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

Научная статья / Research article

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

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.

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

Введение

Современная архитектура евразийской безопасности переживает период фундаментальной трансформации, обусловленной динамичным изменением характера угроз и стремительной цифровизацией всех сфер общественной жизни. На геополитической карте Евразии сформировалась уникальная многоуровневая система международных организаций, где Евразийский экономический союз (ЕАЭС), Шанхайская организация сотрудничества (ШОС) и Организация Договора о коллективной безопасности (ОДКБ) представляют собой взаимодополняющие, но недостаточно интегрированные институциональные структуры в сфере цифровой безопасности, что обусловлено как нормативно-правовыми пробелами, так и некоторым технологическим отставанием стран-членов. Цифровая трансформация, с одной стороны, создает новые уязвимости, а с другой — открывает беспрецедентные возможности для совершенствования системы коллективной безопасности.

Актуальность исследования обусловлена стремительной цифровизацией и появлением новых трансграничных угроз, требующих пересмотра традиционных подходов к обеспечению региональной безопасности. Особую значимость приобретает необходимость преодоления фрагментарности существующих механизмов безопасности в условиях нарастания гибридных угроз, включая кибератаки на критическую инфраструктуру, энергетические кризисы и экологические катастрофы.

Целью исследования является разработка комплексной модели цифровой субрегиональной безопасности, интегрирующей технологические решения с институциональными механизмами евразийских объединений для государств Центральной Азии и России. В рамках достижения данной цели предполагается провести сравнительный анализ эффективности существующих структур безопасности, выявить системные пробелы в охвате современных угроз и разработать многоуровневую систему координации с применением передовых цифровых технологий.

Научная новизна исследования состоит в представлении новой интегрированной цифровой платформы субрегиональной безопасности — Шаблона цифровой субрегиональной безопасности (ШЦСБ), содержащего дорожную карту, иерархическую структуру, функционал, предложения по его внедрению и проч.

Создание интегрированной цифровой платформы субрегиональной безопасности, как представляется, позволит существенно повысить оперативность реагирования на современные вызовы за счет обеспечения совместимости систем пяти национальных субъектов (России, Узбекистана, Казахстана, Кыргызстана и Таджикистана)[1], внедрения предиктивной аналитики и реализации многоуровневой киберзащиты. Предполагается, что предлагаемая модель сможет эффективно дополнить существующие институты безопасности за счет устранения нормативных и технологических разрывов, а также усилить синергию между национальными ведомствами и интеграционными структурами в цифровой сфере.

Отличительной особенностью исследования является ориентация на практическую реализацию предлагаемой модели через создание пилотных зон и механизмов технологического трансфера в рамках внедрения предлагаемой модели в деятельность профильных ведомств и интеграционных объединений.

Материалы и методы

Проблемы цифровой безопасности на уровне государственных и корпоративных институтов, защиты критической инфраструктуры от кибератак, включая возможности меж-

[1] В силу закрытости данных в перечень субъектов Шаблона не был включен Туркменистан.

дународного сотрудничества в сфере цифровизации, а также цифрового неравенства и суверенитета поднимались в конце 1990-х – в 2000-е гг. в ряде западных[2], российских (Гаврилов, 2020; Бухарин, 2016; Зиновьева, Шитьков, 2023; Володенков и др., 2021) и китайских исследований (Ма и др., 2019; Duan, 2022; Xiao, Xie & Wu, 2020; Chen et al., 2019). При этом китайский экспертный опыт больше ориентирован на внутренние цифровые проекты Поднебесной, а также цифровизацию своего проекта «Шелкового пути». Российские же разработки кроме собственно российских цифровых проектов выступают как основа для исследования международных, субрегиональных цифровых форматов, в частности в системе «Россия — Центральная Азия».

Тема использования новых технологий и искусственного интеллекта (ИИ) в сфере безопасности учеными из Центральной Азии исследована слабо, преимущественно авторами из Казахстана и Узбекистана (Даубасова, Алаева, Джумабаева, 2024). Публикации в основном посвящены использованию правовому регулированию ИИ в обороне и национальной безопасности (Мустафина, Далелхан, Ногаева Карача, 2025) и проблемам и перспективам внедрения информационных технологий с ИИ в государственном секторе государств региона (Аминов, Очилов, Ботирова, 2025; Умаров, 2025). Тематические публикации из Кыргызстана Таджикистана и Туркменистана в академических базах данных отсутствуют, что указывает на пробелы в региональном дискурсе о цифровизации.

Методологическая база исследования основана на комплексном подходе, сочетающем системный подход, который позволяет анализировать архитектуру региональной безопасности как целостный комплекс взаимосвязанных элементов, а применение сравнительного метода обеспечивает выявление специфики функционирования ключевых интеграционных структур, таких как ОДКБ, ШОС и ЕАЭС, в контексте их адаптации к современным вызовам. Институциональный анализ позволил определить компетенции и зоны ответственности существующих механизмов безопасности, в то время как структурно-функциональный метод способствовал проектированию многоуровневой модели управления угрозами.

Сценарное моделирование в рамках данного исследования проводилось на основе системного анализа трансформации угроз и возможностей, возникающих в процессе цифровизации пространства евразийской безопасности для оценки устойчивости и потенциальной эффективности предлагаемой модели Шаблона цифровой субрегиональной безопасности (ШЦСБ) в условиях различных траекторий развития региональной ситуации. Моделирование строилось на разработке и сопоставлении ряда альтернативных сценариев, учитывающих переменные факторы, такие как динамика гибридных угроз, скорость технологической адаптации интеграционных структур и глубина межгосударственной координации. Прогнозная аналитика выступила ключевым связующим звеном между институциональным проектированием и технологическим наполнением разрабатываемой комплексной модели безопасности.

Критерии отбора организаций для сравнительного анализа базируются на их системообразующей роли в архитектуре евразийской безопасности и непосредственной релевантности для целевого субрегиона (Россия и Центральная Азия). ОДКБ, ШОС и ЕАЭС были избраны как необходимый и достаточный набор, поскольку в совокупности они исчерпывают ключевые форматы сотрудничества (военно-политический, широкой региональной безопасности и экономической интеграции), полностью охватывая государства, для которых проектируется модель цифровой безопасности. Сравнительный анализ этих организаций позволяет выявить функциональные пересечения, нормативно-технологические разрывы и институциональные пробелы в цифровой сфере, что непосредственно обосновывает необходимость разработки новой интегриро-

[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). См. также: (Denning,1999; Schneier, 2003).

ванной платформы, призванной дополнить и синхронизировать существующие, но фрагментированные механизмы системы цифровой безопасности в Центральной Азии.

Междисциплинарный характер исследования потребовал интеграции методологического аппарата из смежных областей знания: теории международных отношений, кибербезопасности и цифровой экономики. Такой подход обеспечил всесторонний анализ проблематики и способствовал разработке сбалансированной модели, учитывающей как технологические, так и политико-правовые аспекты интеграции цифровых технологий в систему региональной безопасности.

Результаты исследования

На современной геополитической карте Евразии сформировалась уникальная многоуровневая система международных организаций, каждая из которых решает специфические задачи в сфере безопасности. ЕАЭС, ШОС и ОДКБ представляют собой три столпа этой архитектуры. Их цели и функции часто пересекаются, но сами организации имеют четкие различия, от преимущественно экономической интеграции до военно-политического союза.

ОДКБ, созданная в 2002 г., представляет собой военно-политический альянс оборонительной направленности, являющийся ключевым элементом системы безопасности на постсоветском пространстве. Организация, включающая шесть государств, базируется на принципе коллективной обороны: агрессия против одного участника рассматривается как агрессия против всех. Институциональная структура ОДКБ включает как политические (Совет коллективной безопасности, советы министров), так и военные органы (Объединенный штаб). Помимо задач коллективной обороны организация координирует противодействие терроризму, наркоторговле, нелегальной миграции и киберугрозам (табл. 1).

ШОС (создана в 2001 г.) является более широкой региональной платформой безопасности, включающей не только постсоветские страны, но и Китай, Индию, Пакистан и Иран. Ключевой особенностью организации является специализированная Региональная антитеррористическая структура (РАТС), координирующая взаимодействие спецслужб, формирование баз данных по терроризму и проведение совместных учений. Высшими политическими органами ШОС выступают советы глав государств и правительств (см. табл. 1).

ЕАЭС (образован в 2015 г.) – экономический союз пяти государств, интегрирующий вопросы безопасности в хозяйственные процессы. Ключевой институт – Евразийская экономическая комиссия, чьи департаменты обеспечивают безопасность через таможенное регулирование, контроль стандартов и фитосанитарию. Механизмы защиты включают противодействие недобросовестной конкуренции, сохранение конфиденциальности данных и прослеживаемость товаров (см. табл. 1).

Сравнительный анализ функций, состава и структур этих организаций (см. табл. 1) позволил выявить различные подходы к безопасности. ОДКБ фокусируется на военно-политической составляющей и коллективной обороне, ШОС специализируется на нетрадиционных угрозах через координацию спецслужб, а ЕАЭС интегрирует безопасность в экономические процессы. По составу ОДКБ и ЕАЭС объединяют постсоветские страны, тогда как ШОС, как уже отмечалось, представляет собой более широкую платформу с участием крупных азиатских государств. Взаимодействие этих организаций формирует многоуровневую систему безопасности, где каждый институт занимает свою нишу. Процесс цифровизации в рамках евразийских интеграционных структур привнес значительные преобразования в механизмы межгосударственного взаимодействия. Ключевым преимуществом стало повышение эффективности кооперации между странами-участницами. Создание единых информационных систем, таких как РАТС ШОС, способствует ускорению обмена данными и улучшению координации совместных действий. Цифровизация таможенных процедур в рамках ЕАЭС приводит к существенному сокращению времени обработки грузов и минимизации коррупционных рисков (табл. 2).

Таблица 1. **Функции, состав и структура ключевых организаций евразийской безопасности**

Наименование / тип организации	Организация Договора о коллективной безопасности (ОДКБ)	Шанхайская организация сотрудничества (ШОС)	Евразийский экономический союз (ЕАЭС)
	Военно-политический альянс	Платформа по безопасности и взаимодействию в Азии	Экономическая интеграция с элементами безопасности
Назначение	Обеспечение коллективной обороны участников Координация действий в сфере борьбы с международным терроризмом, незаконным оборотом наркотиков, нелегальной миграцией и кибербезопасностью	Укрепление взаимного доверия и добрососедских отношений Совместное противодействие терроризму, сепаратизму и экстремизму Развитие сотрудничества в политической, торгово-экономической, культурной и иных областях	Формирование единого экономического пространства, обеспечение «четырех свобод» (движение товаров, услуг, капиталов и рабочей силы) Проведение скоординированной экономической политики
Состав участников	Армения Беларусь Казахстан Кыргызстан Россия Таджикистан	**Государства-члены:** Россия, Китай, Казахстан, Кыргызстан, Таджикистан, Узбекистан, Индия, Пакистан, Иран, Беларусь **Государства-наблюдатели:** Афганистан, Монголия **Партнеры по диалогу**: Азербайджан, Армения, Камбоджа, Непал, Турция, Шри-Ланка и др.	Армения Беларусь Казахстан Кыргызстан Россия
Внутренняя структура и функции	СКБ — высший орган, принимает стратегические решения СМИД и СМО — координация внешнеполитической и военной деятельности КССБ — выработка подходов к противодействию современным вызовам и угрозам ПС — текущая работа и координация ГС — обеспечение реализации решений ОШ ОДКБ — подготовка и применение сил и средств системы коллективной безопасности	СГГ ШОС — высший орган, определяет приоритеты и стратегию РАТС ШОС— ключевой исполнительный орган в сфере безопасности СНК ШОС — координация взаимодействие внутри организации СГП, и СМИД, СМО — решение вопросов практического взаимодействия	ЕЭК — наднациональный регулирующий орган СБ ЕЭК — защита конфиденциальной информации КЕЭК — решения по ключевым вопросам функционирования внутреннего рынка МПС — координация действий пограничных ведомств СПТ — противодействие контрабанде и мошенничеству

Примечание. ОДКБ — Организация Договора о коллективной безопасности; СКБ ОДКБ — Совет коллективной безопасности ОДКБ; СМИД — Совет министров иностранных дел ОДКБ; СМО — Совет министров обороны ОДКБ; КССБ — Комитет секретарей советов безопасности ОДКБ; ПС — Постоянный Совет ОДКБ; ГС — Генеральный секретариат ОДКБ; ОШ ОДКБ — Объединенный штаб ОДКБ.

ШОС — Шанхайская организация сотрудничества; СГГ — Совет глав государств ШОС; РАТС — Региональная антитеррористическая структура ШОС; СНК — Совет национальных координаторов ШОС; СГП — Совет глав правительств ШОС; СМИД — Совет министров иностранных дел ШОС; СМО — Совет министров обороны ШОС.

ЕАЭС — Евразийский экономический союз; ЕЭК — Евразийская экономическая комиссия ЕАЭС; СБ ЕЭК — Совет по безопасности ЕЭК ЕАЭС; КЕЭК — Коллегия Евразийской экономической комиссии ЕАЭС; МПС — Механизмы пограничного сотрудничества ЕАЭС; СПТ — Системы прослеживаемости товаров ЕАЭС.

Источник: составлено С.Г. Лузяниным и О.М. Умаровым.

Существенно усиливаются возможности обеспечения безопасности. Совместные системы кибермониторинга, разрабатываемые под эгидой ОДКБ[3], позволяют своевременно выявлять и нейтрализовывать киберугрозы. Формирование общих баз данных по терроризму и экстремизму в рамках ШОС (Румянцева, Рахимов, 2022) повышает точность и эффективность превентивных мер.

[3] Замахина Т. Парламенты ОДКБ приняли концепцию борьбы с киберугрозами // Российская газета. 30.11.2020. URL: https://rg.ru/2020/11/30/parlamenty-odkb-prinialikoncepciiu-borby-s-kiberugrozami.html (дата обращения: 28.08.2025).

Таблица 2. **Сравнительный анализ цифровых стратегий безопасности в рамках ОДКБ, ШОС и ЕАЭС**

Критерий	Организация		
	ОДКБ	**ШОС**	**ЕАЭС**
Основной фокус цифровизации	Военно-политическая безопасность, киберзащита, управление кризисами	Противодействие терроризму, сепаратизму и экстремизму, киберсуверенитет	Экономическая интеграция, снижение неэкономических рисков
Ключевые структуры и механизмы	Координационный центр по кибербезопасности (с 2017 г.), информационная система ОДКБ	Региональная антитеррористическая структура (РАТС), базы данных по терроризму и киберугрозам	Интегрированные информационные системы, «цифровые транспортные коридоры», электронные сертификаты
Основные направления деятельности	Мониторинг и противодействие киберугрозам, обмен информацией о кибератаках, гармонизация законодательств, проведение учений (например, «ПРОРЫВ»)	Интеграция информации из национальных источников, предиктивный анализ угроз, регулирование контента, противодействие «цветным революциям»	Реализация проектов прослеживаемости товаров, минимизация рисков контрабанды и мошенничества, гармонизация требований к безопасности
Специфические особенности	Оперативный обмен данными в режиме реального времени, акцент на гибридных угрозах	Продвижение концепции государственного контроля над интернет-пространством, инициативы по цифровой торговле	Фокус на экономической безопасности, обеспечение «четырех свобод» (движение товаров, услуг, капиталов и рабочей силы)

Источник: составлено С.Г. Лузяниным и О.М. Умаровым.

Анализ архитектуры ОДКБ, ШОС и ЕАЭС также позволил обнаружить системные пробелы в охвате современных нетрадиционных угроз. Несмотря на развитое сотрудничество в сферах кибербезопасности и противодействия терроризму, остаются неструктурированными ключевые сферы: энергетическая безопасность (отсутствуют механизмы кризисного реагирования и защиты инфраструктуры); экологические угрозы (нет систем мониторинга и ликвидации трансграничных катастроф); продовольственная безопасность (не созданы системы раннего предупреждения и адаптации агропромышленных комплексов стран-участниц); социально-демографические вызовы (не развиты механизмы управления миграцией и демографическими угрозами); технологические риски (отсутствует регулирование ИИ и биобезопасности).

При этом вопросы безопасности на евразийском пространстве актуальны как никогда. На саммите ШОС, прошедшем 31 августа 2025 г. в г. Тяньцзине (Китайская Народная Республика (КНР)), было одобрено соглашение об Универсальном центре по противодействию вызовам и угрозам безопасности странам – членам объединения и об Антинаркотическом центре, а также утверждена дорожная карта по развитию энергетического взаимодействия до 2030 г.[4] 9 октября 2025 г. в рамках саммита «Центральная Азия – Россия» в Душанбе заместитель председателя правительства РФ Дмитрий Григоренко провел совещание по развитию цифрового сотрудничества в регионе[5].

Однако существующая архитектура евразийской безопасности сохраняет реактивный характер, ориентированный на традиционные вызовы. Отсутствие проактивных механизмов создает серьезные уязвимости перед новыми угрозами, для противодействия которым необходима комплексная цифровая стратегия, включающая создание специализированных подразделений безопасности в ключевых сферах (энергетика, экология, миграция и др.), а также научно-аналитических центров раннего предупреждения. Критически важным является формирование постоянно действующих рабочих групп с применением ИИ для анализа угроз и разработки многоуровневой системы координации между всеми механизмами безопасности.

[4] Совет глав государств — членов ШОС одобрил Тяньцзиньскую декларацию // РИА Новости. 01.09.2025. URL: https://ria.ru/20250901/shos-2038770495.html (дата обращения: 03.11.2025).

[5] Второй саммит Россия — Центральная Азия // Президент России. 09.10.2025. URL: http://kremlin.ru/events/president/news/78180 (дата обращения: 30.10.2025).

В условиях стремительной цифровой трансформации и роста трансграничных угроз актуализируется необходимость формирования согласованных механизмов обеспечения безопасности на субрегиональном уровне. Предлагаемая модель Шаблона цифровой субрегиональной безопасности призвана объединить усилия пяти государств — Российской Федерации, Республики Узбекистан, Республики Казахстан, Республики Таджикистан и Киргизской Республики в сфере противодействия современным вызовам в киберпространстве, энергетике, экологии, борьбе с трансграничной преступностью и координации действий при чрезвычайных ситуациях.

Концептуальные основы ШЦСБ

ШЦСБ базируется на принципах совместимости систем, предиктивной аналитики и многоуровневой киберзащиты. Реализация Шаблона предполагает создание интегрированной цифровой экосистемы, включающей:

– единую платформу мониторинга и прогнозирования чрезвычайных ситуаций (ЧС), объединяющую данные национальных служб министерств по чрезвычайным ситуациям (МЧС) с использованием ИИ для моделирования сценариев развития катастроф, разработку общих стандартов для систем мониторинга и предупреждения ЧС, обучение и подготовку кадров в области цифровых технологий для МЧС, включая симуляции и обучение на основе данных;

– межгосударственную систему противодействия киберпреступности и наркотрафику, основанную на распределенных реестрах (блокчейн) для отслеживания перемещения запрещенных грузов и машинного анализа криминальных сетей с использованием больших данных, а также разработки протоколов обмена информацией между правоохранительными органами для быстрого реагирования на угрозы;

– цифровые двойники энергосистем с элементами *Smart Grid*, обеспечивающие устойчивость к кибератакам и оптимизацию распределения энергоресурсов;

– создание единой экосистемы для мониторинга экологической ситуации в регионе с использованием спутниковых данных и IoT-устройств — Экологического цифрового атласа, аккумулирующего данные дистанционного зондирования Земли, показания датчиков и гидрометеорологические наблюдения для прогнозирования экологических угроз; разработка цифровых инструментов для оценки воздействия на окружающую среду, включая системы раннего предупреждения о природных катастрофах; обмен данными о состоянии экосистем между странами для более эффективного реагирования на экологические угрозы.

Систематизация основных направлений цифровой трансформации в рамках ШЦСБ позволяет составить предварительную *дорожную карту* реализации этой структуры в виде комплексного стратегического плана, направленного на поэтапное внедрение цифровых технологий в ключевые сферы обеспечения региональной безопасности, где последовательно раскрываются основные векторы развития, конкретные мероприятия, технологическая база и прогнозируемые результаты трансформационных процессов (табл. 3).

Предложенная модель безопасности основана на синергии решений, где меры в одной области (экология) приносят пользу другим (МЧС, энергетика). Четкие показатели эффективности обеспечивают объективную оценку прогресса. Дорожная карта интегрирует технологические инновации с межгосударственным сотрудничеством, формируя методологическую основу цифровой трансформации безопасности. Дальнейшая работа требует конкретизации финансирования, создания рабочих групп и запуска пилотных проектов.

Предложенная дорожная карта реализует принцип последовательного и нарастающего внедрения, где временные рамки этапов (2026–2030 гг.) определены с учетом технологической сложности, степени институциональной готовности и необходимости формирования доверия между участниками.

Первый этап фокусируется на создании базовой технологической и нормативной платформы через относительно менее чувствительные, но критически важные направления, цифровизацию МЧС и экологический мониторинг, что закладывает основу для обмена данными.

Таблица 3. **Дорожная карта ШЦСБ: задачи, мероприятия, технологии и результаты**

Задачи	Ключевые мероприятия	Технологические решения	Ожидаемые результаты*	Этапы реализации
Цифровизация МЧС	Создание единой межгосударственной платформы обмена данными о ЧС. Разработка общих стандартов мониторинга. Подготовка кадров с использованием цифровых симуляторов	Облачные технологии, ИИ-аналитика, VR-тренажеры	Повышение оперативности реагирования на 30–40 %, сокращение времени принятия решений	1-й этап (2026-2028 гг.)
Борьба с трансграничной преступностью	1. Внедрение системы анализа преступной деятельности. 2. Разработка протоколов обмена информацией 3. Создание механизмов отслеживания наркотрафика	Big Data, блокчейн-технологии, криптографическая защита	Увеличение раскрываемости преступлений на 25 %, снижение объемов нелегального трафика	2-й этап (2027–2029 гг.)
Энергетическая безопасность	1. Развертывание системы мониторинга энергопотоков 2. Стандартизация управления инфраструктурой 3. Реализация проектов ВИЭ	Smart Grid, цифровые двойники, системы автоматизации	Оптимизация энергопотребления, снижение потерь до 15–20 %	2-й этап (2027–2030 гг.)
Экологический мониторинг	1. Создание единой системы экоконтроля 2. Разработка инструментов оценки воздействия 3. Организация обмена экоданными	Дистанционное зондирование, IoT-датчики, спутниковый мониторинг	Улучшение прогнозирования катастроф, снижение экологического ущерба	1-й и 2-й этапы (2026–2030 гг.)

Примечания. Раздел по ожидаемым результатам основан на оценках: 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). См. также: (Eom & Lee, 2022; Kostina & Kostin, 2022; Brayne, 2018; Антипова, 2026; Kabeyi & Olanrewaju, 2023).

Условные обозначения: ЧС — чрезвычайные ситуации, ИИ — искусственный интеллект, ВИЭ — возобновляемые источники энергии, VR — виртуальная реальность (*virtual reality*); Big Data — большие массивы информации, их сбор, обработка и аналитика; IoT — Интернет вещей (*Internet of Things*), то есть сеть физических объектов («вещей»), оснащенных датчиками, программным обеспечением и сетевыми модулями, которые позволяют им обмениваться данными через Интернет с другими устройствами и системами без участия человека.

Источник: составлено С.Г. Лузяниным и О.М. Умаровым.

Второй этап, являясь логическим продолжением первого, параллельно запускает более комплексные и политически деликатные модули борьбы с преступностью и энергетической безопасности, однако их различная длительность (2027–2029 и 2027–2030 гг. соответственно) отражает объективные различия в масштабе задач, от интеграции программных решений и протоколов до синхронизации физической инфраструктуры и масштабных инвестиций.

Хронология этапов внедрения ШЦСБ не является жестким коридором, а представляет собой гибкую схему, где проекты, сгруппированные по логике запуска, имеют индивидуальные сроки реализации, обусловленные их спецификой и необходимой глубиной трансформации.

Таблица 4. **Иерархическая структура Шаблона цифровой субрегиональной безопасности**

Подразделение	Составляющие	
Высший совет	Министры цифрового развития	
	Министры безопасности	
	Министры энергетики	
	Министры экологии	
	Министры МЧС 5 стран	
Исполнительный комитет	Постоянные представители государств	
	Международные эксперты	
Центры компетенций	Центр кибербезопасности и противодействия преступности	ФСБ (РФ) КНБ (Казахстан) СНБ (Узбекистан)
	Центр цифровых систем МЧС	МЧС России Казселезащита МЧС др. стран
	Центр энергетического мониторинга	Россети KEGOC Барки точик
	Центр экологического мониторинга	Росгидромет Казгидромет Узгидромет и др.
Технологическая инфраструктура	Единая облачная платформа	
	Блокчейн-системы	
	IoT-сети	
	Ситуационные центры в каждой стране	

Примечания. ФСБ РФ — Федеральная служба безопасности Российской Федерации (РФ); КНБ (Казахстан) — Комитет национальной безопасности Республики Казахстан (РК); СНБ (Узбекистан) — Служба национальной безопасности Республики Узбекистан (РУ); МЧС России — Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий; Россети — ПАО «Федеральная сетевая компания Россети», один из крупнейших в мире электросетевых холдингов; KEGOC — АО KEGOC (*Kazakhstan Electricity Grid Operating Company*), национальный оператор электрических сетей Казахстана; Барки точик — (ОАХК «Барки Точик»), государственная энергетическая компания Республики Таджикистан; Росгидромет — Федеральная служба по гидрометеорологии и мониторингу окружающей среды РФ; Казгидромет – Республиканское государственное предприятие «Казгидромет», гидрометеорологическая служба РК при Министерстве экологии и природных ресурсов РК; Узгидромет — Центр гидрометеорологической службы при Кабинете министров Республики РУ.

Источник: составлено С.Г. Лузяниным и О.М. Умаровым.

Структура ШЦСБ

Для обеспечения эффективного функционирования, необходимого уровня прозрачности и международной привлекательности предлагаемой модели ШЦСБ требуется создание комплексной организационной архитектуры, включающей несколько взаимосвязанных уровней управления и координации. Концепция ШЦСБ представляет собой сложную многоуровневую систему, где каждый элемент выполняет строго определенные функции при сохранении гибкости взаимодействия с другими компонентами структуры (табл. 4).

На вершине иерархической структуры располагается *Высший совет* (ВС) ШЦСБ, выполняющий функции стратегического руководящего органа. В его состав входят профильные министры пяти государств-участников, отвечающие за ключевые направления сотрудничества: цифровое развитие, национальную безопасность, энергетику, экологию и чрезвычайные ситуации. ВС может функционировать под эгидой существующих интеграционных структур (ОДКБ, ШОС, ЕАЭС). Этот коллегиальный орган определяет стратегические приоритетные векторы развития сотрудничества и принимает основополагающие политические решения, которые затем транслируются на нижестоящие уровни управления. Его задачи включают гармонизацию нормативно-правовых баз, проведение совместных учений по кибербезопасности и выработку протоколов обмена данными (табл. 4).

Оперативное воплощение решений Высшего совета обеспечит *Исполнительный комитет*, состоящий из постоянных представителей государств и привлекаемых международных

экспертов (см. табл. 4). Данный орган выполняет критически важную функцию трансформации стратегических установок в конкретные программы действий, одновременно осуществляя мониторинг их реализации и подготовку аналитических материалов для корректировки курса. Особенностью данной структуры является ее способность оперативно адаптироваться к изменяющимся условиям благодаря включению в состав независимых экспертов с различными профессиональными профилями.

Функциональная составляющая системы реализуется через сеть специализированных *Центров компетенций*, организованных по отраслевому принципу, каждый из которых фокусируется на конкретном направлении сотрудничества.

Центр кибербезопасности и противодействия преступности объединяет оперативные возможности национальных спецслужб (ФСБ России, КНБ Казахстана, СНБ Узбекистана), создавая единое информационное пространство для выявления и нейтрализации трансграничных угроз. Параллельно *Центр цифровых систем МЧС* обеспечивает интеграцию технологических решений в области предупреждения и ликвидации чрезвычайных ситуаций, используя передовые методы анализа рисков и прогнозирования.

Центр энергетического мониторинга обеспечивает интеграцию данных от ведущих сетевых операторов региона (Россетей, KEGOC, «Барки точик» и др.), что через координацию их действий позволяет не только повышать надежность энергосистем, но и оптимизировать распределение ресурсов.

Центр экологического мониторинга объединяет возможности гидрометеорологических служб (Росгидромета, Казгидромета, Узгидромета и др.) в области контроля состояния окружающей среды. Экологический мониторинг позволяет обеспечивать комплексный контроль состояния окружающей среды с применением современных технологий дистанционного зондирования.

Технологическая инфраструктура ШЦСБ представляет собой сложный симбиоз цифровых решений. Технологическую основу ШЦСБ могут составить:

– единая защищенная облачная платформа для хранения и обработки данных, служащая основой для хранения и обработки данных и обеспечивающая при этом необходимый уровень безопасности и доступности информации;

– блокчейн-системы обеспечения доверия и отслеживания транзакций — для создания доверенной среды обмена данными, особенно в чувствительных областях, таких как отслеживание трансграничных преступных схем;

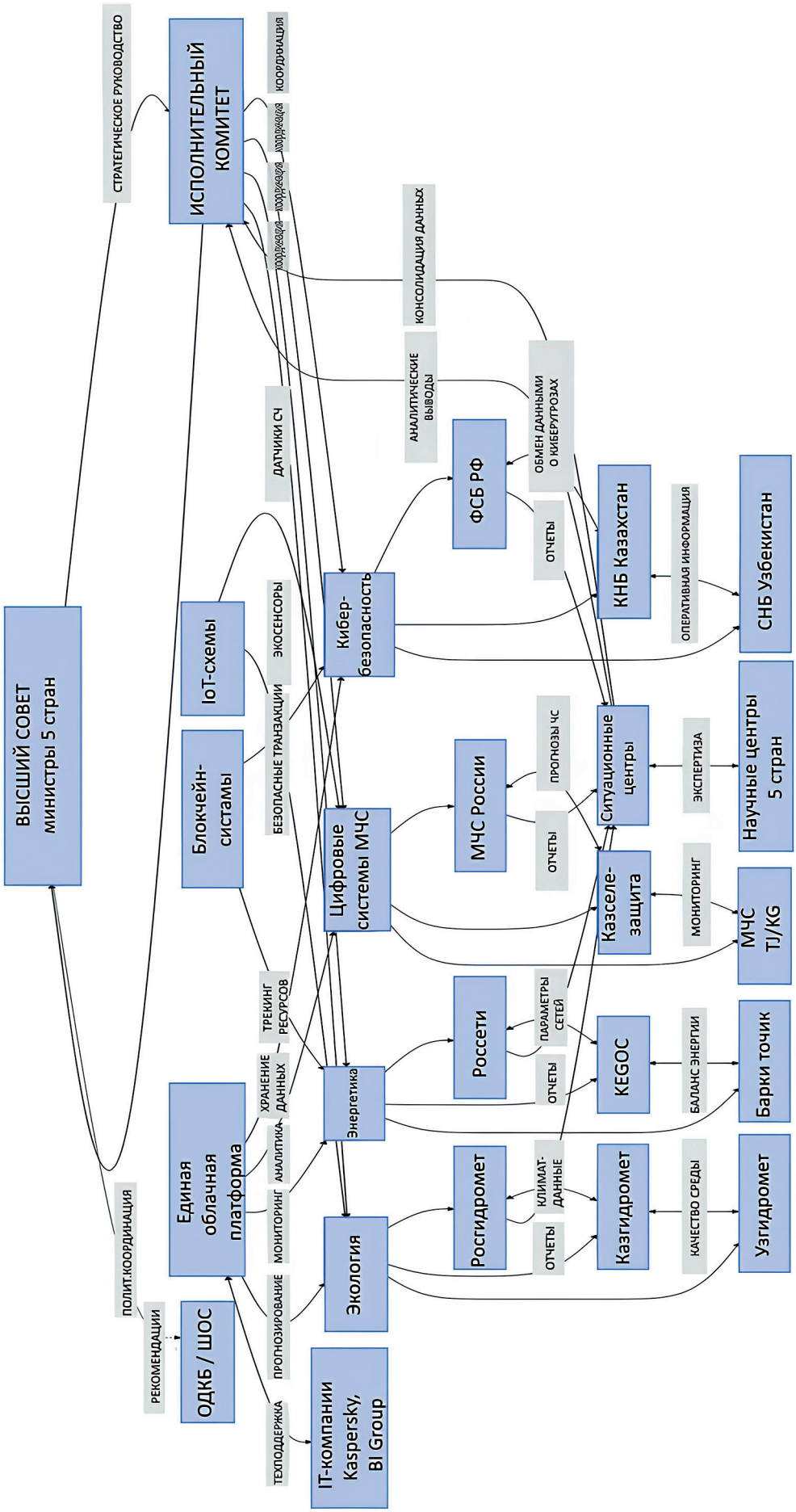
– распределенная сеть IoT-устройств, образующая распределенную систему мониторинга в реальном времени;

– сеть ситуационных центров в каждой стране-участнице, которая будет обеспечивать оперативную обработку поступающей информации (см. табл. 4).

Технологические особенности реализации ШЦСБ требует поэтапного развертывания защищенной облачной инфраструктуры с применением российских и совместно разработанных странами-участницами криптографических решений. Учитывая различия в уровне цифровизации вовлеченных государств, целесообразно предусмотреть механизмы технологического трансфера (например, создание региональных центров компетенций на базе ведущих IT-вузов России и Казахстана).

Информационные потоки в системе ШЦСБ организованы по принципу многоуровневой фильтрации и верификации данных (рис.). Вертикальные коммуникации обеспечивают передачу стратегических решений сверху вниз и оперативной отчетности снизу вверх. Горизонтальные связи между национальными ведомствами различных стран создают основу для оперативного обмена информацией и координации действий. Особое внимание уделено кросс-функциональным взаимодействиям, позволяющим интегрировать данные из различных источников для комплексного анализа угроз.

Технологическая интеграция достигается через систему стандартизированных интерфейсов, обеспечивающих совместимость разнородных информационных систем участников. Внешние взаимодействия с международными организациями и научными учреждениями осуществляются через специально разработанные протоколы, гарантирующие защиту суверенных интересов участников при сохранении открытости к сотрудничеству.



Структурно-функциональная организация ШЦСБ с визуализацией информационных потоков

Источник: составлено С.Г. Лузяниным и О.М. Умаровым.

Эффективность ШЦСБ напрямую зависит от адаптации к политико-экономическим реалиям Центральной Азии. Это предполагает:

– разработку многоязычных интерфейсов платформ с поддержкой русского и национальных языков;

– гибкие схемы финансирования, включающие взвешенное распределение затрат между более развитыми (РФ, Казахстан, Узбекистан) и нуждающимися в инфраструктурной модернизации (Таджикистан, Кыргызстан) участниками;

– создание пилотных зон для тестирования решений (например, трансграничный мониторинг рек Сырдарья/Амударья в рамках экологического модуля).

С точки зрения ожидаемых эффектов внедрение ШЦСБ позволит повысить оперативность реагирования на ЧС за счет автоматизированного анализа рисков, усилить контроль над незаконными трансграничными потоками через цифровую идентификацию грузов, снизить потери энергии путем оптимизации режимов работы энергосетей, а также сформировать научно обоснованную базу для принятия решений в экологической политике.

В результате проведенного исследования сложился предварительный конструкт Комплексной структуры реализации Шаблона цифровой субрегиональной безопасности (табл. 5).

Таблица 5. **Комплексная структура реализации ШЦСБ**

Компонент	Элементы	Участники / механизмы	Финансирование
Технологическая архитектура	– Единая защищенная облачная платформа (российские/гибридные решения) – Децентрализованные системы обмена данными (блокчейн, IoT) – Ситуационные центры с едиными стандартами	Технические специалисты всех стран-участниц, ИТ-компании	Инвестиции в инфраструктуру Технологический бартер (обмен мощностями)
Правовая база	– Многостороннее соглашение о кибербезопасности – Протоколы взаимопомощи (по образцу ОДКБ/ШОС)	Юридические службы государств, МИД, интеграционные объединения (ШОС, ЕАЭС)	Финансирование правовых разработок Гранты на гармонизацию законодательства
Институциональная структура	**Россия:** Минцифры, ФСБ, Росгвардия, Росгидромет, Ростех	Национальные ведомства, координационные советы, международные эксперты	Бюджетное финансирование госорганов Поддержка интеграционных объединений
	Казахстан: МЦРИАП, КНБ, KEGOC, Казгидромет		
	Узбекистан: Министерство ИКТ, СНБ, Узгидромет, Нацгвардия		
	Таджикистан/Кыргызстан: Агентства по ИБ, МЧС, гидромет, энергорегуляторы		
Финансовая модель	**Бюджетные источники:** долевое участие; целевые фонды ШОС/ОДКБ/ЕАЭС	Министерства финансов, международные организации, частный сектор	РФ, KZ — 30 %; UZ — 20 %; TJ, KR — 10 %; ШОС/ОДКБ/ЕАЭС (до 40 %)
	– **Внебюджетные источники:** Гранты (ООН, ВБ —для экологических и антикриминальных модулей) – ЧГП (*Kaspersky*, *BI Group*, *Uzbektelecom* и др.)		
	Технологический бартер (РФ предоставляет облачные мощности, Казахстан — дата-центры и т. п.)		

Примечания. Расшифровка аббревиатур и условных обозначений: РФ — Российская Федерация, KZ — Республика Казахстан, UZ — Республика Узбекистан, KR — Киргизская Республика, TJ — Республика Таджикистан; МЦРИАП — Министерство цифрового развития Казахстана, КНБ — Комитет нацбезопасности Казахстана, KEGOC — энергосети Казахстана, ИБ — информационная безопасность, ВБ — Всемирный банк, ЧГП — частно-государственное партнерство.

Источник: составлено С.Г. Лузяниным и О.М. Умаровым.

Таблица 6. **Общие цифровые проблемы, решаемые ШЦСБ**

Сфера	Проблемы	Решение через ШЦСБ
Цифровизация стандартов и платформ МЧС	Несовместимость систем оповещения, слабая координация при ЧС	Единая платформа мониторинга и реагирования на ЧС с ИИ-аналитикой
Цифровизация данных трансграничной преступности и наркотрафика	Разрозненные базы данных, низкий уровень обмена информацией	Общая криптозащищенная система анализа преступных сетей и блокчейн-трекинг грузов
Цифровизация энергетических вопросов	Дисбалансы в энергосетях, кибератаки на инфраструктуру	Умные сети (Smart Grid) с общей киберзащитой и прогнозной аналитикой
Цифровизация экологических тем	Отсутствие единого мониторинга загрязнений, климатических угроз	Цифровой экологический атлас с датчиками и спутниковым анализом

Источник: составлено С.Г. Лузяниным и О.М. Умаровым.

Реализация концепции ШЦСБ связана с определенными рисками и вызовами, что требует дополнительных усилий заинтересованных сторон (табл. 6).

Предлагаемая модель не является жесткой конструкцией, а представляет собой динамичную, гибкую систему, способную адаптироваться к эволюции угроз. Для ее внедрения можно предложить пилотный проект на базе одной из сфер (например, МЧС) с последующим масштабированием. Финансирование предлагается осуществлять через смешанные фонды (ЕАЭС, ШОС, национальные бюджеты).

Важно отметить, что успешная реализация данной модели требует не только технологических инвестиций, но и укрепления доверия между участниками.

В перспективе ШЦСБ может стать прототипом для аналогичных систем в других макрорегионах Евразии.

Заключение

Проведенное исследование демонстрирует глубокую трансформацию парадигмы евразийской безопасности в условиях цифровой эпохи. Опираясь на системный подход и сравнительный анализ, авторы провели диагностику архитектуры евразийской безопасности и предложили модель ее адаптации к вызовам цифровой эпохи. Полученные выводы структурируются в рамках ключевых задач работы.

Во-первых, подтверждено, что существующие институты (ОДКБ, ШОС и ЕАЭС), являясь необходимыми столпами регионального порядка, демонстрируют функциональную разобщенность и технологическое отставание, что формирует критические пробелы в охвате гибридных угроз от кибератак до экологических катастроф.

Во-вторых, в ответ на этот вызов разработана концепция ШЦСБ как многоуровневой институционально-технологической экосистемы, интегрирующей стратегические, оперативные и экспертные уровни управления через сеть специализированных центров компетенций.

В-третьих, детализирована дорожная карта реализации ШЦСБ, обосновывающая поэтапный переход от пилотных проектов в сферах МЧС и экологии к внедрению сложных модулей энергобезопасности и борьбы с преступностью, с четкой хронологией и инструментами прогнозной аналитики.

Центральным выводом исследования является подтверждение гипотезы о необходимости создания интегрированных цифровых экосистем безопасности, способных обеспечить кросс-граничное сквозное управление рисками. Практическая реализация модели: сочетание блокчейн-технологий, предиктивной аналитики и распределенных систем мониторинга позволит достичь качественно нового уровня координации между государствами-участниками.

Реализация модели ШЦСБ требует конкретных шагов. В качестве первоочередной меры целесообразно заключение межправительственного рамочного соглашения между заинтересованными государствами, определяющего базовые принципы сотрудничества, статус создаваемых органов и протоколы обмена данными, что создаст необходимую правовую

основу для последующей гармонизации национальных законодательств в сфере кибербезопасности и защиты критической инфраструктуры. Финансирование пилотной фазы обеспечит целевой фонд со смешанными источниками посредством взвешенных взносов из национальных бюджетов и грантов ЕАЭС. Для привлечения частных инвестиций может быть создана модель частно-государственного партнерства в форме консорциума IT-компаний, развертывающего платформу на принципах концессии.

Исследование выявило латентные синергетические эффекты, возникающие от интеграции разрозненных систем безопасности в единую цифровую экосистему. Ключевым из них является формирование кросс-доменного аналитического контура, когда данные из одной сферы (экологический мониторинг) автоматически становятся источником для моделирования в других областях (прогнозирование нагрузок на энергосистемы или рисков ЧС). Еще один эффект — взаимное усиление нормативных режимов, при котором стандарты кибербезопасности и протоколы обмена данными, разработанные для одного модуля (энергетика, правоохранительная деятельность), адаптируются для других (МЧС, экология), снижая общие транзакционные издержки системы.

Важным результатом стало подтверждение целесообразности применения принципа «цифрового суверенитета» в региональном масштабе, что позволяет совместить преимущества интеграции с сохранением национальных интересов отдельных государств-участников.

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

Список литературы

Аминов Ф. Б., Очилов А. О., Ботирова К. Б. к. Информационные технологии и искусственный интеллект в Узбекистане: проблемы и перспективы // В центре экономики. 2025. Т. 6, № 1. С. 28–32. URL: https://vcec.ru/index.php/vcec/article/view/153 (дата обращения: 01.11.2025).

Антипова А. Л. Применение алгоритмов ИИ и анализа больших данных в борьбе с преступностью // Интеллектуальные ресурсы — региональному развитию. 2026. № 1. С. 505–510. EDN: IOGFEF

Бухарин В. В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО-Университета. 2016. № 6. С. 76–91. https://doi.org/10.24833/2071-8160-2016-6-51-76-91; EDN: YGCPJX

Володенков С. В., Воронов А. С., Леонтьева Л. С., Сухарева М. Цифровой суверенитет современного государства в условиях технологических трансформаций: содержание и особенности // Полилог. 2021. Т. 5, № 1. С. 5. https://doi.org/10.18254/S258770110014073-2; EDN: WKLJNK

Гаврилов Е. О. Цифровой суверенитет в условиях глобализации: философский и правовой аспекты // Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки. 2020. Т. 4, № 2. С. 146–152. https://doi.org/10.21603/2542-1840-2020-4-2-146-152; EDN: WCSQFR

Даубасова С. Ш., Алаева Г. Т., Джумабаева К. А. Искусственный интеллект и уголовное преследование в Казахстане // Eurasian Scientific Journal of Law. 2024. № 4. С. 19–29. URL: https://esjl.turan-edu.kz/jour/article/view/239 (дата обращения: 01.11.2025).

Зиновьева Е. С., Шитьков С. В. Цифровой суверенитет в практике международных отношений // Международная жизнь. 2023. № 3. С. 38–51. EDN: HBTQYT

Ма Х., Мэн Ч., Ян Д., Ван Х. Цифровая трансформация Китая : опыт преобразования инфраструктуры национальной экономики. Пер. с кит. Москва : Интеллектуальная литература, 2019.

Мустафина А., Далелхан А., Ногаева Карача А. Қазақстан Республикасының әскери ісіндегі жасанды интеллект технологиясының перспективалары мен құқықтық реттелуі [Перспективы и правовое регулирование технологий искусственного интеллекта в военных делах Республики Казахстан] // Мемлекеттік басқару және мемлекеттік қызмет [Государственное управление и гражданская служба]. 2025. Т. 94, № 3. С. 171–179. (На казахском языке). https://doi.org/10.52123/1994-2370-2025-1522; EDN: CSJNFF

Румянцева А. К., Рахимов К. Х. Роль ШОС в противодействии терроризму в странах Центральной Азии // Постсоветские исследования. 2022. Т. 5, № 8. С. 835–846. EDN: MCZNRN

Умаров О. М. Цифровизация в малых государствах Центральной Евразии: общее и особенное, вызовы и риски // Большая Евразия: развитие, безопасность, сотрудничество : ежегодник : материалы VII международной научно-практической конференции : в 4 частях. Вып. 8, ч. 2. Москва, 2025. Москва : ИД «УМЦ», 2025. С. 175–182. EDN: VYFCSI

Brayne S. The Criminal Law and Law Enforcement Implications of Big Data // Annual Review of Law and Social Science. 2018. Vol. 14. P. 293–308. https://doi.org/10.1146/annurev-lawsocsci-101317-030839

Chen Ch., Li Zh., Hao Zh., Chao L., Mengwei W., Hao C. Zhongguo qiyeshuzihua shengcun guanli shijian shijiao de chuangxin yanjiu [Исследование практики управления цифровым выживанием китайских предприятий, ориентированных на инновации] // Guanli kexue xuebao [Журнал управленческих наук (JMAS)]. 2019. No. 10. P. 1–8. (На китайском языке).

Denning D. E. Information Warfare and Security. New York : ACM Press, 1999.

Duan N. Qiye jingying guanli shijiao xia shuzihua zhuanxing de fa zhan tanjiu [Исследование развития цифровой трансформации с точки зрения управления предприятием] // Dianzi tongxin yu jisuanji kexue [Электронные коммуникации и компьютерные науки (EECS)]. 2022. Vol. 4, no. 3. P. 74–76. (На китайском языке). https://doi.org/10.37155/2717-5170-0403-29

Eom S.J., Lee J. Digital Government Transformation in Turbulent Times: Responses, Challenges, and Future Direction // Government Information Quarterly. 2022. Vol. 39, iss. 2. P. 1–9. https://doi.org/10.1016/j.giq.2022.101690; EDN: GWQOEW

Kabeyi M. J. B., Olanrewaju O. A. Smart Grid Technologies and Application in the Sustainable Energy Transition: A Review // International Journal of Sustainable Energy. 2023. Vol. 42, iss. 1. P. 685–758. https://doi.org/10.1080/14786451.2023.2222298; EDN: VVRHKJ

Kostina E. A., Kostin A. V. How Do Smart City Technologies Help to Cope with the Pandemic? // Regional Research of Russia. 2022. Vol. 12, no. 2. P. 241–249. https://doi.org/10.1134/S2079970522020149; EDN: QUZATZ

Schneier B. Beyond Fear : Thinking Sensibly about Security in an Uncertain World. New York : Copernicus Books, 2003.

Xiao J., Xie K., Wu Y. Shuju qudong de chanpin shiying xing chuangxin — shuzi jingji de chuangxin luoji [Адаптивные инновации в продуктах, основанные на данных: инновационная логика цифровой экономики] // Beijing jiaotong daxue xuebao (Shehui kexue ban) [Журнал Пекинского университета Цзяотун (издание по социальным наукам)]. 2020. Vol. 19, no. 1. P. 7–18. (На китайском языке).

Сведения об авторах:

Лузянин Сергей Геннадьевич — доктор исторических наук, профессор департамента зарубежного регионоведения, НИУ ВШЭ; Российская Федерация, 119017, г. Москва, ул. Малая Ордынка, д. 17; профессор кафедры востоковедения, МГИМО (У) МИД РФ; Российская Федерация, 119454, г. Москва, пр-кт Вернадского, д. 76; eLibrary SPIN-код: 2864-9951; ORCID: 0000-0001-9578-6023; e-mail: luzyanin.sergey@mail.ru

Умаров Отабек Мухаммадалиевич — соискатель департамента зарубежного регионоведения, НИУ ВШЭ; Российская Федерация, 119017, г. Москва, ул. Малая Ордынка, д. 17; ORCID: 0009-0008-3091-1872; e-mail: omuhammadaliyevich@mail.ru