

These analyzes once again confirm the relevance of the issue of cyber security, because software vulnerabilities can cause an attacker to remotely access an information system or website, as well as files and data, and leak personal data of citizens. Cyber security measures prevent such situations.

Cyber security for 2020-2023 according to the state program for the implementation of the five priority areas of development of the Republic of Uzbekistan in 2017-2021 in the "Year of Science, Enlightenment and Digital Economy Development" a national strategy and a draft law "On Cyber Security" will be developed.

Legal enforcement of cyber security standards is extremely necessary and worthwhile. The digital world has yet to define its legal status. In this regard, new types and forms of threats are emerging every day, and it is necessary to reflect them in the legislation. The development of a national strategy on cyber security regulates activities in the field of combating crime in the national cyberspace. After all, the harm and danger of crime in the virtual world is no less than in the real world.

Also, 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 cyber attacks will be formed.

The law "On cyber security" provides for the protection of information communication and technology systems from modern cyber threats, the introduction of modern cyber security mechanisms for systems of various levels, the determination of the rights and obligations of state bodies, enterprises and organizations in this field, and the coordination of their activities. etc. are expected to be reflected. The need to unify normative legal documents in this field was felt.

At the heart of all the reforms being carried out in our country is the goal of creating comfort for our people. A special focus on cyber security has been the basis for using digital opportunities in a reliable and secure manner.

References

1. Address of the President of the Republic of Uzbekistan Shavkat Mirziyoyev to the Oliy Majlis.https://uza.uz/oz/politics/zbekiston-respublikasi-prezidentishavkat-mirziyeevning-oliy-25-01-2020.
2. No. PF-5953 of the President of the Republic of Uzbekistan dated March 2, 2020 "Implementation of the Strategy of Actions on five priority areas of development of the Republic of Uzbekistan in 2017-2021 in the "Year of Science, Enlightenment and Digital Economy Development" Decree on the state program on increasing
3. Abdurakhmanov QX Labor economy: theory and practice. Textbook. Revised and supplemented 3rd edition. T.: "FAN", 2019. p. 552.
4. Zokirova NK, Abdurakhmanova G., Sagidullin FR Transformation form zanyatosti v innovationnom razvitii // International scientific review. 2020. No. LXX. - S. 24-28.
5. Odegov Yuriy Gennadyevich, Pavlova Valentina Vasilievna Noviye tekhnologii i ix vliyaniye na rinok truda // Uroven jizni naseleniya regionov Rossii. 2018. No. 2 (208). - S. 60-70.