ISSN NO: 2770-4491
Date of Publication:10-11-2022

Problems and Solutions to Cybersecurity.

Mengniyazov Quvondiq Jumanazar o'g'li
Kashkadarya region
Master of the Tashkent University of Information Technology

Annotation: This article provides general insights into cybersecurity, its problems, and its solutions.

Keywords: Cybersecurity, CSEC2017, testing, information, digital applications,system,network.

Cybersecurity is now one of the newly infiltrated concepts, with different definitions given to it. Specifically, the CSEC2017 Joint Task Force source describes cybersecurity as follows: cybersecurity is an area of computing-based knowledge that incorporates technology, human, information and processes to guarantee the proper implementation of actions in the context of corrupters. It involves creating, implementing, analyzing and testing secure computer systems. Cybersecurity is an integrated area of knowledge of education and involves legal aspects, politics, human factor, ethics and risk management. [1] Cisco, an organization operating in the network industry, describes cybersecurity as follows: Cybersecurity is the practice of protecting systems, networks, and software from offensive attacks. These cyberstalking's usually involve controlling, replacing, or destroying confidential information; withdrawal from users; to disrupt normal work performance. [2] (Matthew 24:14; 28:19, 20) Currently, effective cybersecurity measures are becoming more practically complex as a result of an increase in the size of devices and their types and the potential of disruptors. The necessity of the field of cybersecurity knowledge began to emerge since the first mainframe computers were manufactured. To assist individuals desiring to benefit the worldwide work of Jehovah's Witnesses through some form of charitable planning, a brochure has been prepared in Uzbek. Increasing the need to ensure national security will lead to the emergence of complex and technologically complex security measures. Every specialist currently working in the field of information technology is required to have fundamental knowledge of cybersecurity. There are various approaches to identifying fundamental terms of cybersecurity. Specifically, the CSEC2017 JTF source cites the following six terms of cybersecurity: Confidentiality is such a situation of information or transmitter that it is obtained from an unauthorized acquaintance or copy. [3] Confidentiality is responsible for protecting information from unauthorized "reading." Configuration is very important for Bob in the AOB scenario. That said, Bob doesn't want Tridi to know how much money he has on his balance sheet. Therefore, it is important for Bob to ensure the confidentiality of information about the balance sheet. Risk is a potential benefit or loss, and in general, a risk arises when an event is added to any situation. The ISO described it as "risk – the impact of uncertainty on the goals." For example, let's see the process of going to university. In general, this process itself is not considered a risk. Only when a student passes his or her documents and entrance exams can he or she enroll or not be able to enter. This in turn creates a risk of admission or non-acceptance. Risks in cybersecurity or information security are viewed negatively. Thinking like an attacker is a legitimate user's thought process like an attacker in order to prevent a potential risk. Systematic thinking is a thought process that takes into account the interaction of social and technical limitations to ensure guaranteed actions. In addition, the following concepts are important in the study of the field of cybersecurity. Information security is a state of information, under which information is not allowed to be accidentally or unauthorizedly affected or used without permission. Or, the state of the level of protection of information that ensures that its characteristics (characteristics) such as confidentiality (confidentiality), integrity, and usage are preserved when processing information using technical means. Information protection is a complex of measures aimed at ensuring information security. (Matthew 24:14; 28:19, 20) Jehovah's Witnesses would be pleased to discuss these answers with you.

Active - protected information or resources. Or, everything that is valuable to the organization. A threat is an unwanted event that can damage a system or organization. Or, the threat is a set of conditions and factors that pose a potential or real existing threat that disrupts information security. The threat will be aimed at the assets of the organization. For example, if as an asset there is a document belonging to the enterprise, then a threat can be made against the room where this document is stored.

ISSN NO: 2770-4491
Date of Publication:10-11-2022

The terms "cybersecurity" and "information security" are often used, with their seats exchanged. While some view cybersecurity as synonymous with the concepts of information security, information technology security, and (information) risk management, others, particularly in the realm of government, view it as a national security-related technical concept that includes computer crime and the protection of vital infrastructures. While there are cases of adaptation by employees of various industries to their own ends, there are some significant differences between the concepts of information security and cybersecurity.

Conclusion:

Information security is involved in protecting intellectual rights regardless of the expression of information (paper view, electronic and human thinking, oral and visual). Cybersecurity, on the other hand, protects electronic information (in all cases, from the network to the device, stored, transmitted, and processed in interconnected systems). In addition, government-funded attacks and advanced continuous tads (Advanced persistent threats, APT) also apply to cybersecurity. In a nutshell, understanding cybersecurity as one aspect of information security helps to understand it correctly.

Available publications:

1. S.K.Ganiev, T.A.Kuchkarov. Network Security (Mobility Security). Tutorial. –T.: "Aloqachi", 2019, 140 b.[1]
2. S.K.Ganiev, M.M.Karimov, Z.T.Xudoykulov, M.M.Kadirov. An explanatory dictionary of terms and concepts of information security in Russian, Uzbek, and English. –T.: Economics and Finance, 2017, pages 480.[2]
3. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Information security. T.: Science and Technology, 2016, page 372.[3]
4. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Information security. Security of information and communication systems. Tutorial. –T.: Contact, 2008, page 382.[4]