PROBLEMS OF DIGITIZATION IN THE TERRITORY OF SOME CIS MEMBER STATES IN THE FIGHT AGAINST TERRORISM

F.F.Khasanov

https://doi.org/10.5281/zenodo.8267735

Annotation. In the article, the problems encountered in the territory of some CIS member states in the fight against cyberterrorism are based on statistics, practical examples, and the CIS member states

in the fight against cyberterrorism between the development of norms of international documents, the creation of Information Programs was proposed.

Keywords: international terrorism, cyberterrorism, information terrorism, recruitment, human radicalism, CIS, Russian Federation, China, SCO.

In the modern world, terrorism poses a serious threat to international security. Almost all countries of the world faced this threat. Although counterterrorism has been declared one of the priorities of security by many states, its risks have been increasing over time. This happens mainly because of the penetration of terrorism into science.

The modernization of society and the development of Information Technology has led to the mass use of the internet all over the world. Due to the rapid development of the information environment and the comprehensive digitization of all sectors of society, the threat of information terrorism is becoming more and more intense.

With the advent of the Global network, one of the most dangerous types of cybercrime appeared– cyberterrorism, this type of terrorism, in comparison with traditional terrorism, refers to the newest achievements of Science and technology in the implementation of terrorist acts.

The emergence of new methods of recruitment to terrorist organizations through the Internet poses a special danger in the CIS area as a manifestation of cyberterrorism. Modern terrorists are actively using its capabilities, such as easy access to the network, the almost complete absence of censorship, the scale of the audience, anonymity, etc.

Cyberterrorists do not drop bombs, they do not take anyone hostage. They threaten computer tools - the decommissioning of a large computer network of any company, the destruction of data from bank customers, the failure of factories and power plants, etc. The article examines approaches to the detection and understanding of information terrorism, the necessary conditions for its emergence and development in the post-Soviet space, methods of recruitment using social networks, the main methods in the Society of cyberterrorists, as well as the activities of the Shanghai Cooperation Organization. Although certain achievements have been made in this direction within the framework of the SCO, for example, the conclusion of the SCO agreement on cooperation in the field of ensuring international information security, the problem is facing the participating countries to develop a unified approach corresponding to the pace of technological development in the fight against cyberterrorism.

Thanks to the rapid development of the information and digital environment, countries are not only opening up huge prospects for improving the socio-economic and cultural development of the population, increasing its quality of life, but also new threats to domestic international security. One of these threats was the emergence of terrorism into the digital space, the phenomenon of "cyberterrorism". There is no single view of the problem of cyberterrorism in the field of international relations. Cyberterrorism can be considered a derivative of classical terrorism, that is, it is one of the methods in the Society of terrorist groups[1]. Cyberterrorism, on the other hand, can be seen as a continuation of cybercrime, for example, committing crimes against states, their governments, etc.in cyberspace.

In general, cyberterrorism can be characterized by intentional misinformation as committing illegal actions against public, personal and national security, achieving socio-political goals, that is, parochalizing society, giving false information to undermine the national security of the state, or organizing an attack on the information space[2].

Cyberterrorists employ various methods of destabilizing society, such as disabling socially significant infrastructure(for example, in 2012, the corporate networks of the oil manufacturing company in Saudi Arabia and the Qatar natural gas liquefaction company were almost completely disabled by a difference of several days[3]), stealing personal data from residents, companies and public institutions (government structures of World States, their diplomatic agencies, research institutions, trade and commercial structures, oil and gas companies, cyberattack "Red October", carried out by the aerospace industry[4]).

Almost every state has its own interpretation of the concept of cyberterrorism, its own regulatory framework is being developed, which determines the fight against it. But this is considered ineffective in the context of global digitization. In the field of crime in the digital space, it is possible to arrive at home community agreements: in 2001, the Council of Europe developed a convention on Computer Crimes[5]. In the case of cyberterrorism, there are no comprehensive agreements between several international actors.

After the collapse of the USSR, cyber attacks on important state infrastructures began to occur on the territory of the CIS countries. In 1999, Gazprom was hit by a cyber attack, a system that controlled gas supplies using the Trojan virus was entered. In 2015, an attack was launched on the Ukrainian power grid, leaving more than half a million residents without lights and causing technical damage to a large metallurgical plant. As mentioned above, attacks in cyberspace to harm the state infrastructure and the socio-economic state of society can be equated with cyberterrorism.

[1] *Горбенко А.* Кибетерроризм как новая форма терроризма: проблемы противодействия // Деструктивное влияние террора на политическую систему и правовую среду Российского государства: материалы Всероссийской научно-практической конференции. Под редакцией О. И. Чердакова. М., 2017 С. 105-114.
[2] Чжэн И. Сотрудничество РФ и КНР в борьбе с кибертерроризмом. Вестник МГОУ. 2018.
[3] Saudi Aramco repairing damage from computer attack.26.08.2012. URL: https://www.reuters.com/article/saudi-aramco-hacking/saudi-aramco-repairing-damage-from-computer-attack-idUSL5E8JQ43P20120826
[4] Как "Лаборатория Касперского" охотилась за "Красным октябрем". 19.08.2023. URL: https://ria.ru/20130131/920622193.html
[5] Европа Кенгашининг компютерь жиноятлари тўғрисидаги конвенцияси. 23 .11.2001. // Европа Кенгашининг расмий веб-сайти. URL: https://rm.coe.int/1680081580 (мурожаат санаси: 19.08.2023).

Also, the manifestation of information-assisted influence as a type of cyberterrorism is of particular importance in the territory of CIS member states. First of all, it is going about propaganda work and recruitment of antiterrorist organizations into their ranks[6].

With the advent of international terrorism, the issue of attracting more and more members to terrorist organizations has become one of the most important issues for these organizations. It is worth noting separately the left radical terrorist organizations that have succeeded in this direction, such as the patriotic anti-fascist resistance groups of October 1 (GRAPO) i.e., the "Red Brigades" and Islamic terrorist organizations banned on the territory of the Russian Federation[7], for example, "Al-Qaeda", "the Islamic State".

With the further development of technology, new means of communication and the internet network began to actively enter our lives. And this did not affect the adaptation of terrorist organizations to such new methods.

However, before starting to analyze new methods of direct recruitment, it is necessary to initially determine the main conditions that affect a person's tendency to join such organizations and continue to work in them.

Indeed, many scientists, in particular sociologists, have analyzed this problem, trying to explain the phenomenon of radicalization of personality, including attempts to create new mechanisms against hiring[8]. Unfortunately, taking into account the peculiarities of such work and the fight against terrorism of special services, such as the Federal Security Service, while the implementation of scientific work on such a matter is somewhat difficult, however, the study of this topic continues.

Thus, scientists are studying this problem from the point of view of analyzing the factors that radicalize a person. In particular, socio-economic factors and psychological analysis stand out in this regard. These studies cannot give an accurate "portrait" of the person to be hired, but their result allows you to create a certain Foundation. In particular, it is often a person who has a terrorist education and at the same time has little income. For example, the first study refutes the myth that only uneducated people will join the ranks of terrorists[9]. It can also be assumed that the development of large data analysis technologies will be one of the most promising areas of resistance to hiring in the near future[10].

There are two approaches to hiring people: active and passive. The active type refers to the direct contact of the recruiter with the person. Passive type occurs, in particular, because a person is radicalized independently. Theses on the factors that contribute to the radicalization of this or that person correspond to both types. First you need to consider active hiring. It consists of four stages: first, the mobile potential is formed; second, the recruiting networks

[6] Новицкий, В. Ф. Военная энциклопедия / В. Ф. Новицкий, И. Д. Сытин. — 1-е изд. — Санкт-Петербург:, 1911. – с 212. – Текст: непосредственный.

[7] Россия Федерацияси қонунчилигига мувофиқ террорчи деб тан олинган ташкилотларнинг, шу жумладан хорижий ва халқаро ташкилотларнинг ягона федерал рўйхати. URL: http://www.fsb.ru/fsb/npd/terror.htm

[8] Thomas, Hegghammer The recruiter's dilemma: Signalling and rebel recruitment tactics / Hegghammer Thomas. // Journal of Peace Research. – 2012. – № 50(1). – С. 3–16.

[9] Alan, B. K. What Makes a Terrorist? Economics and the Roots of Terrorism / B. K. Alan. // Prince-ton University Press. – 2007.

[10] Macartan, Humphreys Who fights? The determinants of participation in civil war / Humphreys Macartan, M. W. Jeremy. // American Journal of Political Science. – 2008. – № 52(2). – С. 436–455.

are activated; third, the motivation to participate, the formation of motivation and, fourth, the elimination of barriers to participation[11].

In all these stages, in particular, in the last two, the direct recruiter plays an active role. There is no way to determine in detail the mechanics of personal recruitment of a particular person. It is clear that when hiring, the recruiter should pay attention to behavior, clothing, little things in the worldview and come from them in the application of their methods. In addition, hiring is influenced by many factors, from the street where hiring is taking place to the entire continent[12]. In this regard, it is impossible to determine the factors that cause recruiters to throw their targets.

Passive recruitment remains particularly dangerous due to the development of the internet network and the access of various terrorist organizations to the internet to distribute mediamaterial with the aim of influencing a wide audience. Passive recruitment is done through the dissemination of the organization's own ideas and beliefs through information materials, through video that it presents to a wide range of people, through the media, etc. It should be noted that financing active and passive recruitment often does not matter[13].

In addition to distributing mediamaterials, recruiters resort to the online recruitment method[14]. This method is especially common in the CIS countries.

The recruitment of citizens from various countries that are part of the SCO is one of the risks posed by the terrorist organization “Islamic State”, which is prohibited on the territory of the Russian Federation. It is actively recruiting immigrants from the Central Asian republics into its ranks. According to the federal security service of the RF,

As of 2015, more than 5,000 citizens of the Russian Federation and Central Asian states have fought in the ranks of the “Islamic State”.

The recruitment of citizens from various countries that are part of the SCO is one of the risks posed by the terrorist organization “Islamic State”, which is prohibited on the territory of the Russian Federation. It is actively recruiting immigrants from the Central Asian republics into its ranks. According to the federal security service of the RF, As of 2015, more than 5,000 citizens of the Russian Federation and Central Asian states have fought in the ranks of the “Islamic State” [15].

In order to control the Internet in the Russian Federation, the first law is the “Yarova law”, adopted at the first reading by the State Duma on May 13, 2016 and formulated by amendments in June of the same year[16]. The passage of this law was aimed precisely at combating terrorist activities on the internet. Nevertheless, the Council for the development

[11] Bert, Klandermans Potentials, networks, motivations, and barriers: Steps towards participation in social movements / Klandermans Bert, Oegema Dirk. // American Sociological Review. – 1987. – № 52(4). – С. 519–531.

[12] Michael, Bacharach Trust as type detection. In: Christiano Castelfranchi & Yao-Hua Tan (eds) / Bacharach Michael, Gambetta Diego. // Trust and Deception in Virtual Societies. – 2001. – С. 1-22.

[13] Ширкин, А. А. Теория финансирования вербовки в террористических целях. Анализ связанных с вербовкой расходов / А. А. Ширкин, О. С. Ерашова. // Государственная служба и кадры. – 2018. – № 3. – С. 108-110.

[14] Голяндин, Н. П. Мотивации вербовки в экстремистские и террористические организации / Н. П. Голяндин, А. В. Горячев. // Вестник краснодарского университета МВД России. – 2013. – № 2(20). – С. 37-40.

[15] ФСБ: свыше 5 тысяч граждан из России и стран Центральной Азии воюют на стороне ИГ [Электронный ресурс] // ТАСС. URL:http://tass.ru/politika/2272750 (дата обращения: 19.08.2023)

[16] Справка о результатах голосования по вопросу: (первое чтение) О проекте федерального закона № 1039101-6. — Текст : электронный // Государственная дума Федерального Собрания Российской Федерации: [сайт]. — URL:http://vote.duma.gov.ru/vote/94599 (мурожаат санаси: 19.08.2023).

of civil society and Human Rights Under the president of the Russian Federation reacted negatively to the idea of such a bill[17].

Online recruiting is a modified trading funnel widely used in standard advertising. Initially, a person directly enters the website associated with the ideas of a terrorist organization or this organization. Then the main goal of recruiters is to involve a person in communication. At the same time, it does not matter whether a person criticizes or supports these ideas. Subsequently, increasing the level of discussion, a person is attracted to the continuation of discussions in separate closed chats. Basically, such conversations are created in messengers with increased anonymity and encryption, in particular, “Telegram”. It was the actions associated with the recruitment of terrorist groups and their activities that led to the blocking of this messenger on the territory of the Russian Federation by Roskomnadzor on April 16 , 2018, which caused outrage among citizens[18], and rallies were held to protect the famous Messenger[19].

Another important aspect of online rectruting is, for example, making the hiring process “a big game. System hacking is the gamification of the recruitment process by hosting various games on the Internet” [20] While the Brotherhood of the North society, which hosted the game, was labeled as extremist but not recognized as a terrorist organization, it is difficult to distinguish between them, while the methods of recruiting new members and working on the Internet are similar.

However, linking the reasons why terrorist organizations hire and develop a person exclusively to the Internet is a big mistake, and the factor of a person's social status and its psychological characteristics plays a huge role.

In recent times, special attention has been paid to social networks in terms of direct recruitment. This is due to the fact that these forms of virtual communication penetrate into our daily lives. Facebook Instagram, Facebook, Youtube and other similar social networks, for example, may publish any information about their views and activities (based on appropriate privacy) [21]. The popularity of social networks among terrorists and recruiters also depends on a relatively inexpensive connection, for which it is enough to pay for the internet at an affordable rate . In turn, social networks allow you to spread various myths useful for terrorist organizations and recruiters without significant funds. In particular, the idea that Islam is the most peaceful religion is widespread on the territory of the Union of independent states.

[17] Экспертное заключение на проекты Федеральных законов «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» и «О внесении изменений в отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности». — Текст: электронный // Совет при Президенте Российской Федерации по развитию гражданского общества и правам человека: [сайт]. — URL: http://president- sovet.ru/presscenter/news/read/3151/ (мурожаат санаси: 19.08.2023).

[18] Роско надзор начал процедуру блокировки Telegram. — Текст : электронный // ТАСС : [сайт]. —URL: https://tass.ru/ekonomika/5129977 (дата обращения: 19.08.2023).

[19] Число участников митинга в защиту Telegram достигло 12 тысяч человек. Дуров назвал акцию беспрецедентной. — Текст: электронный // Republic :[сайт]. — URL: https://republic.ru/posts/90679 (дата обращения: 19.08.2023).

[20] Голяндин, Н. П. Мотивации вербовки в экстремистские и террористические организации / Н. П. Голяндин, А. В. Горячев. // Вестник краснодарского университета МВД России. – 2013. – № 2(20). – С. 37-40.

[21] Md, S. H. Social Media and Terrorism: Threats and Challenges to the Modern Era / S. H. Md. // South Asian Survey. – 2018. – № 22(2). – С. 136–155.

Social network users may not think that building a sentence in this way alone provokes interfaith hostility[22].

The internet space really increases the likelihood of spreading yachts and their ideas to various terrorist organizations. This is also due to the lack of a global regulatory framework focused on counterterrorism activities. This is due to the lack of centralized control of the Internet network.

Given the above threats posed by cyberterrorism for the post-Soviet region, the activities of the SCO in the fight against cyberterrorism on the unification of the efforts of participants are of particular importance.

Initially, the SCO was formed to unite the efforts of participating countries in combating and preventing terrorism, separatism and extremism movements in Central Asia. Also referred to is the fight in cyberspace.

The SCO agreement on cooperation in the field of ensuring International Information Security defines the concept of "information terrorism". Information terrorism means the use of information resources and (or) their influence in the information space for terrorist purposes.

Among the mechanisms for combating information terrorism, regular consultations of Representatives and competent bodies of the states provided for by the contract are noted, the competent authorities of the participating countries can directly cooperate on this issue, as well as conclude relevant agreements of an interdepartmental nature[23]. However, if this can harm national interests, or if the data falls into the category of state secrets, the transfer of information between participants is not provided[24]. The agreement was initially ratified by Russia, China, Kazakhstan, Tajikistan and other CIS member states.

The regional counterterrorism center of the Shanghai Cooperation Organization (SCO MATM) is working on creating an effective cooperation mechanism against terrorist activities in cyberspace[25], the cooperation of this center in the field of cyberterrorism is as follows: development and implementation of joint measures to combat cyberterrorism, improvement of the regulatory framework in this area; regular monitoring and general response to cyber threats; ; in order to combat cyberterrorism, it is planned to implement in the directions of improving the legislative base of the Member States of the SCO.

In 2018, at the next meeting of the prosecutor general of SCO countries in Dushanbe, an initiative was put forward by a representative of Kazakhstan to adopt a universal joint legal document on combating cyberterrorism[26]. A year later, in Semyan, eight SCO countries held joint exercises on the fight against cyberterrorism, the purpose of which was to improve coordination between participants in the field of internet counterterrorism[27]. Under the

[22] Голяндин, Н. П. Мотивации вербовки в экстремистские и террористические организации / Н. П. Голяндин, А. В. Горячев. // Вестник краснодарского университета МВД России. – 2013. – № 2(20). – С. 37-40.

[23] Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009. URL: http://docs.cntd.ru/document/902289626

[24] Қаранг: ўша манба.

[25] РАТС ШОС создал механизм по борьбе с кибертерроризмом. Центральный интернет портал Шанхайской Организации сотрудничества. URL: http://infoshos.ru/ru/?idn=15066

[26] Казахстан предложил странам ШОС вместе бороться с кибертерроризмом. Центральный интернет портал Шанхайской Организации сотрудничества. URL: http://infoshos.ru/ru/?idn=19351

[27] Страны ШОС провели учения по борьбе с кибертерроризмом. Центральный интернет портал Шанхайской Организации сотрудничества. URL:http://infoshos.ru/ru/?idn=17542

leadership of the SCO, a seminar-training on the fight against cyberterrorism was held in Hyderabad, India for representatives of law enforcement agencies[28].

It should be noted that the solidarity indicated in assessing the risk of cyberterrorism among SCO member states did not lead to the creation of a special document that defines the basic principles and mechanisms for combating it. This is now complicated by the fact that the concept of cyberterrorism is not entrenched in the criminal laws of the participating countries.

The basis for creating effective protection systems from cyberterrorist attacks can be the programs of the main participants of the SCO – the RF and the PRC. In accordance with the Federal Law No. 187-FZ of July 26, 2017" on the security of important information infrastructures of the Russian Federation", a state system for detecting, preventing and eliminating the consequences of computer attacks (Gossopka) has been created in Russia for several years. Within the framework of this system, a system for exchanging information about cyberattacks between the most important organizations of the country works effectively. In 2018, more than 4.3 billion computer impacts on critical information infrastructure were identified using the Gossopka system[29].

One of the functions of China's Golden Shield system ("golden shield", an electronic barrier that controls information flows) is to combat cyberterrorism. The principle of operation of this system is that all the digital data of Chinese users passes through the "gateways" that filter it. A distinctive feature of the system is a small number of companies that support the operation of switches and provide network access around the world. This system is criticized by the West as limiting the civil rights of the Chinese population, due to which it cannot be universal for all participants in the SCO. However, some principles of system work can be applied to combat the destructive potential of cyberterrorism.

International terrorism has become especially deadly in the information age. Firstly, new ways of destabilizing society appeared in terrorist groups and organizations, and secondly, the influence of digital technologies on the functioning of society's life and public infrastructure increased. Cyberspace responds quickly to a changing political situation, while terrorist organizations are able to make technical innovations faster than state structures. Economic damage is done to the state and society through cyberattacks, while there is no centralized control over the cyberattack, which is becoming the basis for terrorist organizations to spread their ideas and expand their networks by hiring people.

In conclusion, it can be said that the effectiveness of the Shanghai Cooperation Organization, especially its work on the Prevention of terrorist actions in Central Asia, has grounds for becoming a Regional Center for coordinating the fight against internet terrorism. The main problem on the way to becoming such a center is the delay in the development of the appropriate regulatory framework. As a result, there is an increasing discrepancy between the pace of technological development and the attitude of the institutions of the Member States of the SCO towards it.

[28] Спецслужбы ШОС обсудят в Индии вопросы борьбы с кибертерроризмом. Центральный интернет портал Шанхайской Организации сотрудничества. URL: http://infoshos.ru/ru/?idn=20555

[29] В России выявили свыше четырех млрд кибератак на критические инфраструктуры. РИА. URL: ttps://ria.ru/20181211/1547799590.html

References:

1. Абрамов А.В., Федорченко С.Н., Курылев К.П. Сетевая природа международного терроризма и возможности консолидации российского общества // Вестник РУДН. Серия: Международные отношения. 2017. Т. 17. №4. С. 738-748.
2. Alan, B. K. What Makes a Terrorist? Economics and the Roots of Terrorism / B. K. Alan. // Prince-ton University Press. – 2007.
3. В России выявили свыше четырех млрд кибератак на критические инфраструктуры. РИА. URL: ttps://ria.ru/20181211/1547799590.html
4.Горбенко А. Кибетерроризм как новая форма терроризма: проблемы противодействия // Деструктивное влияние террора на политическую систему и правовую среду Российского государства: материалы Всероссийской научно-практической конференции. Под редакцией О. И. Чердакова. М., 2017 С. 105-114.
5.Чжэн И. Сотрудничество РФ и КНР в борьбе с кибертерроризмом. Вестник МГОУ. 2018.
6. Saudi Aramco repairing damage from computer attack. 19.08.2023. URL: https://www.reuters.com/article/saudi/aramco-hacking/saudi-aramco-repairing-damage-from/computer-attack-idUSL5E8JQ43P20120826
7.Как “Лаборатория Касперского” охотилась за “Красным октябрем”. 19.08.2023. URL: https://ria.ru/20130131/920622193.html
8. Европа Кенгашининг компютерь жиноятлари тўғрисидаги конвенцияси. 23 .11.2001. // Европа Кенгашининг расмий веб-сайти. URL: https://rm.coe.int/1680081580 (мурожаат санаси: 19.08.2023).
9. Новицкий, В. Ф. Военная энциклопедия / В. Ф. Новицкий, И. Д. Сытин. — 1-е изд. — Санкт-Петербург:, 1911. – с 212. – Текст: непосредственный.
10. Россия Федерацияси қонунчилигига мувофиқ террорчи деб тан олинган ташкилотларнинг, шу жумладан хорижий ва халқаро ташкилотларнинг ягона федерал рўйхати. URL: http://www.fsb.ru/fsb/npd/terror.htm
11. Thomas, Hegghammer The recruiter’s dilemma: Signalling and rebel recruitment tactics / Hegghammer Thomas. // Journal of Peace Research. – 2012. – № 50(1). – С. 3–16.
12. Macartan, Humphreys Who fights? The determinants of participation in civil war / Humphreys Macartan, M. W. Jeremy. // American Journal of Political Science. – 2008. – № 52(2). – С. 436–455.
13. Bert, Klandermans Potentials, networks, motivations, and barriers: Steps towards participation in social movements / Klandermans Bert, Oegema Dirk. // American Sociological Review. – 1987. – № 52(4). – С. 519–531.
14. Michael, Bacharach Trust as type detection. In: Christiano Castelfranchi & Yao-Hua Tan (eds) / Bacharach Michael, Gambetta Diego. // Trust and Deception in Virtual Societies. – 2001. – С. 1-22.
15. Ширкин, А. А. Теория финансирования вербовки в террористических целях. Анализ связанных с вербовкой расходов / А. А. Ширкин, О. С. Ерашова. // Государственная служба и кадры. – 2018. – № 3. – С. 108-110.
16. Голяндин, Н. П. Мотивации вербовки в экстремистские и террористические организации / Н. П. Голяндин, А. В. Горячев. // Вестник краснодарского университета МВД России. – 2013. – № 2(20). – С. 37-40.

17. ФСБ: свыше 5 тысяч граждан из России и стран Центральной Азии воюют на стороне ИГ [Электронный ресурс] // ТАСС. URL:http://tass.ru/politika/2272750 (дата обращения: 19.08.2023)
18. Справка о результатах голосования по вопросу: (первое чтение) О проекте федерального закона № 1039101-6. — Текст: электронный // Государственная дума Федерального Собрания Российской Федерации: [сайт]. — URL:http://vote.duma.gov.ru/vote/94599 (мурожаат санаси: 19.08.2023).
19. Экспертное заключение на проекты Федеральных законов «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» и «О внесении изменений в отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности». — Текст:
электронный // Совет при Президенте Российской Федерации по развитию гражданского общества и правам человека: [сайт]. — URL: http://president-sovet.ru/presscenter/news/read/3151/ (мурожаат санаси: 19.08.2023).
20. Роско надзор начал процедуру блокировки Telegram. — Текст: электронный // ТАСС : [сайт]. —URL: https://tass.ru/ekonomika/5129977 (дата обращения: 19.08.2023).
21. Число участников митинга в защиту Telegram достигло 12 тысяч человек. Дуров назвал акцию беспрецедентной. — Текст: электронный // Republic:[сайт]. — URL: https://republic.ru/posts/90679 (дата обращения: 19.08.2023).
21. Md, S. H. Social Media and Terrorism: Threats and Challenges to the Modern Era / S. H. Md. // South Asian Survey. – 2018. – № 22(2). – С. 136–155.
22. Соглашение между правительствами государств членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009. URL: http://docs.cntd.ru/document/902289626
23. Сизых Е.Ю., Гайнетдинова А.К. Перспективы развития сотрудничества в сфере противодействия кибертерроризму в рамках ШОС. // Global and Regional Research. // Т. 1. 2019. С. 171-175.
24. Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2009. URL: http://docs.cntd.ru/document/902289626
25. РАТС ШОС создал механизм по борьбе с кибертерроризмом. Центральный интернет портал Шанхайской Организации сотрудничества. URL: http://infoshos.ru/ru/?idn=15066
26. Казахстан предложил странам ШОС вместе бороться с кибертерроризмом. Центральный интернет портал Шанхайской Организации сотрудничества. URL: http://infoshos.ru/ru/?idn=19351
27. Страны ШОС провели учения по борьбе с кибертерроризмом. Центральный интернет портал Шанхайской Организации сотрудничества. URL:http://infoshos.ru/ru/?idn=17542
28. Спецслужбы ШОС обсудят в Индии вопросы борьбы с кибертерроризмом. Центральный интернет портал Шанхайской Организации сотрудничества. URL: http://infoshos.ru/ru/?idn=20555