NOVATEUR PUBLICATIONS
JournalNX- A Multidisciplinary Peer Reviewed Journal
ISSN No: 2581 - 4230
VOLUME 7, ISSUE 9, Sep. -2021

THE CONCEPT OF CYBERCRIME, ITS PECULIARITIES AND CYBERSECURITY ISSUES

Nurmatov Zoirjon Pazilovich
Ministry of Internal Affairs of the Republic of Uzbekistan
Director of Andijan Academic Lyceum
E-mail:nurmatovzoirjon0505@gmail.com

Abdullaev Bahodirjon Mahammadjonovich
Ministry of Internal Affairs of the Republic of Uzbekistan
Andijan academic lyceum chair of the department
E-mail:bahodirjon1985@gmail.com

ANNOTATION:

Cybersecurity plays an important role in the world of information technology. Securing data is one of the biggest challenges today. The first thing that comes to mind when we think of cybersecurity is cybercrime, which is growing by the day. The vast potential of the virtual space is being used not only for peaceful purposes, but also for the implementation of threats of various kinds and degrees. Such threats are not limited to fraud, passwords to bank accounts, and theft of personal information. Threats to the Internet, not only for the money of users, but also for their lives, are growing. This article contains the necessary ideas for the prevention of cybercrime in our country, compliance with the rules of cybernetics, ensuring the peace and security of our citizens, protection from cyber attacks in the virtual world.

Keywords: democracy, parliament, chamber, senate, political party, citizenship, reform, civil society, cybersecurity, computer technology, information retrieval, internet, information, world community, computer viruses, violence and terrorism.

INTRODUCTION:

Today, a person is able to send or receive any information via e-mail, audio or video with the click of a button, but have you ever wondered how secure information is exchanged or how securely information reaches another person? The answer to this question lies in cybersecurity. Today, the internet is the fastest growing infrastructure of daily life. As a result of the development of science, the latest technologies in the world of technology are changing the way people live. But because of new technologies, we are unable to keep our information secure even in the most efficient way, and so cybercrime is on the rise. Currently, more than 60% of financial transactions are done online, so the industry requires the best quality security for a large number of transactions. As a result, cybercrime in these areas poses urgent problems for the world community [1].

Cybercrime is the theft, embezzlement or misappropriation of funds by computer technology or modern devices that replace it, the destruction of a computer or its software, as well as the dissemination of terrorist, national and religious destructive ideas by these means. are illegal actions aimed at the peace and security of mankind in the international arena, for its well-being. The U.S. Department of Justice defines the concept of cybercrime as follows: "Cybercrime is any illegal act that uses a computer to gather evidence." For example, network invasion, the spread of computer viruses, and computer-

based options for existing crimes: theft of personal information, violence, and terrorism have become a major problem for individuals and states today. According to many, cybercrime is the theft of personal data, smuggling, and tampering with transactions with incorrect codes using a computer and the Internet [2]. In general, we try to explain the concept of "cybercrime" as follows: the use of information and communication technologies, cyberbullying, viruses and other malware, the preparation and dissemination of illegal information, the mass distribution of e-mails (spam), hacking attacks, illegal access to websites, fraud, data integrity and copyright infringement, theft of credit card numbers and bank details (phishing and farming) and various other offenses.

Nowadays, every small, medium and large company is gradually moving to cloud services. In other words, the world is slowly moving towards the cloud lag. As traffic revolves around previous inspections, the new trend poses major challenges to cybersecurity. In addition, as the number of applications for the cloud grows, web services and web applications also need to develop in order not to lose valuable data. Despite the fact that cloud services themselves are developing new models, there are many problems with their security. Cloud can create many opportunities, but it must be said that as the cloud develops, its security issues will also increase [3]. TDT is a completely new way of cybercrime. Over the years, network security programs, i.e. web filtering or IPS, have played an important role in preventing such organized crime. The number of attackers is growing rapidly and new security techniques need to be integrated with other security services in order to prevent network security attacks. Now we can easily connect with someone on the other side of the world. But for such cases, mobile network security is a big problem. There are big security issues right now. This is because desktop computers, mobile phones, and personal computers require additional information in addition to the software they already have. We need to constantly think about the security of mobile networks. Due to the vulnerability of mobile networks to cybercrime, serious measures should be taken in case of security problems. It is therefore necessary to switch to IPv6 to reduce the risks of cybercrime as soon as possible.

Coding is the process of locking information with characters that hackers or others cannot decipher. In the encoding scheme, the message or data is encoded using an encoding algorithm and brought to the unopened file state. Encoding is usually encoded by characters that indicate how to encode. Coding primarily protects data security and their integrity. But excessive use of encoding poses a number of problems in cybersecurity[4]. Encoding is also used to protect data in transit. Username and keyword are the main way to protect our information. This is one of the main tools of cybersecurity. The information we receive must always be verified before it is received from a trusted source or downloaded to be reliable. This is often done through antivirus software. Quality antivirus software is an effective tool to protect devices from viruses.

This is a program that protects all files on the system from viruses or incorrect code. Viruses and other malware are usually grouped together. Security protects the computer from hackers or malware from entering the computer. All incoming or outgoing messages are considered a security tool that reviews each message and blocks those that do not meet the given criteria. Currently, cyber attacks by viruses are becoming very dangerous. Most of the viruses that are spread are aimed at stealing financial information from there by weakening the global information network that

provides banking services. According to the analysis of 2016, the most used centers in the banking and financial sector, online payment systems, shopping malls, hotels and shopping terminals are the main focus of hackers. For example, the Carbanak cybercrime group and its hackers, SWIFT, extort $ 1 million a year from banks and a number of financial institutions. It steals more than US $. The number of hacking crimes and similar information attacks is on the rise today due to the fact that the commission of this type of crime is costly and difficult to detect.

Financial phishing attacks. In 2016, phishing attacks aimed at financial theft increased in number and professionalism. In particular, the organization of information attacks through the "invisible hook" of hackers increased by 13.4%, accounting for 47.48% of total financial cyber attacks. In particular, there are cases of stealing users' information by offering them banking services, stealing necessary information through the creation of fake banking systems, attacking banking systems via e-mail, organizing various interesting campaigns and quizzes on the Internet. Viruses for the banking system. In 2016, the number of "Trojan" viruses aimed at disabling banking systems increased by 30.55% to 1,088,900. Among them, in particular, "Zbot" is the most common, the family of malicious files "Gozi", "Nymaim", "Shiotob". 17.17 percent of the people affected by such a virus were corporate users of the systems. The spread of such malicious files has been observed mainly in Russia, Germany, Japan, Vietnam and the United States. Today, the number of small firms suffering financial losses due to such viruses is also increasing [5].

Banking viruses for Android. The number of attacks on Android users increased by 430% in 2016, to 305,000 worldwide. In particular, it is known that these viruses are widespread in Russia, Australia and Ukraine. In particular, the family of viruses "Asacub" and "Svpeng" is popular in Russia. This set of viruses is spread through the Google AdSense service, where a certain site owner can get money from them in exchange for allowing them to place ads on the Google site. In this case, an Android user who visits a site with Google ads will infect the malicious file and become a "victim" of hackers. Therefore, experts in the field of information security advise owners of devices running the Android operating system to access reliable sources when using the Internet. In particular, the acquisition of malicious applications on mobile devices with banking and financial applications can lead to huge losses.

Strong competition is contributing to the development of hacking. In recent years, the number of hacker attacks on websites has been on the rise. In the 1960s, the word “hacker” was used to refer to people who were well versed in computers and information technology. Today, the term is used to refer to a person who commits illegal acts using information and communication technologies, hacking into information systems and programs, violating the protection of applications and websites, and organizing cybercrime by spreading viruses. In other words, a "hacker" is a person who enters a computer system without permission to cause harm. " Today, there are different approaches to the word "hacker" by experts, many of whom prefer to study hackers in two ways. That is, they associate hackers with a negative and a positive type of activity. Simply put, the first type of hackers (whitehat) are involved in disabling computer systems, spreading various viruses, stealing funds from accounts, and attacking systems related to the internal secrets and exchange of information between states. The second type, the positive category of hacking (blackhat), is the creators of protection programs that provide a "defense" to protect

against existing attacks, creating a robust cyber security system against the activities described above [6].

We found it appropriate to conditionally study hackers into three types of activities, rather than two, to make it easier for the reader to learn.

1. Hackers engaged in negative (disruptive) activities (whitehat);
2. Hackers engaged in positive (protective) activities (blackhat);
3. Hackers who create dangerous viruses and programs for profit, and then create a protection system to fight the viruses and programs they produce.

Today, the hackers with the highest level of danger to society are the first group of hackers. The cyber-attacks carried out by them resulted in a high level of damage to the software system, a process that left the software system vulnerable for some time [7].

A study by U.S. software maker Arbor Networks found that manufacturing, increased competition between companies has made them a competitor in the virtual world, and companies are hiring hackers to disrupt competitors 'online sales or systems. Through modern cybercrime, today hackers are able to sell their services to the institutions that hire them. They steal data from the systems they access and sell it to their customers. Or they destroy other company's information systems like hired assassins. Hackers are paid $ 2.50 an hour for these services. In particular, there is a growing need for the installation of malicious systems, ie DDoS-attacks, which refuse to provide services on the network of several computers. About 15 million a year. personal data, amounting to $ 50 million in damages to U.S. citizens, mostly company executives, was stolen as a result of attacks on the Internet. Analyzes show that such crimes occur mainly on weekends. Dennis Schwartz, an analyst at Arbor Networks, said it was unexpected for hackers to make $ 2-3 an hour. This is because in developed countries, criminals for hacking are severely punished. It is unfortunate that they commit crimes for a pittance [5].

The International Cyber Security Forum-2017, held on February 7, 2017 in Moscow, recorded the three most common attacks in the world of cybercrime today. Experts say that by stealing data through phishing, accessing electronic devices through secretly targeted mobile apps, and watching unprotected communication channels, many internet users today are becoming victims of Cybercrime. Today, in cybercrime, services such as disseminating information about the geographical location of a particular person or object, hacking into a personal database are popular. Hackers obtain such information by Internet and social network users in exchange for access to various electronic resources without reading the terms of their use.

That is, the services we encounter on social media, such as "How long do you live?", "What does the US president say about you?", "Which Hollywood actor do you look like?" Are actually phishing, you agree to their terms when you use them you will do. This information is sold for large sums of money in large "black information markets" that are secretly organized. "Smart stuff" is the next target of hacking. Evgeny Kaspersky noted that in recent months, major attacks on "smart home" and Internet of Things systems have been identified. It is possible to steal information about the status of "smart homes" through the IP address of any gadget connected to the Internet, to attack botnets that are a network of computers. Hackers remotely disable not only video cameras, car and aircraft computers, but also the "smart lights" that are popular today, and even more serious security systems, and gain control over them. As a result, they artificially cause major accidents, fires and other types of accidents. Research by

Kaspersky Lab has shown that digital keys and systems for remote control of almost all cars connected to the Internet can be remotely controlled [8].

The only remedy is a strong protected platform. Attacks involving hackers shutting down large power plants in Ukraine and Germany in 2016 using viruses could also hack into nuclear power plants, suggesting that they could lead to catastrophic man-made disasters. Evgeny Kaspersky put forward the idea of creating a new powerful platform, taking into account the attack of hackers. According to him, it is impossible to create a fully protected system, but it is possible to create a universal protection system for different devices that can adapt to modern attacks [9].

Kaspersky Lab employs experienced specialists in the development of protection systems against hackers. Kaspersky said that in the development of any system, first of all, its resistance to hacking attacks should be taken into account. Another interesting fact is that Evgeny Kaspersky does not use a smartphone. In his speech at the World Mobile Congress, Kaspersky picked up an old Sony Ericsson phone when the host of the event asked him to show him a mobile device. According to him, it is convenient for him to use an old phone, which will never give him a reason.

According to Kaspersky Lab, 1.6% of cyber-attacks in Uzbekistan are caused by Trojans. Uzbekistan ranks 10th among the top 10 countries in the world in terms of the number of users who have been victims of cyber-virus Trojans. According to the geography of mobile devices, mobile devices in Uzbekistan are damaged by 1,000 to 50,000 malicious applications a year. In accordance with the National Program adopted in this area, we need to further develop telecommunications technologies, communication systems and infrastructure, form information systems and "e-government" database" [5].

Means of protection of large and small business. Today, at a time when the business sector is developing, trade relations are moving to digital systems, the issue of information security is becoming increasingly important. According to a Verizon Data Breach Report analysis, 71 percent of all cyberattacks are targeted at large companies with at least 100 employees. If these attacks are successful, the “victim” institution will suffer at least $ 36,000 in damage [4].

Setting strong passwords: The need to update passwords that allow access to computer systems every 6 months has become a habit of most companies around the world. Most hackers attack with common passwords.

Employee training is essential: it is important to note that the employee is the most sensitive point of safety. Phishing attacks try to steal information through a user’s email, social media pages. The hacker sends employees the addresses of fake, identical sites, trying to identify logins and passwords. To prevent this cybercrime, the employee needs skills and knowledge.

Data control: - The situation where confidential information falls into the hands of hackers is more associated with former employees. It is also necessary to take strong protection measures against weak websites, especially online payment and sites where systems are installed.

Encryption of information: - Important information must always be stored in encrypted form. That is, it is advisable to install data encryption systems.

- According to experts, if every Internet user and service provider did not forget to be as careful in cyberspace as in real life, most cybercrimes would have been prevented. Evgeny Kaspersky, head of Kaspersky Laboratories, argues that "the biggest type of cybercrime in the coming years will be the

proliferation of highly skilled cybercrime groups and attacks on infrastructure." In his opinion,

- The first trend is cybercrime. Unfortunately, during the economic crisis, this problem is especially acute. The ranks of criminals are now filling up. In July 2020, more than 400,000 malicious software appeared worldwide every day. It is difficult to answer the question of how many hackers will be needed to spread so many malicious viruses every day. Of course, they have the ability to automate, automatically generate codes. In total, the number of hackers is more than 100 thousand.
- The second trend is the emergence of highly qualified cybercriminal groups. By the way, the first such structure - the group "Sarbanak" appeared in 2014. Prior to that, state-sponsored hackers and ordinary criminals were active. Sarbanak was followed by many other professional groups.
- The third trend is that the number of attackers on infrastructure has been growing in recent years. "I can't assess the pace because it's hard to predict which path they're going on, which topic is relevant for such groups. The activities of criminals depend on many factors. not up to us.

Kaspersky also talks about the specialization of hackers in different parts of the world, with Chinese cybercriminals working more on botnets (a network of computers infected with malware), Russians programming on digital signage, and Latin American hackers working on financial scams. Interestingly, criminals have specializations. The Chinese work more with botnets, hackers using digital codes often speak Russian, and hackers engaged in financial fraud are mostly from the Latin American region. In particular, we need to teach cybercrime rules to all segments of the population who use social networks in the prevention of cybercrime. The better we master these rules of cybersecurity, the stronger we will be protected from becoming victims of cyber “attacks”.

We believe that adherence to the following rules of ethics in the use of social networks will prevent the violation of moral norms in society from a human point of view, and from the point of view of legality will lead to the prevention of offenses.

Therefore, we recall the most important rules of cybernetics:

1. Use the Internet to communicate or share ideas with others. Email and instant messaging is the best way to stay in touch with friends and family, keep in touch with colleagues, and share ideas with people in the city or the world.
2. Don’t be violent on the internet. Don’t nickname people, don’t lie about them, don’t spread their personal pictures, and don’t do anything else that is harmful to them.
3. The Internet is the world’s largest library where you can find information in any field, so use it properly and legally.
4. Do not access other people's accounts using their passwords.
5. Do not share your personal information with anyone. Otherwise, they will have the opportunity to misuse your information and this can end in a scandal.
6. Don’t try to deceive others with fake accounts while you are on the internet, if the account owner has a problem, you will too.
7. Always use copied data and download only allowed games and videos.

The above is a code of ethics that everyone should follow when using the internet. We need to follow the rules in life as we follow the rules in cyberspace [10].

According to experts, this is done by promoting the development of developing countries, influencing the minds of citizens under the guise of universal democratic principles, subjugating them to their goals in various ways. Unfortunately, in the process of organizing cyber-attacks, attempts to

"effectively" use the unprecedented capabilities of the global Internet in this way are gaining momentum. The role of social media, their producers and sponsors in “interfering” in the internal affairs of a sovereign state has not been fully explored, so sometimes such “interference” is not yet recognized as anti-state.

There is no international legal basis for the owners of social networks to be prosecuted for inciting the overthrow of the state system on the pages of these networks. However, according to the substance of every criminal act or omission committed, it must certainly not go unanswered and unpunished. Websites appear suddenly, often changing format and then location. That is why some experts are proposing to abandon the original concepts, such as the complete openness of the Internet, and move to a new system.

The main essence of the new model is to waive the anonymity of network users. This allowed the network to be more protected from criminal encroachment. As an example, we can cite the Chinese state, which has moved to a closed network system, and the Russian state, which is preparing for such a process. In our country, which is integrating into the world community, a consistent state policy on the effective use of information and communication technologies, information systems and modern computer technologies is being pursued.

Modern digital technologies introduced in our country today open the door to a number of conveniences and opportunities for our citizens. Along with this process, of course, there is the problem of ensuring the security of digital technologies and information systems. This is one of the most pressing issues - ensuring cyber security, preventing and combating possible cybercrime. In ensuring cybersecurity against cybercrime, which is improving day by day, we can protect against cybercrime by fulfilling the following basic requirements, namely: cybersecurity:

- Teaching employees the basics of information security;
- Regular testing of vulnerabilities in the software used;
- Use a reliable antivirus program;
- Use of licensed official programs;
- The use of multifactor authentication in the protection of information systems;
- Adhere to a strong password storage policy when using passwords;

encrypt data on computer hard drives on a regular basis.

Recently, there have been an increase in reports on social networks about hacking sites and spreading virus programs. Cybercrime has become one of the most serious problems, especially during a pandemic. According to the analysis, the damage caused to the world community by cybercrime since 2015 amounted to 1.1 billion. By 2019, the figure will reach $ 3.5 billion. Made up the amount of U.S. dollars [7].

In order to prevent such cases in the Republic of Uzbekistan, the Resolution of the Cabinet of Ministers of the Republic of Uzbekistan dated September 5, 2018 No 707 "On measures to further improve information security on the World Wide Web" . Including; - “Encouragement to forcibly change the existing constitutional order and territorial integrity of the Republic of Uzbekistan; - propaganda of war, violence and terrorism, as well as religious extremism, separatism and fundamentalism; - disclosure of information that is a state secret or other secret protected by law; - Dissemination of information that incites national, racial, ethnic or religious hatred, as well as infringes on the honor and dignity of citizens or business reputation, allowing interference in their private lives; - promotion of narcotic drugs, their analogues, psychotropic substances and precursors; - promotion of

pornography; "It is prohibited by law to commit other acts that may give rise to criminal or other liability".

There are about 60 types of offenses punishable under the national legislation of the Republic of Uzbekistan (17 in the Code of Administrative Offenses and 42 in the Criminal Code). types of punishment.

LIST OF USED LITERATURE:

1) Constitution of the Republic of Uzbekistan. T .: O'zbekiston, 2020. 12-p.
2) Address of the President of the Republic of Uzbekistan Sh. Mirziyoyev to the Oliy Majlis of December 29, 2020
3) Sh.M.Mirziyoev. we will resolutely continue our path of national development and raise it to a new level. –T .: "Uzbekistan" .2017. - 15 b.
4) Criminal Code of the Republic of Uzbekistan. https:// www. lex.uz/ acts/111453.
5) Article 121 of the Law of the Republic of Uzbekistan "On informatization" https://www.lex.uz/docs/3893085.
6) 6.Karimov I.A. The concept of further deepening democratic reforms and development of civil society in our country. T .: O'zbekiston, 2010. 42-43-p.
7) Karimov I.A. Our ultimate goal is a free and prosperous homeland, a free and prosperous life. T.8. T.: O'zbekiston, 2000. 333-p.
8) Islomov Z.M. Uzbekistan towards modernization and democratic development. T .: O'zbekiston, 2005. 130-131-p.
9) Jumayev R.Z. The state and society: on the path to democratization. T .: "Sharq", 1998. 34-35-p.
10) S.B.Sodiqov, B.A.Sulaymonov, M.M.Sultonov. Cybersecurity Dictionary. Academy Publishing Center. -T.2020.-45 b.