CYBERSECURITY AND CURRENT GLOBAL THREATS IN CENTRAL ASIA

Marzhan ORUMBAYEVA *Doctoral student in International Relations, Sorbonne-Kazakhstan Institute, KazNPU named after Abai, Almaty, Kazakhstan, orumbaeva_marzhan@mail.ru*

Aimen KURMANGALI* *Doctor of Political Sciences, Associate Professor, Sorbonne-Kazakhstan Institute, KazNPU named after Abai, Almaty, Kazakhstan, aymena@mail.ru*

DOI: 10.52123/1994-2370-2022-657
UDC 327
CICSTI 11.25.15

Abstract. Cybersecurity issues have become the main feature for internal security in Central Asia, since today everything is subject to digitization processes: personal documents, video surveillance, electronic dossiers on suspects, interception of cellular communications, forecasting and information collection, etc. Cyber defense, like nuclear deterrence, began to be implemented through deterrence, so here the fundamental strategic balance may be disrupted with relatively modest resources. One of the significant topics associated with the regulation of numerical space is represented as a guarantee of cybersecurity. Against the background of increasing extremism, this problem is extremely topical for CA. Even if the Central Asian states have not yet achieved the level of a high-tech community, the subject of cybersecurity has takeover the regional media in an ambivalent context.
Keywords: cybersecurity, cyberterrorism, cyber defence, Central Asia, cyber shield.
JEL code: F50.

Аңдатпа. Киберқауіпсіздік мәселелері Орталық Азиядағы ішкі қауіпсіздіктің басты ерекшелігіне айналды, өйткені бүгінде барлығы цифрландыру процестеріне ұшырайды: жеке құжаттар, бейнебақылау, күдіктілерге арналған электрондық құжаттар, ұялы байланысты ұстап қалу, болжау және ақпарат жинау және т. б. киберқорғаныс, ядролық тежеу сияқты, тежеу арқылы жүзеге асырыла бастады, сондықтан мұнда іргелі стратегиялық теңгерім күдіктілерге қатысты болған кезде бұзылуы мүмкін. қарапайым ресурстар. Сандық кеңістікті реттеуге байланысты маңызды тақырыптардың бірі киберқауіпсіздік кепілі ретінде ұсынылған. Өсіп келе жатқан экстремизм аясында бұл мәселе Орталық Азия үшін өте өзекті. Егер Орталық Азия мемлекеттері жоғары технологиялық қоғамдастық деңгейіне әлі жетпесе де, киберқауіпсіздік тақырыбы аймақтық БАҚ-ты екі жақты контексте қабылдады.
Түйін сөздер: киберқауіпсіздік, кибертерроризм, киберқорғаныс, Орталық Азия, киберқалқан.
JEL коды: F50.

Аннотация. Вопросы кибербезопасности стали главной особенностью внутренней безопасности в Центральной Азии, поскольку сегодня все подвергается процессам оцифровки: личные документы, видеонаблюдение, электронные досье на подозреваемых, перехват сотовой связи, прогнозирование и сбор информации и т.д. Киберзащита, как и ядерное сдерживание, начала осуществляться посредством сдерживания, поэтому здесь фундаментальный стратегический баланс может быть нарушен при относительно скромных ресурсах. Одна из значимых тем, связанных с регулированием числового пространства, представлена как гарантия кибербезопасности. На фоне растущего экстремизма эта проблема чрезвычайно актуальна для ЦА. Даже если государства Центральной Азии еще не достигли уровня высокотехнологичного сообщества, тема кибербезопасности захватила региональные СМИ в двойственном контексте.
Ключевые слова: кибербезопасность, кибертерроризм, киберзащита, Центральная Азия, киберщит.
JEL код: F50.

Introduction

The relevance of the topic is triggered by the development of the digital world, which in turn has led to the emergence of a new branch of security in cyberspace issues. Cybersecurity is based on local or international knowledge of technical infrastructure and ethical norms. Today, nations around the world are exposed to various attacks that compromise the security of their cyberspace.

Recent leaks regarding the U.S. cyber arsenal, especially regarding the use of Stuxnet against Iran's nuclear facilities, confirm that cyber warfare has become part of a modern defence strategy.

* *Corresponding author: A. Kurmangali, aymena@mail.ru*

In Central Asia, as in the rest of the world, cyber security is primarily important for energy infrastructure facilities and industrial resource extraction.

We believe that law enforcement agencies will use cyber security as an effective mechanism in managing possible asymmetric conflicts in the event of public protests or terrorist attacks.

One of the significant topics associated with the regulation of numerical space is represented as a guarantee of cybersecurity. Against the background of increasing extremism, this problem is extremely topical for the countries of Central Asia. Cybersecurity issues are still being considered in the context of the highest level of "cyberterrorism threat".

Methodology

Applying the historical-sociological method to international relations and its predictive capabilities to the study of the international system, it can be predetermined that cybersecurity is one of the main components of global security. The predictive capabilities of this method are still unreviewed and lead to its use in theoretical analysis of international realities.

This paper also used quantitative methods, which include a set of mathematical and statistical methods used to analyze data. The quantitative research in this paper is based on rigorous statistical models and large samples are used. This makes it possible not just to obtain opinions and assumptions, but to find out the exact quantitative (numerical) values of the indicators under study.

The method of content analysis of documents gained particular importance when solving the tasks of collection, processing and analysis of publications (messages) in the media on this topical issue of international life.

Results and discussion

Thus, there is a need for a more strategic approach to digital defense. Yet its actual framing remains incipient. Numerous cyber defense techniques exist, though the appropriate terms - namely, digital defense, digital arsenal, digital assaults, digital criminal activity, digital terrorism, digital containment, etc. - are quite complicated to determine.

Even if the Central Asian states have not yet achieved the level of a high-tech community, the subject of cybersecurity has takeover the regional media in an ambivalent context. First of all, it is linked to the debate on "information warfare" - that is, the widespread, conspiratorial idea that world superpowers wage ideological warfare through the media, and, it is suspected, through computer technology.

Cybersecurity issues are also seen in the context of a high degree of 'cyber-terrorism threat'. This approach allows Central Asian governments to legitimize the strengthening of their security institutions vis-à-vis underground movements, as well as to control lively spaces on the internet and social media. Cell phone markets in Kazakhstan, Kyrgyzstan and Tajikistan are nearing the "one phone per person" mark, and are expanding swiftly in Uzbekistan and Turkmenistan as well *(Tadviser, 2021)*.

What's more, China is also a safe haven for cybercriminals, most notably those who engage in economic crime. An American report published in 2011 critiqued both states for using high technology cyber spying for their own development and called China home to "the most active and persistent criminals engaged in economic espionage" *(Baldor, 2011)*.

Increasingly, countries in Central Asia face daily cybercrime. Despite the fact that Kazakhstan ranks 18th in the world in terms of the amount of spam received and 7th in terms of the danger of Web surfing *(Kursiv.kz, 2011)*.

Kazakhstan was the target of 85% of Internet attacks in Central Asia, compared with 8% in Uzbekistan, 4% in Kyrgyzstan, 2% in Turkmenistan, and 1% in Tajikistan, reported Kaspersky Security Network *(CIDRIS, 2011)*.

Large cyberattacks targeted mostly government websites for financial information up until recently. As the digital infrastructure has grown, Kazakhstan has become the main target of such attacks in Central Asia.

In January 2021, there were just over 3,000 cyber-attacks in Kazakhstan - 2.8 times more than in January last year. At the same time, a year earlier, the number of cyber-attacks showed a 30.5% decline.

The security of Kazakhstani personal data is a top priority for the Republic of

Kazakhstan. Thus, the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan announces a call for proposals to the draft law on strengthening personal data protection. Proposals can be submitted until March 15 of this year.

The Republic of Kazakhstan is implementing the State Programme "Digital Kazakhstan", where one of the target indicators is to increase the level of digital literacy of the population from 77% to 83% from 2018 to 2022. In 2019, the actual level of digital literacy of the population was 82.1%, while the target was 78.5%. Kazakhstan ranks 40th in the UN cybersecurity ranking, with only 63% awareness of cybersecurity threats *(Official Information Source of the Prime Minister of the Republic of Kazakhstan, 2020)*.

Of the more than 3,000 cyber-attacks in January 2021, 2,700 were botnets - infecting computers through malware for further exploitation by attackers without their owners' knowledge. The number of botnet incidents increased 3.2 times over the year.

The number of incidents in which access to Internet resources was denied was 176, a 69.2% increase year-on-year. The number of cyber-attacks related to the theft of personal data of Kazakhstanis, i.e. cases of phishing, remained unchanged: 43 incidents. The number of malware-related incidents increased from 37 to 38 during the year.

At the same time, according to Kaspersky Lab's interactive cyberthreat map, the number of infections detected by On-Access Scan in Kazakhstan averaged just over 222,000 per week over the past month.

On-Access Scan is an automatic scan that shows a stream of malware detected while opening, copying, launching or saving files.

Attackers, incidentally, are by definition hard to identify, like their potential sponsors. Nevertheless, the observed attacks in Central Asia are improbable to be the work of state entities looking to undermine their neighborhoods. Hackers are perhaps drawn mainly from domestic criminal organized groups looking for profitable data in finance and industry. In 2010, the FBI arrested one such group. It ran a network of international cyber criminals based in the former Soviet Union and consisted of Russians, Ukrainians, Belarusians and Kazakhs. The Central Asian governments agreed to set up specialized services to combat cybercrime.

Uzbekistan joined the Computer Emergency Response Team (CERT) in 2005, the international information and communication technology security system currently comprising 27 countries *(Fergana.ru, 2005)*.

International co-operation between post-Soviet countries is also increasing. In October 2011, the Interior Ministers of the Commonwealth of Independent States (CIS) approved a draft concept of cooperation in combating technological and information crimes developed by Belarus *(Nur.kz, 2011)*.

Uzbekistan has also decided to install SCADA systems by the end of 2012 to control gas transportation. In addition, SCADA has the task of quickly solving gas leaks and thereby saving a considerable amount of energy.

It is also worth paying attention to the topic of currently spreading suicidal virtual games. The study showed that the main surge of requests came on February 2-3, 2017, i.e. during the period when the topic was widely discussed in the domestic media *(Official website of the President of the Republic of Kazakhstan, 2013)*.

However, an analysis of the messages themselves showed that the absolute majority of messages contained information calling for a boycott of the above-mentioned games or for active opposition.

The State Committee has already prepared an opinion on the draft Law on Personal Information to streamline the situation in this sector, which, once approved, could remove many of the problematic points in this area *(Stan Radar, 2013)*.

A boom in enquiries about suicidal online games in Kyrgyzstan occurred on February 2-3, 2017. Most of the messages contained a call to boycott the games.

A national cyber security programme was adopted by the State Committee, and as part of the work of the aforementioned Analytical Centre, a state cyber security strategy was jointly developed, which includes an implementation plan for the relevant state information security (IS) programme - the Cyber Security Concept ("Cyber Shield of Kazakhstan"). Overall, the main results of the first phase of implementation of the Cyber Security Concept demonstrate the scope of work carried out between 2017 and 2018. In 2017, Kazakhstan scored 0.352 on the Global Cybersecurity Index, up from 0.176 in 2015. Also with the adoption of national cybersecurity commitments (the Cyber Shield of Kazakhstan Concept and a separate plan for its implementation), our country was ranked as a middle-ranking country in this ranking. It is expected that by the end of this year it is planned to complete implementation of respective information-technical means. After completion of these activities it will be possible to talk about building the first phase of a full-fledged "Cyber Shield of Kazakhstan". From the next year the second stage of implementation of the Cyber Security Concept will already begin, which will last until 2022 *(Strategy 2050, 2018)*.

At present, the work on legislative and technical regulation of the issue of counteraction to terrorism and extremism is being carried out jointly with law enforcement bodies. Moreover, in February the "Central Asian Forum on Counteracting Online Extremism and Terrorism" was held in Bishkek under the auspices of the Secretariat of the Defence Council and the State Communications Committee.

Since the threats noted above are relatively new, of course, the first thing Kazakhstan needs to do is to adapt existing legislation so that we can respond promptly to this type of phenomenon. Kyrgyzstan needs to develop technical capabilities to combat such cyber threats. Regarding the Russian law "Yarovaya Package", currently all draft laws in the field of ICT are widely discussed with the public and civil society, and only after that they are submitted for consideration.

Such laws, according to international human rights and freedom of expression organizations, violate the right to freedom of expression, the right to personal space. Of course, with the gradual development of e-governance, these kinds of issues are becoming more and more acute as more and more personal information inevitably begins to flow through communication channels. One of the problems at the moment is that we do not have an established official body responsible for monitoring and detecting breaches in the storage/processing of personal information.

The mentioned law has an important role in the process of rendering state and municipal services in electronic format, requiring personalization/authentication and personal data processing, as well as in the implementation of interdepartmental interaction procedures of state bodies for electronic services rendering.

The amendments to the current law are aimed at improving the legal regulation of this sphere, harmonization of the Kyrgyz legislation with the legislation of the member states of the Eurasian Economic Union and, above all, the Russian Federation, which is important in connection with the signed commitments of the Kyrgyz Republic to join the said integration association. These changes are important in terms of forthcoming electronic interaction within the EAEU of both state bodies and legal entities and individuals, exchange of personal data of subjects, including issues of cross-border transfer of personal data.

The Law on Personal Information will be the basis for the implementation of e-government in each state. The amendments proposed in the draft law are primarily concerned with establishing the competence of the government of Kazakhstan and the Kyrgyz Republic to issue regulations governing the personal data sphere, including security issues, as required by the Constitution and a number of constitutional laws. The gap is filled by supplementing the relevant articles of the law with the competence of the government to issue normative legal acts.

The law should take into account the possibility and necessity to provide state and municipal services in electronic format, personal data processing in automated mode, as well as the possibility to create a personal data information system. When dealing with personal information, requirements for the security of personal data and the level of their protection must be taken into account. In this regard, the law is supplemented by appropriate provisions.

As a result of the proposed amendments, the law will become one of the fundamental documents necessary for the introduction of e-government and the provision of state and municipal services in electronic (interactive) format, which will ultimately allow for a more efficient organization of the state apparatus.

Critical to the national railway company Kazakhstan Temir Zholy, which seeks to digitize its complex operations, cybersecurity issues have become crucial. The state-owned electricity company KEGOC, which aims to obtain information from its grid to better manage energy flows, exports and imports with neighboring countries, has also become crucial to corporate cybersecurity issues.

In fact, what Kazakhstan is doing is moving well ahead of its neighbors in the area of cybersecurity. It is true that the country is forging ahead with plans for its own National Space Program as well through the state agency Kazkosmos at the Baikonur Cosmodrome, tasked primarily with governing satellite commissions for communications satellites. "KazSat-2," a Kazakh government owned and operated communications satellite that has been in the orbit since 2011, currently aids in supervising the country's numerical data.

In Kazakhstan, the defense industry is intent on promoting ambitious high-volume aero-space electronically based capabilities, for example the Caspian Fleet, whose mission is to use the satellite to keep an eye and trace marine fields, shipping lanes used by oil tankers, environmental risks and smuggling.

Cyber defence, like nuclear deterrence, has come to be pursued through deterrence because here the basic strategic balance can be upset with relatively modest resources.

Internal security in Central Asia is experiencing a digitization process: ID documents, security cameras, electronic dossiers on suspects, cell phone interception, monitoring and information collection systems, etc. Increasingly, in local enforcement agencies, it is going to be a primary force in the handling and control an eventual subsequent public outcry or terrorist attack.

Central Asian governments are drawing on the experience of Russia and China on Internet control issues, borrowing Moscow's methods and procuring controlling software from Beijing.

Most local experts still have more contacts in the Russian post-Soviet space, as well as in China, given the SCO ties, which clearly indicates the political perception of cyber security. Western influence in this critical area is largely absent.

In 2009, the U.S. Department of Homeland Security organized cyber defense training (CDX) for Central Asian countries and Afghanistan. However, these initiatives are all too rare. Central Asian countries are not part of the NATO Cooperative Cyber Defence Centre of Excellence, for example, which could help improve the cyber security skills of Central Asian officers in the area of basic ethical rules. Manipulation by political interests of freedoms in cyberspace carries uncertainty and impedes successful approaches that help reduce the threats associated with the increasing digitization of industrial infrastructure as well as defense tools *(Defence-update, 2010)*.

The pandemic and related economic turmoil have provided the impetus for technological innovation, including major breakthroughs in the areas of cloud and peripheral systems. Long-established companies are reshaping their business model and transforming themselves into completely contactless online services. According to Radware's "The State of Web Application and API Protection" report, 70% of production web applications are now running in the cloud. The large-scale migration of workloads to the cloud and offshore will go beyond 2021 and will be a significant factor in corporate security. The pandemic has spurred many trends, including the move to remote working. With many employees working from home, organisations have seen their attack surface and become more diverse. In this situation, security is the top priority, but if companies want to remain productive, service degradation must also be prevented. Another problem is the lack of face-to-face communication. In today's environment, employers may never meet their employees in person. As a result, more and more organisations are moving towards zero-trust models that prioritise security, protect against social media attacks and minimise the potential threats associated with remote interaction *(Shilov and Mishchenko, 2021)*.

National states have long been known to exploit cyber vulnerabilities to further their political goals. As this trend intensifies in 2021, the cyber capabilities of nation-states are expected to reach a level that surpasses the defences of any organisation. As a response, it is prudent for organisations to take a clear stance. For example, they can protect themselves from attacks by nation-state representatives by forming blacklists based on physical location, thereby gaining some advantage. Hackers representing nation-states and organized crime groups will resort to relatively new tactics in 2021. These attackers will attempt to use security organizations as a resource for attacks, acting through security professionals and through organizations with limited resources. The security industry itself is not immune to hacks and cyber-attacks, so its professionals need to be vigilant. A general increase in the intensity of cyber warfare awaits us. Cybersecurity will continue to be the backbone. But in 2021, international law enforcement organisations will take the lead in showing cybercriminals that wrongdoing will not go unanswered. One thing spoils the picture: most past offensive cyber campaigns have not been particularly successful. Nevertheless, public and private organisations must take account of this changing balance of power on the cyber front in 2021 *(Babash, 2021)*.

Operators and service providers are projected to be shaped by the following factors in 2022. First, some of the attack trends of 2022 will persist. An increase in even more sophisticated and more intense lower volume attacks is expected. However, low-volume attacks bring greater challenges. Phantom flood attacks use relatively low bandwidth spectrum and therefore are not detected by detection tools, especially in high-bandwidth networks. Such attacks can be just as dangerous as large-scale attacks hitting newscasts. To detect and prevent this new type of attack, service providers will need to use more automated, specialized and dynamic security tools.

Organised cybercrime, particularly ransomware attackers, have shifted their focus to small and medium-sized organisations. Criminals understand that targeting the largest companies is not always the best tactic. They are increasingly aware of the prospect of being targeted by authorities and the risk of being caught in the harsh prosecution of their cybercrime. A case in point is the Blackmatter virus group, which is a new version of DarkSide. Its members announced that they had ceased operations under pressure from law enforcement.

In 2021, Radware experts recorded an increase in zero-day attacks by more technically advanced attackers, and suggest that this trend will continue. Given the vast stores of cryptocurrency accumulated by ransomware virus distributors, it is very likely that they will also become customers of "specialists" implementing zero-day attack mechanisms *(Hein, 2022)*.

Conclusion

With the development and penetration of the Internet in all spheres of life and its impact on the development of society and economy, cybersecurity issues are becoming increasingly important. Thus, one of the challenges of rapid development of information technology for society may become an increase in cyber-attacks. This problem is becoming more and more acute. On an average, specialists detect 227 thousand malicious software samples in a day. Experts predict that the number of cyber-attacks will increase by 30%. Damage from global cybercrime in 2016 alone is already $600 billion, which is almost 1% of global GDP. Every day, 1.5 million people fall victim to cyber-attacks, and 18 people every second. Such technological challenges require the state to pursue a policy of timely restructuring, economic diversification, and systemic reforms in all spheres of society. At the same time, the speed and frequency of technological change will only increase.

Going forward, criminals will increasingly target small and medium-sized businesses. Smaller targets make themselves feel freer. Although the financial results of such actions are incomparable to corporate attacks, they are offset by a lower level of risk.

Cybersecurity enhancement efforts, difficult to implement in any country, find it extremely difficult to achieve in Central Asia for a number of reasons.

1. Funding as well as enabling access to technology are two key balancing factors. Failure to invest in affordable levels of defense means inadequate anti-virus hardware and software for central and local governments, including in Kazakhstan, one of the most developed countries in the region.

2. There is a shortage of qualified professionals involved in education of state employees or those in the private sector in

how they can use digitized data. And while there are vacancies for cybersecurity experts in Kazakhstan's armed forces, as well as in the Caspian navy, which is planning to develop massive electronic solutions in the aerospace industry, this demand cannot be met by the existing supply.

3. However, the lack of visibility of digital information in Central Asia and the absence of civil debate about the extent of digital information in society are other reasons for the underdevelopment of cybersecurity in Central Asia: the refusal of the authorities to share sensitive information, especially with their strategic partners; the non-cooperation among companies, whose businesses are likewise targeted by cyber-attacks; and inadequate awareness raising among the public about the extent of digital information.

REFERENCES

Hein, D. (2022). 32 Experts Share Advice on Information Security in 2022. *Information Security Solution Review.* https://solutionsreview.com/security-information-event-management/32-experts-share-advice-on-information-security-in-2022/.

CIDRIS. (2011). *Accord de coopération cyber entre Inde et Kazakhstan.* http://cidrisnews.blogspot.com/2011/04/accord-de-cooperationcyber-entre-inde.html. (In French).

Defense-update. (2010). FBI Clamp Down on International Cyber Network, http://www.defenceupdate.net/wordpress/tag/kazakhstan.

Stan Radar. (2017). Kak Kyrgyzstan planiruet borot'sya s kiberugrozami, https://stanradar.com/news/full/24598-kak-kyrgyzstan-planiruet-borotsja-s-kiberugrozami.html. (In Russian).

TADVISER. (2021). Kiberprestupnost' v mire, https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5. (In Russian).

Strategy 2050. (2018). «Kibershchit Kazahstana»: pervye itogi realizacii, https://strategy2050.kz/ru/news/52085/. (In Russian).

Kursiv.kz. (2011). Na dolyu Kazahstana prihoditsya 95,19% spama Central'noj Azii, http://www.kursiv.kz/novosti/vkazakhstane/1195213705-na-dolyu-kazaxstanaprixoditsya-9519-spama-ca.html. (In Russian).

Official Information Source of the Prime Minister of the Republic of Kazakhstan. (2020). Prem'er-Ministr RK A. Mamin provel zasedanie Komissii pri Prezidente RK po voprosam vnedreniya cifrovizacii, https://primeminister.kz/ru/news/premer-ministr-rk-a-mamin-provel-zasedanie-komissii-pri-prezidente-rk-po-voprosam-vnedreniya-cifrovizacii-255041. (In Russian).

Official website of the President of the Republic of Kazakhstan. (2013). Prezident Kazahstana Nursultan Nazarbaev prinyal uchastie v zasedanii Soveta glav gosudarstv-chlenov SHanhajskoj organizacii sotrudnichestva, https://www.akorda.kz/ru/events/international_community/foreign_visits/prezident-kazahstana-nursultan-nazarbaev-prinyal-uchastie-v-zasedanii-soveta-glav-gosudarstv-chlenov-shanhaiskoi-organizacii-sotrudnichestva. (In Russian).

Adilsoz.kz. (2010). V Kazahstane sozdana Sluzhba reagirovaniya na komp'yuternye incidenty», http://news.nur.kz/200694.html. (In Russian).

Fergana.ru. (2005). V Uzbekistane sozdaetsya Sluzhba reagirovaniya na komp'yuternye incidenty, http://www.fergananews.com/news.php?id=1596. (In Russian).

Shilov, A., Mishchenko, V. (2021). *Informacionnaya bezopasnost' finansovogo uchrezhdeniya*. M.: LAP Lambert Academic Publishing, 2021. - 164 p. (in Russian).

Babash, A. V. (2021). *Informacionnaya bezopasnost'*. M.: KnoRus, 136 c. (In Russian).

Baldor, L.C. (2011). U.S. report blasts China, Russia for cybercrime. *USA Today*. http://www.usatoday.com/tech/news/story/201111-03/china-russia-cybercrime/51064724/1.

ОРТАЛЫҚ АЗИЯ ЕЛДЕРІНДЕГІ КИБЕРҚАУІПСІЗДІК ЖӘНЕ ҚАЗІРГІ ЗАМАНҒЫ ЖАҺАНДЫҚ ҚАТЕРЛЕР

Маржан ОРУМБАЕВА*, Халықаралық қатынастар саласындағы докторант, Сорбонна-Қазақстан институты, Абай атындағы ҚазҰПУ, Алматы, Қазақстан, orumbaeva_marzhan@mail.ru*

Аймен ҚҰРМАНҒАЛИ*, саясаттану ғылымдарының докторы, қауымдастырылған профессор, Сорбонна-Қазақстан институты, Абай атындағы ҚазҰПУ, Алматы, Қазақстан, aymena@mail.ru*

КИБЕРБЕЗОПАСНОСТЬ И СОВРЕМЕННЫЕ ГЛОБАЛЬНЫЕ УГРОЗЫ В СТРАНАХ ЦЕНТРАЛЬНОЙ АЗИИ

Маржан ОРУМБАЕВА*, докторант в области международных отношений, Институт Сорбонна-Казахстан, КазНПУ имени Абая, Алматы, Казахстан, orumbaeva_marzhan@mail.ru*
Аймен КУРМАНГАЛИ, *доктор политических наук, ассоциативный профессор, Институт Сорбонна-Казахстан, КазНПУ имени Абая, Алматы, Казахстан, aymena@mail.ru*