THE ROLE OF CYBERSECURITY CHALLENGES IN COUNTERING TERRORISM

Rizvangul SADYKOVA*	*Ass. Prof. Ph.D., MD, MA, LLM, M. Narikbayev KAZGUU University, Astana, Kazakhstan, rizvanaholland@mail.ru*
Aliya KINTONOVA	*Ass. Prof., candidate of technical sciences, Department of Artificial Intelligence Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, aliya_kint@mail.ru*
Aiymgul GABDULLINA	*Master student, Department of Artificial Intelligence Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, aiym.g.e@mail.ru*
Roman KARAS	*Ass. Prof., MSs, Candidate of political sciences, Department of Information Analytics and Political Technologies, Bauman Moscow State Technical University, Moscow, Russian Federation, romankaras2009@gmail.com*

Manuscript received: 05/12/2023

DOI: 10.52123/1994-2370-2023-1140
UDC 004.056.5
CICSTI 81.93.29

Abstract. Cybersecurity threats represent one of the major challenges that all nations are currently facing. Cyberspace plays an important role in our modern life, uniting people and communities around the world, and providing them with the opportunity for socialization and self-organization. However, cyberspace is also subject to various threats that can have a serious impact on national security, public safety, and the economy. Information warfare covers a wide range of actions, ranging from attacks on communication systems and critical infrastructure to the use of information and communication technologies (ICT) to implement psychological impact techniques.
Cybercriminals actively use various methods and techniques to carry out cyber attacks, including unauthorized access to systems, theft of personal information, financial fraud, and the distribution of malicious software. Such criminal acts in cyberspace pose a threat to both individuals and organizations. Cyberterrorism is also a danger since cyber attacks can be used to create chaos and disrupt the normal functioning of critical infrastructures, such as energy and transport.
At the international level, it is important to establish dialogue and cooperation between various countries and international organizations, such as the UN, the European Union, NATO, and others. This will make it possible to coordinate strategies, exchange information about cyber threats, and coordinate measures to prevent and respond to cyber-attacks. International agreements can also contribute to the establishment of responsibility for cyber aggression and the creation of mechanisms for the investigation and prosecution of cybercriminals.
Keywords: cyberspace, cybersecurity threats, cyberterrorism, cybersecurity cooperation.

Аңдатпа. Киберқауіпсіздік қатерлері қазіргі уақытта барлық мемлекеттер бетпе-бет келіп отырған негізгі проблемалардың бірі болып табылады. Киберкеңістік біздің қазіргі өмірімізде маңызды рөл атқарады, бүкіл әлемдегі адамдар мен қауымдастықтарды біріктіреді, оларға әлеуметтену және өзін-өзі ұйымдастыру мүмкіндігін береді. Дегенмен, киберкеңістік ұлттық қауіпсіздікке, қоғамдық қауіпсіздікке және экономикаға елеулі әсер етуі мүмкін түрлі қауіптерге ұшырайды. Ақпараттық соғыс коммуникациялық жүйелер мен маңызды инфрақұрылымға шабуылдардан бастап психологиялық әсер ету әдістерін жүзеге асыру үшін ақпараттық-коммуникациялық технологияларды (АКТ) пайдалануға дейінгі әрекеттердің кең ауқымын қамтиды.
Киберқылмыскерлер жүйеге рұқсатсыз кіру, жеке ақпаратты ұрлау, қаржылық алаяқтық және зиянды бағдарламалық қамтамасыз етуді таратуды қоса алғанда, кибершабуылдарды жүзеге асыру үшін әртүрлі әдістерді белсенді пайдаланады. Киберкеңістіктегі мұндай қылмыстық әрекеттер жеке адамдарға да, ұйымдарға да қауіп төндіреді. Кибертерроризм де қауіпті, өйткені кибершабуылдар хаос тудыру және энергетика мен көлік сияқты маңызды инфрақұрылымдардың қалыпты жұмысын бұзу үшін пайдаланылуы мүмкін.
Халықаралық деңгейде БҰҰ, Еуропалық Одақ, НАТО және т.б. әртүрлі елдер мен халықаралық ұйымдар арасында диалог пен ынтымақтастық орнату маңызды. Бұл стратегияларды үйлестіруге, киберқауіптер туралы ақпарат алмасуға және кибершабуылдардың алдын алу және оларға қарсы әрекет ету шараларын үйлестіруге мүмкіндік береді. Халықаралық келісімдер киберагрессия үшін жауапкершілікті орнатуға және киберқылмыскерлерді тергеу мен қудалау тетіктерін құруға да ықпал ете алады.
Түйін сөздер: киберкеңістік, киберқауіпсіздік қатерлері, кибертерроризм, киберқауіпсіздік саласындағы ынтымақтастық.

* *Corresponding author: R. Sadykova, rizvanaholland@mail.ru*

Аннотация. Угрозы кибербезопасности представляют собой одну из основных проблем, с которыми в настоящее время сталкиваются все страны. Киберпространство играет важную роль в нашей современной жизни, объединяя людей и сообщества по всему миру, предоставляя им возможность социализации и самоорганизации. Однако киберпространство также подвержено различным угрозам, которые могут оказать серьезное влияние на национальную безопасность, общественную безопасность и экономику. Информационная война охватывает широкий спектр действий: от атак на системы связи и критически важную инфраструктуру до использования информационно-коммуникационных технологий (ИКТ) для реализации приемов психологического воздействия.
Киберпреступники активно используют различные методы и приемы для осуществления кибератак, включая несанкционированный доступ к системам, кражу личной информации, финансовое мошенничество и распространение вредоносного программного обеспечения. Подобные преступные действия в киберпространстве представляют угрозу как для отдельных лиц, так и для организаций. Кибертерроризм также представляет опасность, поскольку кибератаки могут быть использованы для создания хаоса и нарушения нормального функционирования критически важных инфраструктур, таких как энергетика и транспорт.
На международном уровне важно наладить диалог и сотрудничество между различными странами и международными организациями, такими как ООН, Европейский Союз, НАТО и другие. Это позволит координировать стратегии, обмениваться информацией о киберугрозах и координировать меры по предотвращению и реагированию на кибератаки. Международные соглашения также могут способствовать установлению ответственности за киберагрессию и созданию механизмов расследования и преследования киберпреступников.
Ключевые слова: киберпространство, угрозы кибербезопасности, кибертерроризм, сотрудничество в области кибербезопасности.

Introduction

Currently, Currently, cyberspace plays a huge role in people's daily lives. According to research conducted by various organizations, the average user spends more than six hours a day on the Internet. They use the Internet to search for information, communicate with friends and relatives, make purchases, order food and services, games, and much more. However, close interaction with cyberspace carries with it certain risks for users. Cybercriminals use various methods to gain access to users' personal information and money [1].

Therefore, there is a need to ensure security in cyberspace. Cybersecurity experts are working on creating various methods and technologies to protect users from cyber threats. They also develop standards and recommendations for organizations and states to ensure network security. This is reflected in several standards and regulatory documents, such as ISO/IEC 27032:2012 [2], NIST CSF [3], ISO/IEC 27001[4], IEC 62443 standard [5]. All these documents help to improve the protection of personal data and information from cyber threats [6]. The main task of the State is to protect national security, which means protecting its citizens, economy, and institutions. Initially, national security protected the nation from military threats, but now its scope is broader and includes security from terrorism and crime, security of the economy, energy, environment, food, critical infrastructure, and, finally, cybersecurity [7].

The materials and methods

Materials and sources in the list of references (articles and scientific publications, textbooks, regulatory and legal documents of countries and international organizations. To write the article, the method of data analysis, research and empirical methods, and the methodology of teaching advanced training courses were used.

The materials and methods used in this study provide a structured framework for examining the role of cybersecurity issues in countering terrorism. Based on a literature review, legal analysis provides a comprehensive examination of the fundamentals of cybersecurity, international initiatives, legislative measures and challenges associated with countering terrorism in the digital age.

Cybersecurity aspects in counter-terrorism

The concept of "cybersecurity" has several interpretations. One such interpretation, proposed by researcher D.B. Dubinina, describes cybersecurity as a set of measures to protect systems, networks, and software applications from digital attacks aimed at gaining access to confidential information, changing it, destroying it, or extorting money from users [8].

Another interpretation proposed by N.A. Moiseeva is related to knowledge and skills in the field of risk assessment of social engineering when working in the digital space, organizing the security of personal data, as

well as awareness of the negative impact of digital devices and gadgets on the environment, as well as on the physical and mental health[9].

In the international standard ISO/IEC 27032:2023 [10], cybersecurity is defined as the property of protecting assets from threats to confidentiality, integrity, and accessibility in cyberspace. In GOST R 56205-2014 IEC/TS 62443-1-1:2009 [11], a broader definition of cybersecurity is given as actions necessary to prevent unauthorized use, denial of service, transformation, declassification, loss of profit or damage to critical systems or information objects. Cybersecurity includes the concepts of identification, authentication, traceability, authorization, accessibility, and privacy [12].In international standards, there are several definitions of the concept of "cyberattack", which cover various aspects of this concept. Below are some of them:

In ISO/IEC 27032:2023 [10], "Cyberattack" is defined as "any action aimed at obtaining unauthorized access to information or at changing, destroying or blocking it, performed using computer engineering means or communication technology."The US National Institute of Standards and Technology (NIST) defines a cyberattack as "any unwanted event or action directed at a computer system or network that violates the confidentiality, integrity or availability of a computer system or network."

In GOST R ISO/IEC 27005-2010 [13], "Cyberattack" is defined as "any undesirable event that causes a violation of the confidentiality, integrity or availability of information stored, processed or transmitted in an information system."It is also worth noting that cyberattacks may have their specific definitions and characteristics in different contexts and spheres. For example, in the context of cybersecurity of the US national infrastructure, a cyberattack is defined as "any action directed at the national infrastructure that can cause serious damage to national security, our economy, or our citizens."

At the same time, one of the main programs of the United Nations is the Cybersecurity and New Technologies programme which was launched in the UN Office of Counter-Terrorism.

United Nations since 2001 has significantly expanded its activities in countering terrorism. Today's terrorist organizations are concerned with millions of dollars of income, with an internal division of labor and specialization, with training camps, workshops, warehouses, shelters, printing houses, hospitals, and laboratories. They can widely use the latest types of weapons, means of communication, and transportation, practicing the most diverse and largely new methods and techniques. Their "staff" consists of ideologists and practitioners, leaders and performers, specialists in sabotage, and so on [14]. All this testifies that there is not a single state in the world that could live today in peace and with full confidence that this phenomenon would not affect its citizens in the future. We must introduce a collective opposition of all subjects of anti-terror to a socially destructive phenomenon to create a real opportunity to curb global threats to the security of all mankind. Many scholars who deal with this subject believe that the direction of terror is becoming more and more concrete, and the goals of terrorists are becoming obvious.

Most powerful terrorist organizations known in the world have their spiritual leaders and mentors. Also, they improved and built a more complex hierarchical and organizational structure, their ideology and strategy of action, and strong, wealthy patrons. Along with a large number of terrorist organizations and groups, an equally large number of supporting structures arose, up to entire sponsoring states. Neither highly developed nor economically and socially lagging countries with different political regimes and systems of government are immune from outbreaks of terrorism. The ongoing processes of globalization that are changing the nature of the modern world order, and the emergence of new global means and systems of communication and information reduce the importance of state borders and other traditional means of protection against terrorism.

Unfortunately, since the year 2000, we can observe some activation of extremist organizations in Central Asia, including Kazakhstan. At the legislative level, to combat terrorism, the Law of the Republic of Kazakhstan "On Combating Terrorism" dated July 13, 1999, was adopted. This law defines the legal and organizational framework for the fight against terrorism, the procedure for the activities of state bodies and organizations, regardless of ownership, as well as the rights, obligations, and guarantees of citizens in connection with the implementation of the fight against terrorism. Also, this law provides definitions of such concepts as “terrorism”,

“terrorist activity”, “terrorist action”, “act of terrorism”, etc. [15].

Since that time, the presence of sponsoring states that finance terrorist organizations greatly complicates the fight against terrorism, since the capabilities and influence of these groups are significantly increased [16].

Dealing with all aspects of combating terrorism, it is necessary not to forget about the protection of human rights in a conflict, since the terrorist attacks themselves already violate one of the many aspects of human rights - the right to life. Considering this problem, more than a decade ago the Minister of Defense of the Republic of Kazakhstan, Mukhtar Altynbayev, noted that the relevance of the issues of combating terrorism is of paramount importance today. Manifestations of international terrorism and extremism have already affected many countries, regardless of their economic and military potential. The search for optimal and effective antiterrorist measures becomes all the more significant.[17]. It has already been said more than once that the struggle must be universal and be waged by all available means. But here it turns out, not everything is so simple. No one argues that modern terrorism, accompanied by unimaginable cruelty, the killing of innocent people, the taking of hostages, the seizure of vehicles, and torturing for political purposes, is an extreme form of violation of human rights. According to some former senior staff of the National Security Committee of the Republic of Kazakhstan, the state should pursue a tougher policy towards certain religious organizations and private educational institutions of dubious origin. He believes that today there is a need for detailed legislative regulation of the activities of missionaries on the territory of Kazakhstan. The tendency of the emergence of mosques according to national characteristics is alarming. We do believe that more precise and restrictive legal regulations on the establishment of various humanitarian funds with a religious component should be introduced. He also underlined that there is a real threat to the security of the country from certain foreign terrorist organizations, the most dangerous of which are Al-Qaeda and the Islamic Party of Turkestan. Under these conditions, it is necessary to intensify ideological work and give. The more attention to dissemination of necessary information to prevent those destructive activities. One should admit, no matter how successful the actions of the special services to eliminate terrorist structures, all this will be a "blow to the tails." It is important to develop a social immunity that rejects any manifestation of terrorism or aiding suspects. In this aspect, the fight against lack of spirituality and lack of culture is especially relevant. First of all, it is vitally important to work with leaders and activists in the youth environment. The information space does not tolerate emptiness. In case if public organizations and clergy do not improve their involvement, someone else will take their place [17].

According to a decision by the Supreme Court of the Republic of Kazakhstan seven international organizations - "Asbat al-Ansar", "Muslim Brotherhood", "Taliban", "Boz Gurd", "Jamaat of the Mujahideen of Central Asia", "Lashkar-e-Taiba" and "Society for Social Reforms" - were recognized as a terrorist and banned on the territory of Kazakhstan. The activity of this organization, according to the Law of the Republic of Kazakhstan "On countering extremism", must be recognized as an extremist, and it is outlawed in Kazakhstan [18].

One should admit that the United Nations' leading role and establishment of the UN Office of Counter-Terrorism was the most important step in a global struggle against terrorism. Now this Office is the leading organization that coordinates all international activities in the fields of new technologies. One of the main programs is the Cybersecurity and New Technologies program. According to resolution 2341 (2017), the Security Council Calls upon Member States “to establish or strengthen national, regional and international partnerships with stakeholders, both public and private”, and advises to share information and experience to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities. It is envisaged that joint training and the use or establishment of relevant communication or emergency warning networks will contribute to its implementation.

We must recall that the UN Office of Counter-Terrorism initiated several steps within the field of new technologies. The Cybersecurity and New Technologies program is aimed to enhance the capacities of Member States and private organizations in preventing and mitigating the misuse of technological progress by leaders of terrorist organizations

and violent extremists. This includes countering the threat of cyber-attacks carried out by terrorist actors against vital community services, and critical infrastructure, as well as developing the use of social media to collect open-source information and digital pieces of evidence to counter online terrorism and violent extremism while respecting Human Rights. In addition, the program of the UN Office of Counter-Terrorism introduced expertise to determine the possibility of using unmanned aerial systems (UAS) by terrorist organizations and will develop further programming in a similar area. The project also should help to mitigate the impact and recover and restore the targeted systems should such attacks occur.

During the sixth review of the Global Counter-Terrorism Strategy (A/RES/72/284), Member States expressed concern at the increasing use by terrorist organizations and single actings members of those organizations of information and communications technologies (ICT), in particular the internet and other media, and the use of such technologies to commit, incite, recruit for, fund or plan terrorist acts. Member States give due attention to the importance of cooperation among stakeholders in the implementation of the Strategy, including among Member States, international, regional, and sub-regional organizations, the private sector, and civil society. In 2021, the UNCCT Global Programme on Cybersecurity and New Technologies launched one of its very important documents which provided tailored, extensive one-year support on cybersecurity and digital forensics to Burkina Faso and strengthened the country's law enforcement capacities to collect digital evidence to prosecute and adjudicate terrorist offenses. The Programme was launched to assist legal, forensic, and other relevant agencies of Burkina Faso, Bangladesh, Maldives, Malaysia, and the Philippines to enhance their skills and capacities and apply investigative techniques for the acquisition and analysis of digital evidence from encrypted and open sources. All these skills are required to bring terrorists to justice, with full respect for human rights and the rule of law. Thanks to the UNCCT's strategic engagement with NAUSS, the Programme provided joint training to 49 criminal justice officials from West Africa and the Arab States at NAUSS training facilities. As a result, trainees not only enhanced their skills in digital forensics but also strengthened regional collaboration and engagement in countering terrorism. All participants acknowledged that UNCCT's training increased their understanding of the impact of the acquisition and analysis of digital evidence on human rights and how to mitigate human rights risks in their investigative work [19].

Types of threats and attacks

Nowadays we can encounter many threats and attacks in the cyber environment that can lead to a breach of cybersecurity. As a result, it will cause damage on various levels to businesses, organizations, and personal users. individual users. We can enumerate the most common types of threats and attacks in the cyber environment. Currently, the term - Cyberterrorism means the use of computer technology and cyberspace to carry out terrorist actions, for example, to shut down critical systems or to obtain confidential information. Usually, viruses and other malicious software are distributed via email, also it can be a result of downloads from the Internet, which can cause serious damage to computers and networks. It means that all these can be used by cyber terrorists to damage target systems and networks, as well as help them to collect confidential information. At the same time, cyberterrorists can create and distribute various types of malware, such as viruses, Trojans, and spyware, which cause various threats including identity theft, blocking computers and networks, as well as deleting or changing important information. The purpose of such attacks may be to discredit a certain company or government, as well as to carry out terrorist acts. There are different types of attacks on personal data to obtain confidential information such as passwords, credit card numbers, etc.[20,21].

We must accept that the manipulation of people using basic principles of human psychology and behavior and social engineering is now becoming another growing threat to virtual communities and one of the effective means to harm attacking information systems. Manipulation in social media especially among young generations is very dangerous in the longterm perspective. First youth are quite vulnerable and can easily be subject to false ideologies coming through terrorist propaganda. Another important problem is the proper protection of access to security systems, which always could the

attention of potential terrorists and extremists. Therefore, the issue of training employees and those staff who have access to confidential information is extremely vital [22]/

One of the most often used threats is DDoS attacks: usually, these are attacks that are carried out by creating a huge number of requests to a specific server or site, which can lead to its overload and failure. By these means, cyberterrorists can damage important systems and networks. Often cyberterrorists can use botnets - networks of infected computers from which they can spread a large number of requests to servers. As a result, these servers are overloaded and become inaccessible to users. It is most dangerous not only for banks or any financial systems but also for facilities of critical infrastructure power supply systems, nuclear installations, transport management systems, etc.

It is known, that initially botnets were developed to perform certain tasks within a group or network so that make jointly perform a task. But now, we observe that it is being used by intruders and hackers who are trying to gain access to the network to inject any malicious code or malware. What is most alarming is that currently botnet attacks are aimed against large enterprises and corporations due to their huge access to data [23].

Another type of threat is Cyber Espionage which has a long history of its existence. Usually, it consists of two parts: the monitoring and collection of confidential information about companies, governments, or other organizations to get commercial data political secrets, intellectual property, etc. One of the most known is the ransomware program, which is a special file encryption program that uses a unique, reliable encryption algorithm to encrypt files on the target system. The authors of ransomware programs take advantage of this and usually demand a significant amount of ransom from victims for providing a decryption code or decrypting data. Nevertheless, there is no guarantee that the data could be recovered even after payment of the ransom.

Now, we can observe many more types of cyberterrorism like Cyberbullying, which is one of the aggressive forms of targeted harassment, insults, and threats using modern means of communication. Cyber-extremism is another type of propaganda that incites various extremist views in cyberspace, including ugly scenes of cruelty, alcohol, drugs, etc. which can contradict common norms of morality [6] [9] [23].

Methods of Protection

In any information system, nothing can provide absolute protection, so almost every system can be hacked. But even if it is impossible to provide full protection to any user, it is better to use tools and follow the rules for the safe use of resources. For protection, you can use antiviruses, make a backup copy, and update security programs, all of the above are the most basic rules of cyber defense. Now social networks also pose a great danger, so it is important to use complex passwords and change them more often, not open websites through unfamiliar links, and not spread personal data. If you do not follow these rules, the chance that you will be hacked increases [20], [24].

Cyber security is especially important now because cyberterrorists use the most advanced technologies to disrupt the protection of important state infrastructures. Cyberterrorists mainly target systems such as healthcare and energy, transportation systems, and government agencies. And technologies that allow remote attacks on systems are highly valued by terrorist organizations, including Al-Qaeda and ISIS. It is necessary to improve the methods and technologies of system protection to prevent cyber attacks or eliminate the consequences in time and restore the functioning of systems.

Every year there are more and more digital services, that is, states are becoming more technologically advanced. Although it makes life easier, these technologies can be used with malicious intent, so you need to think in advance about methods to counteract their misuse [25].

Cyberspace threats can cause problems not only to one state, country, or specific organization, but the whole international community and even the entire world. Therefore desperately need to increase the role of international cooperation in the field of the cybersecurity sector. Such cooperation in the field of cybersecurity consists of the following: exchanging of information and proficiency, synchronization of actions, the improvement of principles and regulations of activities in cyberspace, and course joint efforts to avoid and react to cyber threats. Thanks to international collaboration in the field of cybersecurity all parties can reach the

exchange of information and know-how in the field of cyber protection and fight against cybercrime. It allows international organizations to create standards and swap proposals in the field of cybersecurity, which can be used and accustomed by various countries.

Today there are several organizations and initiatives focused on strengthening the role of international cooperation in the field of cybersecurity, for example: the International Telecommunication Union (ITU), the Organization for Economic Cooperation and Development (OECD), the Cybersecurity Forum within the framework of the World Economic Forum, etc. Each country tries to conclude bilateral and multilateral treaties on cybersecurity issues. Also, it is necessary to organize regular international exercises and training to prepare specialists in the field of cybersecurity and professional progress. All these will help to build up and clarify measures for responding to cybersecurity threats and advance information defense systems.

To defend from cyberattacks and cybercrimes related to terrorism, States and private companies should work out comprehensive measures to improve cybersecurity. In particular, they should reinforce security procedures such as two-factor verification, encryption, network filters, and multi-level security instruments. However, it should be borne in mind that cybersecurity is not only technical measures but also personnel preparation. We do believe that any governments and private companies should remember that staff training is one of the most vital aspects of ensuring cybersecurity. Any Human Resources Department should recognize that its employees of the organization may be unaware of cybersecurity therefore should be trained to understand fraudulent attempts, use strong passwords, work with email and other tools, and comply with given instructions on security policies.

Finally, we do believe that it is a good idea to introduce a new curriculum “Cyber security and the fight against terrorism in the context of globalization” for master’s students at the Institute of Public Administration and the Institute of Diplomacy of the Academy of Public Administration under the President of the Republic of Kazakhstan. We also propose to introduce the teaching of similar topics in retraining and advanced training courses for civil servants at primary, middle, and senior levels.

Particularly important, in our opinion, is training under such a program for civil servants of law enforcement agencies, such as the Ministry of Defense, National Security, the Ministry of Internal Affairs, the Prosecutor General's Office, etc. Experts from international organizations, including UNDP, the UN Counter-Terrorism Committee in New York, as well as the OSCE Counter-Terrorism Office, the UN Office for Combating Drug Trafficking and Crime, etc., could take part in the preparation and improvement of the above program.

We also propose to provide the opportunity for students of the Academy of Public Administration and civil servants of relevant departments, especially government agencies of law enforcement agencies, to undergo internships abroad within the framework of scholarships provided by relevant non-governmental and other international organizations.

Conclusion

In the modern world, cybersecurity is one of the most important parts of national, public, and economic security. In general, the problem of cybersecurity requires constant attention and decisive actions on the part of governments, and organizations to protect national interests and public welfare. We advise introducing to study of this issue in training courses for civil servants and staff of national companies and security organisations.

We propose to raise more awareness of the fact that with the development of information technologies, cybersecurity threats are becoming more diverse and serious, which requires constant improvement of methods and technologies for protecting information systems and data within problems connected to terrorism and other criminal actions. The information space is becoming an integral part of the lives of people and organizations around the world, which makes it vulnerable to cybercrime and cyberterrorism. The information war that is taking place in cyberspace can have serious consequences for national and public security.

We believe that the introduction of a new curriculum on educational courses on cybersecurity within academic and training programs on counter-terrorism, including distance courses, will help to raise awareness and competence in the field of cybersecurity

among the general public, including government officials, business leaders, and ordinary Internet users. Also, this will help to form a culture of security in society and prevent potential threats in the field of cybersecurity. Thus, according to our research, we consider it appropriate to expand the training program for future civil servants, schools and universities, law enforcement agencies, police, and other related agencies.

In this regard, it is necessary to strengthen international cooperation in the field of cybersecurity and counter-terrorism in Kazakhstan, and in the region of Central Asia, as a whole, within the framework of main international and regional organizations. First of all, it should include the UN Counter-terrorism Committee, UNODC, and financial and law enforcement agencies to develop new technologies and methods for protecting information systems and data, as well as raise public awareness of possible cybersecurity threats and how to protect their data.

References

1. Tsakanyan, V.T. The Role of Cybersecurity in World Politics [Text] / V.T. Tsakanyan // Vestnik Rudn - International Relations. -2017. - №2. -P.339 - 348.

2. ISO/IEC 27032:2012. Information technology — Security techniques — Guidelines for cybersecurity. – URL: https://standards.iteh.ai/catalog/standards/iso/941c888d-2440-469f-862c-426e3a27b5bd/iso-iec-27032-2012 (Date of access: 25.10.2023).

3. NIST CSF. National Institute of Standards and Technology Cybersecurity Framework. – URL: https://www.nist.gov/cyberframework (Date of access: 28.11.2023).

4. ISO/IEC 27001. Information Security Management Systems Standard. – URL: https://www.iso.org/ru/standard/27001 (Date of access: 20.11.2023).

5. IEC 62443. International Electrotechnical Commission. – URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (Date of access: 20.11.2023).

6. Voskrekasenko O.A., Kireeva A.A., Shchelina T.T. Formation of Cybersecurity Culture in the System of Vocational Training of College Students as a Pedagogical Problem [Text] / O.A. Voskrekasenko, A.A. Kireeva, T.T. Shchelina // Modern High–Tech Technologies // -2022. -№ 10. - P.125-128.

7. Khlopov O.A. Problems Of Cybersecurity And Protection Of Critical Infrastructure [Text] / O.A. Khlopov // Political Sciences. -2020. - №45. – P.64-69.

8. Dubinina D.B. The problem of media security and cybersecurity of the personality of a schoolboy and a student in the modern information space [Text] / D.B. Dubinina // Ecology of the media environment. - 2019. - P.96–101.

9. Moiseeva N.A. Cybersecurity as an important component of digital literacy of Generation Z [Text] / N.A. Moiseeva // Digitalization and cybersecurity: modern theory and practice. -2021. - P.191-196.

10. ISO/IEC 27032:2023. Information Technology. Security methods. Cybersecurity Guidelines. -URL: https://cdn.standards.iteh.ai/samples/76070/be57667fdd0b432490c253ca538c9938/ISO-IEC-27032-2023.pdf (Date of access: 29.10.2023).

11. GOST 56205-2014 IEC/TS 62443-1-1:2009. Industrial communication networks. Network and system security. -URL: https://docs.cntd.ru/document/1200114169 (Date of access: 29.11.2023).

12. Putyato M.M., Makaryan A.S. Cybersecurity as an Integral Attribute of Multilevel Protected Cyberspace / M.M. Putyato, A.S. Makaryan // CASPIAN: Control and High Technologies. -2020. -№. 3 (51). – P. 94-102.

13. GOST ISO/IEC 27005-2010. Information Technology. Information Security Risk Management. -URL: https://docs.cntd.ru/document/1200084141 (Date of access: 29.11.2023).

14. Is the threat of terrorism in Kazakhstan real? / Sayasat. -1999. -№ 10. -P. 8.

15. Satpaev D. Terrorism as a phenomenon of political life / D. Satpaev // Sayasat. -№10. -P. 10-11.

16. Bukina Zh. Outlawed [Text] / Zh. Bukina // Kazakhstanskaya Pravda. -№60. -P. 1.

17. International Convention for the Suppression of the Financing Terrorism / General Assembly of the United Nations. -1999. - URL: https://treaties.un.org/doc/db/terrorism/english-18-11.pdf (Date of access: 29.11.2023).

18. On countering extremism / Law of the Republic of Kazakhstan. – 2006. -№ 31. -URL: https://adilet.zan.kz/eng/docs/Z050000031_ (Date of access: 29.11.2023).

19.Cybersecurity and New Technologies. Office of Counter-Terrorism. -URL: https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity (Date of access: 29.11.2023).

20. Gubenkov A.O., Lukyanova V.V. Actual Problems Of Cybersecurity In Social Networks [Text] / A.O. Gubenkov, V.V. Lukyanova // Personal Autonomy. - 2021. -№ 3(26). – P.46-53.

21. Matkarimov A., Berdieva B., Ashyrova M. Basics of Cyber Security and Its Need [Text] / A. Matkarimov, B.Berdieva, M. Ashyrova // Cognitio Rerum. - 2023. - №3. – P.111-114.

22. Vorobyova I.A., Sazonov A. Methods of Social Engineering in the Context of Cybersecurity Informatics and Computer Engineering And Management [Text] / I.A.Vorobyova, A. Sazonov // Natural and Technical Sciences. -2020. -№ 1. – P.111-114.

23. Chernova E. V., Dokolin A. S., Gavrilova I. V. Formation of Readiness to Ensure Personal Cybersecurity in Early Adolescence [Text] / E. V. Chernova, A. S. Dokolin // Computer Science and Education. - 2018). - №7. – P.16-26.

24. Alekperov I.D. Gorbacheva A.A. Types of Cybersecurity Threats and Ways to Combat Hacking / I.D. Alekperov, A.A. Gorbacheva // Applied Aspects of Soft Modeling in Management in the Context of Digital Transformation. - 2021. -№. 2. – P.34-40.

25. Cybersecurity Challenge. Countering Digital Terrorism // United Nations. – 2019. – URL: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2091207_press_release_cyberchallenge_final.pdf (Date of access: 29.11.2023).

ТЕРРОРИЗММЕН КҮРЕСТЕ КИБЕРҚАУІПСІЗДІК МӘСЕЛЕЛЕРІНІҢ РӨЛІ

Ризвангуль САДЫКОВА, *лектор, PhD, MD, MA, LLM, М. Нәрикбаев КАЗГЮУ Университеті, Астана, Қазақстан, rizvanaholland@mail.ru*

Алия КИНТОНОВА, *т.ғ.к., ЖИТ кафедрасы профессорының м.а., Л. Н. Гумилев Еуразия ұлттық университеті, Астана, Қазақстан, aliya_kint@mail.ru*

Айымгүл ГАБДУЛЛИНА, *ЖИТ кафедрасының магистранты, Л. Н. Гумилев Еуразия ұлттық университеті, Астана, Қазақстан, aiym.g.e@mail.ru*

Роман КАРАСЬ, *п.ғ.к., ақпараттық талдау және саяси технологиялар кафедрасының доценті Бауман МГТУ, Мәскеу, Ресей Федерациясы, romankaras2009@gmail.com*

РОЛЬ ПРОБЛЕМ КИБЕРБЕЗОПАСНОСТИ В БОРЬБЕ С ТЕРРОРИЗМОМ

Ризвангуль САДЫКОВА, *лектор, PhD, MD, MA, LLM, М. Нарикбаев Университет КАЗГЮУ, Астана, Казахстан, rizvanaholland@mail.ru*

Алия КИНТОНОВА, *к.т.н., и.о. профессора, кафедра технологии искусственного интеллекта, Л.Н. Гумилев Евразийский национальный университет, Астана, Казахстан, aliya_kint@mail.ru*

Айымгул ГАБДУЛЛИНА, *магистрант кафедры ТИИ, Л.Н. Гумилев Евразийский национальный университет, Астана, Казахстан, aiym.g.e@mail.ru*

Роман КАРАСЬ, *к.п.н., доцент кафедры информационной аналитики и политических технологи, МГТУ им. Баумана, Москва, Российская Федерация, romankaras2009@gmail.com*