І БӨЛІМ. ХАЛЫҚАРАЛЫҚ ҚАТЫНАСТАРДЫ ЗЕРТТЕУДІҢ ТЕОРИЯЛЫҚ МӘСЕЛЕЛЕРІ
РАЗДЕЛ I. ТЕОРЕТИЧЕСКИЕ ВОПРОСЫ ИССЛЕДОВАНИЯ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ
PART I. THEORETICAL ISSUES OF INTERNATIONAL RELATIONS RESEARCH

UDC 327.8
IRSTI 11.25.91
https://doi.org/10.48371/ISMO.2025.60.2.001

ACTUAL PROBLEMS OF CYBERSECURITY RESEARCH IN MODERN INTERNATIONAL RELATIONS

*Sayatbek S.S.[1], Baissultanova K. Ch.[2]
*[1,2] Kazakh Ablai khan University of International Relations and World Languages, Almaty, Kazakhstan

Abstract. In the modern world, in the context of intensive digitalization of the economy, cyberspace is recognized as the main factor in global security. This situation requires a revision of the norms of international law, improvement of mechanisms for cooperation between states. In this article, the authors aim to comprehensively analyze the current challenges of cybersecurity in international relations and make an attempt to propose ways to overcome them.

In this study, the authors conducted a comparative analysis of scientific papers and official documents for the period 2021-2025. The contradictions between the concept of "digital sovereignty" in cyberspace management and the need for global regulation are revealed. In addition, the authors point to the lack of international legally binding norms as the main difficulties in ensuring cybersecurity, the complexity of attributing cyber attacks, and the unfair distribution of resources.

The authors of the article argue that in order to strengthen cybersecurity, it is necessary to increase trust in states, improve the legal framework and expand international cooperation. It concludes that the security of cyberspace is the common interest of all mankind, so harmonious action and open dialogue should be the main priority.

Key words: cybersecurity, International Relations, Information Security, digital sovereignty, international law, cyberspace, norms of behavior of states, cyber threats

Introduction

At the end of the XX and the beginning of the XXI centuries, cyberspace has become a new platform for global competition and cooperation of states.

The rapid development of information and communication technologies (ICT) penetrated into all spheres of society's life and at the same time posed a serious threat to national and international security. A number of researchers highlight cybersecurity as an important area of modern international security. In the era of digitalization, the main problem is to ensure the peaceful development of cyberspace and prevent the escalation of conflicts.

In addition, the service in cyberspace is characterized by anonymity and anonymity, which complicates the classical application of international law [1]. In this regard, states are striving to form common norms of behavior in cyberspace at the bilateral and multilateral levels. Within the framework of the UN, dialogue platforms such as the Group of Government Experts (GGE) and The Open-Ended Working Group (OEWG) are working. However, it is not yet possible to reach a common agreement on legally binding norms. Some countries consider the existing international principles to be sufficient, while others argue about the need to adopt special international legal documents [2].

Global cooperation in the field of cybersecurity is hampered by geopolitical contradictions between the leading powers – the United States, Russia, China. Increased insecurity makes it impossible to coordinate joint efforts. However, as the modern experience of International Relations shows, there are no cases of full-fledged cyber warfare between states. The perception of cyber attacks as a "red line" contributes not to aggravate the situation.

Materials and Methods

The study in the framework of the article relies on an interdisciplinary methodology at the junction of the theory of international relations and modern cybersecurity research. The article aimed to analyze the behavior and positions of states in cyberspace, taking into account the mutual contradiction of liberal and realistic theories. Liberal theory served as the basis for explaining the positions of Western countries in favor of freedom of information and multilateral cooperation. Meanwhile, the realistic approach made it possible to characterize the position of Russia, China and their partners, who put national sovereignty and the interests of the state in the first place.

A comparative expert approach was used as the methodological basis of the study, and cybersecurity strategies and positions of various countries and organizations were analyzed. the expert method was carried out through a qualitative examination of the content of selected documents and a comparative analysis of the experience of different countries.

The selection of materials was carried out on such keywords as "cybersecurity", "international security", "digital sovereignty", taken from scientific databases such as Scopus, Web of Science and open government platforms. The collected texts were studied by the method of thematic coding. In particular, events related to international law, national interests and technological threats were identified. An empirical and Case Study of specific cyber events such as WannaCry, NotPetya, and SolarWinds has been conducted. In addition, the study took into account the relationship between political, legal and technological aspects to justify practical recommendations.

Thus, the study was carried out by combining scientific approaches in the fields of international law, security policy and Information Technology.

Within the framework of the article, the research materials were selected based on current works and official documents published in the period from 2021 to 2025, leading analytical centers and peer-reviewed scientific articles.

UN resolutions and reports, materials of international organizations such as the International Telecommunication Union (ITU), NATO, the European Union, national cybersecurity strategies of various countries, as well as scientific publications of Russian and foreign experts were used as the main sources.

Results

In the course of the analysis of cybersecurity issues in international relations, a number of topical issues were identified. One of the most important of these is the lack of normative clarity.

Although many states generally recognize the application of international law to cyberspace, the regulation of this area by a single legally binding instrument has not yet been implemented. Countries have different positions on this issue.

For example, the United States and the European Union consider the UN Charter and current international norms to be sufficient. In their opinion, the new rules in cyberspace should be of a recommendatory nature, that is, optional.

And Russia and China, on the contrary, support the development of mandatory international legal norms in this area. At the same time, they note the need to put the national sovereignty and domestic legislation of states at the forefront. This position is also reflected in the joint proposals of Russia and China, which state the need to respect the autonomy of each state in the information Space [3].

So far, the lack of agreed universal legal standards (Table 1) causes ambiguity in the views of countries. While one party advocates the openness and freedom of information of the Internet, the other party demands control of the national network and protection of Information Security. Modern accepted norms remain only at the level of non-binding recommendations and require their transformation into concrete actions.

Table 1. comparative analysis of the views of the main world actors on cybersecurity issues

Actor	**Basic principles and priorities**	**Attitude to international norms**	**Examples of initiatives**
USA / EU (Western countries)	Protection of free internet and critical infrastructure; international cooperation with private sector participation.	Support for the current UN norms; development of mechanisms of voluntary behavior. It is believed that the existing norms are sufficient.	US National Cybersecurity Strategy; European Cybersecurity Strategy (2020); cyber diplomacy tools.

Russia/PRC (non-Western countries)	The concept of information security and digital sovereignty; state control of ICT.	Promotion of legally binding norms. Supports the priority of national law and sovereignty.	Code of Conduct initiative (2011); UN General Assembly resolutions on International Information Security (IIS); SCO – IIS cooperation plan.
International organizations	Strengthening trust and developing general rules; technical and institutional support for countries.	Pay attention to the voluntary norms and guidelines for the use of the UN Charter in cyberspace. Promotes the exchange of information and capacity building.	Reports and resolutions of the UN; work of the GGE/OEWG; reports of the ITU (Global Cybersecurity Index); UNOCT projects.

(compiled by the authors)

Secondly, geopolitical factors and trust issues play a major role. The relationship of the leading powers in the cyberspace largely depends on the general political situation. On the one hand, the dialogue at the UN level continues. An example of this is the joint resolution of the United States and Russia on ICT security negotiations in 2021. On the other hand, the tension of Western rhetoric against the PRC and the Russian Federation hinders effective cooperation. Despite this, at the moment there were no cases of open cyberconfliction among the major powers. Experts argue that states still avoid the transition of "red lines" without launching destructive attacks against each other. At the same time, covert conflicts in the form of cyber espionage, cyber attacks on critical targets and misinformation campaigns are increasing, which creates mutual suspicion.

Thirdly, the technical complexity of threats and the pace of development create new challenges. One of the most important issues is the attribution of cyberattacks, that is, the identification of the real culprits of the events. Comparing the difficulties of cyberdiplomacy, the lack of unambiguous attribution significantly complicates the diplomatic reaction and negotiations. International norms even provide a formal algorithm of action for the aggrieved party, but in practice it is often difficult to collect "unconditional evidence". In addition, including the rapid development of artificial intelligence, quantum computing and IoT technology will allow attackers to automate attacks and create new types of threats. For example, AI can be used to generate fake news and audio-video manipulations during election campaigns. Expert reports emphasize that one of the main risks in 2024 is the use of artificial intelligence by attackers. The increase in the complexity of attacks requires states to adapt legal and technical measures, however, the gap between rapid technological changes and the slow process of creating norms remains large [4].

The fourth aspect is the uneven distribution of resources and opportunities. Small and developing countries will face significant difficulties in creating a

sustainable cybersecurity system. So, highlighting "cybersecurity poverty line", experts point to the gap between organizations and states that have sufficient resources and states that do not have them. Among the poorest countries in the south of the world, there are the least stable cyber systems. It is now known as the "cybersecurity poverty line", which reduces the overall level of global security. At the same time, infrastructure vulnerabilities and lack of qualified personnel remain a problem for developed states as well. This forces some countries to use outsourcing or rely on international assistance [5].

Finally, organizational and procedural barriers. The public-private partnership necessary to protect modern networks is not always established in all countries. Some researchers cite difficulties in coordinating efforts between states, international organizations and the private sector. Cyberattacks reporting mechanisms and advisory forums do not work effectively enough due to differences in existing approaches. For example, in the UN, representatives of different countries often debate about the signs of "sovereignty in cyberspace", which remain under a hidden ban.

The results are systematized in Table 1, which compares the main positions of major actors on the main issues of cybersecurity (norms of behavior, priorities, means of cooperation). The table confirms that there are fundamental discrepancies in the accents of Western and non-Western countries.

Current events in the field of international cybersecurity and their consequences

1-event

On May 12, 2017, more than 230,000 systems in 150 countries around the world were attacked by a malware called "WannaCry". The attack caused great damage to the UK National Health Service (NHS), at least 19,000 receptions and operations were postponed, and patients had to be moved to other hospitals [6].

Political and legal consequences in 2018, the US Department of Justice brought charges against North Korean hacker Park Chin hake and officially linked the attack to the Lazarus Group [7]. Based on this event, the UN adopted Resolution A/RES/73/27 and developed recommendations for the protection of critical infrastructure. The European Union adopted the NIS Directive (2018/1972) and accelerated the creation of CSIRTnetworks (Computer Security Incident Response Teams) in the Member States.

This event demonstrated a serious threat to peaceful sectors such as health care and made cybersecurity a hot topic in international humanitarian law. It also increased pressure on the states to officially identify (attribute) the attacker.

2-event

The attack "NotPetya", which took place in June 2017, was carried out by M.E. Doc was spread by updating the accounting program. The attack spread around the world and destroyed the data without the possibility of recovery. Thus, only the Maersk company suffered losses of about USD 200-300 million;

the total global damage was estimated at долларға 8-10 billion [8]. In 2018, the United States, Canada, Japan, Australia, New Zealand, Denmark and the United Kingdom linked the attack to the Russian military intelligence service (GRU) – this was the first collective attribution. NotPetya dealt a heavy blow to the private sector and supply chains, prompting states to act together and discuss the possibility of cybersecurity for the first time.

3-event

Attack "Solar Winds" in December 2020

More than 18,000 organizations, including the US Department of the Treasury, the Department of Commerce and the National Security Agency, were attacked by malicious code embedded in the SolarWinds Orion program. The US government adopted the CISA directive and Presidential Decree 14028 and approved the "Zero Trust" Architecture and software materials list SBOM (Software Bill of Materials) as a mandatory standard [9,10]. In addition, the declaration on the security of the supply chain was discussed at the G7 site.

This attack showed that the vulnerability of only one supplier threatens the entire system. Supply chain security has become an important element of the international principle of due diligence.

These three events prompted states to form cybercrime rules, attribution procedures, and confidence-building measures. They make it clear that technological progress and the transition of critical infrastructure to private are ahead of international law, and therefore new risk management mechanisms are needed at the global, regional and national levels.

Discussion

The main contradictions in international cybersecurity are associated with the difference in the strategic concepts of states. On the one hand, Western countries (USA, EU, NATO) are trying to maintain the "transparency" of the internet and are based on multilateral voluntary norms. On the other hand, Russia, China and their partners support the approach of digital sovereignty, demanding global recognition of national laws and strict rules. The discussion around this issue reflects the big problem of the theory of international relations – the incompatibility of liberal and realistic approaches in the digital sphere [11].

The opinion of Russian researchers E. Zinovieva and Ya. Bai rightly characterizes the theoretical and practical contradictions that exist in today's international cyberspace and digital control system.

Indeed, Western countries such as the United States and the EU are proposing a model of governance based on multilateral, voluntary norms, advocating the preservation of the openness and freedom of the internet. This position relies on liberal theory. According to the liberal view, it is believed that states and societies can ensure global security by strengthening openness and cooperation. Freedom of information and the borderless nature of cyberspace are the basis of this position.

Russia, China and their partners, on the contrary, promote the priority of national sovereignty and state control. This approach is based on the realist theory, which considers it important for states to protect their interests, put national laws and security first. The concept of digital sovereignty clearly reflects this point of view, where each state seeks to keep its information space in full control.

The conflict between these two different approaches makes it difficult to form unified global rules for managing cyberspace. The incompatibility of liberal and realistic views increases distrust between states and hinders the possibility of reaching a global agreement on cybersecurity.

However, in modern difficult conditions, the search for ways to reconcile these two approaches is relevant. To resolve this contradiction in the theory of international relations, a balanced approach is needed. This approach should seek to harmonize internet freedom on the one hand and national security on the other.

It is important to note that the implementation of norms of responsible behavior in cyberspace strongly depends on trust between states. The studied circumstances indicate that during the escalation of the geopolitical conflict, agreed security measures become difficult. As zinovieva noted, after the outbreak of a large-scale military conflict in Europe, the dialogue between the United States and Russia on IIS practically stopped. Similarly, attempts to agree on confidence-building measures (for example, within the OSCE or UN) have previously only temporarily yielded results. Thus, the paradox is that the higher the tension in the international arena, the less opportunities for cooperation on cybersecurity, although in the context of this confrontation, such cooperation would be the most demanded [12].

At the present stage, there is an increase in the pace of development of Defense and attack technologies in cyberspace. Many countries of the world are investing heavily in strengthening cyber armies and intelligence structures. As a result, defense structures (for example, Cyber Command, CERT) are forced to adapt to new threats.

According to the latest research, in order to manage cyber conflicts, a number of countries began to introduce rules for distinguishing between military cyber units and civilian CERTs (Computer Emergency Response Teams). However, the legislative regulation of cyber attacks within the framework of international law has not yet been fully resolved. It remains unclear exactly how the UN Charter will apply to cyberattacks against civil infrastructure.

Modern international norms are not binding legal acts, but are often adopted at the level of political agreements. Therefore, their implementation depends on the political will of the parties. Although such principles as non-attacks on infrastructure and assistance in cyber incidents are supported by the state, there are no clear mechanisms for monitoring and fulfilling these obligations. Such a situation can increase the risk of "responding to unfriendly actions" and lead to a period of "post-embargo".

States should not limit themselves to declarations, but increase interaction through the exchange of accurate information, technical cooperation and joint exercises. These steps will strengthen global confidence and stability.

At the same time, Asian, African and Latin American countries are lagging behind in the development of infrastructure and regulation. This leads to common risks for the whole world, because cyber threats are not subject to borders. Therefore, it is necessary to expand technical assistance programs, training courses and experience exchange activities within the framework of the UN and regional organizations. We believe that it will be possible to implement such steps through regional initiatives, such as the information security plan of the Shanghai Cooperation Organization.

During the COVID-19 pandemic, the vulnerability of health systems to cyber attacks was revealed at an unprecedented level. Hospitals and laboratories have urgently implemented VPNs, cloud services, and telemedicine platforms to provide quick access to remote employees; however, such "rapid digitalization" took place without a security audit. As a result, attackers easily found servers with no patches installed, outdated Windows machines, and poorly configured remote access gateways. 2020 21. in Europe alone, cases of phishing and ransomware targeting the health sector increased by 47% [13]. Programs such as Conti and Ryuk have disabled the Irish HSE system, and Maze USA has disabled more than 400 more clinics. Attacks were also recorded by state APT groups against research centers that were engaged in the development of a vaccine – they were intended to steal intellectual property and personal data of patients [14,15]. Taking advantage of the shortage of personnel during the pandemic, cybercriminals tricked and obtained permits through fake medical logins. An additional danger is the fact that digital medical devices (CT, perfusors) are connected to the network, but also work in old OS, which is not supported by the manufacturer: these were continuously used in the infection departments, so it was not possible to update in time. The pandemic has exposed the imbalance between the rapid expansion of digital infrastructure and the resources allocated for security, and has proved that the health sector will be a weak link in future crises if cybersecurity is not systematically strengthened.

Conclusion

In the course of the study within the framework of the article, topical areas of international cybersecurity issues were systematized and analyzed. It was found that the massive digitalization of the social and military sphere poses new challenges for diplomacy and security policy. It has been noticed that there are disagreements between the major powers of the world over the ways of managing cyberspace. This includes the divergence of opinions regarding the legal obligation of cybernetics and the concept of digital sovereignty.

At the same time, the development of artificial intelligence and quantum technologies poses new threats that are complex and rapidly changing. Based on the analysis of scientific literature and official documents in this area, we have found that the lack of uniform standards weakens the joint defense of states and increases inequalities in technical capabilities.

Based on the results of case and empirical studies of the events of WannaCry, NotPetya, SolarWinds, the idea was expressed that a single attribution mechanism should be created with the support of the UN. This requires reducing the influence of politics in the investigation of attacks and introducing a procedure for collecting evidence and storing artifacts. National cybersecurity protection must be complemented by open requirements for Supply Chain Security and mutual obligations not to attack infrastructure.

In summary, cybersecurity research requires an interdisciplinary approach. This requires the Coordination of technical solutions and mechanisms of reliable cooperation, bringing together political scientists, lawyers and IT specialists.

To strengthen cybersecurity, the international community needs to transform political will into concrete actions and take systematic steps to overcome technological inequalities. This will make it possible to form global response mechanisms that will protect the interests of all states.

REFERENCES

[1] Надёжин А.Д. Международная кибербезопасность как новый вызов в эпоху цифровизации // Аспирантские чтения – 2022: материалы конференции. – Казань, 2022. – С. 156–163.

[2] United Nations. Security Council Report S/2023/412. – New York, 2023.

[3] Farnsworth T. China and Russia Submit Cyber Proposal // Arms Control Today. – 2011. – November.

[4] World Economic Forum. Global Cybersecurity Outlook 2024: Insight Report. – Geneva, 2024.

[5] Shanghai Cooperation Organization. Meeting of the SCO Expert Group on International Information Security (18–19 April 2024), https://eng.sectsco.org/

[6] National Audit Office (UK). Investigation: WannaCry Cyber Attack and the NHS, https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/

[7] U.S. Department of Justice. North Korean Regime Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Financial Crimes, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged

[8] Digital Guardian. The Cost of a Malware Infection: Maersk's 300 Million USD Lesson, https://www.digitalguardian.com/blog/cost-malware-infection-maersk-300-million

[9] TechTarget. SolarWinds Hack Explained: Everything You Need to Know, https://www.techtarget.com/whatis/feature/solarwinds-hack-explained

[10] NIST. Executive Order 14028 – Improving the Nation's Cybersecurity: Resource Center, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

[11] Зиновьева Е., Бай Я. Практика цифрового суверенитета в России и КНР. – М.: Российский совет по международным делам, 2023. – 22 февраля.

[12] Hogeveen B. The UN Cyber Norms: Guidance and Gaps for Offensive Cyber // The Cyber Defense Review. – 2022. – Fall. – P. 131–152.

[13] ENISA. 47 % Rise in Cybersecurity Incidents in the Health Sector in 2020, https://www.hstoday.us/subject-matter-areas/cybersecurity/eu-agency-reports-47-rise-in-cybersecurity-incidents-in-the-health-sector-in-2020/

[14] Health Service Executive. Conti Cyber Attack on the HSE: Full Report, https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

[15] Newman L. Universal Health Services Hit by Ransomware Attack // Wired. – 2020. – 29 сентября, https://www.wired.com/story/universal-health-services-ransomware-attack/.

REFERENCES

[1] Nadezhin A. D. Mezhdunarodnaya kiberbezopasnost′ kak novyj vyzov v epokhu tsifrovizatsii [International Cybersecurity as a New Challenge in the Digital Age] // Aspirantskie chteniya – 2022: materialy konferentsii. – Kazan′, 2022. S. 156–163 [in Russ.].

[2] United Nations. Security Council Report S/2023/412. – New York, 2023.

[3] Farnsworth T. China and Russia Submit Cyber Proposal // Arms Control Today. – 2011. – November.

[4] World Economic Forum. Global Cybersecurity Outlook 2024: Insight Report. – Geneva, 2024.

[5] Shanghai Cooperation Organization. Meeting of the SCO Expert Group on International Information Security (18–19 April 2024), https://eng.sectsco.org/

[6] National Audit Office (UK). Investigation: WannaCry Cyber Attack and the NHS, https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/

[7] U.S. Department of Justice. North Korean Regime Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Financial Crimes, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged

[8] Digital Guardian. The Cost of a Malware Infection: Maersk's 300 Million USD Lesson, https://www.digitalguardian.com/blog/cost-malware-infection-maersk-300-million

[9] TechTarget. SolarWinds Hack Explained: Everything You Need to Know, https://www.techtarget.com/whatis/feature/solarwinds-hack-explained

[10] NIST. Executive Order 14028 – Improving the Nation's Cybersecurity: Resource Center, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

[11] Zinov′eva E., Baj Ya. Praktika tsifrovogo suvereniteta v Rossii i KNR [The Practice of Digital Sovereignty in Russia and China]. – Moskva: Rossijskij sovet po mezhdunarodnym delam, 2023. – 22 fevralya [in Russ.].

[12] Hogeveen B. The UN Cyber Norms: Guidance and Gaps for Offensive Cyber // The Cyber Defense Review. 2022. Fall. P. 131–152.

[13] ENISA. 47 % Rise in Cybersecurity Incidents in the Health Sector in 2020, https://www.hstoday.us/subject-matter-areas/cybersecurity/eu-agency-reports-47-rise-in-cybersecurity-incidents-in-the-health-sector-in-2020/

[14] Health Service Executive. Conti Cyber Attack on the HSE: Full Report, https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

[15] Newman L. Universal Health Services Hit by Ransomware Attack // Wired. – 2020. – 29 сентября, https://www.wired.com/story/universal-health-services-ransomware-attack/

ҚАЗІРГІ ХАЛЫҚАРАЛЫҚ ҚАТЫНАСТАРДАҒЫ КИБЕРҚАУІПСІЗДІКТІ ЗЕРТТЕУДІҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ

*Саятбек С.С.[1], Байсултанова К Ч.[2]

*[1,2] Абылай хан атындағы Қазақ халықаралық қатынастар және әлем тілдері университеті, Алматы, Қазақстан

Аңдатпа. Қазіргі әлемде экономиканы қарқынды цифрландыру жағдайында киберкеңістік жаһандық қауіпсіздіктің негізгі факторы ретінде танылды. Бұл жағдай халықаралық құқық нормаларын қайта қарауды, мемлекеттер арасындағы ынтымақтастық тетіктерін жетілдіруді талап етеді. Бұл мақалада авторлар халықаралық қатынастардағы киберқауіпсіздіктің өзекті мәселелерін жан-жақты талдауға және оларды еңсеру жолдарын ұсынуға тырысады.

Бұл зерттеуде авторлар 2021-2025 жылдарға арналған ғылыми еңбектер мен ресми құжаттарға салыстырмалы талдау жүргізді. Киберкеңістікті басқарудағы «цифрлық егемендік» ұғымы мен жаһандық реттеудің қажеттілігі арасындағы қайшылықтар анықталды. Сонымен қатар, авторлар киберқауіпсіздікті қамтамасыз етудегі негізгі қиындықтар, кибершабуылдарды жатқызудың күрделілігі және ресурстарды әділетсіз бөлу ретінде халықаралық заңды күші бар нормалардың жоқтығын көрсетеді.

Мақала авторлары киберқауіпсіздікті нығайту үшін мемлекеттерге деген сенімді арттыру, құқықтық базаны жетілдіру және халықаралық ынтымақтастықты кеңейту қажет деп санайды. Онда киберкеңістіктің қауіпсіздігі бүкіл адамзаттың ортақ мүддесі болып табылады, сондықтан үйлесімді іс-қимыл мен ашық диалог басты басымдық болуы керек деген қорытындыға келеді.

Тірек сөздер: киберқауіпсіздік, Халықаралық Қатынастар, Ақпараттық Қауіпсіздік, цифрлық егемендік, халықаралық құқық, киберкеңістік, мемлекеттердің мінез-құлық нормалары, киберқауіптер

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИССЛЕДОВАНИЯ КИБЕРБЕЗОПАСНОСТИ В СОВРЕМЕННЫХ МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ

*Саятбек С.С.[1], Байсултанова К. Ч.[2]
*[1,2] Казахский университет международных отношений и мировых языков имени Абылай хана, Алматы, Казахстан

Аннотация. В современном мире, в условиях интенсивной цифровизации экономики, киберпространство признается главным фактором глобальной безопасности. Сложившаяся ситуация требует пересмотра норм международного права, совершенствования механизмов сотрудничества между государствами. В данной статье авторы ставят своей целью всесторонне проанализировать современные вызовы кибербезопасности в международных отношениях и попытаться предложить пути их преодоления.

В данном исследовании авторы провели сравнительный анализ научных работ и официальных документов за период 2021-2025 гг. Выявлены противоречия между концепцией «цифрового суверенитета» в управлении киберпространством и необходимостью глобального регулирования. Кроме того, авторы указывают на отсутствие международных юридически обязывающих норм в качестве основных трудностей в обеспечении кибербезопасности, сложность приписывания кибератак и несправедливое распределение ресурсов.

Авторы статьи утверждают, что для укрепления кибербезопасности необходимо повышать доверие к государствам, совершенствовать правовую базу и расширять международное сотрудничество. В ней делается вывод о том, что безопасность киберпространства является общим интересом всего человечества, поэтому гармоничные действия и открытый диалог должны быть главным приоритетом.

Ключевые слова: кибербезопасность, международные отношения, информационная безопасность, цифровой суверенитет, международное право, киберпространство, нормы поведения государств, киберугрозы

Information about authors:

Sayatbek S.S. - Master of Social Sciences, 1st year doctoral student, educational programm “International Relations”, Kazakh Ablai Khan University of International Relations and World Languages, Almaty, Kazakhstan, e-mail: fo_pre@mail.ru

Baissultanova K. Ch. - candidate of political sciences, professor, Kazakh Ablai khan University of International Relations and World Languages, Almaty, Kazakhstan, e-mail: bayisultanova.k@ablaikhan.kz

Авторлар туралы мәлімет:

Саятбек С. С. - әлеуметтік ғылымдар магистрі, «Халықаралық қатынастар» оқу бағдарламасының 1-курс докторанты, Абылай хан атындағы Қазақ халықаралық қатынастар және әлем тілдері университеті, Алматы, Қазақстан, e-mail: fo_pre@mail.ru

Байсултанова К.Ч. - саясаттану ғылымдарының кандидаты, профессор, Абылай хан атындағы Қазақ халықаралық қатынастар және әлем тілдері университеті, Алматы, Қазақстан, e-mail: bayisultanova.k@ablaikhan.kz

Сведения об авторах:

Саятбек С.С. - магистр социальных наук, докторант 1 курса, образовательная программа «Международные отношения», Казахский университет международных отношений и мировых языков имени Абылай Хана, Алматы, Казахстан, e-mail: fo_pre@mail.ru

Байсултанова К. Ч. - кандидат политических наук, профессор, Казахский университет международных отношений и мировых языков имени Абылай Хана, Алматы, Казахстан, e-mail: bayisultanova.k@ablaikhan.kz

Received: April 11, 2025