CYBER SECURITY, ARTIFICIAL INTELLIGENCE, DATA PROTECTION

Ma'rufjonov Maqsudjon Mansurjon o'g'li
Murodullayeva Rayhona Abdurahmon qizi
Nabiyev Iskandar Farxodjon o‘g‘li
Muhammad Al- Khorazmi TATU in the name of Fergana branch students
https://doi.org/10.5281/zenodo.8414406

Abstract: This article provides information on the elements of cyber security and its methods of protecting computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. This article explains the basics of security, including security principles, critical security controls, and cybersecurity best practices. Guidelines are provided for security software to analyze user behavior for potential malware and learn how to better detect new infections.

Keywords: Electronic, security, protocols, virus, mobile, information, cyber security, mail, technology, business, cybercrime.

In the modern world, new technologies and electronic services have become an integral part of our daily life. Given that society is becoming more and more dependent on information and communication technologies, the protection and use of these technologies is becoming a crucial and urgent issue for the national interest. In order to ensure cyber security for every organization, employees engaged in this field are being recruited, and a number of seminars and training sessions are being organized to continuously acquaint employees with cyber security knowledge. The passing of cyber security as a subject in higher education institutions is a clear example of this.

Cybersecurity is a relatively new concept, and it has many different definitions. Specifically, the CSEC2017 Joint Task Force source defines cybersecurity as follows: Cybersecurity is a computationally-based field of knowledge that includes technology, human, information and embodies processes. It includes the creation, implementation, analysis and testing of secure computer systems. Cybersecurity is an interdisciplinary field of study that includes legal aspects, policy, human factors, ethics, and risk management. The Cisco organization, which operates in the field of networks, defined cyber security as follows: Cyber security is the practice of protecting systems, networks and applications from digital attacks. These cyber-attacks usually involve the manipulation, alteration or destruction of confidential information; collect money from users; aims to disrupt normal functioning. Effective cyber security measures are now becoming

more and more difficult in practice due to the fact that there are more devices and their types than people, and the potential for attackers is increasing.

The need for cyber security knowledge has been around since the first mainframe computers were invented. Multi-level security measures have been implemented to protect these devices and their functions. The growing need to ensure national security has led to the emergence of complex and technologically sophisticated reliable security measures.

Today, every aspect of life is being digitized, from birth to death, movement, currency value movements, online trading, as well as distance education, distance management etc. The way of life based on these tools gives us incomparable conveniences, but today it is easier than ever before to devalue the person, to spread personal information around the world, to become a victim of fraud. The root cause of this is that we live on the basis of digital control. The growth and decline of population demographics and crime rate is the digital world. In the introduction to M. Ethan Katsch's 1995 book, Law in a Digital World, William Gates quotes: "In the future, everything will be digital" (Katsch, 1995). 27 years have passed since then, and we are seeing confirmation of this idea. As mentioned above, every industry and every aspect of life is digitizing. According to the data provided by www.datareportal.com, a total of 5 billion people worldwide use the Internet today - that is 63% of the world's population. Similar information is provided by www.statista.com. According to Joseph Johnson's analysis, "in April 2022, 4.65 billion of the world's population will be social network users." Internet users also continue to grow, with the latest data showing that the world's internet-connected population grew by almost 12 million in the 200 months to April 2022. This means that the population is getting connected with the global Internet every day. Such statistical data can be an impetus for development due to their positive nature. However, it should not be forgotten that the relevance of the issue is not precisely in the above positive aspects.

The harmful effects of cyber-attacks, cybercrime, and hacking have fundamentally changed the views on privacy and personal data privacy in the digital world. The process, which is now called "new industrial revolution" by us, has a positive significance on the one hand, as it presents a new society and a new environment, but on the other hand, it also creates a real danger. Despite its unprecedented development, the Internet has brought us new forms of fear, new forms of danger. According to Majir Yar and Kevin F. Steinmetz, “Cyberspace, the realm of computerized interactions and exchanges, presents many new

opportunities for criminals and deviant activities (Yar, Majid, and Kevin F. Steinmetz, 2019). Also, in most sources, the concept of "cybercrime" is called by names such as "cyberattacks", "crimes committed on a computer" or "computer crimes", which was put forward by Goodman and Benner at the beginning of the 21st century (Goodman, Brenner, 2002). However, it should be noted that these concepts do not mean the same thing. For example, the term "cybercrime" differs in that it represents a narrower concept than computer-related crimes. The reason is that it covers only the computer network and the criminal acts committed with it. Computer-related crimes even include crimes that have nothing to do with the network, but only affect personal computer systems (Gercke, 2012). Cybercrime is an emerging form of transnational crime. At the 10th United Nations Congress on the Prevention of Crime and Prevention of Offenders, two basic definitions for crimes committed through digital technologies were developed as part of a relevant workshop. In a narrow sense, cybercrime (computer crime) is understood as a violation of the security of computer systems and the processing and use of information by computers for malicious purposes. Cybercrime, in the broadest sense, (computer-related crimes) is any illegal act committed through a computer system or network, or specifically against a computer and digital systems, including illegal activities through a computer system or network. covers crimes such as possession and providing or distributing information.

Information security is the state of information, according to which it is not allowed to accidentally or intentionally affect the information without permission or use it without permission. Or, the status of the level of information protection, which ensures the preservation of its characteristics (properties), such as secrecy (confidentiality), integrity and usability, when processing information using technical means.

Information security is the state of information, according to which it is accidental to informationor deliberate unauthorized exposure or unauthorized use is not permitted. Or, its confidentiality in the processing of information using technical meanscharacteristics such as (confidentiality), integrity and usabilityThe state of the level of protection of information that ensures the preservation of (its properties).

Cyber security is divided into 8 areas of knowledge:

1. Data security;
2. Software security;

3. Security of organizers;
4. Communication security;
5. System security;
6. Human safety;
7. Security of the organization;
8. Social security.

In fact, Uzbekistan is one of the developing countries. Therefore, the economy of our country and many other areas are being digitized. From the banking sector to the medical sector, from the military sector to agriculture, the digitization process is underway. This certainly raises security issues for the national information system. In particular, information on politics and the military should never be disclosed. However, due to insufficient attention to cyber security in our country, cyber attacks and illegal activities are being carried out against the official Internet network of Uzbekistan.

Legislation of cyber security standards is essential. The digital world has not yet been able to define its legal status. The fact that new types and forms of threats are emerging day by day requires their reflection in 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. Therefore, in 2020, 297 researches and examinations were conducted during the implementation of measures to increase the security of modern information systems and resources of the national "UZ" domain. As a result of the work carried out, 695 vulnerabilities were identified and the owners of information systems and resources were immediately informed about the vulnerabilities was seen.

In our opinion, the only solution to these problems is the training of personnel based on advanced foreign experience in this direction, well-versed in national and international foreign experience, who think at a high level about improving the field of cyber security, not from the top, but from the bottom up, up to school. implementation of a consistent pedagogical-methodical approach of education-school-lyceum-college-higher educational institution-post-higher education period, textbooks and training suitable for the mental capabilities of students of each educational period one of our urgent tasks today is to launch a single mechanism that will increase the knowledge and potential of cyber security by preparing manuals, gradually training them in digital skills.

In general, in today's fast-moving digital world, first of all, the safety of a person, as well as data, depends on the scope and level of impact of the measures being implemented. As mentioned and analyzed above, cybercrime is becoming one of the most dangerous enemies of society and the state. In the fight against it, it is required to introduce the most effective systems, put them into practice, and strengthen integration. Another important aspect is the formation of cyber security, digital rights and digital hygiene, making them an integral part of everyday life.

Referens:

1. Umaraliyev, J., Abdurakhimov, O .AN ARTICLE ON THE PROGRESS OF MODERN TECHNOLOGIES IN SOCIETY. SCIENCE, EDUCATION, CULTURE AND INNOVATION, 2(6), 15-17.
2. Stop it son, UJ., Azimjon son, AO. , & Ilhomjon daughter, IS. (2023). THE TRANSFORMATIVE ROLE AND IMPORTANCE OF TELECOMMUNICATION TECHNOLOGIES IN OUR DAILY LIVES. ONLINE - CONFERENCES; PLATFORM, 138–139. Retrieved from
3. http://papers.onlineconferences.com/index.php/titfl/article/view/1260
4. Umaraliyev, J., Abdurakhimov, O., & Isokjonova, S. (2023, June). USE AND EFFECTIVENESS OF INFORMATION TECHNOLOGIES IN MEDICINE. In Academic International Conference on Multi-Disciplinary Studies and Education (Vol. 1, No. 11, pp. 148-151).
5. Umaraliyev, J., Turdaliyev, K., Isoqjonova, S., & Abdurakhimov, O. (2023). ITS APPLICATIONS AND PROSPECTS IN EDUCATION. Interpretation and Researches, 1(11). search the horse
6. Muxtarov, F., & Tojidinov, A. (2023). Tarmoq xavfsizligini url filtirlash bilan yaxshilash. Research and implementation, 1(4), 39-44.
7. Muxtarov, F., & Sadirova, X. (2023). Korxonada axborot xavfsizligini ta'minlashning zamonaviy usullari. Engineering problems and innovations.
8. Muxtarov, F., Turdimatov, M., & Mominova, M. (2023). Umumiy o'rta ta'limga kiberxavfsizlik fanini tizimli isloh qilishning ustuvor yo 'nalishlari. Engineering problems and innovations.
9. Muxtarov, F., Umarov, A., & Ro'zaliyev, A. (2023). Axborot tizimlarida xavfsizlik tahdidlarining tasnifi. Engineering problems and innovations.
10. Рахимджон, Х. (2022). 6 Новых языков программирования, которые стоит изучить. Academicia Globe: Межнаучные исследования, 3 (04), 126–135 стр.