INTERNATIONAL JOURNAL OF RECENTLY SCIENTIFIC RESEARCHER'S THEORY

HOW TO CONSIDER AND AVOID POTENTIAL SOCIAL MEDIA ATTACKS: CYBER SECURITY AGAINST CYBERCRIME

Iroda Egamberdiyeva
teacher, Andijan State Institute of Foreign Languages

Rakhimova Madinabonu
student, group 21-4 (304), Andijan State Institute of Foreign Languages

Annotation: *Information and information systems are developing in today's modern world. At the same time, this popularization caused the emergence of a new type of crime, namely cybercrime. This, in turn, ensures the protection of the system and its information. This article highlights the importance of cyber security in the digital economy of countries and the concepts of cybercrime that have created it.*

Keywords: *Cyber crime, cyber security, cyber attack, cyber threat, national segment, fraud.*

INTRODUCTION

In the modern world, new technologies and electronic services have become an integral part of our daily life. Given that society is becoming more and more dependent on information and communication technologies day by day, the protection and use of these technologies is becoming a crucial issue for the national interest. It has been a long time since cybercrime, which is being mentioned in new forms, has 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 cannot turn a blind eye to the fact that people's lives are greatly threatened by the spread of false information.

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, which poses a direct or potential threat to human life and health, causes or causes

significant damage to material objects is a political cause that is the origin or purpose of possible, socially dangerous consequences.

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.

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.

As an example, we can cite China, which has switched to a closed network system, and Russia, which is preparing for such a process.

In our country, which is integrating into the world community, a consistent state policy on effective use of information communication technologies, information systems and modern computer technologies is being carried out.

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.

In providing cyber security against cybercrime, which is improving day by day, we can protect against them, i.e. cyber security, by fulfilling the following basic requirements:

- 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.

At this point, it should be emphasized that certain tasks are assigned to the competent state agencies that prevent and fight against cybercrimes in our country.

In particular, they ensure the protection of the security of individuals, society and the state and their interests from external and internal cyber threats, which are carried out or enable the Republic of Uzbekistan and its people through information technologies and communications in the fight against cybercrime, legality and the rule of law in this area. strengthening, prevention, detection and elimination of cybercrimes and cybercrimes.

Also, to investigate cybercrimes and cybercrimes and make the necessary decisions on their detection, elimination and prevention, participation in the development of drafts of normative legal documents on combating cybercrime, combating cyberterrorism, cyberextremism, organized crime, state identify and fight against cyber threats that threaten the interests and cyber security of the bodies, carry out investigations and preliminary investigations before the investigation of cyber crimes, carry out rapid search activities, the reasons and conditions that enable the commission of cyber crimes that threaten the rights and freedoms of citizens they should perform important tasks such as detection and elimination.

According to the analyzes of the "Cybersecurity Center" DUK (State Unitary Enterprise), in 2020 more than 27 million malicious and suspicious network attacks were observed on the websites of the national segment of the Internet (.uz). The majority of these were related to activity in botnet systems, which accounted for 19,491,783, followed by 4,631,375 attacks on the vulnerable http protocol and relatively smaller cyberattacks in other incidents.

Conclusion. Legal enforcement of cyber security standards is imperative.The digital world has not yet been able to define its legal status. The fact that new types and forms of threats are emerging day by day requires their reflection in legislation.The development of a national strategy on cyber security regulates activities in the field of combating crime in the national cyberspace. After all, the harm and danger of madness in the virtual world is no less than in the real world. Therefore, in 2020, during the implementation of measures to increase the security of modern information systems and resources of the national ".UZ" domain area, 297 studies and examinations were conducted. As a result of the work carried out, 695 vulnerabilities were identified and information system and

resource owners were immediately informed about the vulnerabilities. The main part of identified weaknesses was taken measures in the order of medium (466), medium risk (205) and low risk (24) events.According to the 2019 summary of the global rankings for cyber security, Uzbekistan ranks 90th in the National Cyber Security Index, 52nd in the Global Cybersecurity Index, ICT Development Index) has been occupying 95th place. All of the practices listed above are aimed at ensuring national security. Because ensuring the economic, social and cultural confidentiality of the country is one of the urgent problems of today.

References

1. Ganiyev S.K. "Cybersecurity Basics". Study guide.
2. Niall Adams, Nicholas Heard. "Data Analysis for network cyber-security".
3. www.itu.int is the official website of the International Telecommunication Union
4. https://tace.uz - the official website of the Cyber Security Center state unitary enterprise
5. www.iiv.uz website