GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 11, Issue 10, Oct. (2023)

BASICS OF CYBERSECURITY, TECHNOLOGIES AND IMPORTANT NUANCES

Batirov Farxod Avazovich,
Head of the Educational Process-Planning Department,
Educational and Methodological Department,
University of Public Safety Republic of Uzbekistan
farxod-batirov@mail.ru

ABSTRACT

The article is widely covered from a scientific point of view. Cybersecurity plays an important role in the world of information technology. Currently, data security is one of the biggest problems. The first thing that comes to mind when we think about cybersecurity is cybercrime, which is developing rapidly day by day. To protect yourself from any threat that may come from cyberspace, it is necessary that the self-defense system is always in a phase of flexible response, while for protection it is necessary to use the opportunities created by cyberspace, the Internet and social networks, and similar information.

Keywords: cybersecurity/ cybercrime/ cyberterrorism/ cyberattack/ cyberspace/ Internet/ social networks.

INTRODUCTION

Cyberspace primarily refers to the concept of open space used in the world through computers and computer memory. According to reports, the term cyberspace was first used in William Gibson's 1984 novel “Burning Chrome”. French philosopher Pierre Lévy believes that cyberspace is a smooth, highly defined, interactive and real-time processing space. This space makes it possible to obtain, transmit, model and register information.

According to the latest report of the international electrology Union (IEU), half of the world's population uses the internet. In developed countries, the online population accounts for more than 80% of the total population. However, at the same time, the number of online users in developing countries is constantly increasing. If in 2005 this figure was 7.7 percent, now this figure is 43.5 percent. According to IEU, the African region has the highest growth. In Africa, 2% of the population used the internet in 2005, compared to 25 percent in 2018. The report stated that the lowest growth was in Europe and America. The Asia-Pacific Basin has the lowest utilization rates.

Cybersecurity is the implementation of measures to protect systems, networks and software from digital attacks[1]. Such attacks are usually carried out with the aim of accessing confidential information, modifying it, destroying it, obtaining funds from users, disrupting the normal activities of organizations or companies. Implementing effective cyber security measures is already a very difficult process. Because the number of devices on which attacks are carried out today is several times more than the number of people, and cybercriminals use new inventions every day. "The concept of "cybercrime", using the means of information and communication technology, is used to terrorize the virtual network, prepare and distribute viruses and other malicious programs, illegal information, mass distribution of electronic letters (spam), hacking attack, illegal access to websites, fraud, violation of data integrity and copyright, theft of credit card numbers and bank details (phishing and farming) and are explained by various other offenses”[5].

A successful cybersecurity approach is defined as a multi-layered defense of computers, networks, applications, or data that is important for protection. Employees, business processes and technologies must complement each other in order to effectively protect against cyber attacks. Employees of this industry should understand the basic principles of information security, choose strong passwords, pay attention to the sent and received email and attached files, ensure the safety of information to other sources. Cyberterrorism - the use of computer and telecommunication technologies (mainly the Internet) in the path of terrorist goals. Cyberterrorism also provides for the seizure of computer control networks through special hacker programs and the occurrence of terrorist attacks on the Internet using computer viruses, disabling the Internet network [8].

Each organization must take a number of basic measures against ongoing or successful attacks. A reliable action plan should be managed from a single center. These comprehensive measures should explain how to identify attacks, protect systems, identify threats, eliminate them, and restore operations after attacks.

Technology is an important element in providing organizations and individual users with the necessary tools to protect them from cyber attacks. The main components that need to be protected are computers and smart devices, routers and modems, network and cloud environments. Among the most common technologies used to protect listed components are the implementation of a new generation of network routers, DNS filtering, malware protection, downloading anti-virus software, and email protection.

In the modern world, advanced cyber protection programs protect the interests of each user. On an individual level, a cyberpudofaa attack can have negative consequences such as theft of personal information, loss of valuable information such as cash or family photos, and disclosure of state and military secrets on a large scale. The protection of all important infrastructures such as power plants, hospitals, financial services banking sector and other institutions is essential to ensure the life and activities of our society[2].

Each network user benefits from research on cybertahdids, such as Talos' 250 cyberspace cyberattacks exploring cyberattack strategies and emerging and emerging threats. They identify new weaknesses and weaknesses, inform the public about the importance of cybersecurity, and increase the reliability of systems through open source software codes. The work of these professionals is to make the internet safer for each user.

The rapid development of information and communication technologies led to the emergence of cybercrime and its increase day by day. The United Nations report states that every year more than 1.5 million people are victims of cybercrime, and the total cost of cybercrime exceeds $ 1 billion [6].

The increase in cybercrime makes it urgent to improve public administration, banking, transportation, national security and other systems and expand cybersecurity measures around the world. In the final approval of the 2012 NATO summit in Chicago, United States, the facts of the increase in the number and quality of cyberattacks were once again mentioned, and it was noted that the alliance member states are separate, as well as the importance of establishing a unified cyberpudofaa with international organizations (UN, European Union, European Council, etc.

The United States, Russia, China, England, France, Germany and a number of other developed countries have already created their own special cyberspace. Although these states claimed that their primary purpose was to protect their networks, offensive operations were also envisaged here. For many years, there has been extensive evidence that the United States and Russia have conducted large-scale electronic espionage practices against current presidents, even their closest allies, in their campaigns. Recent elections in the United States and Mexico have transformed the global information network, the internet, into a global battleground.

In one of the secret documents of the US National Security Agency, there is information that the next large-scale conflict will begin in cyberspace. The United States is the only state that has actually started a cyberwarfare. It's no secret that former US President Obama ordered a cyberattack to destroy thousands of Iranian nuclear centrifuges. As a result of a powerful technological attack carried out with computer viruses, American hackers managed to reverse the nuclear program for two years, causing significant material damage to Iran. Now no one is trying to hide this quick information, that is, the practice of “cyber forces”, as diligently as before [3].

Since 2012, the Internet in Syria has been blocked by the United States. Recall that three years ago in the US Army there were about 20 thousand employees in the structure of the cyber forces, which was established as an independent type of Army. We should point out that the main tactical and strategic directions of cyber warfare are part of the United States military doctrine. Since 2012, the Internet in Syria has been blocked by the United States. Founded three years ago in the US Army as an independent type of Army, the Cyber Force has about 20,000 personnel.

Many armies around the world are already incorporating practical combat exercises against cyberattacks into their combat training programs. Participants were even "trying to stop a moving arrow train"during the training sessions organized last year by the NATO Center for anti-cybersecurity (CCDCOYE), which was founded in 2008. A group of hackers who were trainees succeeded: they managed to stop the train, break the control system and block the engine. Hackers participating in these trainings are only included by invitation [7].

Due to the “sensitive nature” of cyberspace, the name and number of guests are kept secret. Only the general purpose of "cutting" is known: to make a map of the enemy network, to find a weak point, and from there to enter the network and control it. In one similar exercise held earlier, US and UK hackers “attacked” each other's information systems. High-level permits for training by former President Barack Obama and former prime minister David Cameron indicate that cyberspace is given great importance. This type of bilateral or multilateral training, carried out jointly by various relevant institutions, can play a special role in the training of highly qualified cyber security specialists and the real assessment of their qualifications. We hope that this proposal will be considered by the relevant institutions.

Serious attention is paid to the implementation of continuous cybersecurity measures in this area in the extensive implementation of modern information and communication technologies (ICT) in Uzbekistan, a part of the world. The official position of the Republic of Uzbekistan, which at different times took part in international events dedicated to cyber and information security issues, was to pay special attention to the development of this sphere and declare it a priority. Baku continues to actively engage with the Council of Europe, the European Union, NATO, the international power communication union and other international organizations on cyber security and information security issues. In order to form a legal framework in this area, Uzbekistan joined international conventions and programs, and also improved the domestic legislative framework.

Protection, stability of information processes in the Republic and to ensure continuity, to protect the information resources of state bodies, to prevent, analyze and prevent threats in this area, to coordinate the activities of state and non-state information infrastructure entities and their users in the field of cybersecurity and to manage risks in the field of cybersecurity, to prepare and warn the president of the Republic of Uzbekistan on May 31, 2023

"On additional measures to improve the system of ensuring cybersecurity of important information infrastructure facilities of the Republic of Uzbekistan" [4] President Decree -167 was signed.

Today, security issues that are decisive for cyber security, online security, network reliability are considered as one of the most important priorities. In order to achieve effective international cooperation, multilateral dialogue, successful adoption and implementation of these decisions, various regional and world-wide events are held annually by state, non-governmental and international organizations. This, in turn, makes it possible to continue the policy implemented by our state in this area even in the international arena, to create a common base for studying the latest news, sharing ideas and experiences. As you can see, cybersecurity is a very broad, urgent problem, and the state of Uzbekistan is taking appropriate measures, assessing the existing loopholes and threats in this area.

Cyberbullying is one of the main threats of the modern era. Threats in cyberspace are not a new phenomenon. Modern cyberspace requires the creation of a defense system from the point of view of national security. Because computers and internet technologies are widely used in the management and use of many important areas, and this can lead to the failure of those systems as a result of cyberattacks at any time. Hacker is an English word meaning hack. In the early days, a hacker was understood to be a person who was at a higher level with more programming. But over the years, the term hacker is more often understood as a criminal who uses his extensive knowledge of computers for illegal and harmful activities.

Recall that hackers first appeared in the artificial intelligence laboratories of the Massachusetts State Institute of technology in the 60s of the last century. Unauthorized access to telephone systems common in the 70s.

In the 80s, it began to manifest himself in the field of computing. In the 80s, computers used an electronic publishing system-BBS. In the 80s, hacking groups began to develop, and groups such as the Legion of Doom appeared in the US, The Chaos Computer Club in Germany. Increased unauthorized access to government and company computers forced the U.S. Congress to take specific measures. As a result, Congress passed a law making hacking a crime. However, the law did not apply to persons under a certain age.

A student named Robert Morris, who is called 23-year-old father at Cornell University worked for the National Security Bureau, had planted a self-replicating virus in the government-owned ARPANET data network (now the "father" of the internet). The Virus spread rapidly across a data network of 6,000 computers, preventing access to government and university computers. In 1988, the virus which R.Morris planted on the internet rendered many computers unusable. R. Morris was expelled from Cornell University, served a three-year probation, and was fined $ 10,000.

After a protracted investigation in 1990, U.S. Special Services launched a major "hacking operation" in 14 cities. In the operation, a huge number of people were caught cheating with a computer, a credit card and a phone. This operation dealt a major blow to the hacking teams. At the same time, the hackers buying and selling each other for amnesty led to a split between them. This operation remained in history under the name "Operation Sundevil".

In the 1990s, the U.S. CIA, NASA and computer systems or websites of important organizations such as the Pentagon have been hacked several times. David Smith, who was 30 years old in those years, made himself known all over the world with a virus named after his Las Vegas girlfriend Melissa.

This virus, which led to the complete deletion of 300 worldwide company data, caused a total of $ 400 million in losses. Captured, Smith was sentenced to five years in prison. After the release of the Windows 98 operating system, 1999 was the "year of security and hacking". A large number of security holes have appeared in the operating system, and a market for products that protect computers from hackers has appeared.

CONCLUSIONS

It should be noted that in our modern era, 500 million attacks are being organized in cyberspace every minute, 95 percent of such attacks have been found to be beneficial. The cyberspace, internet sites, pages on social networks, where the World Pulse is beating, becomes a place of conflict, an aircraft on which most issues find solutions. A number of states resort to certain means to damage rival networks by protecting their data in an effort to ensure information dominance, and this sometimes has extreme consequences. Therefore, in order to protect against any threat that may arise from cyberspace, it is necessary that the self-defense system is always in a flexible response phase, while for defense it is necessary to take advantage of the opportunities created by cyberspace, the internet and social networks.

REFERENCES

1. Kiberterrorizm - noviye ugrozi i predposilki terrorizma: problemi, puti resheniya : sbornik nauchnix statey / Ministerstvo nauki i visshego obrazovaniya RF, Altayskiy gosudarstvenniy universitet, Yuridicheskiy institut, Regionalniy antiterroristicheskiy nauchno-metodicheskiy sentr, Kafedra ugolovnogo prava i kriminologii ; redaktori: Valeriy Anatolevich Mazurov, Mariya Aleksandrovna Starodubseva. - Barnaul : Izd-vo Altayskogo gos. un-ta, 2021. - 168 s.;

2. Osnovi borbi s kiberprestupnostyu i kiberterrorizmom [Tekst] : xrestomatiya / sostavitel zaslujenniy yurist Rossiyskoy Federatsii, doktor yuridicheskix nauk V. S. Ovchinskiy. - Moskva : Norma, 2017. - 527 s.;

3. Klebanov L.R., Polubinskaya S.V. Kompyuterniye texnologii v sovershenii prestupleniy diversionnoy i terroristicheskoy napravlennosti // Vestnik Rossiyskogo uni-versiteta drujbi narodov. Seriya: Yuridicheskiye nauki. 2020. T. 24. № 3. S. 717–734.;

4.Qonunchilik ma'lumotlari milliy bazasi, 02.06.2023 y., 07/23/167/ 0321-son.

E-LEARNING RESOURCES:

5. https://iiv.uz/oz/news/kiberjinoyatchilikka-qarshi-kiberxavfsizlik;
6.https://cyberleninka.ru/article/n/kiberprestupnost-kak-tenevoybiznes.;https: //www.un.org/ru/desa/cybersecurity-demands-global-approach;
7. https://ccdcoe.org/;
8.Kiberterrorizm kak novaya raznovidnost terrorizma URL: https://papers.ssrn.com/sol3 / papers.cfm?abstract_id=3927791.