OPEN ACCESS
INTERNATIONAL JOURNAL
EIJMRMS
Next Scientists
European International Journal of Multidisciplinary Research and Management Studies
SJIF 5.954 2022

EUROPEAN INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND MANAGEMENT STUDIES
ISSN: 2750-8587
DOI: https://doi.org/10.55640/eijmrms-02-04-14

https://eipublication.com/index.php/eijmrms
Volume: 02 Issue: 04 April 2022
Published Date:- 20-04-2022

Page No.-65-72

PEDAGOGICAL FOUNDATIONS OF CYBER SECURITY

Shoira B. Bekchonova

Associate Professor, Department Of "Mathematics And Information Technologies In Education" Tashkent State Pedagogical University, Uzbekistan

ABSTRACT: - This article discusses the current topic of cybersecurity in the modern process of globalization, the need to study and teach the correct use of digital technologies used in pedagogy, in what areas it is used, the dangers posed by viruses, and measures to eliminate them. outlined.

KEYWORDS: Cyber security, digital technologies, learning efficiency, viruses, software.

INTRODUCTION

New technologies, e-services have become an integral part of our daily lives. As society becomes more and more dependent on information and communication technologies, the protection and use of these technologies is crucial for the national interest. Therefore, in order to ensure cyber security, each organization is involved in the field of cyber security, and a series of training seminars are organized to familiarize employees with the knowledge of cyber security. A clear example of this is the introduction of cybersecurity as a science in higher education.

THE MAIN RESULTS AND FINDINGS

Along with the development of information technology in the country, special attention is paid to the elimination of information security in economic and public administration, in particular, computer-related security issues. The Action Strategy for the further development of the Republic of Uzbekistan for 2017-2021 sets tasks, including "... improving the system of information security and information protection, timely and appropriate response to threats in the field of information »And special attention is paid to the detection of cybercrime. In addition, the Decree of the President of Uzbekistan "On the State Program for the Year of Science, Enlightenment and Digital Economy" sets the

tasks of "developing a national strategy and bill on cyber security until September 1, 2020." The development of cybersecurity training manuals is also an important consideration in carrying out these tasks.

Cybersecurity is one of the most relevant concepts in the age of digital technology, and there are various definitions of it. In particular, the CSEC2017 Joint Task Force source defines cybersecurity as follows: integrates processes. It involves the creation, implementation, analysis, and testing of secure computer systems. Cybersecurity is an integrated field of knowledge in education that includes legal aspects, policies, the human factor, ethics and risk management.

Cisco, a network organization, defines cybersecurity as follows: Cybersecurity is the practice of protecting systems, networks, and applications from digital attacks. These cyberattacks typically control, exchange, or destroy confidential information; collecting money from users; aims to disrupt normal performance. Implementing effective cybersecurity measures is now becoming more difficult in practice due to the large number of devices and their types and the potential for intruders.

The need for cybersecurity knowledge began to emerge with the advent of the first mainframe computers. Multi-level security measures have been taken to protect these devices and their functions. The growing need for national security is leading to the emergence of complex and technologically complex reliable security measures.

Nowadays, every professional working in the field of digital technologies is required to have a basic knowledge of cybersecurity. The structure of the field of cybersecurity can be described as follows (Figure 1).

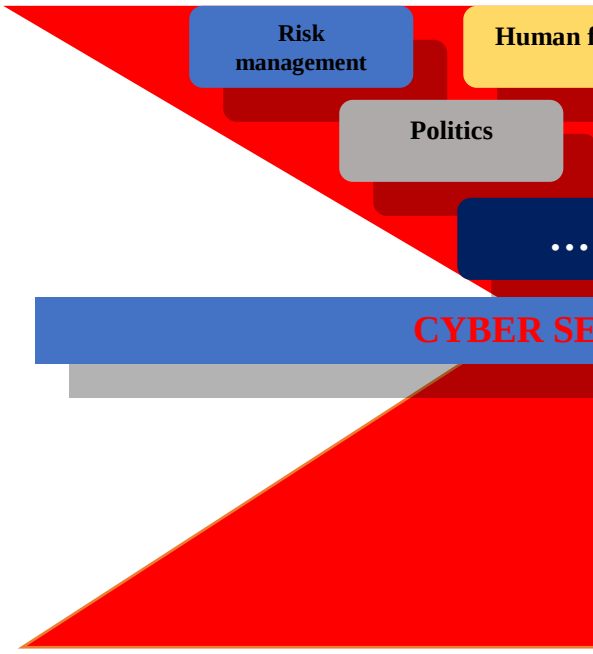

Figure 1- The structure of the field of cybersecurity.

There are different approaches to defining the fundamental terms of cybersecurity. In

particular, the CSEC2017 JTF source lists the following 6 terms of cybersecurity:

Confidentiality is the state of the information or its delivery that prevents unauthorized access or copying. Confidentiality is the protection of information from unauthorized "reading".

Integrity is the property of information to be present in an undamaged form (unchanged in relation to any recorded state). Integrity is concerned with protecting information from unauthorized "writing" (i.e., altering information) or at least determining whether it has been altered.

Utility is the ability to have information ready and usable for an authorized logical object request. Utilization is the process of protecting information (or systems) from unauthorized "failure". In the AOB scenario, Bob's inability to use the AOB website is a usability issue for Alice's bank and Bob. Because in this case, Alice will not be able to earn money from remittances, and Bob will not be able to run his own business. The most common of these attacks is Denial of Service (DOS).

Risk is the potential benefit or harm that generally arises when the probability of an event being added to any situation. ISO defines risk as the effect of uncertainty on goals.

For example, consider the process of applying to a university. In general, this process is not considered a risk. Only when the applicant submits the documents and entrance exams can he or she be admitted or not. This, in turn, increases the risk of admission or rejection. Risks in cybersecurity or information security are viewed negatively. Assault thinking is the process by which a legitimate user thinks like an attacker in order to avoid potential danger.

Systematic thinking is social to ensure guaranteed action and a thought process that takes into account the interaction of technical constraints. In addition, the following concepts are important in the study of cybersecurity.

Information security is the state of information under which information may not be accidentally or intentionally compromised or used without permission. Or, the level of protection of information, which ensures the preservation of its characteristics, such as confidentiality, integrity and usability in the processing of information by technical means. [1]

Information security is a set of measures aimed at ensuring information security. In practice, the protection of information means promoting the integrity, usability and, if necessary, the confidentiality of information and resources in the entry, storage, processing and transmission of information.

Active - Protected information or resources. Or, all things valuable to the organization.

A threat is an unwanted event that could damage a system or organization. Or, a threat is a set of conditions and factors that create a potential or real threat to information security. The threat will be directed at the organization's assets. For example, if an asset contains a document held by an entity, then the room in which the document is stored may be threatened.

A vulnerability is a defect in an organization's asset or management system that allows it to carry one or more threats.

Management tools are actions that change risk and result in changes in vulnerabilities or threats. In addition, the control tool itself may have vulnerabilities that can be exploited by various threats. For example, fire extinguishers can be used as a means of

controlling the information in the form of paper stored in the organization.

The difference between information security and cybersecurity. The terms "cybersecurity" and "information security" are often used interchangeably. Some see cybersecurity as synonymous with the concepts of information security, information technology security, and (information) risk management, while others see it as a technical concept related to national security, especially in government, including computer crime and the protection of critical infrastructure. While there are instances of different industries adapting to their own goals, there are some important differences between the concepts of information security and cybersecurity.

The field of information security deals with the protection of intellectual property rights, regardless of the expression of information (on paper, in electronic and human thinking, verbal and visual). Cybersecurity is the protection of information in electronic form (in all cases, from the network to the device, stored, transmitted and processed in interactive systems). In addition, government-funded attacks and advanced persistent threats (APT) are also related to cybersecurity. In short, understanding cybersecurity as an area of information security can help you understand it. [2]

Areas of knowledge of cybersecurity. According to the CSEC2017 JTF source, cybersecurity is divided into 8 areas of knowledge, each of which is subdivided into subsectors (Figure 2).

Figure 2. Areas of knowledge of cybersecurity.

The goal of Data Security is to provide protection for the storage, processing, and transmission of data. Mathematical and analytical algorithms are used in this field of knowledge to fully implement the defense.

The Software Security knowledge area focuses on the process of developing and using the system or information security software used.

Organizational Security focuses on the design, procurement, testing, analysis, and maintenance of integrated systems in large systems. System security is sometimes different from the security of the founders. Organizer security depends on how the system is designed, built, purchased, connected to other components, and how it works and is maintained. [3]

The field of Communication security focuses on the protection of communication between the founders, combining physical and logical connections.

The System Security knowledge area focuses on aspects of system security, including components, connections, and software. Understanding the security of a system requires not only understanding its components and their connections, but also considering their integrity. That is, you need to review the entire system. This area of knowledge, along with the areas of "Organizer Security" and "Communication Security", addresses the security of organizer connections and their use in higher systems.

In addition to studying Human behavior related to cybersecurity, the field of human activity security focuses on the protection of information and privacy in organizations (e.g., employees) and in private life.

Organizational Security focuses on risk management to protect an organization from cybersecurity threats and to support the organization's success.

The field of Social security education focuses on cybersecurity factors that affect society to one degree or another. Cybercrime, laws, ethics, politics, privacy and their relationship to each other are key concepts in this field of knowledge.

So, it can be said that the field of cybersecurity is a necessary field for IT professionals.

The most important human factors include:

Lack of knowledge in the field of cybersecurity leads to large-scale vulnerabilities. Because the field of cybersecurity is concerned with traditional security, the speed of technological adaptation increases the number of vulnerabilities that can occur in many cases. On the other hand, it is not always enough for a person to acquire the latest technological knowledge in the field.

Inadequate risk mitigation and reporting can lead to recurring and unexpected cybersecurity breaches. Although people usually know that there is a serious risk to their organization, they do not disclose it. The main reason for this is that the risk does not directly affect the person, his financial situation, or when it is disclosed, the person's reputation is damaged.

Problems in culture and relationships can be caused by the organization itself or by a dissatisfied and neglected employee who knows the organization’s internal information. Most cybersecurity problems are internal and result from various disagreements between employees and the poor environment within the organization. These reasons, in turn, lead to serious problems in most cases because the employee is well acquainted with the internal structure of the organization.

Low spending on security training is due to a lack of information on managed safety risks. Typically, employees in industry do not learn cybersecurity rules independently. That's why cybersecurity rules need to be communicated to employees in the form of special training. This requires the organization to spend enough on security training.

Incomplete security due to non-uniformity of the registration point. In practice, it is important to ensure that security is monitored at one point. Single-point security control is more reliable than distributed. However, due to the complexity of security controls in organizations, controls are usually managed on a distributed basis.

Data is obtained from the user using traditional espionage techniques when bypassing security checks based on social engineering. Even an organization with the best cybersecurity system can be threatened by a social engineering threat. This is especially true when users neglect their personal information on various social networks.

This can also be seen in software. For example, while most programs are licensed, crack versions of them are widely used in various ways. For example, unlicensed Windows 10 OS, antivirus software, office software, etc. [4]

Technical means of copyright protection. Copyright protection is used in a variety of ways. They can range from protecting data on CDs / DVDs to unauthorized copying, and limiting the ability to edit simple PDF files. However, most people think that I can buy a licensed CD and copy it.

Security. The safe use of information on the Internet has been the subject of ethical debate. This is primarily a matter of protecting the public good or protecting the rights of the individual. The number of cybercrimes is growing due to the increase in the number of Internet users and the increase in personal data.

Reliability. Due to the availability of the Internet and the nature of some individuals or communities, data reliability is becoming a challenge. In other words, who is responsible for the reliability of the information on the Internet? There is also a lot of controversy about who fills in the information on the Internet and who is responsible for its errors and omissions.

Usage, censorship and filtering. The topics of usability, censorship, and information filtering cover many ethical issues related to cybernetics. The existence of these issues calls into question our understanding of privacy and privacy and our participation in society.

Freedom of information. Freedom of information, that is, freedom of speech, as well as freedom to search, receive, and transmit information, raises the question of who and what helps in a cyber-attack. The right to freedom of information is usually subject to restrictions that affect a society or its culture. Restrictions can take many forms.

Digital barriers. In addition to ethical issues related to freedom of information, there is a type of problem called the digital barrier, which represents the social gap between people with limited access to cyberspace. This gap between the countries or regions of the world is called the global digital barrier.

Prohibited content (pornography). The use of prohibited content on the Internet by minors has always been the subject of ethical debate. In some countries, the use of such content is strictly prohibited, while in others it is allowed. [5]

Gambling. This problem is also one of the debates in the ethical issue, where some people consider it harmful, while others do not like legal interference in them.

Ethics of computer use. The Institute of Computer Ethics is a non-profit organization whose mission is to promote technology from an ethical perspective.

Here are 10 rules of ethics for this organization:

- Do not use your personal computer to the detriment of others;
- Do not interfere with other users' computer work;
- Do not look at other users' computer files;

- Do not use a computer for theft;
- Do not use the computer for malicious purposes;
- Do not use or copy software that you have not purchased for your own money;
- Do not use someone's computer without permission;
- Do not harm anyone as a result of intellectual labor;
- think about the social consequences of the program you have created;
- Use your computer wisely and respectfully.

In these cases, the following security measures are required:

- identification of the caller;
- use of number identification service;
- Ignore unknown links in SMS-message.

With the development of computer technology, computer viruses are also evolving as they adapt to their new habitat. At any given time, new, previously unknown, or known computer viruses, Trojans, and worms may appear for new computer hardware. New viruses can use unknown or previously unknown distribution channels, as well as new technologies for implementation in computer systems. To eliminate the risk of virus poisoning, the system administrator of the corporate network must not only use anti-virus methods, but also constantly monitor the world of computer viruses.

Detection of malware. There are basically three approaches used to detect malware. The first and most common is signature-based identification, which is based on finding a template or signature in a malware. The second approach is based on detecting changes and identifying files that have changed. An unexpected file is considered damaged when it changes. The third approach is based on identifying anomalous, unusual, or virus-like files and situations. [6]

An important way to fight computer viruses is to prevent them in a timely manner. The following precautions should be taken to significantly reduce the risk of virus infection and to ensure reliable storage of data on disks:

use only licensed software;

provide the computer with modern antivirus software and update it regularly;

perform an antivirus scan of each storage device before reading data recorded from another computer;

scan after extracting archived files;

Double-checking of computer disks with antivirus programs;

use antivirus software to control all executable files received from computer networks.

CONCLUSION

Based on the above, it is possible to teach the subject of cybersecurity, to contribute to the development of pedagogy on the basis of teaching, to teach the proper use of digital technology, and, of course, to increase the effectiveness of education. Because a teacher who uses digital technology correctly teaches it to his students, and parents teach it to their children. This ensures information security and prevents any student from knowingly posting incorrect pictures or information on the Internet. This will save the Internet from unnecessary information. Of course, young people who travel the Internet can achieve our goals only if they use the necessary information there.

REFERENCES

1. Kostopoulos G. Cyberspace and cybersecurity. – CRC Press, 2017, -316 p.

2. Easttom C. Computer security fundamentals. – Pearson IT Certification, 2019, -447 p.
3. Ganiev S.K., Khudoykulov Z.T., Islomov Sh.Z., Selection suitable biometrics for cryptographic key generators // TUIT BULLETIN, Tashkent, 2016, №4 (40), – P. 80-92
4. http://smartkardtechnologies.com/productdetails/acr39u-smart-card- rader
5. https://www.rutoken.ru/
6. https://www.cyber.gov.au/
7. Karimov, N., & Doniyorov, A. (2019). Conflicting views regarding the hadiths. IJITEE, ISSN, 2278-3075.
8. Odilov, B. A., & Karimov, N. R. (2020). Analysis of Targeted Research in 20-30 Years of the XX Century. PalArch's Journal of Archaeology of Egypt/Egyptology, 17(6), 8887-8893.
9. Lakka-Kolari, J. (2021). Pedagogical aspects in cyber security trainings offered by private companies.
10. Karimov, N. R. (2020). A True Successor of Great Central Asian Scholars. Journal «Bulletin Social-Economic and Humanitarian Research,(7), 62-69.
11. Katsantonis, M., Fouliras, P., & Mavridis, I. (2017, April). Conceptual analysis of cyber security education based on live competitions. In 2017 IEEE Global Engineering Education Conference (EDUCON) (pp. 771-779). IEEE.