IRSTI 11.25.00 https://doi.org/ 10.63051/kos.2026.2.70

[1]Gumarova A.N. **[2]Baisultanova K.Sh.** **[3]Ashekey D.A.**
[1,2]Ablai Khan Kazakh University of International Relations and World Languages, Almaty, Kazakhstan
[3]K.I. Satpayev Kazakh National Research Technical University, Almaty, Kazakhstan
E-mail: [1]gumarova.aruzhan@gmail.com, [2] bayisultanova.k@ablaikhan.kz,[3] dimashashekei@gmail.com

CURRENT STATE AND PROSPECTS OF DIGITAL PLATFORMS AND LEGAL MECHANISMS OF CYBERSECURITY WITHIN THE SCO FRAMEWORK

Abstract. The article examines the current state of digital platforms and the prospects for developing political and legal mechanisms of cybersecurity within the framework of the Shanghai Cooperation Organization. The SCO digital agenda is analyzed through two interconnected dimensions: the normative and institutional dimension, which includes international information security, digital sovereignty and political and legal cooperation, and the practical platform-based dimension, which covers digital trade, financial services, logistics, e-commerce, big data and digital public services. The results of the study show that at present digital cooperation within the SCO space is becoming increasingly measurable and operational. At the same time, the development of digital platforms is progressing faster than the formation of common political and legal mechanisms for their regulation. This gap is reflected in the insufficient coordination of approaches to cross-border data flows, digital platform liability, cybersecurity standards, mutual recognition of electronic signatures and digital dispute resolution. The article argues that for Central Asian states, the SCO digital agenda creates both opportunities and risks. The opportunities include access to infrastructure, digital trade, technological modernization, professional training and cybersecurity cooperation. The risks are related to potential technological dependence, political and legal fragmentation and unequal levels of digital development. The study concludes that the future effectiveness of digital cooperation within the SCO will depend on the formation of a balanced framework of political and legal regulation that combines the protection of digital sovereignty and cybersecurity with openness, interoperability and regulatory predictability.

Keywords: Shanghai Cooperation Organization, digital platforms, cybersecurity, digital sovereignty, cross-border data, legal regulation, Central Asia.

Introduction

The rapid expansion of digital technologies has significantly transformed contemporary international relations, economic governance, and regional security mechanisms. The increasing integration of artificial intelligence, cross-border digital platforms, big data systems, and transnational information networks has created not only new opportunities for economic cooperation, but also new vulnerabilities related to cybersecurity, digital sovereignty, and data governance.

In this context, the Shanghai Cooperation Organization (SCO) has gradually expanded its agenda beyond traditional security cooperation toward issues related to digital transformation and information security. Over the past decade, the SCO member states have intensified collaboration in areas such as digital infrastructure, cross-border connectivity, cybersecurity coordination, and the regulation of information space. At the same time, the uneven level of technological development and differences in legal and institutional approaches among member states continue to complicate the formation of a unified digital governance framework.

The growing role of artificial intelligence, digital platforms, and data-driven governance mechanisms has further intensified discussions surrounding cybersecurity and digital sovereignty within the SCO region. While some member states, particularly China and Russia, possess relatively advanced digital and regulatory capacities, other states remain dependent on external technological solutions and continue to face significant legal and institutional challenges in ensuring data security and cyber resilience.

Current developments in digitalization have increasingly shaped the study of international relations and regional processes. In particular, digital interaction within different institutional frameworks has become a subject of growing interest among scholars and policy experts.

Despite the increasing relevance of digital governance issues within the SCO framework, many existing studies remain either overly descriptive or narrowly focused on technological aspects, without sufficient attention to the institutional and legal mechanisms of cybersecurity cooperation. In this regard, the present study aims to analyze the current state and future prospects of digital platforms and legal cybersecurity mechanisms within the SCO, with particular attention to regulatory asymmetries, digital sovereignty, and the challenges of regional digital integration.

Materials and methods

During the preparation of this article, the author primarily relied on academic publications, official documents of the Shanghai Cooperation Organization, legal acts, analytical reports and review-based information sources that directly or indirectly examine the development of digital platforms, cybersecurity mechanisms, digital sovereignty, cross-border data flows and legal regulation within the SCO framework (Agreement, 2009). Particular attention was paid to studies devoted to the construction of SCO digital platforms, including digital legal service platforms, since these works demonstrate how technological modernization within the SCO increasingly intersects with legal cooperation, data governance and the regulation of transnational economic interaction (Jiang, Huang, 2025).

In the process of collecting and interpreting the research material, the study primarily employed the method of systemic analysis. This method made it possible to consider digital platforms and legal cybersecurity mechanisms not as isolated phenomena, but as interconnected elements of the emerging regional digital architecture of the SCO. Such an approach allows the study to identify the relationship between technological development, legal regulation, national strategies of digital sovereignty and institutional mechanisms of international cooperation (Statement, 2023).

Secondly, the comparative political and legal method was applied in order to examine differences in the approaches of SCO member states to the regulation of data, cybersecurity, digital platforms and cross-border information flows. This method is particularly important because the SCO space includes states with different levels of digital development, different political and legal traditions, and different models of state control over cyberspace. As a result, comparative political and legal analysis makes it possible to reveal not only the existing regulatory asymmetry, but also the prospects for creating more coordinated political and legal mechanisms in the field of cybersecurity and data protection (Jiang, Sun, 2025).

The case study method was also used in the article. It allows the research to move beyond a purely descriptive analysis of official documents and to examine how the SCO digital agenda is reflected in specific practical initiatives. These include the development of digital legal service platforms, digital economy projects, cross-border data exchange mechanisms, cooperation in artificial intelligence, cybersecurity initiatives and digital infrastructure projects. The use of practical cases makes it possible to identify the gap between declared institutional goals and the actual difficulties of implementation, including the absence of unified legal standards, the problem of data localization, unequal technological capacities and insufficient interoperability between national regulatory systems (Jiang, Huang, 2025).

The study applies institutional analysis in order to assess the role of the SCO as a regional international organization in shaping digital governance and cybersecurity cooperation. This method makes it possible to determine whether existing SCO mechanisms are sufficient for regulating digital platforms, protecting data and ensuring cybersecurity, or whether the organization requires a more coherent and legally binding framework. The institutional approach is especially relevant because the SCO digital agenda is developing at the intersection of political coordination, economic integration, legal cooperation and security policy.

Discussion

The results of the study reveal a structural imbalance between the practical and legal dimensions of SCO digital cooperation. On the practical level, digital platforms are already expanding in trade, finance, logistics, e-commerce, big data, digital contracts and public services. On the legal level, however, cooperation remains based mainly on information security agreements, intergovernmental declarations, legal cooperation mechanisms and national legislation. This means that the SCO has developed a certain normative and institutional foundation, but it has not yet transformed this foundation into a coherent regulatory architecture for digital platforms.

This imbalance is especially visible in the field of digital legal services. The examined literature emphasizes that the expansion of international economic and trade cooperation among SCO member states increases the demand for digital legal services. A digital legal service platform could support international commercial entities, improve access to legal information, assist in dispute resolution and strengthen legal predictability in cross-border cooperation (Jiang, Huang, 2025). However, the same body of research identifies several barriers: the absence of special multilateral agreements, unclear service content, differences in dispute resolution models, uncertain operational models and compliance problems related to cross-border data flows (Jiang, Huang, 2025). Therefore, the key problem is not the lack of digital initiatives, but the insufficient legal coordination behind them.

The issue of digital sovereignty further complicates this process. A number of studies on the legal protection of digital sovereignty within the SCO framework argue that digital sovereignty has become an extension of national sovereignty in cyberspace and that member states need legal mechanisms for data localization, jurisdiction, digital control and the regulation of major digital actors (Jiang, Sun, 2025). This position is important, but it should not be interpreted one-sidedly. For Central Asian states, the protection of digital sovereignty is necessary, but excessive digital closure may reduce the benefits of regional cooperation. Therefore, their strategic interest is not to copy the most restrictive models of digital governance, but to use SCO mechanisms selectively: to strengthen cybersecurity, expand access to infrastructure and training, develop digital trade and preserve regulatory autonomy.

This is particularly relevant in relation to Russia. Russia remains an important actor within the SCO, including in the field of information security and legal cooperation. However, its current digital environment is increasingly shaped by internet restrictions, platform limitations and a more closed model of sovereign internet governance. A politically neutral assessment would be that such a model may serve domestic security and control objectives, but it is less suitable as a universal model for open regional digital integration. For Central Asian states, a more beneficial scenario is a balanced framework that combines cybersecurity and sovereignty with interoperability, diversified partnerships and access to cross-border digital services.

The main analytical conclusion is that the SCO digital agenda is characterized by a gap between practical digitalization and legal harmonization. Platforms are expanding rapidly, but legal mechanisms remain fragmented and largely dependent on national legislation, bilateral agreements or sectoral initiatives. This creates both opportunities and risks for Central Asian states. The opportunities include access to infrastructure, professional training, digital markets, financial services, e-commerce tools and technological modernization. The risks include regulatory dependence, unequal technological capacity and exposure to dominant external digital models.

Therefore, the most sustainable model for SCO digital cooperation would be a balanced legal architecture that protects digital sovereignty and cybersecurity while preserving openness, interoperability and practical benefits for smaller and medium-sized member states. Such an architecture should include clearer rules on cross-border data flows, platform responsibility, cybersecurity standards, electronic signatures, digital dispute resolution and the protection of critical information infrastructure. Without these mechanisms, digital integration within the SCO may remain fragmented: platforms will continue to develop, but their legal regulation will remain uneven and insufficiently coordinated.

Thus, the discussion demonstrates that the SCO digital agenda is shaped by the tension between rapid technological integration and slower legal harmonization. Digital platforms already support trade, finance, logistics, e-commerce, big data and public services, but their regulation still depends largely on fragmented national and sectoral mechanisms. For Central Asian states, this creates a dual effect: access to new digital opportunities and infrastructure, but also exposure to regulatory dependence and unequal technological influence. Therefore, the long-term effectiveness of SCO digital cooperation will depend on the ability of member states to develop a balanced legal framework that combines cybersecurity, digital sovereignty, interoperability and openness to regional digital interaction.

Research results

The analysis of the collected academic, legal and analytical researches shows that the digital agenda of the Shanghai Cooperation Organization is developing through two interconnected dimensions. The first dimension is normative and institutional. It includes legal documents, intergovernmental statements, expert coordination, legal education and cooperation in the field of international information security. The second dimension is practical and platform-based. It includes digital trade platforms, cross-border financial services, e-commerce mechanisms, big data cooperation, digital signatures and national digital government systems. The results indicate that practical digital cooperation within the SCO is already measurable, while the legal regulation of these processes remains less unified.

The legal basis of SCO digital cooperation was formed primarily through the security agenda. The 2009 Agreement on Cooperation in Ensuring International Information Security established the legal and organizational framework for cooperation in the field of information security and identified key threats related to the use of information and communication technologies (Agreement, 2009). Later, the 2023 Statement of the Council of SCO Heads of State on Cooperation in the Field of Digital Transformation expanded this agenda by linking digital transformation with inclusive growth, digital infrastructure, public services, interoperability, financial technologies, digital platforms and data protection (Statement, 2023). This demonstrates that the SCO digital agenda has gradually moved from a narrow focus on information security toward a broader model of regional digital governance.

The reviewed studies also show that legal cooperation among SCO member states has already developed through several institutional mechanisms. These include the China National Institute for SCO International Exchange and Judicial Cooperation, training courses for specialists in international legal services, training programs for judicial officers, the Committee on Legal Services for the SCO and the Association of Law Universities of the SCO (Jiang, Huang, 2025). These institutions form an important basis for legal capacity-building and expert coordination. However, they do not yet constitute a unified digital legal infrastructure capable of fully supporting cross-border legal services, digital dispute settlement, data compliance and platform governance.

The practical materials examined in this study show that platform-based cooperation within the SCO is developing more rapidly than legal harmonization (SCO China, 2025). Digital initiatives already cover trade, finance, logistics, e-commerce, big data, digital contracts and national digital public services. The most illustrative examples are presented in Table 1.

Table 1. Practical cases of SCO-related digital cooperation and their legal relevance

Case / mechanism	Practical data	Legal relevance	Discussion point
2009 SCO Agreement on International Information Security	Adopted on 16 June 2009	Basic legal framework for information security cooperation	Strong normative basis, but not detailed enough for modern platform governance
2023 SCO Statement on Digital Transformation	Covers digital infrastructure, public services, financial technologies, data protection and digital platforms	Expands the SCO agenda from security to digital governance	Shows the shift from cybersecurity alone to broader digital integration
SCO legal cooperation institutions	Includes the China National Institute for SCO International Exchange and Judicial Cooperation, Committee on Legal Services and Association of Law Universities	Builds legal capacity and expert coordination	Legal cooperation exists, but digital legal infrastructure remains incomplete
China-SCO Demonstration Area, Qingdao	Nearly 5,000 enterprises, 731 suppliers, 191 purchasers registered; 31 freight train routes to 54 cities in 23 countries; trade with SCO countries grew from 850 million yuan in 2019 to 8.1 billion yuan in 2022	Requires regulation of trade data, logistics data, customs data and platform compliance	Economic platforms are developing faster than legal harmonization
"Financial Supermarket" cross-border platform	Online virtual accounts can be opened in as little as 10 minutes; works with 24 banks; service centers in Almaty and Moscow	Raises issues of financial data protection, digital identity, banking compliance and cross-border settlement	Digital finance needs stronger SCO-level cybersecurity and data rules
China-SCO Big Data Cooperation Center	9 training sessions, more than 300 participants, over 20 institutions involved	Supports capacity-building in data governance and digital transformation	Useful for Central Asia, but should be linked to transparent legal standards
China-Kyrgyzstan-Uzbekistan fiber-optic cable	Regional network latency reduced by 40%	Improves connectivity and data transmission	Infrastructure integration must be matched with cybersecurity safeguards
MeetSOHO Silk Road e-commerce platform	Nearly 30 Central Asian buyers	Requires rules on e-contracts, consumer	E-commerce creates practical benefits but also regulatory

	connected with more than 500 suppliers from Jiangsu	protection, payments and personal data	risks
China's cross-border e-commerce with SCO member states	Imports from SCO member states increased by 34% year-on-year in 2024	Strengthens need for predictable digital trade regulation	Digital trade is becoming measurable, not only declarative
Digital signatures, encryption and electronic seals	Used for cross-border contracts; more than 100 clients in China and Russia	Requires mutual recognition of electronic legal instruments	Legal interoperability is becoming a practical necessity
Kazakhstan eGov / eGov Mobile	More than 26 million online public services in H1 2025; 12 million via mobile; over 14.8 million registered users; eGov Mobile audience reached 11 million	Demonstrates national digital capacity in Central Asia	Kazakhstan can participate in SCO digital cooperation from a stronger position
Kazakhstan cybersecurity capacity	94.04/100 in the 2024 Global Cybersecurity Index; Tier 2; maximum score in legal and cooperation measures	Shows progress in national cybersecurity regulation	Central Asian states are not only recipients; they are developing their own regulatory capacity

The data presented in Table 1 show that the SCO digital agenda is no longer limited to declarations or general political statements. It already includes measurable practical initiatives in trade, logistics, finance, e-commerce, big data, digital signatures and public services. The China-SCO Demonstration Area in Qingdao demonstrates the practical expansion of trade and logistics cooperation, while the "Financial Supermarket" platform shows the growing role of digital financial services in cross-border interaction (Financial Supermarket, 2026). The China-SCO Big Data Cooperation Center, the China-Kyrgyzstan-Uzbekistan fiber-optic cable and the MeetSOHO Silk Road e-commerce platform indicate that digital cooperation is also developing in infrastructure, training and electronic commerce (China-SCO Demonstration Area, 2023).

The Kazakhstan case is especially important for evaluating the role of Central Asian states in this process. The eGov.kz and eGov Mobile indicators show that Kazakhstan has already developed a significant national digital government infrastructure. In the first half of 2025, more than 26 million public services were provided online, including 12 million through the mobile application. In addition, Kazakhstan's score of 94.04 out of 100 in the 2024 Global Cybersecurity Index indicates progress in national cybersecurity capacity (eGov.kz, 2025), (Global Cybersecurity Index, 2024). These results suggest that Central Asian states should not be viewed only as passive recipients of external digital infrastructure. They are also developing their own digital governance capacity and can participate in SCO digital cooperation from a more active position.

At the same time, the results show that SCO digital cooperation has moved beyond declarative political statements and is gradually becoming a measurable practical process. The collected data demonstrate the development of digital platforms, cross-border financial tools, logistics networks, e-commerce mechanisms, big data cooperation and national digital government systems. At the same

time, the results confirm that these initiatives are not yet fully integrated into a unified SCO-wide legal regime. This indicates that the main empirical finding of the study is the gap between the practical expansion of digital platforms and the slower development of common legal mechanisms for their regulation.

Conclusion

The conducted analysis demonstrates that the digital agenda of the Shanghai Cooperation Organization is gradually becoming one of the key directions of regional cooperation. Initially, the SCO approached digital issues mainly through the prism of international information security, cybersecurity and the protection of national information space. However, the development of digital platforms, cross-border trade, digital finance, e-commerce, big data, artificial intelligence and electronic public services has expanded this agenda and transformed it into a broader issue of regional digital governance.

The SCO already has a certain legal and institutional basis for digital cooperation. This basis includes the 2009 Agreement on Cooperation in Ensuring International Information Security, later statements on digital transformation, expert coordination mechanisms, legal cooperation institutions and educational platforms. At the same time, these mechanisms remain fragmented and do not yet form a unified legal framework capable of fully regulating modern digital platforms, cross-border data flows, platform liability, cybersecurity standards, digital signatures and digital dispute resolution. In other words, the SCO has developed a normative foundation, but this foundation has not yet become a complete regulatory architecture.

The digital cooperation within the SCO is already measurable and operational. The China-SCO Demonstration Area in Qingdao, cross-border financial service platforms, the China-SCO Big Data Cooperation Center, e-commerce projects, fiber-optic infrastructure and Kazakhstan's digital government indicators show that digital integration is no longer only a political declaration. It is becoming a practical process involving trade, logistics, finance, public services, data exchange and digital infrastructure. However, these initiatives are developing faster than the legal mechanisms needed to regulate them.

The main conclusion of this is that the current digital development of the SCO is characterized by a gap between practical platform-based cooperation and legal harmonization. Digital platforms create new opportunities for regional connectivity, economic modernization and technological capacity-building, especially for Central Asian states. At the same time, the absence of unified legal standards creates risks related to data protection, cybersecurity, regulatory dependence, unequal technological influence and fragmentation of digital governance.

For Central Asian countries, participation in the SCO digital agenda may be particularly beneficial if it is used not as a mechanism of dependence on stronger digital actors, but as an opportunity to strengthen national digital capacity, expand access to infrastructure and markets, improve cybersecurity standards and develop legal expertise. In this regard, the most sustainable model of SCO digital cooperation should be based on balance: protection of digital sovereignty and cybersecurity should be combined with openness, interoperability, legal predictability and practical benefits for all member states.

Therefore, the future effectiveness of SCO digital cooperation will depend not only on the creation of new platforms, but also on the ability of member states to develop common legal principles for their functioning. Such principles should include clearer rules on cross-border data flows, mutual recognition of electronic legal instruments, platform responsibility, cybersecurity compliance, protection of critical information infrastructure and mechanisms for resolving digital disputes. Without this legal coordination, digital integration within the SCO may remain technologically active but institutionally incomplete.

References:

Agreement, 2009 – Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization. 2009. URL: https://eng.sectsco.org/20090616/207486.html (accessed 12.12.2025).

China-SCO Demonstration Area, 2023 – SCO demonstration area offers opportunities for win-win cooperation. 2023. URL: https://english.www.gov.cn/news/202306/17/content_WS648cecddc6d0868f4e8dcf01.html (accessed 16.01.2026).

eGov.kz, 2025 – Since the beginning of 2025, over 26 million state services have been provided to citizens of Kazakhstan online. 2025. URL: https://egov.kz/cms/en/news/public_services_online (accessed 17.01.2026).

Financial Supermarket, 2026 – Qingdao launches cross-border finance platform for SCO countries. 2026. URL: https://global.chinadaily.com.cn/a/202604/29/WS69f1e946a310d6866eb464cb.html (accessed 02.02.2026).

Global Cybersecurity Index, 2024 – Kazakhstan advances in Global Cybersecurity Index 2024. 2024. URL: https://astanatimes.com/2024/09/kazakhstan-advances-in-global-cybersecurity-index-2024/ (accessed 19.01.2026).

Jiang, Huang, 2025 – Jiang S., Huang T. The construction of the Shanghai Cooperation Organization digital legal service platform // Vestnik of Saint Petersburg University. Law. 2025. Vol. 16. Issue 1. P. 252–269. DOI: https://doi.org/10.21638/spbu14.2025.118.

Jiang, Sun, 2025 – Jiang S., Sun Ch. The system of legal protection of the digital sovereignty of the Shanghai Cooperation Organization member states // Vestnik of Saint Petersburg University. Law. 2025. Vol. 16. Issue 2. P. 572–584. DOI: https://doi.org/10.21638/spbu14.2025.219.

SCO China, 2025 – SCO countries join hands to build a bright digital future. 2025. URL: https://www.scochina2025.org.cn/en/n3/2025/0902/c518818-20361232.html (accessed 13.12.2025).

Statement, 2023 – Statement of the Council of SCO Heads of State on Cooperation in the Field of Digital Transformation. 2023. URL: https://eng.sectsco.org/images/07e8/0c/17/1628373.pdf (accessed 06.01.2026).

[1]Гумарова А.Н. [2]Байсултанова К.Ш. [3]Әшекей Д. А.
[1,2]Абылай хан Қазақ халықаралық қатынастар және әлем тілдері университеті, Алматы, Қазақстан
[3]Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы, Қазақстан
E-mail: [1]gumarova.aruzhan@gmail.com, [2] bayisultanova.k@ablaikhan.kz,
[3] dimashashekei@gmail.com

ШЫҰ АЯСЫНДАҒЫ ЦИФРЛЫҚ ПЛАТФОРМАЛАР МЕН КИБЕРҚАУІПСІЗДІКТІҢ ҚҰҚЫҚТЫҚ ТЕТІКТЕРІНІҢ ҚАЗІРГІ ЖАҒДАЙЫ ЖӘНЕ ДАМУ ПЕРСПЕКТИВАЛАРЫ

Аңдатпа. Мақалада Шанхай ынтымақтастық ұйымы аясындағы цифрлық платформалардың қазіргі жағдайы мен киберқауіпсіздікті құқықтық реттеу тетіктерінің даму перспективалары қарастырылады. Зерттеуде ШЫҰ-ның цифрлық күн тәртібі екі өзара байланысты бағыт арқылы талданады: біріншісі – халықаралық ақпараттық қауіпсіздік, цифрлық егемендік және құқықтық ынтымақтастыққа қатысты нормативтік-институционалдық негіз; екіншісі – сауда, қаржы, логистика, электрондық коммерция, үлкен деректер және мемлекеттік цифрлық қызметтер салаларындағы практикалық платформалық бастамалар. Зерттеу нәтижелері ШЫҰ кеңістігінде цифрлық ынтымақтастықтың нақты

практикалық сипат алып келе жатқанын көрсетеді. Сонымен қатар цифрлық платформалардың дамуы оларды реттейтін ортақ құқықтық механизмдерге қарағанда жылдамырақ жүріп жатыр. Бұл жағдай трансшекаралық деректер айналымы, платформалардың жауапкершілігі, киберқауіпсіздік стандарттары, электрондық қолтаңбаларды өзара тану және цифрлық дауларды шешу мәселелерінде құқықтық үйлестірудің жеткіліксіздігін көрсетеді. Мақалада Орталық Азия мемлекеттері үшін ШЫҰ-ның цифрлық күн тәртібі бір жағынан инфрақұрылымға, технологиялық тәжірибеге, цифрлық саудаға және киберқауіпсіздік саласындағы ынтымақтастыққа қол жеткізу мүмкіндігін берсе, екінші жағынан технологиялық тәуелділік пен құқықтық фрагментация тәуекелдерін туындататыны негізделеді. Осыған байланысты ШЫҰ аясындағы цифрлық ынтымақтастықтың тиімділігі цифрлық егемендік пен киберқауіпсіздікті сақтай отырып, ашықтықты, өзара үйлесімділікті және құқықтық болжамдылықты қамтамасыз ететін теңгерімді құқықтық архитектураны қалыптастыруға байланысты болады.

Кілт сөздер: Шанхай ынтымақтастық ұйымы, цифрлық платформалар, киберқауіпсіздік, цифрлық егемендік, трансшекаралық деректер, құқықтық реттеу, Орталық Азия.

[1]Гумарова А.Н. [2]Байсултанова К.Ш. [3]Ашекей Д. А.
[1,2]Казахский университет международных отношений и мировых языков имени Абылай хана, Алматы, Казахстан
[3] Казахский национальный технический исследовательский им.К.И. Сатпаева, Алматы, Казахстан
E-mail: [1]gumarova.aruzhan@gmail.com, [2] bayisultanova.k@ablaikhan.kz, [3] dimashashekei@gmail.com

ТЕКУЩЕЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ ЦИФРОВЫХ ПЛАТФОРМ И ПРАВОВЫХ МЕХАНИЗМОВ КИБЕРБЕЗОПАСНОСТИ В РАМКАХ ШОС

Аннотация. В статье рассматриваются текущее состояние цифровых платформ и перспективы развития правовых механизмов кибербезопасности в рамках Шанхайской организации сотрудничества. Цифровая повестка ШОС анализируется через два взаимосвязанных направления: нормативно-институциональное, включающее международную информационную безопасность, цифровой суверенитет и правовое сотрудничество, и практическое платформенное, охватывающее цифровую торговлю, финансовые сервисы, логистику, электронную коммерцию, большие данные и государственные цифровые услуги. Результаты исследования показывают, что цифровое сотрудничество в пространстве ШОС уже приобретает измеримый и практический характер. Вместе с тем развитие цифровых платформ опережает формирование общих правовых механизмов их регулирования. Это проявляется в недостаточной согласованности подходов к трансграничному обмену данными, ответственности цифровых платформ, стандартам кибербезопасности, взаимному признанию электронных подписей и разрешению цифровых споров. В статье обосновывается, что для государств Центральной Азии цифровая повестка ШОС создает как возможности, так и риски. Возможности связаны с доступом к инфраструктуре, цифровой торговле, технологической модернизации, профессиональной подготовке и сотрудничеству в сфере кибербезопасности. Риски выражаются в возможной технологической зависимости, правовой фрагментации и неравномерности цифрового развития. Делается вывод о том, что дальнейшая эффективность цифрового сотрудничества в рамках ШОС будет зависеть от формирования сбалансированной правовой архитектуры, которая сочетает защиту цифрового суверенитета и кибербезопасности с открытостью, совместимостью и правовой предсказуемостью.

Ключевые слова: Шанхайская организация сотрудничества, цифровые платформы, кибербезопасность, цифровой суверенитет, трансграничные данные, правовое регулирование, Центральная Азия.

Авторлар туралы мәлімет:

Гумарова Аружан Нурлановна – PhD докторант, Абылай хан Қазақ халықаралық қатынастар және әлем тілдері университеті, PhD докторант, ҚР ҒЖБМ ҒК "Ғылым ордасы" ШЖҚ РМК, Алматы, Қазақстан

Байсултанова Кулипа Шарипкановна – саяси ғылымдарының кандидаты, профессор, Абылай хан Қазақ халықаралық қатынастар және әлем тілдері университеті, Алматы, Қазақстан

Әшекей Дінмұхамед Айдарұлы – 2 курс магистранты, М095 Ақпараттық қауіпсіздік, Ақпараттық қауіпсіздікті кешенді қамтамасыз ету, Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы, Қазақстан

Information about the authors:

Gumarova Aruzhan Nurlanovna – PhD doctoral student, Ablai Khan Kazakh University of International Relations and World Languages; PhD doctoral student, RSE on REM “Gylym Ordasy” of the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan, Almaty, Kazakhstan

Baisultanova Kulipa Sharipkanovna – Candidate of Political Sciences, Professor, Ablai Khan Kazakh University of International Relations and World Languages, Almaty, Kazakhstan

Ashekey Dinmukhamed Aidaruly – 2nd-year master’s students, M095 Information Security, Comprehensive Information Security, K.I. Satbayev Kazakh National Research Technical University, Almaty, Kazakhstan

Информация об авторах:

Гумарова Аружан Нурлановна – PhD докторант, Казахский университет международных отношений и мировых языков имени Абылай хана; PhD докторант, РГП на ПХВ «Ғылым ордасы» Комитета науки Министерства науки и высшего образования Республики Казахстан, Алматы, Казахстан

Байсултанова Кулипа Шарипкановна – кандидат политических наук, профессор, Казахский университет международных отношений и мировых языков имени Абылай хана, Алматы, Казахстан

Ашекей Динмухамед Айдарович – магистранты 2 курса, М095 Информационная безопасность, Комплексное обеспечение информационной безопасности, Казахский национальный исследовательский технический университет имени К. И. Сатпаева, Алматы, Казахстан

Келіп түсті 16 наурыз 2026 жыл
Қабылданды 5 мамыр 2026 жыл