CYBER SECURITY AGAINST CYBERCRIME

Student of the Faculty of Telecommunication Technologies of Tashkent University of Information Technologies

Omonov Fayziddin Komil o'g'li

2nd year student of Oriental University, Pedagogy and Psychology

Abduraxmonova Dilnoza Alisher qizi

Annotatsiya: *Mazkur maqolada kiberjinoyatchilikka qarshi kiberxavfsizlik, kiberxavfsizlikni ta'minlash, sodir etilishi mumkin bo'lgan kiberjinoyatlarning oldini olish va unga qarshi kurashish masalalari haqida ma'lumotlar berilgan.*

Kalit So'zlar: *Kiberjinoyatchilik , global, spam, veb-sayt, Kiberterroristik, ekspert, kiberxavfsiz.*

INTRODUCTION

It has been a long time since cybercrime, which is mentioned in new forms, entered the list of global problems of our century. It is known to us to distribute virus programs, hack passwords, embezzle funds from credit cards and other bank details, as well as illegal information over the Internet, in particular, defamation, moral We can't ignore the fact that spreading misinformation is putting the lives of humanity at great risk.

The concept of "cybercrime" is the use of information and communication technology tools to terrorize the virtual network, create and distribute viruses and other malicious programs, illegal information, mass distribution of e-mails (spam), hacking, illegal access to websites, fraud, etc. is explained by the violation of data integrity and copyright, theft of credit card numbers and bank details (phishing and pharming) and various other offenses.

At this point, it should be noted that the scale of cyber terrorism and its danger to the life of society is also increasing. Cyber-terrorist act (cyber-attack) - carried out with the help of computers and information communication tools, causing direct or potential danger to human life and health, causing great damage to material objects or similar It is a political cause that is the beginning or the goal of socially dangerous consequences that can lead to. The attractiveness of using cyberspace for modern terrorists is due to the fact that carrying out a cyberattack does not require large financial costs. according to the experts' conclusion, this is done by supporting the development of developing countries, influencing the minds of citizens under the guise of establishing universal democratic principles , subjugating them to their goals in various ways.

Unfortunately, in this process, attempts to organize cyber-attacks and to "effectively" use the unparalleled capabilities of the global network of the Internet are becoming more and more frequent.

REFERENCES AND METHODOLOGY

Because the role of "interference" in the internal affairs of a sovereign state has not been fully studied by the social networks available on the Internet, their producers and sponsors, it has not yet been recognized that such "interference" is sometimes against this state.

There are no international legal grounds for prosecuting the owners of social networks for inciting the overthrow of the state system on the pages of these networks. However, every criminal act or omission should not go unanswered and unpunished.

Internet sites appear suddenly, often changing their format and then their address. That's why some experts suggest abandoning the initial concepts such as complete openness of the Internet and moving to its new system.

The main essence of the new model is to abandon the anonymity of network users. This made it possible to ensure that the network is more protected from criminal attacks.

RESULTS

As an example, we can cite the state of China, which has switched to a closed network system, and the state of Russia, which is preparing for such a process. Our country, which is integrating into the world community, is conducting a consistent state policy on the effective use of information communication technologies, information systems, and modern computer technologies.

Today, the modern digital technologies introduced in our country open the door to a number of conveniences and opportunities for our citizens.

In addition to this process, there is, of course, the problem of ensuring the security of the digital technologies and information systems being created.

This is one of the most urgent issues - ensuring cyber security, preventing and combating potential cybercrimes. By implementing the following key requirements in cyber security against the ever-evolving cybercrime, they

- protection, i.e. cyber security, we can provide:
- teaching employees the basics of information security;
- continuous testing of the vulnerabilities of the software products in use;
- using reliable antivirus software;
- use of licensed official software;
- use of multi-factor authentication in protecting information systems;
- adhere to a strong password retention policy when using passwords;
- regularly encrypt data on computer hard drives.

CONCLUSION

Investigating cybercrimes and cybercrimes and making the necessary decisions on their detection, elimination and prevention, participating in the development of regulatory legal documents on combating cybercrime, combating cyberterrorism, cyberextremism, organized crime, in the interests of state bodies and identifying cyber threats that threaten cyber security and combating them, conducting an investigation and preliminary investigation of cyber crimes before investigation, conducting rapid search activities, determining the reasons and conditions that enable the commission of cyber crimes that threaten the rights and freedoms of citizens, and they should perform important tasks such as elimination.

REFERENCES USED:

1. Akbarov D.A. Cryptographic methods of ensuring information security and their application. - Tashkent, "Mark of Uzbekistan" publishing house, 2009-432 page 2. Russian-Uzbek explanatory dictionary of information security terms. 2- mashr. Under the general editorship of XPXasanov. Tashkent, 2016 - 733 pages.

2. DYAkbarov, PFXasanov, XPXasanov, OPAkhmedova, U. Kholimtayeva. Mathematical foundations of cryptography. Study guide. T: OzMU named after M.Ulugbek, 2018-144 p.

3. Rakhimjon, H. (2022). 6 NEW PROGRAMMING LANGUAGES TO LEARN. Academicia Globe: Interscience Research, 3(04), 126-135.