RELEVANT ENVIRONMENT OF CENTRAL ASIA IN CYBER-SECURITY POLICY

УДК 327

Abstract. In the century of the widespread use of high technologies and the Internet, cybercrime is one of the major threats to international peace and security. All groups ranging from individuals, businesses to governments are exposed to cyberattacks. Large cyberattacks in the region have mostly criminal nature desiring to have access to financial and industrial data, to realize financial operations, to use of the information and material contained in web sites, data-bases of government agencies. As a result of analysis of cyberattacks, we have an opportunity to identify weaknesses, which contributes to the subsequent improvement of system services. It can be also noted that countries of these regions create institutions to combat cybercrime at the state level and improve their regulatory instruments. At the same time, there is a process of collaboration with using of their resources and efforts to prevent internal and external threats in cyberspace by taking into account the peculiarities and opportunities of each country.

Key words: cyber-security, Central Asia, national security, Cyber-security Council, Cybersecurity Concept, regional integration.

Аңдатпа. Жоғары технологиялар мен ғаламтор кең тараған заманда киберқылмыс - халықаралық бейбітшілік пен қауіпсіздіктің басты қауіпі болып табылады. Барлық топтар, жеке тұлғалардан бастап үкіметтерге дейін кибершабуылға ұшырайды. Аймақта ірі кибершабуылдар көбінесе қылмыстық сипатқа ие, қаржылық және өндірістік деректерге қол жеткізуге, қаржылық операцияларды жүзеге асыруға, веб-сайттардағы ақпараттар мен материалдарға, мемлекеттік органдардың деректер базасына қол жеткізуді қалайды. Кибершабуылдарды талдау нәтижесінде жүйелік қызметтерді одан әрі жетілдіруге ықпал ететін кемшіліктерді анықтау мүмкін болады. Аймақта елдердің киберқылмыспен мемлекеттік деңгейде күресу және олардың нормативтік құралдарын жетілдіру үшін институттар құратындығын атап өту керек. Сонымен бірге, мемлекеттерге қол жетімді ресурстарды және киберкеңістіктегі ішкі және сыртқы қауіптерді болдырмау жөніндегі күш-жігерді пайдалана отырып, әр елдің қабілеті мен мүмкіндіктеріне сай ынтымақтастық үдерісі жүріп жатыр.

Тірек сөздер: киберқауіпсіздік, Орталық Азия, ұлттық қауіпсіздік, киберқауіпсіздік кеңесі, киберқауіпсіздік тұжырымдамасы, аймақтық интеграция.

Аннтотация. В век широко распространенного использования высоких технологий и Интернета киберпреступность является одной из основных угроз международному миру и безопасности. Все группы, от частных лиц, предприятий до правительств, подвергаются кибератакам. Крупные кибератаки в регионе носят в основном криминальный характер, желающие иметь доступ к финансовым и промышленным данным, осуществлять финансовые операции, использовать информацию и материалы, содержащиеся на веб-сайтах, базы данных государственных учреждений. В результате анализа кибер-атак появляется возможность выявить недостатки, которые способствуют последующему улучшению системных услуг. Следует отметить, что страны региона создают институты для борьбы с киберпреступностью на государственном уровне и улучшают свои нормативные инструменты. В то же время наблюдается процесс сотрудничества с использованием имеющихся у государств ресурсов и усилий по предотвращению внутренних и внешних угроз в киберпространстве с учетом особенностей и возможностей каждой страны.

Ключевые слова: кибербезопасность, Центральная Азия, национальная безопасность, Совет по кибербезопасности, Концепция кибербезопасности, региональная интеграция.
JEL code: F5

ZH. KERIMKUL master of International Relations

A. KUSSAINOVA PhD., Associate Professor of International Relations Department
L.N. Gumilyov Eurasian National University

At the beginning of the 21st century, the information and communications technology has continued to advance rapidly. Today, many users choose the information space as the repository for data and information, even the states are focused to develop the electronic government. Many financial transactions, banking services available online. The development of information and communication technologies has led to the need to provide security conditions in order to prevent cyber threats with different nature for all social groups. Victims of cyber-attacks and private information leaks become users of the Internet, governments as well as business structure.

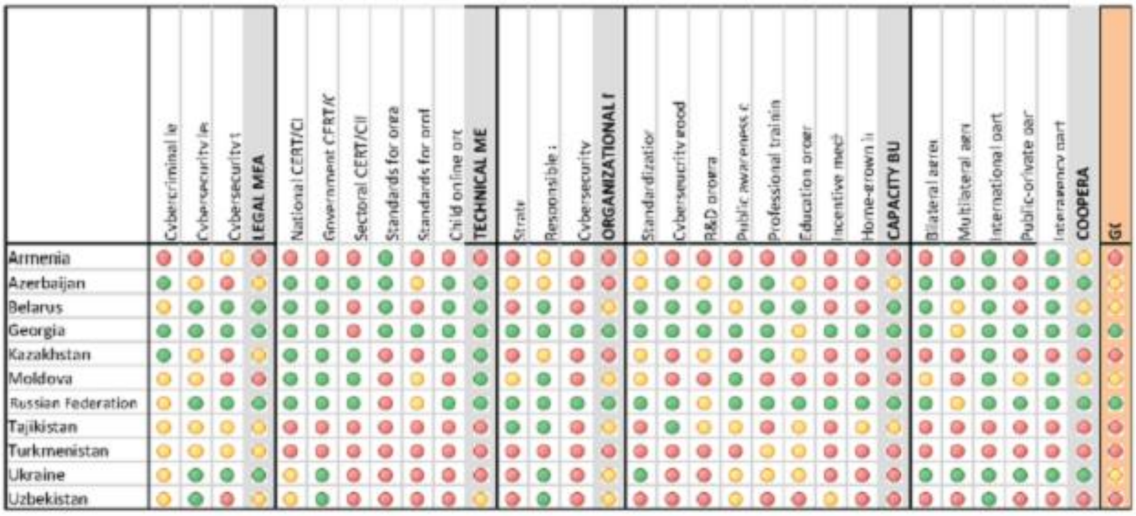
For this reason, the implementation of relevant activities to ensure cybersecurity requires an integrated approach. States, international and regional integrations aim to create a common understanding of problems and methods for their settlement. The development of a legal framework at the national and international level provides an opportunity to achieve the basic concepts, ensure cybersecurity and amend the states' legislation. International cooperation against the cybercrime contributes to the future elimination of cyber threats.

However, there are differences between states on the level of interest and development degree. Priority areas for ensuring cyber protection are varied, if the protection of the government information base is the main task for someone, the protection against cyber-attacks on personal, corporate financial data make difficulty for another.

Cybercrime has considerable negative effects for the sustainable development of the country, its defense, domestic and foreign policy, economy, also for livelihoods of the population. The issue of ensuring cybersecurity is a task that falls to all law enforcement agencies of the state. The private sector, the civil society are also interested in ensuring common security policy in coordination with the government. Activities of research institutes, private organizations to ensure information security contribute to the development of technical side of this issue. That looks easier solving the task of establishing a single legislative base for states. Holding international workshops is a platform for sharing knowledge and experiences to understand real threats.

Methodology of this paper is based on studying social processes and phenomena. The nature of the assigned research tasks predetermined the need to use also such methods as the comparative-historical, comparative-legislative, method of system analysis and the sociological method. Method of comparisons effected to analyze different degrees of the legislative basis of national and international law, development of states and corporations on the problems of research. The empirical basis for research of the current situation of international and regional cooperation consists of statistical data on cybercrime compiled by international organizations, national and international laws, content analysis of international institutes, data on cybercrime in the Republic of the Kazakhstan and Central-Asian countries.

For Central Asian countries, the issue of ensuring cybersecurity is becoming increasingly discussed. In recent years, countries are making fullest efforts in their first steps to create a legal framework for resolving these problems. Nowadays it can be noted that their efforts show a clear understanding of the situation, and their phased approach. But according to the Global cybersecurity index 2017 which evaluates on five pillars as legal, technical, organizational, capacity building and cooperation [1], Central Asian states demonstrate low rates and that needs to include this issue to essential regional danger *(See Table 1 and 2).*



	Cybercriminal le	Cybersecurity le	Cybersecurity t	LEGAL MEA	National CERT/CI	Government CERT/C	Sectoral CERT/CII	Standards for orga	Standards for prof	Child online pr	TECHNICAL ME	Strate	Responsible	Cybersecurity	ORGANIZATIONAL I	Standardizatio	Cybersecurity good	R&D progra	Public awareness c	Professional trainin	Education progr	Incentive mech	Home-grown i	CAPACITY BU	Bilateral agree	Multilateral agre	International part	Public-private par	Interagency part	COOPERA	GC
Armenia	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🔴
Azerbaijan	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟡	🟡	🔴	🔴	🟡	🟢	🟡	🟢	🟢	🟡	🔴	🔴	🟡	🟢	🟢	🟢	🔴	🟢	🟢	🟡
Belarus	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🔴	🟢	🟢	🔴	🟢	🔴	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🔴	🟢	🟢	🟡	🟢	🔴	🟢	🟡	🟡
Georgia	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢
Kazakhstan	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🔴	🔴	🟢	🟢	🔴	🟡	🔴	🔴	🟡	🔴	🟡	🔴	🟢	🟡	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴
Moldova	🟡	🟡	🔴	🔴	🟢	🟢	🟢	🔴	🟡	🔴	🟢	🟡	🟢	🔴	🟡	🟡	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🟡	🟢	🟡	🟡
Russian Federation	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢
Tajikistan	🟡	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🟢	🔴	🟡	🔴	🟢	🟡	🟡	🔴	🟡	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Turkmenistan	🟡	🟡	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Ukraine	🟡	🟢	🟢	🟢	🟡	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟡	🟢	🔴	🔴	🟡	🟡	🟡	🔴	🔴	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟡
Uzbekistan	🟡	🟢	🔴	🟡	🟡	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🟢	🔴	🟡	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴

Table 1. CIS region scorecard, Global cybersecurity index 2017 [1].

COMMONWEALTH OF INDEPENDANT STATES (CIS)	Region Score	Global Rank
Georgia	0.819	8
Russian Federation	0.788	10
Belarus	0.592	39
Azerbaijan	0.559	48
Ukraine	0.501	59
Moldova	0.418	73
Kazakhstan	0.352	83
Tajikistan	0.292	91
Uzbekistan	0.277	93
Kyrgyzstan	0.270	97
Armenia	0.196	111
Turkmenistan	0.133	132

Table 2. ITU Member States Global Cybersecurity Commitment Score By Region, Global cybersecurity index 2017 [1].

In turn, Kazakhstan is certainly considered cyber-threats as one of the new threats to national security. The state rapidly includes a new threat of global dimension in its security policy and recognizes the devastating impact for the country's development.

The issues of cybersecurity in the national legislation of the Republic of Kazakhstan are still at the initial stage. The government constantly conducts comprehensive measures aimed to ensure the optimal operation of e-government, protect of electronic information resources and information systems from external and internal threats. The State Technical Service carries out an annual certification of the sustainable operation of government information systems [2]. All this makes it possible to identify vulnerabilities for further elimination and creation of new ways to deal with the problem.

The Law of the Republic of Kazakhstan "On informatization" of November 24, 2015 [3] is one of the first documents to ensure the security of the information infrastructure. Significant progress in securing cybersecurity was made by the creation of the Committee of information security under the Ministry of Defense and Aerospace Industry of the Republic of Kazakhstan [4]. As a result of the Message to the people of Kazakhstan (January 31, 2017), "The Third Modernization of Kazakhstan: Global Competitiveness", a new Cybersecurity Concept (Концепция кибербезопасности «Киберщит Казахстана») [4] was proposed, taking into account the approaches of the "Kazakhstan-2050 Strategy", which defined the basic definitions and priorities for the fight against cybercrime. The concept analyses of the current situation, explains effected works in the information and communication infrastructure, ensuring information security, protecting the secured operations of information objects, and has been identified the key problems. The concept expanded the previous legislation, based on the experience of foreign countries in accordance with the international standards.

Also, the Action Plan on implementation of the Cybersecurity Concept («Киберщит Казахстана») until 2022 defines a strategy for the overall operation of state agencies to achieve the intended goals. A significant step is the increase of government educational grants in order to provide highly qualified professionals. At the same time, the growth of private organizations and research centers in Kazakhstan who study this issues make large consultation to government and businesses by the testing their information bases to cyber-attack [4].

Therefore, today Kazakhstan is now on the right path toward to ensure information security, where the activities of government structures are defined on the prevention threats for the state's national security.

In Uzbekistan, the creation of secure cyberspace has fast gathered. The Government of Uzbekistan considers the improvement of ICT and ensuring cybersecurity as one of the priority directions in the growth of the national economy of the country on the Strategy for Action on the five priority development directions of the Republic of Uzbekistan in 2017-2021 [5].

A fundamental step for Uzbekistan was the creation of the Information Security Concept, as in the case of Kazakhstan. This Concept will be focused on the strategic definition of basic measures to ensure cybersecurity. Taking into account the fact that today Uzbekistan is focused on expanding the use of information technology, the introduction of e-government, the adoption of the concept will give more clear visions considering all the perspectives at the initial stage. Involvement into the drafting of the concept the specialized bodies, civil society and the private sector demonstrates a common high interest in the feasibility on preventing possible threats. In this regard, it is necessary to note the leading role of the Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan and the Center for Information and Public Security. The Center conducts statistics on the quantity and direction of cyber-attacks, which revealed their growth in 2017 compared to 2016. Recommendations of the Center's experts contribute to improve information resources of the public and private sectors [6].

The situation of ensuring cybersecurity in Kyrgyzstan is at first stage unlike neighboring countries. From recent, specialized bodies such as the Committee on Information Technologies and Communication have begun a study to determine the current situation, and they prevue the future design of the national strategy on the control cyberspace [7] as part of the Digital CASA-Kyrgyzstan project in conjunction with the World Bank office in Bishkek and the Global Center for Cybersecurity Development (Oxford University, UK). A great advantage offered is the involvement of foreign experts in consulting work as Russian experts who are well acquainted with the cyberspace of the region [8]. In the second half of 2017, the Analytical Security Center was established, which is aimed to carry out complex work on monitoring the situation of ICT, creating a state plan and strategy for cybersecurity.

Improving the cyberspace of Kyrgyzstan requires a qualitative approach to solving the problem, as well as defining a national strategy in connection with the implementation of the nationwide digital transformation program "Taza Coom" [9]. In the effected work, it is noticed the close participation of civil society, private organizations and NGOs (Civil Initiative of Internet Policy).

Among the case of Tajikistan, the definition of cybercrime is presented only in the Criminal Code. They have no legislation to resolve this contemporary issue. However, special agencies for cybercrime under the Office for Combating Organized Crime and the Criminal Investigation of the Ministry of Internal Affairs realize monitoring the Internet consultations by the citizens in order to prevent the establishment of links with terrorist organizations.

Cyber security does not create broad problems for the government of Turkmenistan, given the level of censorship [10] and limited access to Internet resources [11]. However, at the 72nd session of the General Assembly of the United Nations, representatives of Turkmenistan proposed a fundamental approach to the issue of ensuring global cybersecurity [12] in accordance with the development of the contemporary world.

Thus, it can be noted that the countries of Central Asia are developing at the initial level in the issue of cybersecurity and differ from each other. But at the same time, the states are trying to put this problem in the priority, establishing a confidential dialogue between the countries. And there is a process of sharing information and knowledge to ensure regional stability.

In 2017, the Central Asian Forum on Internet Governance in Dushanbe was held for the second time [13]. This platform is an excellent example of cooperation, where all professionals from the public and private services gathered to discuss a common issue and identify the main threats facing all areas.

Since 2006, the SCO has been operating a group of experts on international information security. Meetings held by a group of experts improve the quality and understanding of the situation among experts, which in turn contributes to the development of control methods at the state level. The main document in this sphere is the Agreement among the Governments of the SCO member States on cooperation in the field of ensuring international information security in 2009 [14]. The Astana Declaration of 2017 defined the role of cybersecurity in cooperation within the SCO framework arguing that "member states will continue to strengthen practical cooperation on countering propaganda and the justification of terrorism, separatism and extremism in the information space" [15].

A new initiative in the region is the aim of creation a Cybersecurity Council, for which already the necessary negotiations are held by the parties [16]. Also at the end of 2017 on the summit with participation of the heads of Defense Ministry, the Ministry of Foreign Affairs and secretaries of the CSTO Security Councils presented a draft agreement on countering cybercrimes which present the real motivation of states to cooperate [17].

Within the framework of the CIS, there is a process of discussing the Concept of cooperation on combating crimes committed with the use of information technologies [18].

Thus, it is necessary to highlight the main problems in the development of cybersecurity in the Central Asian region:

- the lack of a common legal framework for the region on cybersecurity;
- the different level of access to information bases, the Internet;
- the different level of understanding of the threat and development of states to ensure a secure and resilient cyberspace, the lack of a specific strategy of states;
- the lack of specialists in the protection of information technology and cybersecurity.

The fight to establishing security of the cyberspace is an insufficient for the single state. Only the origin of the crimes being prosecuted and based on the public telecommunication network, related with the specific questions of the legislative, specific methods of law enforcement agencies on the investigation this crime, promotes to the increasing and the development of the cybercrime. For the serious offence with the global cybercrime it should cooperate on the international, bilateral and multilateral bases by signing agreements, conventions and states participation on international organizations and conferences. It is essential to realize the well-organized activities of the multilateral mechanism of the information exchange, timely response system to the cybercrime and current mechanism of the cooperation on the international security policy on the cyberspace. For the creation and control of the function of the legislative basis on the fight against cybercrime it should accept the basic standards of the cyber security and responsible on the world policy.

With the potential for a single cybercrime to exploit a vast array of technology whilst spanning a globally distributed crime scene that can cross several legislative boundaries, makes cybercrime investigation a challenging and often difficult task. As with all investigations, law enforcement must quickly gather and evaluate what initial information is known about the illicit actions of the cybercriminal in order to establish the necessity and proportionality of any response.

REFERENCES

1. Global Cybersecurity Index (GCI) / https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

2. Аттестационное обследование на соответствие требованиям информационной безопасности / http://sts.kz/ru/services

3. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» (с изменениями и дополнениями по состоянию на 28.12.2017) / https://online.zakon.kz/ Document/?doc_id=33885902#pos=0;0

4. Официальный интернет-ресурс Министерства оборонной и аэрокосмической промышленности Республики Казахстан, Комитет информационной безопасности / http://mdai.gov.kz/ru/kategorii/komitet-informacionnoy-bezopasnosti

5. О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций, Указ Президента Республики Узбекистан / http://www.uzbekistan.de/ru/ nachrichten/nachrichten/

6. Статистика инцидентов за 2017 год / https://uzcert.uz/usefulinfo/statistika-intsidetov-za-2017-god/

7. Кыргызстан старается защититься от кибератак / http://m.gezitter.org/society/58974 _kyirgyizstan_staraetsya_zaschititsya_ot_kiberatak/

8. В Кыргызстане изучат развитие потенциала в области кибербезопасности / http://www.islamsng.com/kgz/news/12244

9. О Программе цифровой трансформации Кыргызской Республики «Таза Коом» / http://tazakoom.kg/

10. Democratic governance challenges of cyber security, Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler, DCAF HORIZON 2015 WORKING PAPER No. 1 / https://www.dcaf.ch/sites/default/files/publications/documents/Horizon_1_Good_Governance_CyberSecurity_RUS.pdf

12. Turkmenistan 2017 Crime & Safety Report, United States department of State, Bureau of diplomatic security / https://www.osac.gov/pages/ContentReportDetails.aspx?cid=21673

13. На заседании совета старейшин Туркменистана обсуждены ключевые задачи поступательного развития страны / http://www.mfa.gov.tm/ru/news/441

14. 2ой Центрально-Азиатский форум по управлению интернетом, 22-23 июня 2017г., г.Душанбе, Таджикистан / https://caigf.org/ru/dokladchiki/

15. ШОС выступает за безопасное функционирование и развитие сети Интернет / http://rus.sectsco.org/news/20180126/376304.html

16. В г. Сучжоу (КНР) с участием ШОС прошла международная конференция по кибербезопасности / http://rus.sectsco.org/news/20171220/366849.html

17. Страны Центральной Азии хотят создать совет по кибербезопасности / https://digital.report/stranyi-tsentralnoy-azii-hotyat-sozdat-sovet-po-kiberbezopasnosti/

18. Страны ОДКБ будут совместно обеспечивать кибербезопасность / https://digital.report/stranyi-odkb-budut-sovmestno-obespechivat-kiberbezopasnost/

19. Эксперты Центральной Азии: Кто должен отвечать за кибербезопасность? / https://digital.report/ekspertyi-tsentralnoy-azii-kto-dolzhen-otvechat-za-kiberbezopasnost/