IRSTI 20.01.04

Musabekov M.O.

Master student, E. Buketov Karaganda State University,
Kazakhstan, Karaganda, e-mail: maratx88@mail.ru

THE CONCEPT OF "NATIONAL SECURITY" IN KAZAKHSTAN

The concept of "national security" is not something unchanged and may change depending on the historical, political, economic conditions and the emergence of unexpected threats and challenges for the state and the people. Ensuring national security is the fundamental responsibility of any government. Without feeling secure, people cannot trust their government, local government structures, even their neighbors, nor can they focus on their daily needs and activities, their short-term and long-term goals, because they are concerned about their ability to provide well-being and normal living conditions. to their families or to plan adequately for the future. Without reliance on the foundation of personal and collective security, people work in an extremely unstable environment that does not contribute to their traditional functioning as members of society and leads to a serious distrust that they have in all institutions and individuals in power. Many societies around the world face this global and daily challenge in trying to provide the practically necessary elements of a security system in the lives of their citizens (1). The last few decades were marked by the gradual transition of humanity from industrial society to the age of information technology. The development of communication technologies and the wide distribution of electronic devices associated with this process create new threats that will be considered in this paper.

Key words: cyber security, cyber defense, cyberspace, cyber-terrorism, national security.

Мусабеков М.О.

[1]магистрант, Е.А. Букетов атындағы Қарағанды мемлекеттік университеті,
Қазақстан, Қарағанды қ., e-mail: maratx88@mail.ru

Қазақстандағы «Ұлттық қауіпсіздік» құрамы

«Ұлттық қауіпсіздік» тұжырымдамасы тұрақты ұғым болып табылмайды және жаңа қауіп-қатерлердің пайда болуына байланысты өзгеруі мүмкін. Ұлттық қауіпсіздік кез келген үкіметтің негізгі міндеті болып табылады. Қауіпсіздік болмаса, адамдар өз үкіметтеріне немесе көршілеріне сене алмайды, сондай-ақ отбасыларын асырап, болашаққа алаңдағандықтан биік мақсаттарға көңіл бөле алмайды. Негізгі қауіпсіздік болмаса, адамдар өте тұрақсыз ортада жұмыс істейді. Бұл орта олардың қоғамда атқаратын қызметін қолдамайды және бүкіл институттар мен билік басындағы жеке тұлғаларға деген сенімсіздікке әкеледі. Әлемдегі көптеген қоғамдар бұл қиындықтарға тап болып, азаматтарының күнделікті өмірінде қауіпсіздіктің барлық қажетті элементтерін іс жүзінде қамтамасыз етуге тырысады. Соңғы бірнеше онжылдықта адамзаттың индустриалды қоғамнан ақпараттық технологиялар дәуіріне біртіндеп аяқ басқаны белгілі. Мақалада коммуникациялық технологиялардың дамуы мен электронды құрылғылардың кең тарауы нәтижесінде туындайтын жаңа қауіп-қатерлер қарастырылған.

Түйін сөздер: кибер қауіпсіздік, кибер-қалқан, кибер кеңістік, кибер-терроризм, ұлттық қауіпсіздік.

Мусабеков М.О.

магистрант 2 курса обучения, Карагандинский государственный университет имени Е.А. Букетова,
Казахстан, г. Караганда, e-mail: maratx88@mail.ru

Концепция «национальной безопасности» в Казахстане

Концепция «национальная безопасность» не является чем-то неизменным и может меняться в зависимости от исторических, политических, экономических условий и возникновения нео-

жиданных угроз и вызовов для государства и народа. Обеспечение национальной безопасности является фундаментальной обязанностью любого правительства. Без ощущения себя в безопасности люди не могут доверять своему правительству, местным структурам власти, даже своим соседям, а также не могут сосредоточиться на повседневных нуждах и деятельности, реализации своих краткосрочных и долгосрочных целей, потому что они обеспокоены своей способностью обеспечивать семьи или адекватно строить планы на будущее. Без опоры на фундамент личной и коллективной безопасности люди работают в условиях крайне нестабильной среды, которая не способствует их традиционному функционированию как членов общества и ведет к серьезному недоверию, которое они испытывают ко всем институтам и отдельным лицам, находящимся во власти. Многие общества во всем мире сталкиваются с этой глобальной и ежедневной проблемой, пытаясь обеспечить практически необходимые элементы системы безопасности в жизни своих граждан. Последние несколько десятилетий ознаменовались постепенным переходом человечества от индустриального общества к веку информационных технологий. Связанные с этим процессом развитие коммуникационных технологий и широкое распространение электронных устройств создают новые угрозы, которые будут рассмотрены в данной работе.

Ключевые слова: кибербезопасность, киберщит, киберпространство, кибертерроризм, национальная безопасность.

Introduction

The development of technology today has a huge impact on various aspects of modern society, which few people suspected a few years ago. Our goal is to consider only one side of this multidimensional and integrated process, namely the impact of new information technologies on the national security of states. For a deeper understanding of the situation, some theoretical approaches and system principles of technological progress should be considered. The work of the famous American philosopher Alvin Toffler, which is translated into different languages of the world, including Russian (Toffler. E., 2010), states that with the development of technology, humanity naturally moves from one stage of its development to another (respectively, from an agrarian type society to an industrial and further to the current information). According to this, in general, not to the doubtful assumption, the modern economy ceases to be based, as it was before, on the mass production of industrial goods, and it moves to a new innovation and information base. This means that if in an industrial society, capital and labor were strategic and transformative resources, then in the modern world such resources are the possession of knowledge and information.

In the same way, it is obvious that at the same time there is a change of priorities and objects in the field of ensuring the national security of modern states. In an industrial society, the protection of the means of production and the transportation of resources was the basis for the safe life of states, and in modern post-industrial society the protection of information and communication is becoming much more important for the internal and external interests of the state. For example, the destruction of ground communications (bridges, roads, etc.) can no longer be considered a serious threat to national security compared to hacking information communications tools, databases related, for example, with financial transactions, or confidential information containing strategic military secrets. This situation radically breaks the existing schemes and systems and leads to a change in the means and methods of warfare.

Main body

A new form of warfare is to obtain vital information about the enemy and at the same time protect your own information. The party with superiority in information technology will have a significant advantage even over an adversary who owns a large amount of conventional weapons (Franklin D. Kramer, Stuart H. Starr, and Larry K., 2009.).

In other words, if in the past the presence of a strong army and a large amount of military equipment was the key to victory in the war, then in the modern world, possession of information and communication technologies is a more important means in achieving victory (Ronfeldt, D., 1992).

At the beginning of the twenty-first century, there was a significant increase in the use of computer devices and means of communication for autonomous control of various types of systems and production facilities. For example, in the modern world, financial transactions between financial institutions do not imply a transfer of the physical volume of the money supply, but rather a transfer in the form of various types and standards of information. In other words, there is an exchange of information in monetary terms. It is difficult to calculate what

damage the American economy can cause in the Wall Street information system, which carries out financial transactions, and this, incidentally, relates to the financial system of any modern country. An even greater danger is the attack on the information system of the military command headquarters, which contains information about the movement or location of strategic and tactical military units and weapons. Accordingly, the "information war" is a new concept, implying the destruction of the enemy's information, a decrease in the credibility and possibility of information transfer, as well as a restriction in access to communication systems. It is worth noting here that information wars, though they took place in the past, did not cause such damage to the side of the enemy, as it happens at the present time. This is due to the fact that never before has humanity been able to distribute, receive and store such a huge amount of information in such a short period of time as it is today.

The wide distribution of computers of the new generation of various modifications, their integration into various complexes, devices, networks, the availability of the possibility of a full or sectoral connection between them created an absolutely new space - cyberspace. Cyberspace includes all interconnected electronic devices and databases, regardless of the distance between them, which are stored, transmitted and processed between them. Information wars were observed and had certain meanings in the past history of mankind, when various means of searching, intercepting and using information about the enemy were used. However, the phenomenon of cyberspace generates a completely new understanding and concept of information wars. Cyberspace allows you to significantly expand and diversify functions, identify new targets, use the latest weapons and previously unknown methods of warfare.

The war in cyberspace is not limited to military operations, it covers a completely different sphere of society. The fact is that today computer technologies are widely used in the management of important infrastructure facilities, they operate with electrical networks, power stations, banking systems, etc. The formation of cyberspace allows you to easily and safely hit infrastructure facilities, the living environment of the population through invisible cyberspace, without the use of force and physical presence in the zone of warfare (Ben-Israel I. and Tabansky L., 2011). It is important to note that the so-called "cyber attacks" became a reality of the modern world. An example is the well-known situation in Estonia in 2007, a massive attack was carried out against the information systems of banks, government, police and other institutions, it paralyzed the country's vital activity for several days (https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm).

Another example is the impact on the command centers of Iran's nuclear facilities in 2010. The use of malware has caused irreparable damage to the country's nuclear industry (Magazine «Spark». Publisher: Kommersant JSC. - №39, 04.10.2010). If we look at the situation in our country, we are witnessing that more than 600 major incidents of this kind were recorded in Kazakhstan in 2016. During the first 9 months of 2017, about 200 incidents occurred. And this, obviously, is not complete information, but only that part of it, which is allowed to be published publicly. It is possible that the real numbers are much higher. In many cases, hackers attack banks, national companies and the domain zone gov.kz. It is possible that the main cause of hacking cases is the "cyber-illiteracy" of employees of these companies. According to statistics, 95% of cyber crimes are committed due to the negligence of users. According to official data, the Information Security Concept of the Republic of Kazakhstan for 2013-2017 was developed and adopted for action in 2011 to strengthen information security in Kazakhstan. In 2018 To counter the hackers, Cybershield security systems and Tealab antivirus software were prepared and implemented (https://24.kz/ru/news/social/item/214494-kazakhstan-zanyal-83-mesto-v-globalnom-indekse-po-kiberbezopasnosti).

In the conditions of existing declared and hidden information wars between countries, the development of technologies increasingly increases the problems and risks to cyber security. That is why for almost all countries this issue has become one of the key at the present time. In the system of measures taken in the framework of cyber security, it is planned to provide all government agencies in Kazakhstan with technical and advisory assistance from relevant structures and private organizations, the national information technologies of NITEK, the KZ-CERT computer incident response service. Thus, the institutions themselves will not need to create special cyber security groups, which will largely save the budget.

NITEK is the largest company in the information technology market of Kazakhstan. Since its inception, it has provided various IT project management services, from the initial stage to the completion of work on the creation, implementation and operation of basic components of e-government

and information systems of state bodies. To date, 157 information systems with more than 1,200 integrations within these systems are integrated into an integration network. The same company monitors 296 GO Internet resources and is responsible for storing information from state databases.

To ensure interaction between local, departmental and corporate telecommunications networks of government, subordinate organizations and local governments, NITEC controls about 11 thousand (10982) IP VPN communication channels and more than 1.7 thousand (1783) Internet access channels. NITEK is building partnerships with global companies such as IBM, Microsoft, SAP, Oracle, HP, Adobe, Cisco, Fujitsu-Siemens, VerySign, InterSystems. For joint projects, experts from the USA, Singapore, South Korea, Great Britain, Austria and other countries are involved (https://www.nitec.kz/index.php/pages/test). At the same time, the Computer Incident Response Service (hereinafter - KZ-CERT) has been established in Kazakhstan. It is based in a single center for users of national information systems and the Internet segment, and provides for the collection and analysis of information on computer incidents, as well as advisory and technical support to users to prevent potential threats to computer security. In this regard, KZ-CERT provides assistance to Kazakhstani and foreign legal entities and individuals in identifying, preventing and suppressing illegal activities related to Kazakhstani network resources (http://kz-cert.kz/ru/about).

Information technologies in Kazakhstan have occupied a niche in the provision of services, this is not about production. The domestic market was occupied by active foreign firms. This is the result of insufficient investment in local manufacturing firms and insufficient attention to the training of local professionals in this field.

In 2011, President Nazarbayev at the summit of the Shanghai Cooperation Organization in Astana called for the creation of cyber police to repel network attacks. The United States has experience of such a structure, which earlier than others adopted a tough cyber security doctrine and developed a set of measures to counter cyber threats and cyber terrorism (https://www.youtube.com/watch?v=du68MJ4vfaY).

Along with the already existing new terms, it is necessary to introduce new concepts into international law, such as "e-frontier", "e-sovereignty" and others. Of course, there is some undesirable extreme in the strategy of implementing cyber security, we should not shut off the network flow that carries us constructive ideas and new technologies. However, the rapidly developing international cybercrime is striking in scope and professionalism of actions, according to expert estimates, more than 40 million hackers work in different countries of the world. According to the research, they caused $ 500 billion in damage to states. In our country, they also became more active, and as a result, in 2017, the President of Kazakhstan, Nursultan Nazarbayev, proposed creating a reliable barrier to protect the digital space of the state.

On February 22, 2019, a series of successful attacks on the websites of several universities took place in Kazakhstan. An unknown group of hackers, who call themselves KazHackMe, hacked the websites of AUPET universities, KarSU and the Kazakhstan Institute of Engineering and Technology. They publish all their achievements in their blog.

On March 3, 2019, hackers broke into the official website of the international airport Nursultan Nazarbayev, the Center for Analysis and Investigation of Cyber Attacks reported. The attackers posted an animation on the air harbor site with the words "Hacked be x-groups team vn". Users were left without information on flight schedules.

According to experts, Kazakhstan may experience a wave of attacks on the industrial sector. During 2018, the country ranked high in the top 10 countries in the number of industrial production facilities that had been subjected to cyber-attacks (http://www.akorda.kz/ru/events/segodnya-v-astane-glava-gosudarstva-nursultan-nazarbaev-prinyal-uchastie-v-yubileinom-sammite-shanhaiskoi-organizacii-sotrudnichestva).

It becomes obvious that the arrests of leaders and individual members of large criminal groups in this area did not lead to a cessation of attacks on financial institutions. This means that regional attackers will expand their activities, increasing the quality and scope of attacks, including those in Central Asia. Perhaps their next step will be to conduct attacks through theft and use of biometric data, which are gradually being introduced by financial institutions through user authentication systems.

Next year, we should expect the continuation of cyber attacks on suppliers - small companies that provide services to financial institutions around the world. Providers of specialized financial services for large players, such as money transfer systems, banks and exchanges, software for POS-terminals, ATM, online payment platform, are at risk first.

Experts who have studied the situation in the country, believe that the focus of traditional cybercriminals will be focused on simple goals, as

well as to bypass antifraud solutions. Antifraud is a system for monitoring and preventing fraudulent transactions that checks each payment in real time, passing through dozens and sometimes hundreds of filters. Fraud protection mechanisms work in such a way as to monitor whether there is something "unusual" in the payment. The task of the system is to check each transaction, find "suspicious" moments in it and decide to reject the payment or skip it. The fraud protection system consists of several components: automatic transaction monitoring, which includes many customizable filters, cardholder authentication and card validation mechanisms, as well as monitoring transactions in a "manual" mode in extreme cases. The hardest of all will be those who do not require two-factor authentication during transactions. To bypass antifraud systems, criminals can completely copy all system parameters of the computer and browser (https://new-retail.ru/tehnologii/kak_rabotaet_antifrod6645/).

There is a possibility that bypassing the cybersecurity systems of financial institutions using physical devices connected to the internal network will increase. Cybercriminals may attempt to connect a computer or mini-card, specifically configured to intercept data and then transmit it using a 4G or LTE modem, using an insufficient level of physical security in many networks. These cyber-attacks will also enable attackers to gain access to customer data from various financial institutions.

Remind about themselves and attacks on mobile applications for business. Most likely they will be implemented at the web interface level and through a chain of suppliers. In addition, advanced social engineering campaigns aimed at personnel responsible for remittances will continue. Cybercriminals will continue to attack certain people in companies and financial institutions, convincing them that a large amount of money came from business partners or managers. SIM Swap fraud will also be observed when the SIM card used to log into banking is stolen or duplicated.

The number of automated systems is growing, more and more organizations and individual employees have direct or remote access to the automated process control system. All this gives attackers more opportunities for cyber attacks, while reducing profitability and increasing the risk of traditional attacks forces them to look for new targets.

Today, the general public has almost no access to information about information security problems in industrial companies. In organizations, belief in emergency protection systems and the denial of the objective reality of existing threats prevail. All of this has a negative effect on how owners and managers, as well as staff, assess the risk. The current situation may increase the vulnerability of enterprise systems to attacks, be it random infections or targeted campaigns organized by cybercriminals.

The first local companies that are involved in instrumental audits to assess security for compliance with information security requirements and specialize in the study of the circumstances, causes and conditions of information security incidents, as well as technical research of malicious software appeared on the Kazakhstani market. Developed the first domestic anti-virus protection.

In a number of national companies and private structures, there are divisions for monitoring technical events and technological processes, which are on duty around the clock for quick response to emergency situations.

The prevalence of malware for personal computers and mobile devices is increasing with the number of their users. At the same time, the vast majority of users do not use specialized software to protect their personal computers, smartphones, and tablets.

This factor is exploited by hackers, which every day leads to an increase in the number of attacks aimed at infecting subscriber devices with malicious software.

While the number of subscriber devices connected to the Network is increasing and most users continue to ignore the measures of "digital hygiene" in relation to themselves and their devices, the concept of "Internet of things" only increases the problem of their safe use.

If traditional electronic devices such as personal computers and laptops have the ability to install and update anti-virus software, then the Internet of Things users often do not even know how to secure their operation.

Neglect of security concerns when using Internet resources and social networks leads to an increased risk for privacy, unauthorized use or modification of publicly available personal data, as well as disclosure of personal data of limited access or their extraterritorial accessibility to criminal communities or intelligence structures during their storage in the territory other states.

As part of the actualization of digitalization processes, issues of information security of the country become even more relevant. In this regard, the responsibility for the security of the state lies not only with the government, but also with the

national security committee. Numerous plans for the development of our country, the economy, society set specific tasks for the development of the information society in Kazakhstan, the level of literacy of the population in this area. It should also be borne in mind that in the past three years alone, the amount of illegal content has increased 40 times on the Internet, and this increasing flow requires the establishment of a reliable barrier - "Cybershield of Kazakhstan" (https://informburo.kz/novosti/nazarbaev-segodnya-tankami-voevat-ne-nado-zapustit-virus-i-vsyo.html).

"Cybershield of Kazakhstan" needs special project management. It is necessary to form a pool of current research and development topics to finance them. However, there are different models of project implementation, and this depends on the specifics of a particular project.

In order to effectively implement the "Cybershield of Kazakhstan" concept, reasonable protectionism is needed to support domestic scientists and manufacturers of information security tools. Some measures to support domestic manufacturers are spelled out in the "Cybershield of Kazakhstan" concept, but it is proposed to supplement them with another important element of project management - expertise at open scientific seminars. I believe that this will be an effective measure to identify projects that are truly important for the state, as well as support for domestic startups and researchers. It is also proposed to thoroughly and comprehensively study international experience, in particular, the experience of Russia in the issues of import substitution in the field of information protection.

The first model, the classical one, is when the progress of a scientific project is financed. The second model is when the reward to the winner of the competition is given after the completion of the project. The third model is a public-private partnership. It is necessary to study international experience in the management of knowledge-intensive projects of national importance.

Among other tasks, such as retraining and advanced training, it is necessary jointly with NPP Atameken to assist higher education education in the field of information security, that is, to work out issues related to the development of educational learning standards and the choice of elective disciplines for high-quality training of national personnel in information security.

The cyber defense of Kazakhstan national information security system aims to achieve and maintain a high level of protection of electronic information resources, systems and information and communication infrastructure as a whole against external and internal threats (http://www.adilet.gov.kz/ru/leaflet/kibershchit-kazahstana).

The developers of the domestic antivirus program «Teleb» have set a goal - to find and eliminate the threat before it appears. The system attempts to detect an object before it enters the user's computer. The email message is scanned by the antivirus, and in the event of a threat it will be eliminated. Government agencies and security forces (https://24.kz/ru/news/social/item/214494-kazakhstan-zanyal-83-mesto-v-globalnom-indekse-po-kiberbezopasnosti) use this program.

Specific methods and tools used in cyberspace pose a number of complex questions to responsible structures. They need to determine, firstly, whether an attack on electric grids, which paralyzed the country's economic life, is an act of war, for example? How to calculate the economic damage done? What responses are legitimate from the point of view of international law?

Secondly, given the lack of experience in mastering cyberspace, it can be difficult to distinguish a targeted attack on computer systems from an accidental and unintended malfunction, since the effect in both cases will be the same.

Third, taking into account the fact that cyberspace is a virtual phenomenon and is not geographically localized, it is sometimes impossible to identify the perpetrators of a particular hostile act.

Conclusion

Unlike wars customary for mankind, where there are various conventions and norms governing the conduct of war, cyberspace as a new phenomenon is only being formed, and the existing norms in this situation reveal their inconsistency. Since attacks in cyberspace can affect not only the military, but also the civilian sphere, and also taking into account the difficulty of determining their sources, these actions can become one of the convenient tactical tools for terrorists. Perhaps open discussion and study of this problem, participation in it is not only IT. - specialists, but also professionals from various fields, including lawyers, politicians, public figures, scientists, doctors and other experts, could provide the key to solving these acute problems of the beginning of the 21st century.

References

U.S. National Security: A Reference Handbook. Publishing House: ABC-CLIO, 2010.

Toffler. E. Third Wave (The Third Wave). - Publisher: AST., 2010

Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, Cyberpower and National Security. - Washington, DC: Potomac Books, 2009.

Ronfeldt, D. Cyberocracy is Coming // The Information Society Journal. vol.8 (4), 1992.

Ben-Israel I. and Tabansky L. An Interdisciplinary Look at the Information Age // Military and Strategic Affairs. Issue 3 (3), 2011.

https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

Magazine “Spark”. Publisher: Kommersant JSC. - №39, 04.10.2010, p. 24

https://24.kz/ru/news/social/item/214494-kazakhstan-zanyal-83-mesto-v-globalnom-indekse-po-kiberbezopasnosti

https://www.nitec.kz/index.php/pages/test

http://kz-cert.kz/ru/about

https://www.youtube.com/watch?v=du68MJ4vfaY

http://www.akorda.kz/ru/events/segodnya-v-astane-glava-gosudarstva-nursultan-nazarbaev-prinyal-uchastie-v-yubileinom-sammite-shanhaiskoi-organizacii-sotrudnichestva

https://new-retail.ru/tehnologii/kak_rabotaet_antifrod6645/

Pitolin E. Cyber Threats-2019. https://forbes.kz/blogs/blogsid_192920

https://informburo.kz/novosti/nazarbaev-segodnya-tankami-voevat-ne-nado-zapustit-virus-i-vsyo.html

http://www.adilet.gov.kz/ru/leaflet/kibershchit-kazahstana

https://24.kz/ru/news/social/item/214494-kazakhstan-zanyal-83-mesto-v-globalnom-indekse-po-kiberbezopasnosti