ISSN NO: 2769-996X
Date of Publication: 30-11-2022

Management of Cyber Security Processes as a Factor of Ensuring National and International Stability

Batirov Farhad Avazovich,
Head of the section of planning the educational process,
Academic and methodology Department,
University of public safety of the Republic of Uzbekistan
E-mail: Farxod-batirov@mail.ru

Abstract: The article deals with the problems of the development of the information society. Modern cybersecurity management processes are identified, the subjects of these processes and their features are identified. Cyber threats are presented as destructive events in the information and communication environment that undermine information security at the international, regional and national levels. It has been determined that ensuring cyber security and creating means of conducting modern cyber wars are priority areas of state policy in the field of national security. The author notes that it is very difficult for the world community to come to an agreement on a number of fundamentally important issues of political and legal support of cybersecurity and to develop common approaches, which is due to ideological, political and religious differences.

Keywords: cybersecurity / digital space / cybercrime / Internet space / digitalization / security of cyber threats / international security / international security / internet / internet / information society / information society.

Introduction.

From the experience of the developed countries of the world, it becomes clear that today the large-scale development of information technologies and their use by various objects has made problem solving a priority task to ensure cybersecurity. Because military-economic espionage is carried out in cyberspace by various criminal groups. During the development process, the software system seeks to eliminate traditional security solutions in new ways, including artificial intelligence and analytics. Therefore, in addition to cyberspace today, the protection of users' personal data from illegal data collection is also becoming an increasingly urgent problem.

Taking into account the high rates of development of information and communication technologies in prestigious universities and research institutes of the world, scientific research is carried out to protect infrastructure, which is important for the economy, the state and various spheres of life, to prevent an increase in cyber attacks on information systems, to prevent cyber attacks and cyber attacks on economic, financial, banking, Here we are talking about protection of both civilian and military cyberspace, which can damage interconnected networks and information infrastructure. The need for conceptual (strategies - principles) approaches to solving these problems arises from the need for coordinated, reliable functioning of the country's infrastructure. It is aimed at coordinating the efforts of the public, private sectors, society and international organizations in cyberspace.

Considering Uzbekistan's cybersecurity strategy, we want to focus on the following issues: we believe that it is necessary to build a strategy embodying the proportional interests of the individual, society and the state. The interest of the individual lies in the exercise of constitutional rights to use information, as well as in physical, mental and intellectual development, ensuring personal security. Much attention was paid to the need for public-private cooperation in cyber strategy, which together makes it possible to combat emerging threats and strengthen the protection of the national information infrastructure.

Analysis of the literature on this issue (literature review).

Due to the significant increase in the use of the Internet and social networks, all issues related to information have become serious. Especially specialties, professions, courses, seminars, etc., which begin with the word Cyber. The word "kubernan", which means "reorientation" in Greek, first appeared in English as "cybernetics" in 1948. In 1958, Lois Suffignal used it as a "cyber" to explain the connection between living beings and robots. In the process of forming the global cyberspace, military and civilian computer technologies are converging with each other, new means and methods of active influence on the information infrastructure of potential adversaries are being intensively developed in leading foreign countries, various specialized cybernetic centers and management units are being created. Thus, the United States, China, England, France, Germany, Israel and a number of other countries already have their own official cybersecurity system.

The confrontation in cyberspace is becoming an entirely new area of confrontation between states. "Cyber..." the term and definitions with the prefix are widely used in both international and domestic discussions and documents and are reflected in the strategic doctrines of individual states and international organizations, including NATO. The rapid growth of interest in cyberspace in the world is largely due to the activity of the United States in cybersecurity and cyber defense. Cybersecurity is aimed at protecting the information resources of people, organizations and governments from cyber attacks in cyberspace. Today, the growth of cybercrime is directly related to the large amount of information available through Internet services, social networking platforms, intranets, Internet of Things devices and others.

In foreign countries, E. Serra, T. Parenti, P. Troncon, Karl Olbing, Y. Diogenes and other similar scientists have investigated various aspects of this problem based on the directions of their fields [1]. Cybersecurity risk for individuals, businesses and governments increases with the number of modern devices connected to the Internet. Computer security, cybersecurity or information technology security is obvious as the protection of computer systems and networks from leakage of confidential information, theft or damage to hardware, software or electronic data, as well as failures and interruptions in the services provided by them.

From the countries of the Commonwealth of Independent States I.L.Safronova, E.A. Solovyova, A.V.Stoletov, E.N.Molodchaya, M.M.Kucheryavi, E.V.Batueva, V.F. Jafarli, P.A.Karasev, E.S.Zinovieva, A.V. Legal, political and socio-cultural aspects of the problem have been studied in detail by scientists such as Kurilkin and others [2]. From these studies, it becomes clear that artificial intelligence is promising in the field of cybersecurity, and it is mainly related to threat detection systems. Automation not only guarantees the detection of any breakdowns, but can also protect vulnerable areas. Deep learning capabilities are now being used to track logs, transactions (data traffic), and data to identify network threats. The possibilities of self-study of the machine include the search for all possible traces and the identification of anomalies. It has the ability to "learn" to recognize structures and warn about potential attack attempts, and can also adapt and hide repetitive behavior to prevent cybersecurity threats. Such innovative technologies are being improved day by day.

In our country, M.H.Rustambayev, S.Y.Akhrarov, I.Y.Inayatov, A.M.Kambarov, S.O.Atamuradov, R.S.Samarov, A.Sativaldiev, O.S.Temirova, N.J.Eshnaev, Z.S. Alimardanov, B.S. Baymuradov, E.S. Heyitav, R.Samarov and others paid special attention to the study of various aspects of information and public security.

Research Methodology.

In order to regulate the cyber security sector, implement a common policy, and combat problems, it is necessary to improve legislation in the field of cyber security, coordinate threats and risks, and develop approaches and standards. Therefore, it is important to establish the activities of the center, which is engaged in the development of national cyber security strategies in our country. It should be borne in mind that cyber security, which includes cyber-attacks, includes many factors: telecommunications technologies, the regulatory framework – the relationship "individual-society-state-business", etc.

Here are some common methods that threaten cyber security: malware, one of the most common cyber threats, is software created by cybercriminals or hackers to break into or damage a legitimate user's computer. There are several types of malware: Virus: A self-replicating program that attaches to a clean file and spreads through a computer system, infecting documents with malicious code. Trojan: A type of malware disguised as legitimate software.

Cybercriminals deceive users by installing Trojans on their computers, damaging their computers or collecting information. Spyware: An application that secretly records what a user is doing so that cybercriminals can use this information. For example, spyware can get credit card information. Ransom ware: Malicious software that blocks and threatens to delete user documents and data if payment is not made. Adware: Adware that can be used to distribute malware. Botnets: Computer networks that distribute malware used by cybercriminals to perform online tasks without the user's consent. Phishing is the practice of cybercriminals targeting victims using email addresses that require confidential information and appear to belong to a legitimate company. Phishing attacks are often used to trick people into obtaining credit card information and other personal information. Interference in operas. Operative intervention is a type of cyber threat in which cybercriminals break the connection between two people in order to steal information. For example, in an unsecured Wi-Fi network, an attacker can store data transmitted from the victim's device.

Analysis and results.

Just as our security is important in real life, security is important in the virtual world, and this is called cyber security [3]. Cyber security usually includes computer security, transaction security, data protection, personal data security, internet security, and even the security of devices that transmit any signal. The reason these issues are becoming so interconnected and relevant is because of cyber-attacks and the threats they face. As the number and type of cyber-attacks increase, cyber security networks are also expanding. Since the 1980s, such concepts as "cybercriminals", "Ethics in the cyber world", "ethical cyber piracy" have appeared. Although the term "cyber security" is often used interchangeably with the terms "IT (information technology) security" and "information security", the difference lies in the areas of protection. IT security: It is a general term that includes physical security, information security, and cyber security. It is a broad concept that covers the physical and digital aspects of infrastructure and information security in an organization.

Cyber security: The goal is to protect against cyber bullying. Vulnerability scanning, access testing, firewalls and multi-factor authentication schemes belong to the field of cyber security. Information security: The main focus is on the storage of information and information obtained from it, both physical (for example, paper archives) and digital. It includes employee policies on fraud prevention, backup and data protection.

In the first half of 2020, the number of fraud-related crimes in Uzbekistan doubled compared to last year and amounted to 3,881 in six months. In our country, since October 2020, there has been a state of withdrawal of a plastic card number from citizens by fraud. 20 million a day by hackers receives funds in the amount of up to 35 million rubles. At the same time, scammers mainly use the tool of sites that are bought and sold over the Internet.

Today's cyber-attacks are being carried out at an unprecedented level. Because, using the capabilities of information technology, hackers can cross all boundaries to achieve their goals, for example, damaging or destroying confidential information from industrial and military centers, these systems. Cyber-attacks are also carried out on non-military structures. For example, they can disrupt the operation of electricity, air and water transport. Cyber threats are software and a computer. Most cyber threats today are software. They start and spread at a low level. In a word, today we are witnessing a new war, which is becoming more and more dangerous. Therefore, cyber security is very important today. At the moment, it should be noted that, although cyber-attacks are of financial and economic importance, certain funds are invested to neutralize them, but these cyber-attacks indicate the presence of specific hostile actions in this area.

Today, experts predict that such attacks will be more serious in the future. Today, countries such as the United States, China and Russia are already blaming each other for cyber-attacks. The purpose of these attacks is to obtain information of particular importance in the industrial, political and military spheres, damage the infrastructure of a competing state or slander officials. However, the damage from such attacks is not borne by one State, but by all States. In recent years, many companies in the UK, Italy, Russia, Spain, Portugal, Taiwan and Vietnam have become victims of cyber-attacks. In June 2017, a hacker attack disrupted computer programs around the world. Many computers stopped working, and in 2019 a report by the Jupiter research company was published, according to which cyber-attacks on the global economy by 2020

The damage amounted to $8 trillion. And this amount of money is huge, because today many tools are directly connected to the Internet, which are exposed to the threat of cyber-attacks. Small and medium-sized businesses suffer more from such attacks than large companies. And today, companies do not have the budget to prevent such attacks. And the most dangerous thing is that terrorist groups use the cyber environment to achieve their goals.

Experts believe that the civil direction of information dissemination is widely developing among the population today. In this case, the information of individuals is posted on blogs or on various pages available on the social network. But given that the individual's intentions are unclear, often behind the dissemination of such information lies a destructive thought or someone's selfish interest. "In the experience of world journalism, there are cases of effective use of such an amateur method of transmitting information [4]. 239 thousand of these records were sent to the world-famous CNN TV channel in 2009. Among them, they can also be organized or falsified using technical techniques. The channel's employees, referring to this, carefully consider the footage as much as possible and try to contact the authors of what they find interesting and justified from the inside. When they manage to establish contact, they ask the author to comment on the events on the plaque and agree to also mention his name in the program" [5].

French police recently announced that the terrorist group ISIS is using the Internet to recruit new members. The group uses the Internet to spread its ideology in France. To join Muslim immigrants living in Germany and the UK, ISIS conducts virtual operas through its members. The head of European policy, Rob Wainwright, believes that "ISIS has special social networks with which it tries to achieve its goals" [6]. Cyber security is also used for political purposes. The United States has accused Moscow of interfering in the 2016 presidential election. On October 7, 2016, the US government officially accused Russia of damaging the computers of the Democratic National Committee by cyber bullying and infiltrating the computers of some American officials. Because Hillary Clinton's election program and her reputation have been undermined. The US authorities have previously stated that Russia will launch a similar attack. In any case, the Americans claim that it is difficult to prove this accusation.

Conclusions and suggestions.

Cyber security protects devices, applications, networks and data from attacks, damage or unauthorized access caused by cyber threats. It is very important for companies to implement policies and procedures to protect important work and employee information, to be aware and prepared for cyber threats. Cyber security is the practice of protecting computers, servers, websites, mobile devices, electronic systems, networks and data from malicious attacks. For the same purpose, A.K.Rasulev rightly noted that "the study of the threat of crimes and cybercrime in the field of national security information technologies indicates the need to systematize and clarify the fundamentals of state policy in the field of information security. To this end, the concept of information security of the Republic of Uzbekistan should be adopted, the concept should set out the purpose, objectives and main problems of ensuring information security based on an analysis of the current state of information security, indicate objects, risks and their consequences, methods and means of prevention, termination and elimination of risks, as well as specific aspects [7].

The constant reduction of the crime rate in order to ensure the safety of society is one of our priorities. Considering the concept of a nonviolent society as a possible condition for social solidarity, we continue the culture of violence. To prevent the spread of the criminal subculture, we pay special attention to the special rules of behavior established and recognized by the criminal environment. Violence, xenophobia - criminal subculture has no place in our society. Uzbekistan consistently combats the intelligence and destructive activities of foreign intelligence services, the activities of organizations that harm the national interests of Uzbekistan by individuals, international terrorism, other violent manifestations of extremism, domestic and transnational organized crime, weapons, ammunition, and illegal human trafficking. We will also expand and deepen international cooperation in the fight against various forms of crime.

Uzbekistan undertakes to ensure the free and safe movement of people in its migration policy, while balancing with ensuring the national security of the country. We will continue measures to ensure border security, improve the effectiveness of integrated border management, in particular, prevent illegal border crossings, effectively manage cases of illegal migration from a humanitarian point of view, as well as reduce illegal migration of citizens of Uzbekistan. The State introduces effective procedures to prevent the spread of infections that pose a threat to public health.

Well, first of all, today most institutions and organizations rely on computer systems to store very extensive and confidential personal information in order to ensure cyber security. Access to this information has become a kind of arena of struggle for criminals, terrorists, politicians and villains. The threats that this causes can cause very serious and irreparable damage to the organization in terms of finances and reputation. Therefore, the importance of cyber security is increasing day by day, and it is becoming more and more relevant. Cyber-attacks affect all institutions and territories, regardless of size. In recent years, healthcare, manufacturing, financial and public sector institutions have been the most "hot spots" reported. These sectors are more likely to be attacked by cybercriminals because they collect more information, but that doesn't mean others aren't potentially at risk. Any object that is a network user can become a target of cyber-attacks.

Secondly, the world relies more on technology today than ever before. Because the digitization process is accelerating all over the world, which leads to the creation of a huge database. Today, businesses and governments store most of their data in computer systems and transmit it over networks to other computers. This process is carried out through the operation of individual facilities and their main systems. Cybercriminals in one form or another assess the likelihood that these devices or individual components of the system have weaknesses in the network, and use these vulnerabilities to access data. This will eventually lead to a data leak. Data leaks can have a number of devastating consequences for any business.

This can damage or destroy the reputation of the company, losing the trust of consumers. The loss of important information, such as source files or intellectual property, can lead to the loss of the company's competitiveness.

Thirdly, one of the main reasons for the intensification of cyber-attacks is global digitalization in all regions of the world. At the same time, the biggest problem of information security today is its rapid internationalization. An analysis of recent cyber-attacks on the resources of state institutions in Uzbekistan also shows that there are very few repressions inside the country, mainly cyber threats from abroad. In 2021, there was the highest average price of data corruption in the last 17 years, which increased from $3.86 million to $4.24 million per year. Also, when remote performance was a factor, the average cost of data corruption was $1.07 million higher. The most common cause of data leakage was the theft of user account information. This attack vector accounted for 20% of violations, the average cost of which was $4.37 million. The most common cause of data corruption in 2021 was theft. In addition, social engineering attacks have become a serious threat to public institutions, in particular, they accounted for 69% of all offenses in this sector.

Used Literature:

1. Сэрра Э. Кибербезопасность: правила игры : как руководители и сотрудники влияют на культуру безопасности в компании: Эллисон Сэрра ; перевод с английского: Людмила Смилевска. - Москва : Альпина ПРО, 2021.
2. Паренти Т. Кибербезопасность. Что руководителям нужно знать и делать. - Москва : Морозов И.Л. Информационная безопасность политической системы // Полис. Политические исследования. -2002. -№5.
3. Манн, Иванов и Фербер, 2021. Тронкон П. Bash и кибербезопасность : атака, защита и анализ из командной строки Linux: / Пол Трон кон, Карл Олбинг ; [пер. с англ. А. Герасименко]. - Санкт-Петербург [и др.] : Питер, 2020.
4. Диогенес Ю. Кибербезопасность: стратегии атак и обороны : безопасность инфраструктуры с использованием тактик Красной и Синей команд / Юрий Диогенес, Эрдаль Озкайя ; перевод с англ. Д. А. Беликова. - Москва : ДМК Пресс, 2020.
5. Отабоева М., Тафовутлар майдони//Ҳуррият, 2014 йил, 12 февраль, №7 (863)
6. Сафронова И.Л. Политические проблемы обеспечения международной информационной безопасности : диссертация ... кандидата политических наук. - Москва, 2006.

7. Соловьева Е.А. Информационное противоборство в сети Интернет: политологический анализ : диссертация ... кандидата политических наук. - Пятигорск, 2011.
8. Столетов О.В. Стратегия "разумной силы" в политике глобального лидерства : диссертация ... кандидата политических наук. - Москва, 2014. –
9. Молодчая Е.Н. Политика противодействия кибертерроризму в современной России: политологический аспект : диссертация ... кандидата политических наук. - Москва, 2011.
10. Кучерявый М.М. Информационное измерение политики национальной безопасности России в условиях современного глобального мира : диссертация ... доктора политических наук. - Санкт-Петербург, 2014.
11. Батуева Е.В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая : диссертация ... кандидата политических наук. - Москва, 2014.
12. Джафарли В.Ф. Криминология кибербезопасности: монография : в 5 т. / В. Ф. Джафарли ; под редакцией доктора юридических наук, профессора, С. Я. Лебедева. - Москва : Проспект, 2021.; Карасев П.А. Политика безопасности США в глобальном информационном пространстве : диссертация ... кандидата политических наук. - Москва, 2015.
13. Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности : субъекты и тенденции эволюции : диссертация ... доктора политических наук. - Москва, 2019.
14. Курилкин А.В. Информационные и кибернетические операции как инструмент реализации внешней политики : формы, методы, технологии : диссертация ... кандидата политических наук. - Москва, 2021.
15. Расулев А.К. Ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятларга қарши курашишнинг жиноят-ҳуқуқий ва криминологик чораларини такомиллаштириш. Докторлик (DSc) диссертацияси автореферати. –Тошкент, 2018.

II. Электрон Таълим Ресурслари:

1. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.
2. https://www.researchgate.net/publication/265987327_Driving_Citizens_to_Information_and_Communications_Technology
3. Sammons J., Cross M. What is cyber safety? // The Basics of Cyber Safety.Syngress, 2017. – P.1-27. DOI: 10.1016/B978-0-12-416650-9.00001-2
4. https://en.wikipedia.org/wiki/Terrorism_and_social_media