THE ROLE OF CYBER SECURITY IN THE SYSTEM OF INTERNAL AFFAIRS BODIES AND CYBERCRIME PREVENTION

[1]Kamalov M.E., [2]Mamatjonov J.T.
[1]Senior teacher of the Department of Information, Technologies of the Academy of MIA
[2]1-course cadet of the Academy of MIA
https://doi.org/10.5281/zenodo.11552370

Abstract*. The article provides information on the role of cybersecurity in the system of internal affairs bodies and aimed at preventing cybercrime. Cybersecurity refers to the protection of systems connected to the internet, including devices, software and data, from cyber-attacks. This mainly covers information about people, processes and technologies that cooperate to reduce threats and vulnerabilities cover actions such as international cooperation and Computer Network Operations, Information Assurance and law enforcement. This is information about networks, devices, programs and a set of technologies, methods and practices aimed at preventing attacks, theft, damage, modification or unauthorized access to information; the fact that cyber-attacks are a global problem, which causes many fears that can threaten the world economy; the important role of the United Nations Security Council in creating international laws to control and mitigate the consequences of; Today, special attention is paid to the development of an informed society with a healthy Internet environment in our country, aimed at making our citizens close, changing living conditions in a modern form; to ensure cybersecurity of internal affairs bodies and to prolificity of the occurrence of cybercrime, the types of prevention are established by the law of the Republican of Uzbekistan "on the Prevention of; About the law of the Republic of Uzbekistan "on Cyber security" No. 764 and other legislative acts; about activities in the field of cybercrime prevention and types of cybercrime.*

Keywords*: cybersecurity, cybercrime, cyber threats, Internet, Information Technology, cyber-attack, (clouds), cyberspace, internal affairs bodies, cyber threat, cybercrime.*

Introduction. Today, in the global information space, new threats are emerging related to cyberspace. Therefore, the issue of protection against attacks in the virtual world is of serious concern to the world community. In today's technologically advanced era, which relies on the digital ecosystem, the need to provide robust cyber security measures is important. Cyber bullying is diverse in nature, and the number of malicious individuals who are constantly striving to take advantage of the vulnerabilities in our interconnected systems is growing. The cybersecurity landscape is constantly evolving, adapting to new threats and challenges. It is very important for businesses, individuals and organizations to be aware and active in their cyber security practices. Having studied important aspects in the field of cyber security, we can effectively resist risks and strengthen our Digital Protection.

Today, in our country, special attention is paid to the development of an informed society with a healthy Internet environment, aimed at making our citizens close, changing living conditions in a modern form. In this regard, the development and implementation of the digital Uzbekistan-2030 program in the Republic of Uzbekistan, first of all, the formation of thorough and excellent organizational and legal mechanisms, as well as ensuring the continuous cooperation

of state bodies and business entities for the introduction of innovative ideas, technologies and developments, covering production and service in all spheres and industries with digital technologies, it serves to create a "safe informed community" environment in the country. In the case of premature prevention of violations committed using internet networks, it is necessary to effectively use all types of violations prevention and their measures prescribed by law. The types of prevention of Internal Affairs bodies are defined by the law of the Republic of Uzbekistan "on the Prevention of violations «on the provision of cybersecurity and the profile of the occurrence of cybercrime, their prevention. In addition, the law of the Republic of Uzbekistan No. 15.04.2022 of the Republic of Uzbekistan No. 764 "on Cybersecurity» deals with the penalties applied in cyberspace to ensure the interests of the individual, society and the state, to persons who committed cybercrime.

"Cybersecurity" refers to the protection of internet-connected systems, including devices, software, and data, from cyber-attacks. It mainly focuses on people, processes and technologies that cooperate to reduce threats and vulnerabilities cover actions such as international cooperation and Computer Network Operations, Information Assurance and law enforcement. It is a set of technologies, methods and practices aimed at preventing attacks, theft, damage, modification or unauthorized access to networks, devices, applications and data. Cyber-attacks are becoming a global problem. This created many fears that could threaten the world economy. There is a need for companies and organizations, particularly those dealing with information related to national security, health, or financial information, to act to protect their confidential business and personal information from cyber attacks. Several layers of protection are used in an effective cyber security strategy to ensure the security of computers, networks, applications and data. In order to establish a successful defense against cyberspace, the organization's staff, processes and technology will have to support and complement each other.

There are growing cyber-attacks in the future of cybersecurity. When an individual or organization intentionally and maliciously attempts to access the information system of another person or organization, this is called cyberbullying. While most attacks have an economic purpose, the few operations currently underway involve data destruction as a goal. Malicious individuals often seek payment or other means of earning financial income, but attacks can be carried out for a variety of reasons, including political actions. Cyber security will be the main issue that needs to be addressed in cyber security in the future. In the future, clouds may bow under attack. The growing popularity of public cloud domains has led to an increase in cyber-attacks focused on platform resources and important information. As in 2018, incorrect configuration and mismanagement of cloud resources remained the most dangerous for the cloud ecosystem in 2019. As a result, affected cloud assets were subject to a wide range of attacks. The misalignment of cloud infrastructures has been one of the main causes of many data theft incidents and attacks in the current year, in which businesses around the world have suffered. Dosker hosts were exposed and competitors ' cloud-based crypto mining activities were suspended. According to Check Point researchers, the number of exploits against public cloud infrastructures has also increased.

Cyber security personnel must fight several cyber-attacks. Here are a few examples of these: phishing is a common method of cyberbullying that remains one of the most serious risks of cybersecurity in the future. Advanced social engineering avoidance tactics are harming email security mechanisms. According to Check Point analysts, extortion schemes and a business email agreement (bes) are on the rise, threatening victims by blackmailing them or impersonating others

to obtain payment. Both frauds do not always contain malicious attachments or links, making them difficult to identify. On one occasion, some kind of action was revealed as the CIA and warned the victims that they were suspected of distributing and storing some illegal videos about children in April. A group of hackers responded by demanding $ 10,000 for Bitcoin. In the future of cyber security, attacks on mobile devices are increasing. Cybercriminals are introducing General models and methods of the threat landscape to the Mobile World. Compared to 2018, bank-related malware has successfully infiltrated the mobile cyber arena, and their sharp growth has exceeded 50%. Malware that can steal victims 'bank account payment information, account information, and funds has been pushed out of a wide threat environment and has become a particularly common mobile threat because of increased use of banks' mobile apps. In the future of cybersecurity, increased ransom share attacks are expected. Ransom share has become much more popular in recent years. Small local and state government agencies are primarily targeted in the southeastern United States. Cloud computing, cloud-based subscription services, and the rapid spread of mobile devices are weakening traditional network perimeters. With the increase in the number of vectors, the methods of attacking companies also increase. In the fight against such cybercrime, the labor of employees of the internal affairs bodies is considered large.

In recent years, the IT industry has made a significant contribution to the economic well-being of many countries. Required skills: the first and most important requirement is a strong interest in the field. Candidates for cybersecurity positions should have a strong sense of interest and a strong appetite for it. The cyber threat landscape is constantly changing, so if you are interested in this area, you should be prepared to continue learning and put in effort. Below are the cybersecurity skills that beginners should start a successful cybersecurity career: network connectivity. Networking is an early cybersecurity skill on our list. Regular transactions and communication in computer networks require security. In their daily activities, enterprises use different industries. It is very important to learn how to configure Local Area Networks (LAN), wide area networks (WAN) and virtual Private Networks (VPNs) to manage. Coding is a computer programming language used to create software. Understanding the basic concepts of coding in languages such as HTML and Javascript helps to better understand their vulnerability to cyberattacks. Systems and applications knowledge of software and systems is another important skill of cybersecurity. Since computer programs and other applications are important tools of the company, it is necessary to understand everything about them. If you learn how to run and store databases and web servers, you will be ready to improve the security of applications by identifying vulnerabilities. In various fields, IT knowledge needs to be learned about IT in order to understand the systems and processes that form the basis of Technology. An intelligent cybersecurity expert knows how accidents happen and how to prevent them. A good understanding of systems is another important cybersecurity skill. To study the specifics of common operating systems and know everything about mobile systems, it is necessary to familiarize yourself with command-line interfaces such as Linux Terminal or Windows Power shell. Technological innovation. We don't like cybercriminals, but we have to give them one thing: a real innovator spirit. In order for us to be ready to defend ourselves, we must be aware of the new technology and their development. Cybersecurity innovations are building new foundations to protect commercial networks from malicious attacks. The adoption of new work environments during the Covid-19 crisis has shown the importance of cybersecurity even more than before.

Cybersecurity innovations have brought significant advances in the field. Since we are striving for a future with digital capabilities, it is important that cybersecurity professionals have imagination and bring new ideas to life. Jobs and opportunities in the future of cyber security in the future job opportunities in cyber security are very remarkable. When we think about it, it makes a lot of sense that cyber security employment increases above average. As technology increasingly enters every person's daily life, the demand for professional cybersecurity professionals increases. Cyber security salaries are also high and increasing day by day. While future cyber security employment estimates show more opportunities, the reality is that there are now very few professionals qualified enough to work in the field. Due to the shortage of qualified personnel, those who choose a cyber security profession can expect many opportunities, good income and excellent benefits. In the field of cybersecurity, employees of the “cybersecurity center” of the Ministry of internal affairs are working. Qualified employees are fighting cyber-attacks that are taking place in our country and in the virtual world. Every year, graduates of the Academy of the Ministry of internal affairs begin their activities to combat cybercrime in different regions of this center and the Republic. Cadets trained in the field of cybersecurity develop their knowledge in the educational process, in order to combat various cyberattacks. Alternatively, the Tashkent University of Information Technology and other graduates of the University operate in this area.

Cybercrime is a crime without borders, the consequences and consequences of which are endless; the United Nations Security Council must have an important role in creating international laws to manage and mitigate the consequences of these cybercrime that afflict many states. At the end of World War II, there was a need to establish a Security Council to maintain international peace. However, in 1945 the main concern was to have an armed army to prevent one country from invading another. But with the advances in technology, the invention and the widespread use of the Internet, a new threat arose against all states - it is impossible to fight the troops here. The Security Council is the competent authority to implement international policy on cyber security to combat threats arising from cyberwarfare, cyber-terrorism and other cyber threats.

While cybercrime is a relatively new concept, it is a problem that is costing the economies of many countries. Crime weapon-internet and the latest digital technologies. It has the potential to disable the military, strategic sectors of the country. And finding and punishing disruptive hackers is not an easy task, because they are always one step ahead of the state. Today's life is difficult to imagine without modern technology. Recent discoveries in the world of mobile communications and the internet have been far-fetched, heavy-handed, and business opportunities have been expanded. However, these facilities are focusing on another area. Cyber security is a separate strategic issue for each state. “While state secrets and high technology were primarily targeted first, criminals are now taking the target Wider,” says Robert Mueller, head of the US Federal Bureau of search (FBR).

In Uzbekistan, too, this type of crime has increased 8.3 times in the last three years, now reaching almost 5% of the total crime. In particular, through illegal banking and financial operas, there is an increasing number of crimes of appropriation of other people's plastic card funds, distribution of harmful viruses, gambling and risk-based online games, information attacks aimed at religious fanaticism, fraud in the online trading space. The country reported 106 crimes in the information technology sector in 2020. In 2021 it was 2,281, and in 2022 it was 4,332, more than twice as many as a year ago, and 40 times as many as 2 years ago. Of the cases recorded during

the year, 3,372 or 82 percent of the bank's money from plastic cards are crimes related to the embezzlement of funds. It is sad that young people are the majority among individuals who have committed offenses and crimes with the help of Information Technology. In our republic, most of the violations in the virtual world are committed by adolescents-young people between the ages of 16 and 23. It can be seen from this that the issue of ensuring cybersecurity is gaining more relevance today than ever before. In Uzbekistan, 5,500 cybercrime cases were committed in 11 months of 2023, of which 70% were bank card fraud and theft crimes. According to analysis, more than 500 million cyber-attacks are launched every year around the world. Every second, one in 12 people falls victim to attacks in cyberspace. In developed countries such as the United States, France, England, Germany, Belgium, Luxembourg, 60-65% of crimes are being committed through cyber-attacks.

Currently, the United States, Russia, Korea are among the leading countries in cybercrime. Cybercrime is increasing from year to year the main reason for this is digital technologies. Currently, all processes are based on digital technologies. For example, according to scientists, cybercrime grows up to 8-11% per year. It is a little more difficult to find individuals who commit cybercrime, because the Masters of their work, work as a person or as a group. What forces them to do this is money. For them, rather than waiting for a working month and a month's salary in a state job, they will only earn funds in the short term, employing the ability to hack.

Threats to your personal data on your smartphone. For example, threats that can be found on social networks that make our photo on our phone. In order for such situations not to be observed, we must correctly understand and understand each of our affairs by asking ourselves questions about what we are doing this. When weighing personal data, we all have e-mail mail, id-numbers and all kinds of data that are digital data that make it easy for us to go far close, difficult processes by doing a lot of our work. The person who has learned your password, which is put on such Mail, almost controls or controls information and the processes in your lesson, work, everyday life. Seeing your important documents in the workroom until your agreements with partner foreign countries can change or manage them, and can also limit your re-entry into the system.

ID card, Visa Card Management. A type of cybercrime that is very popular now can extort money from your bank account, virtual cards in the form of online communication through various deceptions, or you can be scammed. Many applications over these processes came to the internal affairs bodies in the appropriate order. This process is carried out very easily, and you become a victim of cybercrime. Do not tell yourself the codes that come to your phone number or account by strangers, companies in any case. Be vigilant internet users are also increasing as the time has developed rapidly. Information technology benefits the population, Society, the state and there are programs, platforms, applications that create comfort. But it is better that these are introduced to the public on the security side and after successful passage of other tests.

A cybercrime prevention system will be created in Uzbekistan. This is outlined in the draft decree of Shavkat Mirziyoyev “on the development strategy of New Uzbekistan for 2022-2026”. It is noted that the cyber security strategy of Uzbekistan will be developed for 2023-2026. In this case, the main directions for ensuring the cybersecurity of the internet space of the” uz " domain zone are determined. Comprehensive tasks for the protection of e-government, energy, digital economy systems and other areas related to important information infrastructure will be compiled. There are also plans to revise criminal liability for cybercrime. The system for monitoring

cyberattacks and threats in the information field will be improved. Through this, the technical infrastructure of the unified cyber security network will be expanded. It is planned to further accelerate the activities of the" IT park of innovations in cybernetics". On the basis of the digital technology training centers in the regions of IT park, it is envisaged to ensure the training of young people on the basics of cybersecurity, as well as to conduct annual Republican-scale concourses on the detection of cyberattacks among students and students.

The object of the general prevention of cybercrime is the general public, and individual individuals are not selected in this. For example, neighborhood residents, labor communities (enterprises, institutions, organizations), underage community (schools, colleges and academic lyceums), youth community, etc. In this case, the Prevention of offenses is equally delivered to everyone and is distinguished by a greater range of influence. General preventive activities of violations are activities carried out through comprehensive socio-legal means aimed at identifying and eliminating, influencing, weakening and preventing anti-social phenomena and processes contrary to society, various events, phenomena and circumstances. Carrying out legal propaganda work among the population is important in preventing violations. In this case, the dissemination of explanations on the Prevention of violations committed by competent authorities between communities such as Labor, minors using internet networks, in particular, reading lectures, organizing round tables, preparing propaganda leaflets, is of great effect. In these promotional activities, it is important that various tasks are carried out in relation to the negative consequences of violations committed in citizens through Internet networks, the reasons for their origin and the increase of sympathy of individuals in this regard.

In conclusion: every crime committed in cyberspace must be combated. The contribution of employees of the internal affairs bodies is significant in this, since the control over the cybercrime listed above is carried out by cybersecurity employees. This area is very wide and borderless. Until the end of our article on the role of cyber security in the system of internal affairs bodies and the Prevention of cybercrimes, it is important that cyber security problems have taken their place as one of the most important problems of the present time and have a great need to prevent cyber crimes. The system of internal affairs bodies operating in the field of cyber security is considered one of our most important guides in the fight against cybercrimes. Through this system, it provides great opportunities to train experienced personnel who can prevent cybercrimes and protect citizens, increase cyber security and increase the chances of protecting dangerous networks. Cyber security is also of great importance in the protection of the Internal Affairs system, dangerous networks and databases. It is believed that the system is powerful and effective, plays a major role in preventing cybercrime, and serves an important role in providing citizens with access to dangerous and secure internet.

REFERENCES

1. https://lex.uz/acts/-2387357 Act of“Huquqbuzarliklar profilaktikasi to‘g‘risida”
2. https://lex.uz/uz/docs/-5960604 Act of “Kiberxavfsizlik to‘g‘risida”
3. Ensuring cybersecurity in Uzbekistan – period requirement analysis and recommendations.
4. Cyber Security and the Need for International Governance.Charletta Eugenia Anderson-Fortson of Southern University Law Center May 16, 2016.
5. Hasanov Sharofiddin Shamshurovich. Eurasian journal of law, finance and applied scientific scientific journal special series " outcomes in criminal-procedural relations

6. https://www.gazeta.uz/oz/tag/kiberxavfsizlik/
7. https://daryo.uz/2022/01/04/ozbekistonning-kiberxavfsizlik-strategiyasi-ishlab-chiqiladi/
8. https://texnokun.uz/?p=7123
9. https://cyberleninka.ru/article/n/kiber-jinoyatlar