Journal of Advanced Zoology
ISSN: 0253-7214
Volume 44 Issue S7 Year 2023 Page 827-831

Cybersecurity In Network Technologies: Current Threats And Protection

Khusenov Murodjon Zokhirovich[1]*

[1]*(Lecturer of the Department of Information Systems and Digital Technologies of Bukhara State University, e-mail: m.z.xusenov@buxdu.uz, ORCID: 0000-0002-1533-3102)

***Corresponding Author:** Khusenov Murodjon Zokhirovich
*(Lecturer of the Department of Information Systems and Digital Technologies of Bukhara State University, e-mail: m.z.xusenov@buxdu.uz, ORCID: 0000-0002-1533-3102)

In the modern digital society, cybersecurity and protection of network systems from threats and attacks are becoming key priorities. With the growing number of cyber threats and a variety of hacker attacks on companies and organizations around the world are faced with the need to ensure reliable protection of national information systems. Uzbekistan has recently attached great importance to cybersecurity and the protection of network systems from threats and attacks. With the growing number of Internet users in the republic and the development of information technologies, it is becoming increasingly important to ensure security in the network environment. In this article, we will look at more detailed measures that are being taken in Uzbekistan to protect network systems and combat cyber threats.

Keywords: cybersecurity, network technologies, threats, protection, cyberattacks, viruses, worms, Trojans, phishing, social engineering, mobile security, vulnerabilities, antivirus software, firewall, encryption.

1. Introductions

In today's digital world, where networks penetrate into all areas of our lives, cybersecurity is becoming a matter of critical importance. Threats in network technologies are constantly evolving, the protection of data and systems is becoming an increasingly complex task.
Scientists V.M.Sidorenko[4], S.A.Gnatyuk[5], V.A.Gnatyuk[6], P.Krasev[7], V.Jafarli[8], D.Gaskova[9], E.Batueva[10], S.Sebekin[11] conducted scientific research on the use of modern pedagogical technologies and information and communication technologies in education, information security and cybersecurity.

Cybersecurity – is a field of knowledge, methods and practical actions aimed at protecting information systems from threats associated with unauthorized access, modification or destruction of data, as well as from interrupting the functioning of systems. It includes many technical, organizational and legal measures to ensure information security and protect network systems from threats [3].
One of the most serious threats is cyberattacks, which can cause significant damage to companies, governments and individual users. Cybercriminals use various methods to infiltrate systems, including phishing, malware, denial of service attacks (DDoS) and more. They can steal confidential data, blackmail organizations or damage their reputation.

2. The most common and dangerous threats to the educational process

What is at risk? Most people see the need to protect computer equipment. Cars cost money and therefore have value in themselves. But if you think about why organizations are so willing to spend large amounts of money on their computer systems — for storing, accessing and transmitting information — the value of this information becomes more obvious. After all, it makes no sense to spend a huge amount of limited resources on information processing equipment if the information itself is of no value. And since the information has become so useful, not only the equipment, but also the data requires protection. In the educational community, information about students, staff and other resources is much more valuable for the work of universities. [2]
Let's look at some of the most common and dangerous threats:

Malicious software (viruses, worms, Trojans): Viruses and other types of malicious software are developed by attackers to gain unauthorized access to the system, stolen data or disrupt the normal operation of the network. They can be spread via email, malicious links, infected websites or under the guise of useful applications.

Phishing and Social Engineering: Phishing is a method of fraud in which attackers, under the guise of a reliable organization, try to obtain confidential data such as passwords, credit card details or social security numbers. They can use email, fake websites or social networks to deceive users and lead them to fake data entry pages[13].

The spread of botnets and money scams: Botnets are networks of infected computers that are controlled by attackers without the knowledge of the owners. They can be used to carry out mass attacks, such as DDoS attacks, when a huge number of requests are sent to the target system, overloading it and leading to denial of service for legitimate users. Botnets can also be used for fraud, sending spam, stealing personal information or mining cryptocurrency.

DDoS attacks (Denial of service attacks): DDoS attacks are one of the most common types of attacks that are aimed at overloading the target system. Attackers use botnets or other methods to send a huge number of requests to the target system, which leads to resource overload and denial of service for legitimate users[14].

3. Basic methods of protection against cyber threats

Antivirus software (APO). APO helps to detect, block and remove malware such as viruses, worms, Trojans and spyware. It regularly scans the system for potential threats and warns the user about suspicious activity. It is important to choose a reliable APO and update it regularly to detect new threats.

Firewalls. Firewalls are the first line of defense against unauthorized access to the network. They monitor incoming and outgoing network traffic, analyze data packets and block suspicious activity. Firewalls can be either software built into operating systems or routers, or hardware provided by specialized devices.

Data encryption: Data encryption is used to protect the confidentiality of information, both in the data transmission path and in the storage. Encryption transforms data into a form incomprehensible to outsiders and requires a special key for decryption. There are various encryption algorithms, such as AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman) and others that ensure data security.

Regular software updates. Regular updating of operating systems, applications and devices is an important measure of protection against known vulnerabilities. Software updates often contain fixes, patches, and security improvements that help prevent possible attacks. It is important to keep track of updates and install them immediately after their release.

User training. The human factor is one of the most vulnerable points in security systems. Training employees and users in the basics of online security, such as creating complex passwords, awareness of social engineering, recognition of suspicious links and attachments, helps to reduce risks. Users should be aware of current threats and trained in correct behavior online and even offline.

Multi-factor authentication (MFA). The MFA adds an additional layer of protection, requiring not only a password, but also additional forms of identification, such as fingerprint, one-time codes, authentication via a mobile device, and others. This complicates the task for attackers who will need more than just a password to gain access to the system.

Monitoring and registration of events. Event monitoring and registration systems (Security Information and Event Management - SIEM) allow you to monitor and analyze network activity. They detect suspicious activity, create event logs and warn about anomalies. This helps security operators respond to threats in real time and prevent potential attacks.

All these methods of protection must be implemented in a complex in order to create a reliable cybersecurity system. It is important to constantly update and adapt security measures, as threats are constantly evolving and becoming more complex[12].

The fight against cyber threats is a complex and constantly changing process that requires the use of various algorithms and methods. Here is a general algorithm for preventing cyber threats:

4. Cybersecurity politics in Uzbekistan

Uzbekistan has developed and adopted several legislative acts regulating the field of cybersecurity. One of the key documents in this area is the Law "On Cybersecurity"[1]. It defines the legal framework for protecting information systems and data from threats and attacks. In addition, Uzbekistan has developed a National Cybersecurity Strategy, which defines priority areas of activity in the field of cybersecurity at the national level.

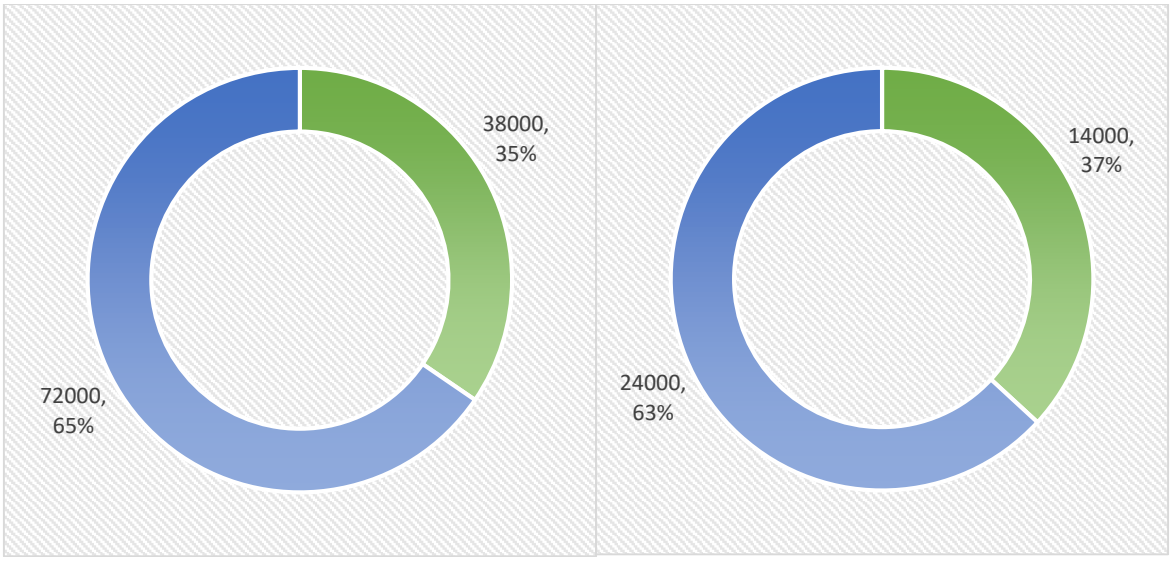
The National Cybersecurity Center (NCSC) has been established in Uzbekistan, which is the central body for coordinating and monitoring cybersecurity in the country. The NCSC is engaged in threat analysis, security policy development, information security of government agencies and assistance in the investigation of cybercrimes. The purpose of the NCSC is to effectively protect the national information infrastructure and ensure the security of information on the network.

Uzbekistan is actively developing cyber infrastructure, including communication networks, server centers and data processing infrastructure. The protection of network systems is a priority in the development of this

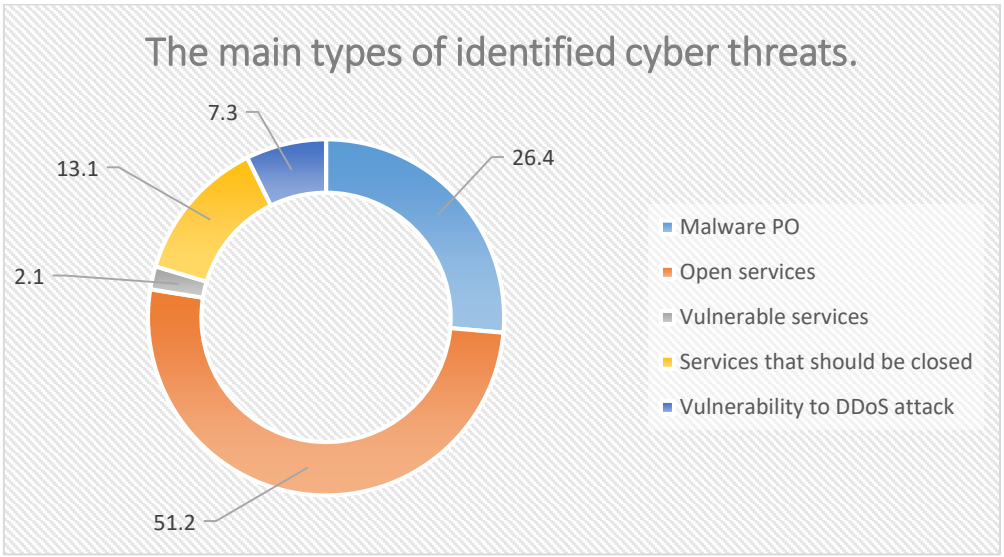
infrastructure. The creation of modern and secure communication networks, the use of modern technologies and architectural solutions helps to strengthen protection against threats and attacks. The Republic is developing its capabilities in the field of cyber defense and incident response. This includes the creation of centers for detecting and responding to cyber attacks, the development of methodologies and tools for detecting and analyzing incidents, as well as the organization of trainings and exercises for cybersecurity specialists.

Uzbekistan cooperates with international organizations and partners in the field of cybersecurity. The country participates in international forums, trainings and exercises, as well as exchanges information and experience with other States. This allows Uzbekistan to improve its cybersecurity practices and fight threats and attacks more effectively.

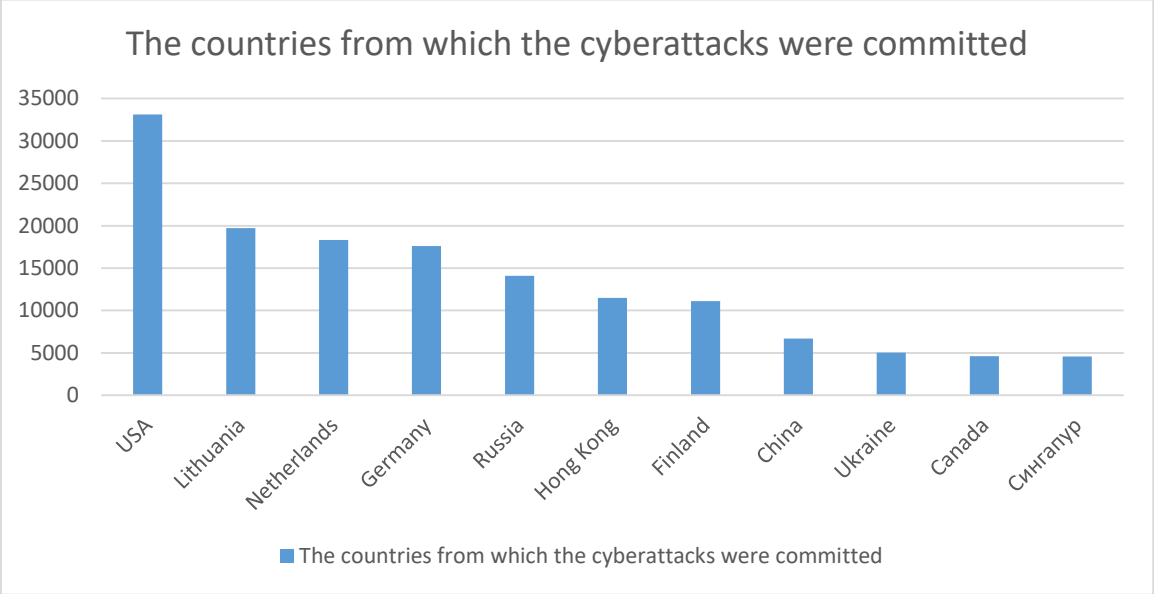
As of the first quarter of 2023, more than 110,000 domains are connected in the "uz" segment of the Internet of the Republic of Uzbekistan, of which more than 38,000 are active domains. Of these, more than 14,000 Domains are protected by a secure SSL certificate.



Also, 1650000 cyber threats related to malicious network activity have been identified in the National Cyberspace. They can be divided into types in the following section



Most of the detected and blocked cyber attacks were carried out from the territory of the USA, Lithuania, the Netherlands and other countries.



5. Conclusion

Uzbekistan attaches great importance to cybersecurity and protection of network systems. The legislative framework, the creation of a National Cybersecurity Center, the development of cyber infrastructure, cyber defense and cooperation with international partners are all important steps aimed at effectively protecting network systems from threats and attacks. The country continues to develop its cybersecurity capabilities to ensure the security of information and protect national interests in cyberspace.

6. References

1. Закон Республики Узбекистан «О кибербезопасности» №ЗРУ-764 от 15 апреля 2022 года
2. Авезов А.А, Хусенов М.З Вопросы безопасности в образовательном учреждении Вестник науки и образования 2022. № 5 (125).Часть 2 с 15-17
3. O. Umurov, M.Xusenov, B. Sherzod Oliy ta'lim muassasasida axborot xavfsizligini ta'minlash "Pedagogical akmeology" international scientific-metodical journal 1(1)2022 БЖ:152-154
4. В.М.Сидоренко. Методы идентификации и оценки состояния кибербезопасности объектов критической информационной инфраструктуры авиационной отрасли, диссертация ... кандидата тех наук, 2018
5. С.А.Гнатюк. Методология поддержки процессов формирования и обеспечения государственной системы кибербезопастности в отрасли гражданской авиации, диссертация ... кандидата тех наук, 2017
6. В.А.Гнатюк. Методы обработки киберинцидентов в информационно-телекоммуникационных системах, диссертация ... кандидата тех наук, 2017
7. П.Красев. Политика безопасности США в глобальном информационном пространстве, диссертация ...кандидата политических наук, Москва, 2015
8. В.Джафарли. Формирование и развитие системы криминологической безопасности в сфере информационно - коммуникационных технологий, диссертации на соискание ученой степени доктора юридических наук, Москва, 2022
9. Д.Гаськова. Методы, модели и комплекс программ анализа киберситуационной осведомленности энергетических объектов, диссертация ... кандидата тех наук, Иркутск, 2021
10. Е.Батуева. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая диссертация ...кандидата политических наук, Москва, 2014
11. С.Себекин. Генезис и развитие стратегий сдерживания киберугроз в США, КНР и России (1990-е – 2014 гг.),диссертация ...кандидата исторических наук, Иркутск 2020
12. "Кибербезопасность и защита информации" - авторы: У. Кафеян, Дж. Брэндон
13. "Principles of Cybersecurity and Security" - автор: В. Скалян
14. "Кибербезопасность: Управление рисками в цифровом мире" - автор: П. Никольс