INTERNATIONAL MULTIDISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
SJIF 2019: 5.222 2020: 5.552 2021: 5.637 2022:5.479 2023:6.563 2024: 7,805
eISSN :2394-6334 https://www.ijmrd.in/index.php/imjrd Volume 12, issue 05 (2025)

THE IMPORTANCE OF CYBERSECURITY IN A DIGITALIZING WORLD

Togaev Jahongir Komil uglu

Termez State University Academic Lyceum

Lecturer in Computer Science.

Oroqov Orif Ashirali ugli

Termez State University Academic Lyceum

Lecturer in Computer Science.

Annotation. This article analyzes the problems of cybersecurity and their solutions associated with the accelerated development of digitalization. At a time when information technology penetrated almost all areas of our lives, ensuring data security has become one of the most important tasks. The article covers the current role of cybersecurity, types of threats, effectiveness of protection measures, and measures taken by governments and organizations. The importance of education and awareness in protecting digital infrastructure will also be considered.

Key words: digitalization, cybersecurity, information security, cyberattack, threat, protection system, digital infrastructure, security strategy.

Today, the process of digitalization takes place at an accelerated pace in almost all spheres of mankind's life. Public administration, healthcare, education, finance, commerce, and many other industries are leveraging digital technology. While these changes increase convenience and efficiency, they also present new risks. Especially information security and cybersecurity have become one of the most pressing issues today.

Safety is the state of being free of danger or threat and being safe. So, if we combine the two words, "cybersecurity" refers to keeping computers, networks, and any device connected to the internet safe from any threat or threat.

Why is cybersecurity important? Cybersecurity is intertwined in our time, especially with all the technological advancements that are taking place. Imagine a country that has no army to protect its resources from other countries that want them. There's no doubt that the country is going to be weak, right? Would you want to live in such a country? Do I need to know how to code to enter the cybersecurity field? You don't need to have a perfect knowledge of the science of programming when you're just stepping into the field of cybersecurity. But then, if you start diligently engaging in the industry, you will definitely need to learn and know how to program. Because there are such complex cyber crimes that you need to be a professional programmer to prevent or counter them.

The development of modern methods of processing, transmitting and collecting information leads to an increase in the threats associated with loss, corruption and disclosure of user information. Therefore, one of the leading directions of development of information technology is the provision of information security of computer systems and networks.

Cybersecurity is a set of measures that ensure that digital systems, networks and information are protected from unauthorized access, alteration or corruption. This understanding includes not only technical tools, but also legal, social, and organizational management strategies. Digital

information is one of the most valuable resources right now, and protecting it is a strategically important task for any government or organization.

Cybersecurity is intertwined in our time, especially with all the technological advancements that are taking place. Imagine a country that has no army to protect its resources from other countries that want them. There's no doubt that the country is going to be weak, right? Would you want to live in such a country?

It's the same with technology and the internet, which you're now using almost every day for study and work; Without cybersecurity, your personal data, location, photos, camera, and much more would remain unprotected and as a result, it turns your sensitive information about your personal life into ready prey for criminals. If criminals have access to this kind of information, they can use your credit cards, steal your money, and even steal identity.

In the modern era, cyberattacks are increasing in scope and sophistication. The most common types of threats are:

- Phishing (data theft via fake pages)
- DDoS attacks (system crash)
- Malware (viruses, trojans, ransomware, etc.)
- Information leakage by internal employees

Social engineering (getting information by influencing the psychology of people)[1; 345,358-b]

These threats often result in identity theft, financial damage, or damage to the organization's reputation.

Ensuring cybersecurity requires an integrated approach. This includes the following measures:

- Use of antivirus and firewalls
- Implement a strong password policy
- Regular system updates
- Providing information security training to employees
- Keeping backups and being prepared for emergencies

Many countries are developing specific laws, regulations, and strategies to strengthen information security. At the international level, too, various coalitions and collaborations are forming. For example, the EU's GDPR rules, the UN's digital security initiatives.[2; 485,492-b]

Cybercrime is a term that refers to any illegal activity that uses a computer as its primary means of committing or stealing. The U.S. Department of Justice is expanding the concept of cybercrime to include any illegal activity that computers use to store evidence. The growing list of cybercrimes includes crimes committed by computers, including network access and the spread of computer viruses, as well as computer variants of existing crimes such as identity theft, stalking, intimidation and terrorism, which have become a serious problem for them. people and peoples. Generally speaking, in ordinary human terms, cybercrime is defined as a crime committed using a computer and the Internet with the aim of stealing an individual's identity, selling smugglers, or harassing victims or disrupting operations through malware.

Data privacy and security will always remain the highest level of security measures that any organization pays attention to. We now live in a world where all information is stored in digital or

cyber form. Social networking sites provide a space for users to safely communicate with their friends and family members.

For home users, cybercriminals continue to target social networking sites to steal personal information. Not only in social networks, but also during banking transactions, a person should take all the necessary security measures.

In our daily lives, we often share our personal information on online platforms, social networks, and other websites. This information may include our name, birth date, address, phone number, e-mail address, or even our credit card information. If this information falls into the wrong hands.

We also need to protect our personal and financial information when we make online purchases, use internet banking services, or fill out tax returns. To maintain the security of these information we need to use trusted websites, choose strong passwords and update them regularly, and avoid visiting suspicious links.
Businesses and organizations should also take cybersecurity seriously.

Vulnerabilities or security flaws in information systems can result in significant financial losses, reputational damage and customer trust. To protect their systems, companies need to install firewalls, anti-virus programs, train employees in cybersecurity, and regularly check their systems.

Government agencies also play an important role in ensuring cybersecurity. They protect the online safety of citizens by developing laws on cybersecurity, combating cybercrime, and educating the public about cybersecurity. A number of measures are being taken in this area in Uzbekistan. In particular, in 2022, the Law "On Cybersecurity" was adopted. This Law regulates the relationship in the field of information technology, defines the rights and obligations of state bodies, legal entities and individuals.

According to the law, state bodies and other organizations are obliged to ensure the security of their information systems, take measures to detect and counter cyber threats. They should also train their employees in the field of cybersecurity and establish international cooperation in this regard.

In conclusion, the Digital Revolution opens the doors of great opportunities for society, but it also brings risks with it. Therefore, ensuring cybersecurity in the digital world is a common task not only of IT specialists, but of each user, organization and state. By ensuring information security, digital advancement can be sustained and reliable.

Individuals are also responsible for protecting their personal information. They are advised to give away their personal information to others carefully, use strong passwords, and update them regularly. They should also install and regularly update anti-virus software on their computers and mobile devices.

Establishes criminal and administrative penalties for cybersecurity offenses. Cybercrimes include unauthorized access to computer systems, data theft or destruction, distribution of computer viruses, fraud, and more.

Cybersecurity is a very pressing issue in today's Information Age. Each of us must have a responsible responsibility for the protection of our personal information and financial resources, and government agencies and organisations are also required to take necessary steps in this regard. Only with concerted efforts can we effectively combat cyber threats and create a safer online environment.

Fostering a culture of cybersecurity and increasing the online safety literacy of the population is also one of the important tasks. To do this, it is advisable to conduct classes and trainings in cybersecurity in educational institutions, give related media reports and articles on the topic, and use social advertisements. In this way, we can instill cybersecurity skills in our youth and protect them from online threats.

It's important to remember that in an era of rapidly evolving technology, the focus on cybersecurity shouldn't be underestimated. As new threats and dangers arise, we must constantly be alert and develop new ways to combat them. After all, cybersecurity is a common issue and responsibility of all of us.

REFERENCES

1. Abdullaeva, N. A. Axborot xavfsizligi va uning dolzarb masalalari. Toshkent: “Iqtisodiyot” nashriyoti. 2022. 345-358

2. Karimov, Sh. M. Kiberxavfsizlik asoslari. Toshkent axborot texnologiyalari universiteti, o‘quv qo‘llanma. 2021. 485-492

3. Soliyev, B. R. “Raqamli transformatsiya jarayonida axborot xavfsizligini ta’minlashning huquqiy asoslari”, Yuridik fanlar jurnali, 1(4), 202345–52.

4. The European Union Agency for Cybersecurity (ENISA). Cybersecurity Threat Landscape. 2023

5. United Nations Office of Counter-Terrorism (UNOCT). Cybersecurity and international cooperation. 2022.

6. Stallings, W. Network Security Essentials: Applications and Standards. 6th ed. Pearson Education. 2020.