МРНТИ 78. (81.93.29)
https://doi.org/10.56132/2791-3368.2023.1-49-04

S.V. Ashenova[1], Li Huiyuan[2]

[1]*International University of Information Technologies, Almaty, Kazakhstan*
[2]*Peking University, Pekin, China*
*(E- mail: saule_ashenova@mail.ru)**

The importance of information security as an integral part of the cyber security program

The development of Internet technologies has led to the problems of ensuring information security and the emergence of risks and threats both for Internet users and for society as a whole. The key concept of cyber security, which previously included primarily technological tools, has now been expanded due to the concepts of virtual communication and virtual extremism. Human capital, as one of the factors of cybersecurity, becoming the object of information influence, can be just as susceptible to cyber attacks as information systems themselves. The article discusses the importance of research approaches in this direction in the context of the fact that it can be of great importance in the education of the personnel of the armed forces of the country, since the security of the state largely depends on them.

Keywords: information space, internet communications, cybersecurity, information security, human capital, armed forces, information threats.

Introduction

Today, information has become a powerful, tangible resource that has even greater value than natural, financial, labor and other resources. Information has become a commodity that is sold and bought. Moreover, it has become a weapon, information wars of various scales and intensity are being waged everywhere. In such conditions, the more common phenomenon of influencing public opinion is not the media, radio and television, but online platforms, networks and mass media operating on the Internet.

It is not for nothing that the XXI century is called the century of high information technologies: the main feature of modernity is computerization and the introduction of the latest means of communication into the sphere of society, technological progress has contributed to the transformation of all communication interactions. The unprecedented growth in the volume of information flows and the possibility of immediate feedback have also influenced the field of political activity, stimulating scientific and practical interest in studying in a new light the issues of the implementation of democratic procedures, the formation of civil society.

Methodological basis

The principles of cognition of social, scientific, empirical phenomena, problems of information security in the context of reorganization and changes of

such a flexible phenomenon as the information environment have determined such methods of cognition as empirical, analysis and synthesis of theoretical material; method of comparison, comparative analysis; meaningful. These methods allowed us to investigate the main trends in the definition of information risks and their impact on the structure of information security in the context of the importance of cybersecurity issues for the state

Main body

The use of technical means in public life has led to the creation of a specific type of mass communication that occurs between the subjects of society and the information space [1]. If during the XX century the main means of mass communication were traditional channels of communication: printed publications and electronic means of communication, then the beginning of the new century was marked by the active development of Internet technologies that qualitatively chan ged the nature of politics, giving it virtual characteristics. Thanks to new opportunities, mass political communication has increased the speed of information dissemination, reaching the consumer in the shortest possible time. The large volume of transmitted information, brevity and memorable imagery of messages increased the intensity of the impact on the audience. The blogosphere, electronic media, social networks, portals, forums and websites, online communications are constantly updated and have an increasingly significant impact on public opinion.

Internet communications give impetus to the development of civil society, promote publicity and openness of social and political processes. In a short time, they provide an effective dialogue between the authorities and society and allow interaction directly with the target audience. The Internet is a kind of an information base that stores and reproduces an unlimited amount of information and provides quick access to a significant audience [2]. They also play an important role in the development of civil society, expanding the possibility of social control of power through network technologies. At the same time, with the development of Internet technologies, the issue of cyber security is becoming acute, which includes the protection of information, but is not limited to it. This is protection against viruses, hacker attacks, data forgery, which can not only delete or steal data, but also affect the work and productivity of employees, use information against a person or structure. Cyber security today is responsible for three factors: systems, processes, and people. Let's consider the most vulnerable, in our opinion, position from the point of view of external non–technological impact - «people». Which, in our opinion, allows us to assert that the concept of information security is today one of the segments of cyber security.

President of Kazakhstan K-Zh. Tokayev, having approved the National Security Strategy for 2021-2025, stressed that the main focus of the program is on countering the key challenges that are projected for the next five years and on ensuring security in the field of human capital – first of all, preserving and multiplying the intellectual potential of the nation [3]. The transition to new criteria

of management strategies based on a competent ideology of the development of a modern democratic society, the implementation of conditions for a social elevator accessible to modern youth, holistic support for the accumulation of intellectual resources; which, in turn, affects the development of the state; cannot but be based on the tasks set by the criteria of national and information security of the country. Intellectual potential as the basis of state management activity is becoming one of the most important resources for ensuring the national security of the country. In turn, the implementation of national state policy is closely related to the need to analyze the role of information security in the context of its impact on the life and stability of a democratic society.

In accordance with research approaches, information security – the ability of the state, society, social group, individual to provide, with a certain probability, sufficient and protected information resources and information flows to maintain vital activity, sustainable functioning and development, to resist information hazards and threats, negative information impacts on the individual and public consciousness of people, as well as on computer networks and other technical sources of information, to develop personal and group skills and safe behavior skills, maintain constant readiness for adequate measures in the information confrontation, no matter who imposed it [4].

Of particular importance today is the use of information systems in the formation of an effective system of management and education of the personnel of the armed forces of the country, since becoming the object of information influence, cadets and young officers automatically bear more responsibility for the decisions taken than the civilian population, being the bulwark and guarantor of the security of the state. The likely enemy will primarily consider this human component as a priority object of its influence, which also requires taking measures for the information protection of military personnel.

The Military Doctrine of the Republic of Kazakhstan notes that the use of diplomatic, political, legal, economic and other non-military means is a priority for the protection of the national interests of the country [5].

The Law of the Republic of Kazakhstan "On National Security of the Republic of Kazakhstan" clearly defines the threats that relate to the information sphere, including:

– violation of the integrity (distortion, substitution, destruction) of information, software and other resources, as well as falsification (forgery) of documents;

– malfunction (disorganization of work) of information systems and communication networks, blocking of information,

– violation of technological processes, disruption of timely problem solving;

– cybercrime in order to establish information dominance;

– information and intelligence operations;

– electronic warfare in order to suppress (disable) technical means of communication and data transmission [6].

These threats have been realized in an active and constantly growing information confrontation between individual countries, military-political alliances

of states, as well as between countries and terrorist organizations, which are usually reflected in the conduct of information wars. Researchers believe that the main directions of ensuring information security in the Armed Forces, other troops and military formations of Kazakhstan are: constant analysis and identification of threats to information security, their sources; improvement of information security tools against unauthorized access, development of secure communication and management systems; certification of software and information security tools; improvement of the structure of information security bodies and coordination of their interaction; improvement of information security techniques and methods; training of information security specialists [7]. If we pay attention to the possibilities of using non-military means, which are mentioned in the Military Doctrine and associated with the concept of threats to information security, then first of all we need to pay attention to the opportunities that the Internet now provides for manipulating consciousness. Of course, technology and technology win wars, but modern methods of information influence can greatly enhance this opportunity.

As mentioned earlier, information today may well be considered an effective type of weapon, as it affects the mind and can undermine the situation in the country from the inside. We can observe this on the example of information wars and technologies of spreading disinformation. During 2020, when anti-racist protests were at their height and against the background of a surge in COVID-19 cases, the human rights organization Avaaz conducted a study that showed that the 100 most «active disinformants» received millions more interactions on Facebook than the top 100 accounts of traditional US media combined. «The scary thing is that it's only for the top 100 accounts – it's not the whole universe of misinformation», – says Fadi Koran, Avaaz campaign director who worked on the report. «It doesn't even include Facebook groups, so their number is likely much larger. In this case, we made a very, very rough estimate» [8]. Facebook's Avaaz identified the 100 most active disinformants on Facebook who shared at least three misinformation posts, according to Facebook's third-party fact-checkers definition, including two within 90 days of each other. On average, the 100 most active disinformants shared eight confirmed misinformation posts each. They refused to correct them after they were flagged by Facebook-related fact checkers.

The susceptibility of people to suggestion, which arises as a result of the suppression of the rational principle of a person in a crowd, creates favorable conditions for the introduction of any ideas and views into the mass consciousness, especially with the help of new information technologies. Their appearance has changed the very ways of expressing protest sentiments and the possibilities of creating revolutionary situations. The so-called «Twitter revolutions» in the XXI century have become an alternative source of influence and regulation of mass unrest. The ability to independently control the selection of facts that did not always meet the principles of fact-checking from different sources gave readers of social networks the illusion of absolute rightness, since, according to most, traditional sources of information filter news at their own discretion, in accordance with editorial policy and in favor of power structures. After the events in Egypt in

2011, the world finally realized the colossal power of social networks in organizing protest movements. When Twitter was actively used at the Iranian protests of 2009, it could be attributed to a combination of circumstances when a protest Tunisian turned to social networks - by coincidence. But with the beginning of unrest in Egypt, a new era finally came. Since in Egypt, Twitter actually played the role of the organizer of the uprising, while its participants did not have a definite leader [9].

Unfortunately, information technologies are actively being adopted by destructive organizations that pose a threat to the national security of countries. We are talking primarily about terrorist organizations and the acts organized by them. Banned in many countries, ISIS actively conducted an information campaign, which researchers considered one of the most successful information wars aimed at capturing virtual space, where victory is achieved through tweets and viral photos. During the assault on Mosul, 40,000 tweets brought the hashtags of terrorists to the top, manipulating the agenda and causing panic with a virtual attack. Thousands of terrifying tweets were published with promises of death to the resisters, stories about killed, executed soldiers, photos of beheaded or crucified bodies. The virtual attack on the city worked in such a way that, according to The Guardian, the defenders of Mosul left their posts only after seeing the symbols of ISIS. The Washington Post, citing a competent source, reported that during the first weeks of the crisis in Iraq, almost ninety thousand soldiers were deserted [10].

Informational and psychological confrontation has long and firmly become an integral component of the preparation and conduct of combat operations. Moreover, in the armies of Western states, the theory and practice of full-scale information and psychological warfare against the troops and population of a possible enemy are intensively developing, special structures and units are being created. This is a global issue that our country cannot stay away from. The Armed Forces of Kazakhstan are systematically working on the formation of national potential in the field of cyberspace and the implementation of the Cybersecurity Concept «Cyber Shield of Kazakhstan».

Noting that every day the world faces millions of cyber attacks in absolutely all spheres of life, the Ministry of Defense of the Republic of Kazakhstan commissioned in 2020 cyber threat recognition systems, target attack analyzers, an antivirus security center and planned to carry out a complete re-equipment of the information (cyber) security units of the Armed Forces with modern software and hardware and information protection systems [11].

But along with this, information methods have become one of the most important elements of the military potential of states, complementing and sometimes replacing military means. Back in 1993, American political strategist Jim Sharp published the book «From Dictatorship to Democracy», which will later be translated into more than 30 languages of the world and will become a reference book of revolutionaries. In his book, he described in detail how to change the current political system and gave 198 specific recommendations for changing the political regime. «It is possible to mobilize world public opinion as much as possible, condemning the dictatorship on humanitarian, moral and religious

grounds. But this is only a modest addition. We can make sure that governmental and international organizations apply diplomatic, political and economic sanctions against the dictatorship» D. Sharpe gave such recommendations in his book, focusing on working with public opinion. Often, for this purpose, work is carried out in the youth environment and among student organizations, thereby accumulating the potential of future resistance. The researcher considered this stage to be realistic planning: «It is important to remember that often many people should participate in actions. Their reliability directly depends on high standards…It is necessary to determine in advance which leadership structure and communication system are most suitable for starting resistance. It is also important what means of communication and solutions will be possible in the course of the struggle in order to ensure constant leadership by both activists and the population as a whole» [12].

Conclusion

With the advent of information threats, the specifics of working with society have advanced so much, that today no country in the world can consider itself protected from cross-border information threats and able to solve information security problems alone. Consequently, global trends and interstate agreements in matters of information security are of great importance for any state. Modern democracy presupposes the participation of citizens in the processes of public life, is based on broad awareness of citizens, it ensures the development of opinions and solutions in the context of a broad discussion in the movement towards agreement. The states-players of the world space are obliged to strive to develop confidence-building measures, including in the field of military use of the information space.

When developing political and legal acts that ensure the information and national security of the country in Kazakhstam, international experience in the field of security of countries such as the USA, Great Britain, Canada, the Russian Federation, India, Estonia was taken into account. The exchange of national concepts of ensuring security in the information space is one of the successful experiences of interaction between states in this matter, but in addition, a well-established operational exchange of information about possible threats in the information space and the development of coordinated measures, consultation agreements, exchange of experience and holding international meetings to strengthen cooperation in resolving military conflict situations is necessary. It should also be noted that the legal mechanisms for ensuring information security and defense need constant monitoring and improvement, since new technologies of the information society do not stand still and the faster their development goes, the more the risks of information threats will increase.

Список литературы:

1. Априянц К.В. «Твиттер-революции»: микроблоги как инструмент выражения протестных настроений гражданского общества // Вестник ВГУ. Серия: Филология. Журналистика. – 2014. – №1. – С. 118-121.

2. Avaaz.org: Мир в действии. [Электронный ресурс]. – Режим доступа: https://secure. avaaz. Org /campaign/ru/disinformation_briefing/ (дата обращения:17.12.2022).

3. Васильченко В. Джихад в Twitter //Antiterror today 26.07.2014. [Электронный ресурс]. – Режим доступа: https://www.antiterrortoday.com/terrorizm/terrorizm-v-informatsionnom-prostranstve /5021 dzhikhad-v-twitter (дата обращения: 18.12.2022).

4. Внуков А.А. Защита информации: учебное пособие для вузов / А. А. Внуков. – 3-е изд., перераб. и доп. – М.: Издательство Юрайт, 2023. – 161 с.

5. Военная доктрина Республики Казахстан [Электронный ресурс]. – Режим доступа: https: //www. akorda.kz/ru/security_council/national_security/voennuyu-doktrinu-respubliki-kazahstan (дата обращения: 24.12.2022).

6. Головин Ю.А. Публичная политика как пространство легитимации власти // Политика и общество. – 2012. – №4. – С. 12-13.

7. Д. Шарп. От диктатуры к демократии. [Электронный ресурс]. – Режим доступа: https://www.aeinstein.org/wp-content/uploads/2013/10/FDTD_Russian.pdf (дата обращения: 24.12.2022).

8. Закон Республики Казахстан «О национальной безопасности Республики Казахстан» [Электронный ресурс]. – Режим доступа: https:/ /adilet. zan.kz/ eng/ docs/ Z1200000527 (дата обращения: 18.12.2022).

9. Кулпендиев Б., Тлеулесов Б. [и др.]. Информационная безопасность: состояние и перспективы развития в Казахстане // Sarbaz. 2017. – №44. – С. 11-12.

10. По ту сторону киберщита армии. [Электронный ресурс]. – Режим доступа https: // mail. kz/ru/news/kz-news/po-tu-storonu-kibershchita-armii. (дата обращения: 01.03.2023).

11. Рогова И. Становление и развитие современной казахстанской государственности. – Нур-Султан, Издательство: РГП, 2019. – С. 17-18.

12. Сковиков А.К. Гаэтано Моска об актах политического управления и власти // Polit Book. – 2012. – №4. – С. 128-129.

13. Токаев К.К. Стратегия нацбезопасности РК на 2021-2025 годы. [Электронный ресурс]. – Режим доступа: https://informburo.kz/novosti/tokaev-utverdil-strategiyu-nacbezopasnosti-271059194 (дата обращения: 21.12.2022).

С.В. Ашенова, Li Huiyuan

Ақпараттық қауіпсіздіктің киберқауіпсіздік бағдарламасының құрамдас бөлігі ретіндегі маңыздылығы

Интернет-технологиялардың дамуы ақпараттық қауіпсіздікті қамтамасыз ету проблемасына және интернет желісін пайдаланушылар үшін де, жалпы қоғам үшін де қауіп-қатер туғызуы мүмкін. Бірінші кезекте технологиялық құралдарды қамтитын Киберқауіпсіздіктің негізгі тұжырымдамасы бүгінгі күні виртуалды коммуникация және виртуалды экстремизм ұғымдарының есебінен кеңейтілді. Адами капитал киберқауіпсіздік факторларының бірі ретінде ақпараттық әсер ету объектісіне айнала отырып, тікелей ақпараттық жүйелер сияқты кибершабуылдарға ұшырауы мүмкін. Мақалада осы бағыттың зерттеу тәсілдерінің маңыздылығы қарастырылады, еліміздің Қарулы Күштерінің жеке құрамын тәрбиелеуде үлкен маңызға ие, өйткені мемлекеттің қауіпсіздігін қамтамасыз ету қорғаныс саласымен тікелей байланысты.

Кілт сөздер: ақпараттық кеңістік, интернет байланысы, киберқауіпсіздік, Ақпараттық қауіпсіздік, адами капитал, Қарулы Күштер, ақпараттық қауіптер.

С.В. Ашенова, Li Huiyuan

Важность информационной безопасности как составной части программы кибербезопасности

Развитие интернет-технологий привело к проблематике обеспечения информационной безопасности и возникновения рисков и угроз как для пользователей интернет-сети, так и для общества в целом. Ключевое понятие кибербезопасности, включавшее ранее в себя в первую очередь технологический инструментарий, сегодня расширено за счет понятий виртуальной коммуникации и виртуального экстремизма. Человеческий капитал, как один из факторов кибербезопасности, становясь объектом информационного воздействия, может быть так же подвержен кибератакам, как и непосредственно информационные системы. В статье рассматривается важность исследовательских подходов в этом направлении в контексте того, что это может иметь большое значение при воспитании личного состава вооруженных сил страны, так как от них во многом зависит обеспечение безопасности государства.

Ключевые слова: информационное пространство, интернет-коммуникации, кибербезопасность, информационная безопасность, человеческий капитал, вооруженные силы, информационные угрозы

References:

1. Apriyants, K.V. (2014). «Tvitter-revolüsii»: mikroblogi kak instrument vyrajenia protestnyh nastroeni grajdanskogo obşestva [Twitter Revolutions: Microblogs as a tool for expressing protest sentiments of civil society. Bulletin of the VSU. Series: Philology. Journalism. No1. P. 118-121.

2. Avaaz. (2020). Mir v deistvii. [The World in Action]. – Retrieved from: https:// secure. avaaz. org/ campaign /ru /disinformation_briefing/ (in Russian).

3. Vasilchenko, V. (2014). Jihad v Twitter [Jihad on Twitter]. Antiterror toda. – Retrieved from: https://antiterrortoday.com/terrorizm/terrorizm-v-informatsionnom.

4. Vnukov, A.A. (2023). Zaşita informasii [Information protection a textbook for universities]. (3 rd ed.). – Moscow: Yurayt Publishing House. – 161 p.

5. Voennaia doktrina Respubliki Kazahstan [Military Doctrine of the Republic of Kazakhstan] (2017, September 29). – Retrieved from: https:// www.akorda. kz/ru/security_ council /national _security/voennuyu-doktrinu-respubliki-kazahstan (in Russian).

6. Golovin, Yu.A. (2012). Publichnaia politika kak prostranstvo legitimasii vlasti [Public policy as a space of legitimization of power]. Politics and Society. No.4. P. – 12-13.

7. Sharp G. Ot diktatury k demokratii [From dictatorship to democracy]. Microsoft Word - FDTD_Russian.doc (aeinstein.org). – Retrieved from: https://www.aeinstein. org/wp-content /uploads/ 2013/ (in Russian).

8. Zakon Respubliki Kazahstan «O nasionälnoi bezopasnosti Respubliki Kazahstan» [The Law of the Republic of Kazakhstan "On National Security of the Republic of Kazakhstan]. (with amendments and additions as of 02/26/2023). Retrieved from:https: //adilet. zan.kz /eng/docs/ Z1200000527 (in Russian).

9. Kulpendiev, B., Tleulesov, B. İnformasionnaia bezopasnöst: sostoianie i perspektivy razvitia v Kazahstane [Information security: The state and prospects of development in Kazakhstan]. Republican military-patriotic newspaper Sarbaz. No.44. P. 17-18.

10. Po tu storonu kiberşita armii. [On the other side of the army's cyber shield]. – Retrieved from: https: // mail. kz/ru/ news /kz- news/po-tu-storonu-kibershchita-armii. (in Russian).

11. Rogov, I. (2019). Stanovlenie i razvitie sovremennoi kazahstanskoi gosudarstvenosti [Formation and development of modern Kazakh statehood]. edited by I. Rogov. Nur-Sultan,

Publishing House: RGP. P. 17-18.

12. Skovikov, A.K. (2012). Gaetano Moska ob aktorah politicheskogo upravlenia i vlasti [Gaetano Mosca on the actors of political governance and power]. PolitBook. No. 4. P. 128-129.

13. Tokayev K.K. Strategia nasbezopasnosti RK na 2021-2025 gody. approved the National Security Strategy of the Republic of Kazakhstan for 2021-2025. What is important in this document (2021, June 21). – Retrieved from: https://informburo.kz/novosti/tokaev-utverdil-strategiyu-nacbezopasnosti-rk-na-2021-2025-gody-chto-vazhnogo-v-etom-dokumente?ysclid =lf3nhutz2z271059194. (in Kaz).

Ашенова Сауле Викторовна	саяси ғылымдарының кандидаты, Халықаралық ақпараттық технологиялар университетінің қауымдастырылған профессоры, Алматы, Қазақстан
Ашенова Сауле Викторовна	кандидат политических наук, ассоцированный профессор Международного университета информационных технологии, Алматы, Казахстан
Ashenova Saule	candidate of Political Sciences, assistant-professor International University of Information Technologie, Almaty, Kazakhstan

Li Huiyuan	Пекин университетінің магистрі, Пекин, Қытай
Li Huiyuan	магистр Пекинского университета, Пекин, Китай
Li Huiyuan	master, Peking university, Pekin, China