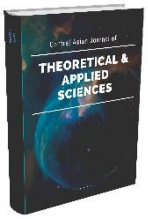

CENTRAL ASIAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES

Volume: 03 Issue: 10 | Oct 2022 ISSN: 2660-5317
https://cajotas.centralasianstudies.org

The Issue of Ensuring the Cybersecurity of the Republic of Uzbekistan in the Process of Implementing the Strategy "Digital Uzbekistan-2030"

Azamat U. Nematullayev
Young researcher

Received 9th Aug 2022, Accepted 8th Sep 2022, Online 9th Oct 2022

Abstract: *This article presents the recent development of information technologies worldwide and achievements of the Republic of Uzbekistan in Information-communication sphere in particular. As it is written, thanks to introduction of information technologies in all sectors of the life, spheres such as public administration, education, healthcare and agriculture developing positively. Economic, social and political reforms that being taken in the country by the Head of state help set many democratic values as never before. With the help of modern information technologies the country's economy liberalized visibly, the public officials became more responsible and accountable in front of citizens. The article also provides a brief information about the strategy "Digital Uzbekistan-2030" that was adopted in 2020 and its implementation by the Ministry in charge. As well as in this work the author tries to develop some recommendations to ensure the cyber security of the Republic of Uzbekistan.*

Keywords: *Information technologies, cybersecurity of Uzbekistan, the strategy "Digital Uzbekistan-2030", ensuring cybersecurity, the law on "cybersecurity" of the Republic of Uzbekistan.*

Introduction

The new industrial revolution, taking place in the world, is based on revolutionary transformations in the field of information technology. Informatization of all spheres of human activity provides enormous opportunities for the development of economics, finance, social security, education, and medicine, fundamental and applied scientific research in all directions. But, any information revolution, in addition to global positive changes, entails global threats. The most dangerous of these threats are cybercrime and cyberterrorism. In fact, none of the major terrorist acts is complete without the use of modern information technology (V.S.Ovchinskiy, 2017).

Due to this, all countries and international organizations over the globe are now developing different algorithms to counter these issues, analyzing new types, forms and way of cybersecurity and cyberterrorism.

For the Republic of Uzbekistan, as a developing country as well as a regional leader in the near perspective, the issue of ensuring cybersecurity is also vital.

From the time Shavkat Mirziyoyev, the incumbent President of the Republic of Uzbekistan, started to serve his presidency period in 2016, he has been carrying out positive economic, social and political reforms in the country. He set democratic values as never before, with the help of modern information technologies the country’s economy liberalized visibly, the public officials became more responsible and accountable in front of citizens. Even the Oliy Majlis, the Parliament of the Republic of Uzbekistan, started to conduct plenary sessions live (Sh.Mirziyoyev, 2021). Moreover, to further implement comprehensive measures for the active development of the digital economy, as well as the widespread introduction of modern information and communication technologies in all sectors and spheres, primarily in public administration, education, healthcare and agriculture the President Sh. Mirziyoyev signed a decree “On the approval of the strategy "Digital Uzbekistan-2030" and measures for its effective implementation” in 2020.

In this article I would like to examine the issue of ensuring the cybersecurity of the Republic of Uzbekistan in the process of implementing the strategy "Digital Uzbekistan-2030" as well as try to develop some recommendations to consolidate both legal and technical basics of the ensuring the cybersecurity of the Republic of Uzbekistan in this highlighted period.

The strategy "Digital Uzbekistan-2030" and its implementation during the past few years

On the 5th October, 2020, the President of the Republic of Uzbekistan approved the Strategy "Digital Uzbekistan — 2030", developed by the Ministry for the Development of Information Technologies and Communications with the participation of interested ministries and departments, representatives of the business community and academia, as well as foreign experts (Zamanov, 2020).

The main objectives of the Strategy are to develop the digital industry in the country, increase the competitiveness of the national economy by digitally transforming primarily economic sectors and regions.

In frame of the Strategy "Digital Uzbekistan — 2030" a range of ambitious plans were made. According to the Presidential Decree “On the approval of the strategy "Digital Uzbekistan-2030" during the years 2020–2022, it is expected to carry out following goals:

- to increase the level of connection of settlements to the Internet from 78% to 95%, as well as by increasing up to 2.5 million broadband access ports, laying 20 thousand kilometers of fiber-optic communication lines and the development of mobile communication networks;
- to implement over 400 information systems, electronic services and other software products in various areas of socio-economic development of the regions;
- to organize the training of 587 thousand people in the basics of computer programming, including by attracting 500 thousand young people within the framework of the "One Million Programmers" project;
- to implement over 280 information systems and software products for automation of management, production and logistics processes at enterprises of the real sector of the economy;
- to secure relevant higher educational institutions in the regions to improve the digital literacy and skills of khokims, employees of state bodies and organizations, training them in information technology and information security, as well as training 12 thousand of their employees in information technology.

Besides,the document also states that by the end of 2020, the digitalization of pre-school education, healthcare and general education schools would be completed. They would be provided with the necessary IT infrastructure, computer equipment. To implement information systems, employees will be sent for training in 13 model districts;

From the November 1st, 2020, it was expected that at least 5% of the total amount of funds from investment projects, as well as international financial institutions, foreign government financial organizations and donor countries would be directed to "digital" components.

A “Road map” for 2020–2022 which was also approved in the frame of the strategy, implies the development of four key areas, namely the development of e-government, digital industry, digital education and digital infrastructure and etc. (Sh.Mirziyoyev, 2020).

With the Presidential Decree, the Ministry for development of information technologies and communications of the Republic of Uzbekistan was appointed as the responsible body in the implementation of the strategy.

The implementation of the Strategy

For the past almost two years The Ministry for development of information technologies and communications of the Republic of Uzbekistan has been carrying out a range of activities to fulfil legal acts on time.

As it is highlighted above, the main objective of the strategy is to develop the digital industry in the country, increase the competitiveness of the national economy by digitally transforming. To complete this task, it is highly important to create appropriate infrastructure.

In January, 2022, The Ministry for development of information technologies and communications of the Republic of Uzbekistan held a briefing on “The results of the Ministry's activities for 2021”.

As it is stated, in order to develop telecommunication networks in Uzbekistan, an additional 50,000 kilometers of fiber-optic lines were laid, and as a result their total length was brought to 118 thousand kilometers, about 67 percent of settlements received access to high-speed communications. In the following years, activities will continue to expand fiber-optic communication lines. **For notes:** The figure was 22.2 thousand km in 2016.

Currently, the total bandwidth of international communication channels is 1,800 Gbit/s, and according to the results of the projects planned for implementation by the end of 2022, this figure is expected to be brought to 3,200 Gbit/s.

In order to develop mobile communications, the speed of mobile Internet was increased 1.5 times, and in 2021, 14,150 stations were installed. Thus, their total number has been brought to 45,890 units.

Currently, the number of Internet users has exceeded 27.2 million people. Including 25.3 million people use the mobile Internet.

Moreover, people through a my.gov.uz portal can use about 300 types of public services in electronic format. It is noteworthy that 185 of them are provided free of charge, and 181 services do not require an electronic digital signature and etc. (Sh.Axmatov, 2022).

Apart from this, O. Pecos, the incumbent first deputy minister of the Ministry for development of information technologies and communications of the Republic of Uzbekistan, in his article published in the magazine “O‘zbekiston iqtisodiy axborotnomasi – Economic Bulletin of Uzbekistan”, also provides some statistics in the field.

As he states, within the framework of the digital development of the republic, special emphasis is placed on providing social facilities with high-speed Internet connection. Currently, 97% of secondary schools, 82% of mahalla (local) gatherings of citizens, 56% of police stations, as well as 100 percent of preschool educational and medical institutions are connected to a high-speed Internet network. The task has been set to fully provide all social facilities with high-speed Internet connection by the end of this year.

Mobile communications are also developing at an accelerated pace by increasing and modernizing base stations. So, if in 2016 the total number of base stations was 17.2 thousand units, then by 2020 this figure has grown to 31.7 thousand. This year, it is planned to install another 2 thousand base stations.

It should be noted that if earlier the expansion of mobile networks was carried out on the basis of 2G technologies; today projects based on 3G/4G technologies are being implemented. So, last year 3.6 thousand base stations were upgraded on the basis of 3G/4G technologies.

There are a range of activities that are underway to develop 5G technology. So, since April of this year in the business quarter of Tashkent – Tashkent City, Ucell (mobile telecommunication operator) has launched a fifth-generation network. In the future, it is also planned to deploy a 5G network in regional centers.

The subscriber base of mobile operators is consistently growing. Within five years, the number of mobile users has grown from 21.2 million in 2016 to 27 million people in the first half of 2021. 23.1 million People use the mobile Internet today.

There have been also carried out some actions to digitalize the government services.

The development of the e-government system in Uzbekistan is considered as one of the priority areas of digital reforms, which will allow to qualitatively reform the activities of public authorities and management. Large-scale e-reforms in the public sector cover all spheres of activity without exception with the broad involvement of ministries and departments (O.Pecos, 2021).

When it comes to digitalization the economy of the country, it can be noted that in 2021 the share of the digital economy in Uzbekistan's GDP was 2.2 percent. The share of the digital economy in Uzbekistan's GDP is planned to increase by 2 times by 2023, and the share of electronic public services is planned to increase to 60% in 2022. Currently, more than 260 projects are being implemented in the republic aimed at the consistent introduction of elements of the digital economy and "electronic government", as well as the digitalization of the banking sector. The system of instant payments for business entities and entrepreneurs has been launched 24/7.

During 2020-2022, it is planned to attract investments in the field of information technology and communications in the amount of 498.1 million dollars. It is planned to implement 1,627 projects for the digital transformation of regions and industries (Abaturov, 2021) and etc.

The issue of ensuring the cybersecurity of the Republic of Uzbekistan

Such a rapid development of the digital economy and other spheres implies a multiple increase in information security risks also. Critical infrastructures are constantly targeted by cyber-adversaries, and we have seen security incidents exert both cascading and crippling effects regionally, nationally, and even internationally, due to the high degree of interconnectedness and interdependency that our global society now involves (Ho, 2014).

According to the experts in the area, Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined (Morgan, 2020).

Today no nation and no country is off such attacks. Uzbekistan may also be in the top list that hackers aim to inflict high loses on the country. Recently, by the company “Comparitech”, a pro-consumer website providing information, tools, reviews and comparisons to help the readers in the US, UK and the rest of the world improve their cyber security and privacy online (Comparitech, 2015), there has been carried out a research on the levels of cybersecurity of the countries around the globe. Within the research, experts analyzed 75 countries, judging each of them with an extended list of 15 criteria. This means countries are ranked from one to 75 with one being the least cyber-secure country and 75 being the most cyber-secure country. In the list, Uzbekistan is found among those countries that were the least cyber-secure country in the world (BISCHOFF, 2021).

In 2020 only, more than 27 million events of malicious and suspicious network activity originating from the address space of the national segment of the Internet, which in turn posed a threat to the safe and stable functioning of information systems and resources of government agencies and other organizations, were revealed in the Republic of Uzbekistan.

According to the data provided by the State Unitary Enterprise “Cybersecurity center”, by the end of 2020, out of 86,679 registered domains, about 30,000 domains were active. Of these, more than 12,500 domains have an SSL security certificate and about 300 domains have expired certificates.

As part of the safe operation of information systems and websites, 680 security events were detected in 2020, including technical problems, which is about 1,000,000 minutes of unavailability of websites. In addition, in the same year, 9,955,152 security events were recorded, of which 94,147 events could lead to unauthorized access and leakage of confidential information and etc..

According to the monitoring carried out by the State Unitary Enterprise “Cybersecurity center”, it is said that as part of the identification of malicious content and the analysis of its involvement in offenses in the information space, investigations of cybersecurity incidents were conducted, during which the causes and methods of their implementation were established.

The main reasons and methods for the successful implementation of hacker attacks are followings:

Brute force account passwords, outdated or vulnerable version of the content management system (CMS), SQL injections, and outdated plugins.

In particular, according to the results of investigations, more than 2,690 malicious files were identified, as well as sources (countries) from which unauthorized destructive actions were carried out: Romania, Germany, the Republic of Slovakia, the USA, Indonesia, China, the Russian Federation, Great Britain, France, Saudi Arabia, Tunisia, Ukraine, the Netherlands, South Korea, Canada, Turkey, Poland, Vietnam and India.

Compared to the same period in 2019, there is a dynamics of an increase in the number of incidents committed against the websites of state and economic bodies by 144% (centre", 2021).

According to the latest research by reputable international companies in the field of geopolitical risks, in recent years there will be a dynamic growth of crimes in the world using information and communication technologies.

According to the latest research of reputable international companies in the field of geopolitical risks, in recent years there will be a dynamic growth of crimes in the world, using information and communication technologies in connection with:

- ✓ the transition to remote work of employees of companies (organizations);
- ✓ online education;
- ✓ making safe purchases in online stores;
- ✓ Widespread use of Internet of Things devices (cameras, devices, sensors, etc.);

- ✓ the spread of ransomware viruses (cryptographers). It is necessary to take into account the rapid growth in the number of new end devices added to the Internet, as the coverage of 4G and 5G networks expands and sensors, cameras and other Internet of Things devices spread.

In addition, the increased demand for shopping in online stores and online trading platforms will create an additional "springboard" for fraudsters on the Internet, as a result of which the theft of funds from citizens' bank cards will increase. Another big threat that public and private companies may have to face will be the so-called ransomware viruses (cryptographers), the distribution of which will mainly be carried out by sending phishing emails or exploiting vulnerabilities in systems. Taking into account the above, such risks as: Internet of Things devices vulnerable to cyber attacks, unauthorized access for destructive purposes to information systems of organizations and the education system, and fraud on the Internet are the main challenges that are likely to be faced in the country.

All mentioned above positive developments in digitalization of economy and social sphere of the Republic of Uzbekistan as well as the cybersecurity incidents happened in recent years strongly recommends thinking one more time to find the ways to ensure cybersecurity of the country in the long run.

Today, The Republic of Uzbekistan is taking some steps to ensure cybersecurity in the country of at the levels of legislation, institutionalism and international.

Legislation

For the past years there have been no exact laws to control thenrelations in the country's cybersecurity. The sphere was partially controlled with the laws such as “On personal data”, The Criminality and Code on administrative responsibility and etc.. What’s more, recently The Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan adopted the bill “On cybersecurity” (Majlis, 2022), where I personally participated in the preparation of this legal act. The need to develop this bill, as already mentioned above, is associated with increased challenges and risks in cyberspace, a sharp increase in cybercrime, an increase in online attacks, and the unpredictable dynamics of cyberspace development in the world. According to the developers of the bill, currently, the Republic of Uzbekistan is actively developing and implementing digital technologies in both the public and private sectors. In addition to the advantages and new opportunities for all spheres of human activity, there are a number of potential risks to the sustainable functioning of information systems and resources of the public sector, the rights and freedoms of citizens, which may pose a real threat to public interests, health and well-being of society and citizens.

In addition, legal norms on information security issues are only partially implemented in the legislation of the Republic of Uzbekistan. To date, this area is controlled by separate decrees and resolutions of the President of the Republic of Uzbekistan, which do not fully cover it, and also meet global trends in the field of information and cybersecurity.

There is no system of interaction between government agencies and telecom operators that allows tracking cyber attacks, preventing their consequences and taking adequate preventive measures.

As before, the objects of the state information and communication infrastructure remain unidentified and unclassified, which can lead to negative and even catastrophic consequences for the economic and social situation of the Republic of Uzbekistan. There are no methods and techniques for assessing the security systems of information systems and resources at critical information infrastructure facilities.

Given the rapid development and variability of cyberspace, the bill should provide an opportunity to respond more quickly to challenges in an ever-changing environment.

In order to minimize administrative procedures and time costs in the event of new fundamental threats in the digital environment, the bill proposes to clearly define the following issues:

basic principles of cybersecurity;

powers, rights and obligations of the authorized state body in the field of cybersecurity;

requirements for ensuring cybersecurity of information systems and resources of state bodies and organizations;

responding to cybersecurity incidents;

formation of the regulatory framework on the level of importance of critical information infrastructures;

creating favorable conditions and stimulating national projects and personnel in the field of cybersecurity.

The main objectives of the adoption of the bill:

1. Regulation of relations in the field of cybersecurity in cyberspace of the Republic of Uzbekistan.
2. Introduction of terms and definitions used in the field of cybersecurity.
3. Establishment of the powers, rights and obligations of the Authorized state body in the field of cybersecurity.
4. Establishment of requirements for ensuring cybersecurity of information systems and resources of state bodies and organizations.
5. Responding to computer incidents (threat detection, detection and prevention of attacks and their consequences), ensuring the effective operation of CERT (Computer Incident Response Centers).
6. Formation of the regulatory framework according to the level of importance of critical information infrastructure objects.
7. Implementation of requirements to ensure cybersecurity of objects and subjects of critical information infrastructure.
8. Establishing the rights and obligations of subjects of critical information infrastructure.
9. Creation of an effective legal framework for the promotion and further development of the domestic cybersecurity industry: adoption of state support measures, training of cybersecurity specialists, creation of a national operating system and software.

Institution

In accordance with the Decree of the President of the Republic of Uzbekistan PD-4024 dated November 21, 2018 "On measures to improve the system of control over the introduction of information technologies and communications, the organization of their protection" were created: "State Inspectorate for Control in the field of Informatization and Telecommunications" of the Republic of Uzbekistan and "Technical Assistance Center" in the form of a state unitary enterprise.

The tasks of the Center include:

- ➢ collection, analysis and accumulation of data on modern threats to information security, development of recommendations and proposals for the prompt adoption of effective organizational and software and technical solutions to prevent acts of illegal penetration into information systems, resources and databases of government agencies and organizations;

- interaction with operators and providers of telecommunications networks, law enforcement agencies in the framework of analysis, identification of violators, methods and means used in the implementation of unauthorized or destructive actions in the information space;
- certification, examination and certification of hardware and software products, information and communication technologies, telecommunication equipment and other technical means at informatization facilities (with the exception of state secrets);
- assistance in the development and implementation of information security policy of information systems and resources of state bodies and organizations;
- development of proposals to improve the regulatory framework in the field of information security of state information systems and resources, as well as the national segment of the Internet;
- Timely notification of national Internet users about emerging threats to information security in the national segment of the Internet, as well as the provision of consulting services for information protection (source, 2022).

International cooperation

Currently The Republic of Uzbekistan has been carrying out a close relationship with the CIS on issues of information security. On June 29, 2021, an international expert Forum on information Security issues was held in Tashkent city, organized by the Institute for Strategic and Interregional Studies under the President of the Republic of Uzbekistan jointly with the Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan and the implementation of the Information Security Strategy of the Executive Committee of the Commonwealth of Independent States (CIS).

The main objectives of the Forum were formulated in accordance with the key directions of the updated Concept for the further development of the CIS and assumed:

- ✓ substantive discussion of topical issues of international information security and ways to solve them in the context of the dynamic development of the digital agenda in the CIS;
- ✓ exchange of experience in strengthening cooperation in the main areas of digital economy development, building an integrated digital infrastructure and ensuring the security of common digital processes;
- ✓ Development of expert recommendations on joint counteraction to security challenges and threats in the information space, including for the development of an Action Plan for the phased implementation of the Information Security Strategy of the Commonwealth.

As a result of the discussion, a final document was adopted containing practical proposals for the governments of the Commonwealth countries on the effective implementation of innovative development strategies, including issues of information security, legal and organizational and technical support for the development of the digital economy, as well as the training of specialized specialists in this area (Committee, 2021).

Recommendations to ensure cybersecurity of The Republic of Uzbekistan

To to ensure cybersecurity of The Republic of Uzbekistan, it is recommended to The Republic of Uzbekistan to carry out the following tasks:

- to establish and ensure the continuous work of institutions in the field of cybersecurity;
- to ensure the stability and security of the functioning of information systems and technologies;

- to create solid legal bases of ensuring the protection of the rights and legitimate interests of business in the digital economy;
- to create of technical tools that ensure safe information interaction of citizens in the digital economy;
- to ensure the manageability and reliability of the functioning of the Russian segment of the Internet;
- to ensure organizational and legal protection of state interests in the digital economy;
- to ensure the stability and safety of the functioning of the unified telecommunication network of Uzbekistan;
- to ensure the technological independence and security of the functioning of hardware and infrastructure;
- to ensure the legal regime of machine-to-machine interaction for cyber-physical systems (Y. Konoplevo, 2019);
- to establish international cooperation in the field of cybersecurity.

Conclusion

By the way of conclusion, I can say that, the Republic of Uzbekistan as a full-right member of the process of globalization has entered to the new era, the era of "Information technologies". The current changes in the world shows that if a state want to develop both economically and socially, has first of all to develop its information infrastructure, digitalize all the spheres of the country. Digitalization help states to carry out a transparent policy. It makes public officials to be more accountable in front of the nation, mitigates the level of corruption and finally endeavors democracy. But on the other hand, there is a flip side of the informatization. As it was many times noted above, recent times the level of crimes related to cyberspace increasing dramatically. The cross-border nature of cybercrimes and spreading fake news, to misconduct peoples mind, are gaining a lot of power due to the Internet. In this condition the republic of Uzbekistan should follow the golden rules of ensuring information security and develop its own and new strategies to combat crimes related to information and information technologies.

Reference List

1. Abaturov, V., 2021. SCO Internet-portal. [Online] Available at: https://e-cis.info/news/566/95743/ [Accessed 9 January 2022].
2. BISCHOFF, P., 2021. Which countries have the worst (and best) cybersecurity?, London: Comparitech.
3. centre", "., 2021. Kiberxavfsizlik markazi DUK. [Online] Available at: https://tace.uz/upload/iblock/5fb/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%A0%D0%B5%D1%81%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D0%BA%D0%B8_%D0%A3%D0%B7%D0%B1%D0%B5%D0%BA%D0%B8%D1%81%D1%82%D0%B0%D0 [Accessed 27 february 2022].
4. Committee, P. S. o. t. C. E., 2021. Internet portal of the CIS. [Online] Available at: https://e-cis.info/news/564/93076/ [Accessed 28 february 2022].
5. Comparitech, 2015. Comparitech. [Online] Available at: https://www.comparitech.com/about-us/ [Accessed 1 February 2022].
6. Ho, K.-K., 2014. Cybersecurity The Strategic View. JSTOR, 1 November, pp. 5-12.

7. Majlis, L. C. o. t. O., 2022. Kiberxavfsizlik sohasidagi munosabatlar qonun bilan tartibga solinadi (Relations in the sphere of cybersecurity will be streamlined by law). [Online] Available at: https://parliament.gov.uz/uz/events/chamber/36954/?sphrase_id=7942492 [Accessed 27 february 2022].

8. Morgan, S., 2020. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine.

9. O.Pecos, 2021. Digital Uzbekistan: goals, objectives, prospects. [Online] Available at: https://mitc.uz/ru/news/view/3011 [Accessed 9 January 2022].

10. P, n.d. [Online].

11. Sh.Axmatov, 2022. A briefing was held on the work carried out by the Ministry for the Development of Information Technologies and Communications in 2021. [Online] Available at: https://mitc.uz/ru/news/view/3577 [Accessed 11 January 2022].

12. Sh.Mirziyoyev, 2020. decree “On the approval of the strategy "Digital Uzbekistan-2030" and measures for its effective implementation”, Tashkent: Lex.uz.

13. Sh.Mirziyoyev, 2021. The Decree of the President of the Republic of Uzbekistan on "Additional measures to ensure the openness of the activities of state bodies and organizations, as well as effective implementation of public control", Tashkent: Lex.uz online.

14. source, o., 2022. Cyber Security uz. [Online] Available at: https://tace.uz/company/ [Accessed 28 february 2022].

15. V.S.Ovchinskiy, 2017. "Fundamentials of fighting against cybercrime and cybersecurity " (Translated from russian). Moscow: Norma.

16. Y. Konoplevo, V. K. D. T., 2019. Kiberbezopasnost kak factor razvitiya sifrovoy ekonomiki. Vestnik Severo-Kavkazskogo federalnogo universiteta, #4(73), pp. 49-55.

17. Zamanov, O., 2020. "Raqamli O'zbekiston-2030" strategiyasi qabul qilindi (The strategy "Digital Uzbekistan-2030" has been signed. tr.), Tashkent: Norma.uz.