Vestnik RUDN. International Relations. ISSN 2313-0660 (Print), ISSN 2313-0679 (Online)
Вестник РУДН. Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ
2026 Vol. 26 No. 2 240–255
http://journals.rudn.ru/international-relations

DOI: 10.22363/2313-0660-2026-26-2-240-255
EDN: HQFCWE

Research article / Научная статья

Integrating Digital Technologies into the Collective Security System of Central Asia and Russia: Developing a Multi-Level Threat Neutralization Model

Sergey G. Luzyanin[1,2], Otabek M. Umarov[1] ✉

[1]National Research University Higher School of Economics, Moscow, Russian Federation
[2]Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation, Moscow, Russian Federation
✉omuhammadaliyevich@mail.ru

Abstract. The study addresses the pressing issue of transforming the collective security architecture in the Eurasian region amidst digitalization and the emergence of new transnational threats. An analysis of contemporary challenges reveals that existing integration structures, such as the Collective Security Treaty Organization (CSTO), the Shanghai Cooperation Organisation (SCO), and the Eurasian Economic Union (EAEU), demonstrate limited effectiveness in countering modern hybrid threats. These include cyberattacks on critical infrastructure, environmental disasters, and energy crises. The acuteness of these problems is further amplified by increasing technological fragmentation and the emergence of new forms of transnational crime. The primary aim of this work is to develop a comprehensive model of a digital subregional security for the states of Central Asia and Russia. This model integrates advanced technological solutions with institutional mechanisms of the Eurasian associations. The scientific novelty of the research lies in the synthesis of institutional analysis and technological modelling. The proposed model accounts for both vertical and horizontal linkages between national agencies and integration structures. The methodological foundation comprises a comparative analysis of the competencies and architecture of Eurasian organizations, supplemented by the design of a multi-level coordination system utilizing artificial intelligence, blockchain, and the Internet of Things technologies. The study's results include the identification of systemic gaps in the coverage of modern threats by existing security mechanisms, the development of a hierarchical security management model—the Digital Subregional Security Template (DSST), the establishment of specific performance indicators for the implementation of digital solutions, and the proposal of adaptive financing mechanisms considering the differentiated capabilities of participating states. A particular value lies in the focus on practical implementation through the creation of pilot zones. This distinguishes the present research from theoretical developments in the field of regional security, and ensures the integration of its findings into the operations of relevant government agencies and integration associations.

Key words: cyber threats, critical infrastructure, interagency cooperation, transnational challenges, artificial intelligence, blockchain, Internet of Things, risk management

Data availability statement. All data obtained during this study are included in the published article.

Authors' contributions. S.G. Luzyanin: research concept, research methodology, analysis of the system of international organizations, development of a comprehensive model of digital subregional security. O.M. Umarov: analysis of the system of international organizations, development of a comprehensive model of digital subregional security. Both authors read and approved the final version of the article.

Conflicts of interest. The authors declare no conflicts of interest.

© Luzyanin S.G., Umarov O.M., 2026

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License
https://creativecommons.org/licenses/by-nc/4.0/legalcode

For citation: Luzyanin, S. G., & Umarov, O. M. (2026). Integrating digital technologies into the collective security system of Central Asia and Russia: Developing a multi-level threat neutralization model. *Vestnik RUDN. International Relations*, 26(2), 240–255. https://doi.org/10.22363/2313-0660-2026-26-2-240-255; EDN: HQFCWE

Интеграция цифровых технологий в систему коллективной безопасности Центральной Азии и России: разработка многоуровневой модели нейтрализации угроз

С.Г. Лузянин[1,2], О.М. Умаров[1] ✉

[1]Национальный исследовательский университет «Высшая школа экономики», Москва, Российская Федерация
[2]Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, Москва, Российская Федерация
✉omuhammadaliyevich@mail.ru

Аннотация. Исследование посвящено проблеме трансформации архитектуры коллективной безопасности в Евразийском регионе в условиях цифровизации и возникновения новых трансграничных угроз. Анализ современных вызовов показывает, что существующие интеграционные структуры, такие как Организация Договора о коллективной безопасности (ОДКБ), Шанхайская организация сотрудничества (ШОС) и Евразийский союз (ЕАЭС), хотя и обладают значительным потенциалом, демонстрируют ограниченную эффективность в противодействии современным цифровым угрозам, включая кибератаки на критическую инфраструктуру, экологические катастрофы и энергетические кризисы. Особую остроту эти проблемы приобретают в контексте усиления технологической фрагментации и появления новых форм трансграничной преступности. Цель исследования — разработка комплексной модели цифровой субрегиональной безопасности для государств Центральной Азии и России, интегрирующей передовые технологические решения с институциональными механизмами евразийских объединений. Научная новизна исследования заключается в синтезе институционального анализа и технологического моделирования, что позволяет преодолеть традиционную фрагментарность подходов к региональной безопасности в сфере цифровизации. В отличие от существующих исследований предлагаемая модель учитывает как вертикальные, так и горизонтальные связи между национальными ведомствами и интеграционными структурами. Методологическую основу составляет сравнительный анализ компетенций и архитектуры евразийских организаций, дополненный проектированием многоуровневой системы координации с применением технологий искусственного интеллекта, блокчейна и Интернета вещей. Особое внимание уделено принципам совместимости систем и предиктивной аналитики. Выявлены системные пробелы в охвате современных угроз существующими механизмами безопасности, разработан Шаблон цифровой субрегиональной безопасности (ШЦСБ), установлены конкретные показатели эффективности внедрения цифровых решений и предложены адаптивные механизмы финансирования с учетом дифференцированных возможностей стран-участниц. Особую важность представляет ориентация на практическую реализацию проекта, внедрение результатов в деятельность профильных ведомств и интеграционных объединений. Предлагаемый подход позволяет существенно повысить оперативность реагирования на современные вызовы и угрозы.

Ключевые слова: цифровизация, киберугрозы, критическая инфраструктура, межведомственное взаимодействие, трансграничные вызовы, искусственный интеллект, блокчейн, Интернет вещей, управление рисками

Заявление о доступности данных. Все данные, полученные в ходе этого исследования, включены в опубликованную статью.

Вклад авторов. Лузянин С.Г.: концепция исследования, методология исследования, анализ системы международных организаций, разработка комплексной модели цифровой субрегиональной безопасности. Умаров О.М.: анализ системы международных организаций, разработка комплексной модели цифровой субрегиональной безопасности. Оба автора ознакомлены с окончательной версией статьи и одобрили ее.

Заявление о конфликте интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования: *Лузянин С. Г., Умаров О. М.* Интеграция цифровых технологий в систему коллективной безопасности Центральной Азии и России: разработка многоуровневой модели нейтрализации угроз // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2026. Т. 26, № 2. С. 240–255. https://doi.org/10.22363/2313-0660-2026-26-2-240-255; EDN: HQFCWE

Introduction

The contemporary architecture of Eurasian security is undergoing a period of fundamental transformation, driven by both the rapidly evolving nature of threats and the accelerating digitalisation of all spheres of public life. On the geopolitical map of Eurasia, a unique multi-tiered system of international organisations has emerged, in which the Eurasian Economic Union (EAEU), the Shanghai Cooperation Organisation (SCO) and the Collective Security Treaty Organisation (CSTO) constitute mutually complementary, yet insufficiently integrated institutional frameworks for digital security. This fragmentation is attributable to both normative and legal lacunae, as well as a certain degree of technological lag among the member states. Digital transformation, on the one hand, engenders novel vulnerabilities, while, on the other, it opens unprecedented opportunities for enhancing the collective security system.

The relevance of the present study is determined by the rapid pace of digitalisation and the emergence of new transboundary threats, which necessitate a fundamental reassessment of traditional approaches to regional security. Of particular salience is the imperative to overcome the fragmentary nature of existing security mechanisms in the face of mounting hybrid threats, including cyberattacks on critical infrastructure, energy crises, and environmental disasters.

The aim of the research is to develop a comprehensive model of digital subregional security that integrates technological solutions with the institutional mechanisms of Eurasian associations for the benefit of the Central Asian states and the Russian Federation. In pursuit of this aim, the study envisages a comparative analysis of the effectiveness of existing security structures, the identification of systemic gaps in coverage of contemporary threats, and the elaboration of a multi-tiered coordination system employing advanced digital technologies.

The scientific novelty of the research lies in the proposal of a novel integrated digital platform for subregional security, the Digital Subregional Security Template (DSST), which encompasses a roadmap, a hierarchical framework, functional specifications, and recommendations for its implementation, among other components.

The creation of an integrated digital platform for subregional security is expected to significantly enhance the responsiveness to contemporary challenges by ensuring the interoperability of the systems of the five national participants (Russia, Uzbekistan, Kazakhstan, Kyrgyzstan and Tajikistan[1]), by introducing predictive analytics and by implementing multi-layered cyber defence. It is anticipated that the proposed model will effectively complement the existing security institutions by bridging normative and technological gaps, and will strengthen synergies between national agencies and integration structures in the digital sphere.

A distinguishing feature of the research is its orientation towards the practical implementation of the proposed model through the establishment of pilot zones and technology transfer mechanisms, as part of the integration of the model into the operations of the relevant specialised agencies and integration associations.

Materials and Methods

Issues of digital security at the level of state and corporate institutions, the protection of critical infrastructure from cyberattacks, including the possibilities for international cooperation in the sphere of digitalisation, as well as digital inequality and sovereignty, have been addressed in a number of Western,[2] Russian (Gavrilov,

[1] Due to the confidentiality of the data, Turkmenistan was not included in the list of subjects of the Template.

[2] Spafford E. H. Cyber Terrorism: The New Asymmetric Threat. Testimony before the House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities. July 24, 2003 // Association for Computing Machinery. URL: https://www.acm.org/binaries/content/assets/public-policy/usacm/privacy-and-security/cybersecurity/03_07_24_spafford1.pdf (accessed: 29.10.2025). See also: (Denning,1999; Schneier, 2003).

2020; Bukharin, 2016; Zinovieva & Shitkov, 2023; Volodenkov et al., 2021) and Chinese studies (Ma et al., 2019; Duan, 2022; Xiao, Xie & Wu, 2020; Chen et al., 2019) from the late 1990s through the 2000s. It should be noted, however, that Chinese expert contributions are predominantly oriented towards domestic digital projects within the People's Republic of China, as well as towards the digitalisation of its Silk Road initiative. Russian developments, by contrast, apart from addressing Russia's own digital projects, serve as a foundation for the study of international and subregional digital frameworks, particularly within the "Russia—Central Asia" system.

The use of new technologies and artificial intelligence (AI) in security has been insufficiently explored by scholars from Central Asia, with contributions emanating primarily from authors based in Kazakhstan and Uzbekistan (Daubassova, Alaeva & Dzhumabayeva, 2024). The relevant publications are devoted chiefly to the legal regulation of AI in defence and national security (Mustafina, Dalelkhan & Nogaeva Karacha, 2025) and to the problems and prospects of implementing AI-based information technologies in the public sector of the states in the region (Aminov, Ochilov & Botirova, 2025; Umarov, 2025). Thematic publications from Kyrgyzstan, Tajikistan and Turkmenistan are absent from academic databases, which indicates a significant lacuna in the regional discourse on digitalisation.

The methodological framework of the study is grounded in a comprehensive approach that combines systemic analysis—enabling the examination of the regional security architecture as an integrated complex of interrelated elements, with the comparative method, which serves to identify the specific operational characteristics of key integration structures, such as the CSTO, the SCO and the EAEU in the context of their adaptation to current challenges. Institutional analysis was employed to delineate the competences and areas of responsibility of the existing security mechanisms, while the structural-functional method facilitated the design of a multi-tiered threat management model.

Scenario modelling within the framework of the present study was based on a systemic analysis of the transformation of threats and opportunities arising in the course of the digitalisation of the Eurasian security space, with a view to assessing the resilience and potential effectiveness of the proposed Digital Subregional Security Template (DSST) under various trajectories of regional development. The modelling was predicated on the development and comparison of several alternative scenarios, taking into account such variable factors as the dynamics of hybrid threats, the rate of technological adaptation of integration structures, and the depth of interstate coordination. Predictive analytics served as the key bridging element between institutional design and the technological content of the comprehensive security model under development.

The criteria for selecting organisations for comparative analysis were based on their system-forming role in the architecture of Eurasian security and on their direct relevance to the target subregion (Russia and Central Asia). The CSTO, the SCO and the EAEU were chosen as a necessary and sufficient set, as taken together they cover the key formats of cooperation—military-political, broad regional security, and economic integration, while fully covering the states for which the digital security model is being designed. The comparative analysis of these organisations permits the identification of functional overlaps, normative-technological gaps, and institutional lacunae in the digital sphere, thereby directly substantiating the need for a new integrated platform intended to complement and synchronise the existing, albeit fragmented, mechanisms of the digital security system in Central Asia.

The interdisciplinary nature of the research necessitated the integration of methodological apparatus from contiguous fields of knowledge,

namely international relations theory, cybersecurity, and digital economics. This approach ensured a comprehensive examination of the problématique and contributed to the elaboration of a balanced model that takes into account both the technological and the politico-legal dimensions of integrating digital technologies into the regional security system.

Results of the Study

On the contemporary geopolitical landscape of Eurasia, a unique multi-tiered system of international organisations has emerged, each addressing specific tasks within the security domain. The EAEU, the SCO and the CSTO constitute the three pillars of this architecture. While their objectives and functions frequently intersect, the organisations themselves exhibit clear distinctions, ranging from predominantly economic integration to military-political alliance.

The CSTO, established in 2002, represents a defensive military-political alliance and constitutes a key element of the security system in the post-Soviet space. The organisation, which comprises six member states, is founded upon the principle of collective defence, whereby an act of aggression against one participant is regarded as an act of aggression against all. The institutional structure of the CSTO encompasses both political bodies—the Collective Security Council and the councils of ministers, as well as military organs, including the Joint Staff. In addition to its collective defence mandate, the Organisation coordinates countermeasures against terrorism, drug trafficking, illegal migration, and cyber threats (Table 1).

The SCO (established in 2001) constitutes a broader regional security platform, encompassing not only post-Soviet states, but also China, India, Pakistan and Iran. A key feature of the Organisation is its specialised Regional Anti-Terrorist Structure (RATS), which coordinates cooperation between intelligence and security services, compiles databases on terrorism, and conducts joint exercises. The highest political bodies of the SCO are the Council of Heads of State and Council of Heads of Government (see Table 1).

The EAEU (established in 2015) is an economic union of five states that integrates security concerns into economic processes. Its key institution is the Eurasian Economic Commission, whose departments ensure security through various measures, such as customs regulation, standardisation control, and phytosanitary measures. Protection mechanisms include countering unfair competition, maintaining data confidentiality, and product traceability (see Table 1).

A comparative analysis of the functions, composition and structures of these organisations (see Table 1) has revealed different approaches to security. The CSTO focuses on the military-political dimension and collective defence; the SCO specialises in non-traditional threats through the coordination of intelligence and security services; and the EAEU integrates security into economic processes. In terms of composition, the CSTO and the EAEU unite post-Soviet states, whereas the SCO, as noted above, represents a broader platform incorporating major Asian powers. The interaction of these organisations forms a multi-tiered security system in which each institution occupies its respective niche.

The process of digitalisation within the framework of Eurasian integration structures has introduced significant transformations into the mechanisms of interstate cooperation. The key advantage has been the enhancement of cooperative efficiency among member states. The establishment of common information systems, such as the SCO RATS, facilitates the acceleration of data exchange and improves the coordination of joint operations. The digitalisation of customs procedures within the EAEU has resulted in a substantial reduction in cargo processing times and the minimisation of corruption risks (Table 2).

Table 1. **Functions, Composition, and Structure of Key Eurasian Security Organizations**

Organization Type	Collective Security Treaty Organization (CSTO)	Shanghai Cooperation Organisation (SCO)	Eurasian Economic Union (EAEU)
	Military-political alliance	Security and cooperation platform in Asia	Economic integration with security elements
Purpose	Ensuring collective defense of members Coordinating actions in combating international terrorism, illicit drug trafficking, illegal migration and cybersecurity	Strengthening mutual trust and good-neighborly relations Joint counteraction against terrorism, separatism and extremism Developing cooperation in political, trade-economic, cultural and other areas	Formation of a single economic space, ensuring "four freedoms" (movement of goods, services, capital and labor) Conducting coordinated economic policy
Member States	Armenia Belarus Kazakhstan Kyrgyzstan Russia Tajikistan	Member States: Russia, China, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan, India, Pakistan, Iran, Belarus Observer States: Afghanistan, Mongolia Dialogue Partners: Azerbaijan, Armenia, Cambodia, Nepal, Turkey, Sri Lanka, etc.	Armenia Belarus Kazakhstan Kyrgyzstan Russia
Internal Structure and Functions	Collective Security Council (CSC)—supreme body, makes strategic decisions Council of Foreign Ministers (CFM) and Council of Defense Ministers (CDM)—coordinate foreign policy and military activities Committee of Security Council Secretaries (CSSC) —developing approaches to countering modern challenges and threats Permanent Council—current work and coordination General Secretariat—implementation of decisions Joint Staff of the CSTO—preparation and deployment of collective security forces	Council of Heads of State—supreme body, determines priorities and strategy Regional Anti-Terrorist Structure (RATS) —key executive body in security Council of National Coordinators—coordinates interaction within the organization Council of Heads of Government and Councils of Foreign and Defense Ministers—address practical cooperation issues	Eurasian Economic Commission (EEC) —supranational regulatory body Security Council of the EEC—protection of confidential information EEC Board—decisions on key issues of internal market functioning Border cooperation mechanisms—coordination of border agencies' actions Commodity traceability systems—combating smuggling and fraud

Note. Abbreviations: CSTO—Collective Security Treaty Organisation; CSTO CSC—CSTO Collective Security Council; CSTO CMFA—CSTO Council of Ministers of Foreign Affairs; CSTO CMD—CSTO Council of Ministers of Defence; CSTO CSSC—CSTO Committee of Secretaries of Security Councils; CSTO PC—CSTO Permanent Council; CSTO GS—CSTO General Secretariat; CSTO JS—CSTO Joint Staff. SCO—Shanghai Cooperation Organisation; SCO HSC—SCO Heads of State Council; SCO RATS—SCO Regional Anti-Terrorist Structure; SCO CNC—SCO Council of National Coordinators; SCO HPC—SCO Heads of Government Council; SCO CMFA—SCO Council of Ministers of Foreign Affairs; SCO CMD—SCO Council of Ministers of Defence. EAEU—Eurasian Economic Union; EAEU EEC—EAEU Eurasian Economic Commission; EAEU SC—EAEU Security Council of the Eurasian Economic Commission; EAEU BoC—EAEU Board of the Eurasian Economic Commission; EAEU BCM—EAEU Border Cooperation Mechanisms; EAEU PTS—EAEU Product Traceability Systems.

Source: compiled by S.G. Luzyanin and O.M. Umarov.

The potential for ensuring security has been significantly enhanced. Joint cyber-monitoring systems being developed under the auspices of the CSTO[3] enable the timely detection and neutralisation of cyber threats. The establishment of common databases on terrorism and extremism within the framework of the SCO (Rumyantseva & Rakhimov, 2022) improves the accuracy and effectiveness of preventive measures.

[3] Zamakhina T. CSTO Parliaments Adopt Concept for Countering Cyber Threats // *Rossiyskaya Gazeta*. November 30, 2020. (In Russian). URL: https://rg.ru/2020/11/30/parlamenty-odkb-priniali-koncepciiu-borby-s-kiberugrozami.html (accessed: 28.08.2025).

Table 2. **Comparative Analysis of Digital Security Strategies within the CSTO, SCO and EAEU**

Organization Criterion	CSTO	SCO	EAEU
Primary Focus of Digitalization	Military-political security, cybersecurity, crisis management	Countering terrorism, separatism, and extremism; cyber sovereignty	Economic integration, reduction of non-economic risks
Key Structures and Mechanisms	Cybersecurity Coordination Center (since 2017), CSTO Information System	Regional Anti-Terrorist Structure (RATS), databases on terrorism and cyber threats	Integrated information systems, "digital transport corridors," electronic certificates
Main Activities	Monitoring and countering cyber threats, sharing information on cyber attacks, harmonizing legislation, conducting exercises (e.g., "PRORYV")	Integrating information from national sources, predictive threat analysis, content regulation, countering "color revolutions"	Implementation of goods traceability projects, minimizing risks of smuggling and fraud, harmonizing safety requirements
Specific Features	Real-time operational data exchange, focus on hybrid threats	Promoting the concept of state control over internet space, digital trade initiatives	Focus on economic security, ensuring the "four freedoms" (movement of goods, services, capital, and labor)

Source: compiled by S.G. Luzyanin and O.M. Umarov.

An analysis of the architecture of the CSTO, the SCO and the EAEU has also revealed systemic gaps in the coverage of contemporary non-traditional threats. Notwithstanding the developed cooperation in cybersecurity and counter-terrorism, key domains remain structurally unaddressed, namely: energy security (without mechanisms for crisis response or infrastructure protection); environmental threats (without monitoring systems and procedures for mitigating transboundary disasters); food security (without early warning systems or mechanisms for adapting the agro-industrial complexes of the member states); socio-demographic challenges (without developed instruments for managing migration and demographic threats); and technological risks (without regulation of artificial intelligence or biosecurity).

At the same time, security issues in the Eurasian space are more pertinent than ever. At the SCO Summit, held on 31 August 2025, in Tianjin, People's Republic of China (PRC), an agreement was reached to establish a Universal Centre for Countering Challenges and Threats to the Security of the Member States, as well as on an Anti-Narcotics Centre. In addition, a roadmap for energy cooperation through 2030 was endorsed.[4] On 9 October 2025, within the framework of the Central Asia—Russia Summit in Dushanbe, Deputy Prime Minister of the Russian Federation Dmitry Grigorenko chaired a meeting on the development of digital cooperation in the region.[5]

However, the existing architecture of Eurasian security retains a reactive character, oriented towards traditional challenges. The absence of proactive mechanisms creates serious vulnerabilities in the face of emerging threats, the countering of which necessitates a comprehensive digital strategy, encompassing the establishment of specialised security units in key domains (energy, environment, migration, among others), as well as scientific and analytical early warning centres. Of critical importance is the formation of standing working groups employing artificial intelligence for threat analysis and the

[4] Council of Heads of State of the SCO Approves Tianjin Declaration // RIA Novosti. September 1, 2025. (In Russian). URL: https://ria.ru/20250901/shos-2038770495.html (accessed: 03.11.2025).

[5] Second Russia—Central Asia Summit // President of Russia. October 9, 2025. (In Russian). URL: http://kremlin.ru/events/president/news/78180 (accessed: 30.10.2025).

development of a multi-tiered coordination system among all security mechanisms.

In the context of the rapid digital transformation and the growing transboundary threats, the need to develop coherent security mechanisms at the subregional level has acquired renewed urgency. The proposed model of the Digital Subregional Security Template (DSST) is intended to consolidate the efforts of five states—the Russian Federation, the Republic of Uzbekistan, the Republic of Kazakhstan, the Republic of Tajikistan and the Kyrgyz Republic—in the sphere of countering contemporary challenges in cyberspace, energy, environmental protection, combating transboundary crime, and coordinating actions in emergency situations.

The conceptual foundations of the DSST are predicated on the principles of system interoperability, predictive analytics, and multi-layered cyber defence. The implementation of the Template envisages the creation of an integrated digital ecosystem encompassing the following components:

– a unified platform for monitoring and forecasting emergency situations (ES), integrating data from national services of the ministries for emergency situations through the use of artificial intelligence for modelling disaster development scenarios; the elaboration of common standards for monitoring and early warning systems; and the training and capacity-building of personnel in digital technologies for emergency services, including data-driven simulations and training,

– an interstate system for countering cybercrime and drug trafficking, based on distributed ledgers (blockchain) for tracking the movement of prohibited cargoes and on machine analysis of criminal networks employing big data, as well as the development of information exchange protocols between law enforcement agencies for rapid threat response,

– digital twins of energy systems incorporating *Smart Grid* elements, ensuring resilience to cyberattacks and the optimisation of energy resource distribution,

– the creation of a unified ecosystem for monitoring the environmental situation in the region through the use of satellite data and IoT devices—an Environmental Digital Atlas aggregating Earth remote sensing data, sensor readings, and hydrometeorological observations for the forecasting of environmental threats; the development of digital tools for environmental impact assessment, including early warning systems for natural disasters; and the exchange of data on the state of ecosystems between countries for more effective responses to environmental threats.

A systematisation of the principal directions of digital transformation within the framework of the DSST permits the formulation of a preliminary roadmap for the implementation of this structure in the form of a comprehensive strategic plan, aimed at the phased introduction of digital technologies into key areas of regional security provision. This roadmap sequentially delineates the main development vectors, specific measures, the technological base, and the projected outcomes of the transformational processes (Table 3).

The proposed security model is predicated on a combination of solutions, in which measures implemented in one domain (environment) yield benefits for others (emergency services, energy). Clear performance indicators ensure objective assessment of progress. The roadmap integrates technological innovations with interstate cooperation, thereby establishing a methodological foundation for the digital transformation of security. Further work will require the specification of funding mechanisms, the establishment of working groups, and the launch of pilot projects.

The proposed roadmap implements the principle of sequential and incremental

Table 3. **Roadmap of the Digital Subregional Security Template: Tasks, Activities, Technologies and Results**

Tasks	Key Activities	Technological Solutions	Expected Results*	Implementation Stages
Digitalization of Emergency Response Systems	1. Creation of a unified interstate platform for emergency data exchange	Cloud technologies, AI analytics, VR trainers	Increase in response efficiency by 30–40%, reduction in decision-making time	Stage 1 (2026–2028)
	2. Development of common monitoring standards			
	3. Personnel training using digital simulators			
Combating Transnational Crime	1. Implementation of a criminal activity analysis system	Big Data, blockchain technologies, cryptographic protection	Increase in crime detection by 25%, reduction in illegal trafficking volumes	Stage 2 (2027–2029)
	2. Development of information exchange protocols			
	3. Creation of drug trafficking tracking mechanisms			
Energy Security	1. Deployment of an energy flow monitoring system	Smart Grid, digital twins, automation systems	Optimization of energy consumption, reduction of losses by 15–20%	Stage 2 (2027–2030)
	2. Standardization of infrastructure management			
	3. Implementation of renewable energy projects			
Environmental Monitoring	1. Creation of a unified environmental control system	Remote sensing, IoT sensors, satellite monitoring	Improved disaster forecasting, reduction of environmental damage	Stages 1 and 2 (2026–2030)
	2. Development of impact assessment tools			
	3. Organization of environmental data exchange			

Notes. The section on expected outcomes is based on assessments drawn from the following sources: Emergency Response Training VR: Preparing Responders with Immersive, Realistic Simulations // Spark. January 8, 2026. URL: https://sparkemtech.co.uk/blog/emergency-response-training-vr-preparing-responders-with-immersive-realistic-simulations (accessed: 03.02.2026); McDermid M. Evolving Technologies Can Enhance Emergency Responses in Smart Cities // StaeTech. January 12, 2022. URL: https://statetechmagazine.com/article/2022/01/evolving-technologies-can-enhance-emergency-responses-smart-cities#:~:text=From%20limited%20budgets%20to%20staffing,by%2030%20to%2040%20percent (accessed: 03.02.2026); Building an AI to Predict Infrastructure Damage from Disasters // NTT Group Information Security Policy. April 25, 2024. URL: https://group.ntt/en/newsrelease/2024/04/25/240425a.html (accessed: 03.02.2026); Harnessing Emerging Technologies for Disaster Risk Reduction // World Meteorological Organization. December 18, 2023. URL: https://wmo.int/media/magazine-article/harnessing-emerging-technologies-disaster-risk-reduction (accessed: 03.02.2026). See also: (Eom & Lee, 2022; Kostina & Kostin, 2022; Brayne, 2018; Antipova, 2026; Kabeyi & Olanrewaju, 2023).

Abbreviations: ES—emergency situations; AI—artificial intelligence; RES—renewable energy sources; VR—virtual reality; Big Data—large volumes of information, encompassing their collection, processing and analytics; IoT—Internet of Things, i.e., a network of physical objects (“things”) equipped with sensors, software and network modules that enable them to exchange data over the Internet with other devices and systems without human intervention.

Source: compiled by S.G. Luzyanin and O.M. Umarov.

deployment, with time frames for each stage (2026–2030) determined based on technological complexity, the degree of institutional readiness, and the necessity of building trust among the participants.

The first stage focuses on creating a foundational technological and regulatory platform through relatively less sensitive yet critically important directions, namely, the digitalisation of emergency services and environmental monitoring, which lays the groundwork for data exchange.

The second stage, which is a logical continuation of the first, simultaneously launches

the more complex and politically delicate modules of crime countering and energy security. However, their differing durations (2027–2029 and 2027–2030, respectively) reflect objective differences in the scale of the tasks involved, ranging from the integration of software solutions and protocols to the synchronisation of physical infrastructure and large-scale investment.

The chronology of the DSST implementation stages is not intended as a rigid framework but rather as a flexible scheme, in which projects grouped according to launch logic possess individual implementation timelines determined by their specific characteristics and the required depth of transformation.

Structure of the DSST

In order to ensure the effective functioning, the necessary level of transparency and international attractiveness of the proposed DSST model, the establishment of a comprehensive organisational architecture is required, encompassing several interrelated levels of management and coordination. The DSST concept represents a complex multi-tiered system, in which each element performs strictly defined functions while maintaining flexibility in its interaction with other components of the structure (Table 4).

At the apex of the hierarchical structure, there is the *Supreme Council* (SC) of the DSST, which serves as a strategic governing body. Its membership comprises the relevant ministers of the five participating states, responsible for key areas of cooperation: digital development, national security, energy, environment, and emergency situations. The SC may function under the auspices of existing integration structures (CSTO, SCO, EAEU). This collegial body determines the strategic priority vectors for the development of cooperation and makes major political decisions, which are subsequently transmitted to the lower levels of governance for implementation. Its tasks include harmonizing normative and legal frameworks, conducting joint cybersecurity exercises, and developing data exchange protocols (see Table 4).

The operational implementation of the decisions of the *Supreme Council* will be ensured by the *Executive Committee*, composed of permanent representatives of the participating states and invited international experts (see Table 4). This body performs the critically important function of translating strategic guidelines into specific action plans, while simultaneously monitoring their implementation and preparing analytical materials for any necessary course correction. A distinctive feature of this structure is its capacity to adapt quickly to changing conditions, owing to the inclusion of independent experts with diverse professional profiles.

The functional dimension of the system is realised through a network of specialised *Centres of Competence* organised along sectoral lines. Each center focuses on a specific area of cooperation.

The Centre for Cybersecurity and Crime Countering consolidates the operational capabilities of national security and intelligence services (FSB of Russia, KNB of Kazakhstan, SNB of Uzbekistan), creating a unified information space to detect and neutralize transboundary threats. In parallel, *the Centre for Digital Systems of Emergency Services* ensures the integration of technological solutions for disaster prevention and response, employing advanced risk analysis and forecasting methodologies.

The Centre for Energy Monitoring ensures the integration of data from the leading grid operators of the region (Rosseti, KEGOC, Barki Tojik, among others), which, through the coordination of their activities, makes it possible not only to enhance the reliability of energy systems, but also to optimise the distribution of resources.

The *Centre for Environmental Monitoring* consolidates the capabilities of hydrometeorological services (Roshydromet, Kazhydromet, Uzhydromet, among others) in the field of

Table 4. **Hierarchical Structure of the Digital Subregional Security Template**

Subdivision	Components	
Supreme Council	Ministers of Digital Development	
	Ministers of Security	
	Ministers of Energy	
	Ministers of Ecology	
	Ministers of Emergency Situations from 5 countries	
Executive Committee	Permanent Representatives of States	
	International experts	
Competence Centers	Center for Cybersecurity and Crime Counteraction	FSB (Russian Federation)
		National Security Committee (Kazakhstan)
		National Security Service (Uzbekistan)
	Center for Digital Emergency Response Systems	EMERCOM of Russia
		Committee of Emergency Situations (Kazakhstan)
		Emergency Ministries of other countries
	Center for Energy Monitoring	Rosseti
		KEGOC
		Barki Tojik
	Center for Environmental Monitoring	Roshydromet
		Kazhydromet
		Uzhydromet, etc.
Technological Infrastructure	Unified Cloud Platform	
	Blockchain Systems	
	IoT Networks	
	Situation Centers in Each Country	

Note. Abbreviations and designations: FSB RF—Federal Security Service of the Russian Federation (RF); KNB (Kazakhstan)—National Security Committee of the Republic of Kazakhstan (RK); SNB (Uzbekistan)—National Security Service of the Republic of Uzbekistan (RU); EMERCOM of Russia—Ministry of the Russian Federation for Civil Defence, Emergencies and Disaster Relief; Rosseti—Public Joint-Stock Company "Federal Grid Company Rosseti," one of the world's largest electric grid holding companies; KEGOC—KEGOC JSC (Kazakhstan Electricity Grid Operating Company), the national electricity grid operator of Kazakhstan; Barki Tojik—(Open Joint-Stock Holding Company "Barki Tojik"), the state energy company of the Republic of Tajikistan; Roshydromet—Federal Service for Hydrometeorology and Environmental Monitoring of the Russian Federation; Kazhydromet—Republican State Enterprise "Kazhydromet," the hydrometeorological service of the RK under the Ministry of Ecology and Natural Resources of the RK; Uzhydromet—Centre for Hydrometeorological Service under the Cabinet of Ministers of the Republic of Uzbekistan.

Source: compiled by S.G. Luzyanin and O.M. Umarov.

environmental quality control. Environmental monitoring permits the comprehensive oversight of the state of the environment using modern remote sensing technologies.

The technological infrastructure of the DSST constitutes a complex symbiosis of digital solutions. The technological foundation of the DSST may comprise the following components:

– a unified secure cloud platform for data storage and processing, serving as the backbone for data storage and processing while ensuring the requisite level of security and information availability,

– blockchain-based trust systems and transaction tracking, designed to create a trusted data exchange environment, particularly in sensitive areas, such as the monitoring of transboundary criminal schemes,

– a distributed network of IoT devices, forming a decentralised real-time monitoring system,

– a network of situation centres in each participating country to ensure the operational processing of incoming information (see Table 4).

The technological implementation of the DSST requires the phased deployment of a secure cloud infrastructure, employing Russian cryptographic solutions as well as those developed jointly by the participating states. In view of the disparities in the level of digitalisation among the involved countries, it is advisable to provide for technology transfer mechanisms (for example, the establishment of regional centres

Table 5. **Comprehensive Framework for the Implementation of the Digital Subregional Security Template**

Component	Elements	Participants / Mechanisms	Financing
Technological Architecture	Unified secure cloud platform (Russian/hybrid solutions)	Technical specialists from all participating countries, IT companies	Infrastructure investments Technology barter (capacity exchange)
	Decentralized data exchange systems (blockchain, IoT)		
	Situation centers with unified standards		
Legal Framework	Multilateral cybersecurity agreement	Legal services of states, Ministries of Foreign Affairs, integration associations (SCO, EAEU)	Funding for legal development
	Mutual assistance protocols (based on CSTO/SCO models)		Grants for legislative harmonization
Institutional Structure	**Russia:** Ministry of Digital Development, FSB, Rosgvardiya, Roshydromet, Rostech	National agencies, coordination councils, international experts	Budget funding for government agencies Support from integration associations
	Kazakhstan: Ministry of Digital Development, National Security Committee, KEGOC, Kazhydromet		
	Uzbekistan: Ministry of ICT, National Security Service, Uzhydromet, National Guard		
	Tajikistan/Kyrgyzstan: Information Security Agencies, Emergency Ministries, Hydromet, Energy Regulators		
Financial Model	Budget sources: Proportional participation; Targeted funds of SCO/CSTO/EAEU	Ministries of Finance, international organizations, private sector	RF, KZ—30%; UZ—20%; TJ, KR—10%; SCO/CSTO/ EAEU (up to 40%)
	Extra-budgetary sources: Grants (UN, World Bank—for environmental and anti-crime modules) PPP (Kaspersky, BI Group, Uzbektelecom, etc.)		
	Technology barter (Russia provides cloud capacity, Kazakhstan—data centers, etc.)		

Note. Abbreviations and designations: RF—Russian Federation; KZ—Republic of Kazakhstan; UZ—Republic of Uzbekistan; KR—Kyrgyz Republic; TJ—Republic of Tajikistan; MCRD—Ministry of Digital Development of Kazakhstan; KNB—National Security Committee of Kazakhstan; KEGOC—Kazakhstan Electricity Grid Operating Company; IS—information security; WB—World Bank; PPP—public–private partnership.

Source: compiled by S.G. Luzyanin and O.M. Umarov.

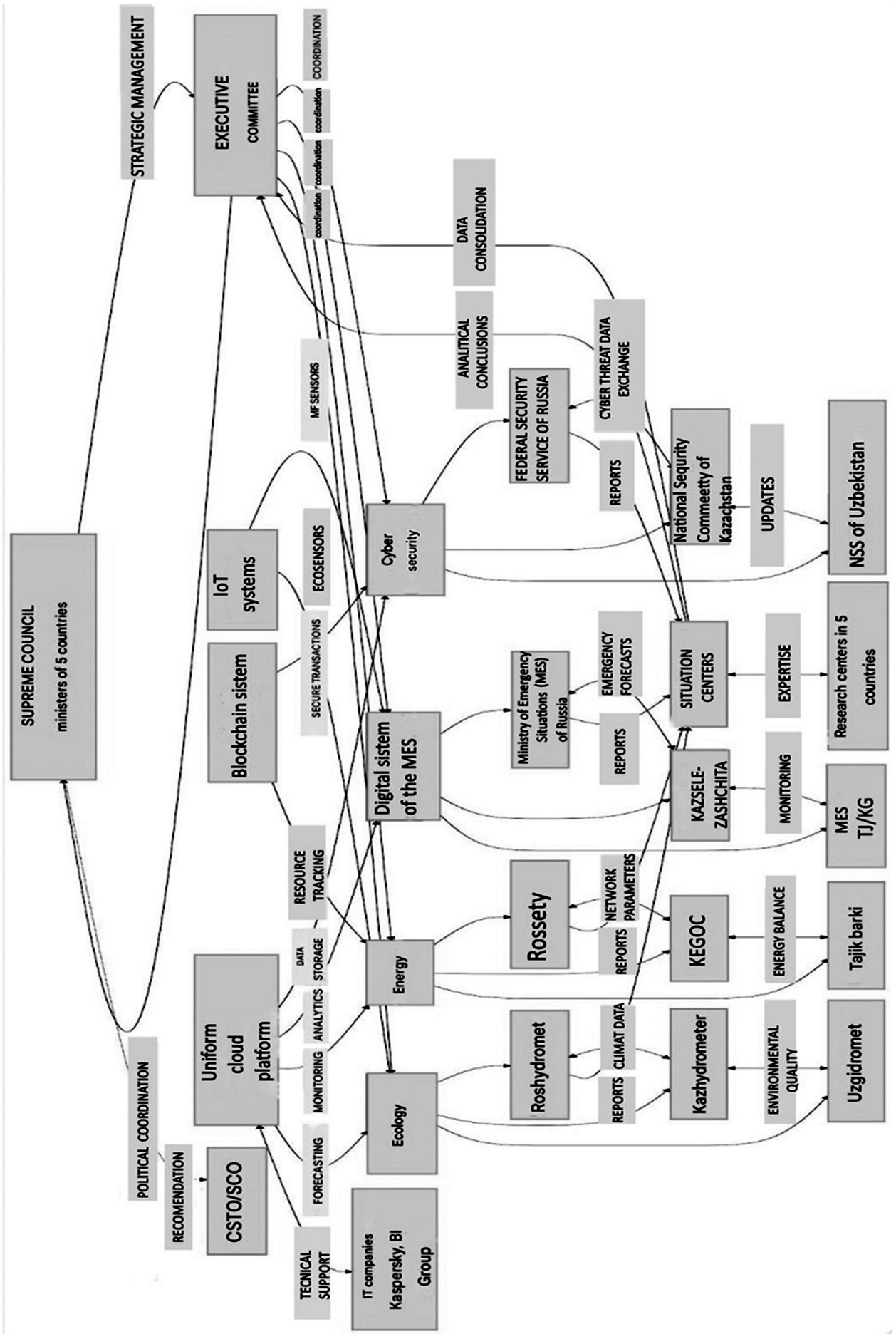
of competence on the basis of leading IT universities in Russia and Kazakhstan).

Information flows within the DSST system are organised according to the principle of multi-level data filtering and verification (Figure). Vertical communications ensure the transmission of strategic decisions from the top down and operational reporting from the bottom up. Horizontal linkages between national agencies of different countries create a foundation for the expeditious exchange of information and the coordination of actions. Particular attention is devoted to cross-functional interactions, which enable the integration of data from diverse sources a for comprehensive threat analysis.

Technological integration is achieved through a system of standardised interfaces, ensuring the interoperability of the heterogeneous information systems used by the participants. External interactions with international organisations and academic institutions are conducted through specially developed protocols that guarantee the protection of the sovereign interests of the participants while maintaining openness to cooperation.

The effectiveness of the DSST is directly contingent upon its adaptation to the politico-economic realities of Central Asia. This entails:

– the development of multi-lingual platform interfaces with support for Russian and national languages,



Structural and Functional Organization of the SCBS with Visualization of Information Flows

Source: compiled by S.G. Luzyanin and O.M. Umarov.

Table 6. **Common Digital Challenges Addressed by the Digital Subregional Security Template**

Area	Problems	Solution via DSST
Digitalization of Emergency Response Standards and Platforms	Incompatible alert systems, weak coordination during emergencies	Unified emergency monitoring and response platform with AI analytics
Digitalization of Transnational Crime and Drug Trafficking Data	Fragmented databases, low level of information sharing	Common cryptographically secure system for criminal network analysis and blockchain-based cargo tracking
Digitalization of Energy Issues	Imbalances in power grids, cyberattacks on infrastructure	Smart Grids with common cybersecurity and predictive analytics
Digitalization of Environmental Issues	Lack of unified pollution monitoring, climate threats	Digital environmental atlas with sensors and satellite analysis

Source: compiled by S.G. Luzyanin and O.M. Umarov.

– flexible financing arrangements, including a proportionate distribution of costs between more developed participants (Russia, Kazakhstan, Uzbekistan) and those needing infrastructural modernisation (Tajikistan, Kyrgyzstan),

– the establishment of pilot zones for testing solutions (for example, transboundary monitoring of the Syr Darya / Amu Darya rivers within the framework of the environmental module).

In terms of expected outcomes, the implementation of the DSST will make it possible to enhance the responsiveness to emergency situations through automated risk analysis, to strengthen control over illicit transboundary flows via digital cargo identification, to reduce energy losses by optimising power grid operating modes, and to establish a scientifically grounded basis for decision-making in environmental policy.

As a result of the conducted research, a preliminary construct of the Comprehensive Implementation Framework for the Digital Subregional Security Template has been developed (Table 5).

The implementation of the DSST concept is associated with certain risks and challenges, which necessitate additional efforts on the part of the stakeholders (Table 6).

The proposed model is not a rigid construct, but rather a dynamic and flexible system capable of adapting to the changing nature of threats. For its implementation, a pilot project may be proposed in one of the domains (for example, emergency services), with subsequent scaling. Financing is proposed to be effected through mixed funds (EAEU, SCO, national budgets).

It is important to stress that the successful implementation of this model requires not only technological investment, but also building trust among the participants.

In the longer term, the DSST could serve as a prototype for analogous systems in other macro-regions of Eurasia.

Conclusion

The conducted research demonstrates a profound transformation of the paradigm of Eurasian security in the context of the digital age. Employing a systemic approach and comparative analysis, the authors have undertaken a diagnostic assessment of the architecture of Eurasian security and proposed a model for its adaptation to the challenges posed by the digital era. The findings obtained are structured within the framework of the key objectives of the study.

First, it has been confirmed that existing institutions (the CSTO, the SCO and the EAEU), while constituting essential pillars of the regional order, exhibit functional fragmentation and technological lag, leading to critical gaps in addressing hybrid threats ranging from cyberattacks to environmental disasters.

Second, in response to this challenge, the DSST concept has been developed as a multi-tiered institutional and technological ecosystem, integrating strategic, operational and expert levels of governance through a network of specialised Centres of Competence.

Third, a roadmap for the implementation of the DSST has been elaborated in detail, substantiating a phased transition from pilot projects in the spheres of emergency services and environmental protection to the deployment of complex modules for energy security and crime countering, with a clear chronology and predictive analytics tools.

The central finding of the study is the confirmation of the hypothesis regarding the necessity of creating integrated digital security ecosystems capable of ensuring cross-border, end-to-end risk management. The practical implementation of the model, which combines blockchain technologies, predictive analytics and distributed monitoring systems, will make it possible to achieve a qualitatively new level of coordination among the participating states.

The implementation of the DSST model requires concrete steps. As an immediate priority measure, it is advisable to conclude an intergovernmental framework agreement between the interested states, defining the basic principles of cooperation, the status of the bodies to be established, and data exchange protocols, thereby creating the necessary legal foundation for the subsequent harmonisation of national legislation in the spheres of cybersecurity and critical infrastructure protection. The financing of the pilot phase will be ensured by a dedicated fund with mixed sources—weighted contributions from national budgets and grants from the EAEU. To attract private investment, a public-private partnership model could be established in the form of a consortium of IT companies deploying the platform on a concession basis.

The study has revealed latent synergistic effects arising from the integration of disparate security systems into a unified digital ecosystem. The key such effect is the formation of a cross-domain analytical loop, in which data from one domain (environmental monitoring) automatically become a source for modelling in other areas (forecasting loads on energy systems or emergency risks). Another effect is the mutual reinforcement of regulatory regimes, whereby cybersecurity standards and data exchange protocols developed for one module (energy, law enforcement) are adapted for others (emergency services, environment), thereby reducing the overall transaction costs of the system.

An important outcome has been the confirmation of the feasibility of implementing the principle of "digital sovereignty" on the regional scale, which makes it possible to combine the advantages of integration with the preservation of the national interests of the individual participating states.

Received / Поступила в редакцию: 10.11.2025
Revised / Доработана после рецензирования: 27.02.2026
Accepted / Принята к публикации: 27.03.2026

References

Aminov, F. B., Ochilov, A. O., & Botirova, K. B. k. (2025). Information technology and artificial intelligence in Uzbekistan: Problems and prospects. *In the Center of Economy*, 6(1), 28–32. (In Russian). Retrieved from https://vcec.ru/index.php/vcec/article/view/153

Antipova, A. L. (2026). Application of AI algorithms and big data analytics in crime prevention. *Intellektual'nye Resursy—Regional'nomu Razvitiyu*, (1), 505–510. (In Russian). EDN: IOGFEF

Brayne, S. (2018). The criminal law and law enforcement implications of big data. *Annual Review of Law and Social Science*, 14, 293–308. https://doi.org/10.1146/annurev-lawsocsci-101317-030839

Bukharin, V. V. (2016). The Russian's digital sovereignty as a technical basis of information security. *MGIMO Review of International Relations*, (6), 76–91. (In Russian). https://doi.org/10.24833/2071-8160-2016-6-51-76-91; EDN: YGCPJX

Chen, Ch., Li, Zh., Hao, Zh., Chao, L., Mengwei, W., & Hao, C. (2019). Zhongguo qiyeshuzihua shengcun guanli shijian shijiao de chuangxin yanjiu [Research on innovation in the practice of digital survival management of

Chinese enterprises from the perspective of innovation*]. Guanli kexue xuebao* [Journal of Management Sciences (JMAS)], (10), 1–8. (In Chinese).

Daubassova, Sh. S., Alaeva, G. T., & Dzhumabayeva, K. A. (2024). AI and criminal surveillance in Kazakhstan. *Eurasian Scientific Journal of Law*, (4), 19–29. (In Russian). Retrieved from https://esjl.turan-edu.kz/jour/article/view/239

Denning, D. E. (1999). *Information warfare and security*. New York: ACM Press.

Duan, N. (2022). Qiye jingying guanli shijiao xia shuzihua zhuanxing de fa zhan tanjiu [Research on the development of digital transformation from the perspective of enterprise management]. *Dianzi tongxin yu jisuanji kexue* [*Electronic Communications and Computer Science (EECS)*], 4(3), 74–76. (In Chinese). https://doi.org/10.37155/2717-5170-0403-29

Eom, S. J., & Lee, J. (2022). Digital government transformation in turbulent times: Responses, challenges, and future direction. *Government Information Quarterly*, 39(2), 1–9. https://doi.org/10.1016/j.giq.2022.101690; EDN: GWQOEW

Gavrilov, E. O. (2020). Digital sovereignty in the context of globalisation: Philosophical and legal aspects. *Bulletin of Kemerovo State University. Series: Humanities and Social Sciences*, 4(2), 146–152. (In Russian). https://doi.org/10.21603/2542-1840-2020-4-2-146-152; EDN: WCSQFR

Kabeyi, M. J. B., & Olanrewaju, O. A. (2023). Smart grid technologies and application in the sustainable energy transition: A review. *International Journal of Sustainable Energy*, 42(1), 685–758. https://doi.org/10.1080/14786451.2023.2222298; EDN: VVRHKJ

Kostina, E. A., & Kostin, A. V. (2022). How do smart city technologies help to cope with the pandemic? *Regional Research of Russia*, 12(2), 241–249. https://doi.org/10.1134/S2079970522020149; EDN: QUZATZ

Ma, H., Meng, Ch., Yang, D., & Wang, H. (2019). *China's digital transformation: Experience in transforming the national economic infrastructure* (translation from Chinese). Moscow: Intellektual'naya literature publ. (In Russian).

Mustafina, A., Dalelkhan, A., & Nogaeva Karacha, A. (2025). Qazaqstan Respublikasynyñ äskeri isindegi jasandy intellekt tekhnologiyasynyñ perspektivalary men quqyqtyq rettelui [Prospects and legal regulation of artificial intelligence technology in military affairs of the Republic of Kazakhstan]. *Memlekettik Basqaru Jäne Memlekettik Qyzmet* [*Public Administration and Civil Service*], 94(3), 171–179. (In Kazakh). https://doi.org/10.52123/1994-2370-2025-1522; EDN: CSJNFF

Rumyantseva, A. K., & Rakhimov, K. Kh. (2022). The SCO's role in countering terrorism in Central Asian countries. *Postsovetskie Issledovaniya*, 5(8), 835–846. (In Russian). EDN: MCZNRN

Schneier, B. (2003). *Beyond fear: Thinking sensibly about security in an uncertain world*. New York: Copernicus Books.

Umarov, O. M. (2025). Digitalisation in small states of Central Eurasia: General and particular, challenges and risks. In *Greater Eurasia: Development, Security, Cooperation:* Yearbook. Proceedings of the 7th International Scientific and Practical Conference. In 4 parts (Iss. 8, part 2, pp. 175–182). Moscow: ID "UMTs" publ. (In Russian). EDN: VYFCSI

Volodenkov, S. V., Voronov, A. S., Leontyeva, L. S., & Sukhareva, M. (2021). Digital sovereignty of a modern state in the context of technological transformations: Content and features. *Polylogos*, 5(1), 5. (In Russian). https://doi.org/10.18254/S258770110014073-2; EDN: WKLJNK

Xiao, J., Xie, K., & Wu, Y. (2020). Shuju qudong de chanpin shiying xing chuangxin — shuzi jingji de chuangxin luoji [Data-driven adaptive product innovation: The innovation logic of the digital economy]. *Beijing jiaotong daxue xuebao* (*Shehui kexue ban*) [*Journal of Beijing Jiaotong University* (*Social Sciences Edition*)], 19(1), 7–18. (In Chinese).

Zinovieva, E. S., & Shitkov, S. V. (2023). Digital sovereignty in the practice of international relations. *Mezdunarodnaa Zizn'*, (3), 38–51. (In Russian). EDN: HBTQYT

About the authors:

Luzyanin Sergey Gennadievich — PhD, Dr. Sc. (History), Professor, Department of Foreign Regional Studies, HSE University; 17 Malaya Ordynka St, Moscow, 119017, Russian Federation; Professor, Department of Oriental Studies, MGIMO University; 76 Prospekt Vernadskogo, Moscow, 119454, Russian Federation; eLibrary SPIN-code: 2864-9951; ORCID: 0000-0001-9578-6023; e-mail: luzyanin.sergey@mail.ru

Umarov Otabek Mukhammadalievich — PhD Candidate, Department of Foreign Regional Studies, HSE University; 17 Malaya Ordynka St, Moscow, 119017, Russian Federation; ORCID: 0009-0008-3091-1872; e-mail: omuhammadaliyevich@mail.ru