pISSN 2073-2872
eISSN 2311-875X

Экономическая политика государства

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СТРАН – ЧЛЕНОВ ШОС В ТЕКУЩИХ ГЕОПОЛИТИЧЕСКИХ РЕАЛИЯХ

DOI: https://doi.org/10.24891/wcbuva
EDN: https://elibrary.ru/wcbuva

Олег Борисович ПИЧКОВ

доктор экономических наук, профессор, декан факультета международных экономических отношений, Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации (МГИМО МИД России), Москва, Российская Федерация
e-mail: o.b.pichkov@yandex.ru
ORCID: 0000-0003-1210-2066
SPIN: 8701-8789

Елена Алексеевна БРЕНДЕЛЕВА

кандидат экономических наук, доцент, заведующий кафедрой экономической теории, Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации (МГИМО МИД России), Москва, Российская Федерация
e-mail: e.brendeleva@inno.mgimo.ru
ORCID: отсутствует
SPIN: 5460-1420

Михаил Сергеевич ГРОМОВ

ответственный автор, преподаватель кафедры экономической политики и государственно-частного партнерства, Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации (МГИМО МИД России), Москва, Российская Федерация
e-mail: gromovmikhailmgimo@yandex.ru
ORCID: 0000-0002-5552-0885
SPIN: 9523-2006

История статьи:
Рег. № 767/2025
Получена 26.11.2025
Одобрена 02.02.2026
Доступна онлайн 30.03.2026

Специальность: 5.2.5

УДК 339.9
JEL: F52

Ключевые слова:
ШОС, информационная безопасность, дифференцированный киберсуверенитет, киберугрозы, вызовы

Аннотация

Предмет. Состояние и перспективы сотрудничества в сфере информационной безопасности в рамках Шанхайской организации сотрудничества в современных геополитических условиях.

Цели. Выявить ключевые вызовы и приоритеты политики Шанхайской организации сотрудничества и разработать практические рекомендации по оптимизации механизмов данного сотрудничества.

Методология. В процессе исследования использовались историко-хронологический анализ эволюции сотрудничества, сравнительное изучение позиций государств – членов ШОС и структурный разбор институциональных механизмов.

Результаты. Определены структурные ограничения интеграции, систематизированы современные угрозы и сформулированы конкретные рекомендации по укреплению взаимодействия.

Выводы. Несмотря на существующие внутренние противоречия и различия в подходах, Шанхайская организация сотрудничества демонстрирует движение к созданию механизмов обеспечения информационной безопасности.

Для цитирования: Пичков О.Б., Бренделева Е.А., Громов М.С. Информационная безопасность стран – членов ШОС в текущих геополитических реалиях // Национальные интересы: приоритеты и безопасность. – 2026. – № 3. – С. 22 – 36. DOI: 10.24891/wcbuva EDN: WCBUVA

В современных международных отношениях цифровое пространство превратилось из чисто технологической среды в арену стратегического соперничества и конфронтации. На этом фоне Шанхайская организация сотрудничества (ШОС), объединяющая ключевые государства Евразии, стремится занять лидирующую позицию в формировании новой архитектуры региональной и глобальной цифровой безопасности [1].

Стратегической основой сотрудничества в сфере международной информационной безопасности в ШОС является создание единого, безопасного и стабильного информационного пространства для всех государств – членов организации [2].

Эта задача эволюционировала от первоначального акцента на военно-политическом доверии и решении пограничных вопросов до комплексного подхода, который сегодня включает кибербезопасность, борьбу с киберпреступностью и совместное противодействие использованию интернета в террористических целях.

Необходимо отметить несколько ключевых этапов эволюции данного сотрудничества.

1. Фундамент (до 2001 г.). Истоки ШОС лежат в механизме «Шанхайской пятерки», где главной задачей было построение доверия и взаимное сокращение вооруженных сил в приграничных районах. Успех в этой области создал атмосферу доверия, необходимую для обсуждения более сложных и современных угроз, включая информационные.

2. Институционализация (2001–2009 гг.). После официального основания ШОС в 2001 г. началась выработка общих принципов. Были подписаны ключевые документы, такие как Хартия ШОС (2002 г.)[1] и Соглашение о сотрудничестве в области обеспечения международной информационной безопасности (2009 г.)[2].

   Эти документы впервые на многосторонней основе закрепили обязательства стран-членов совместно противодействовать использованию информационно-коммуникационных технологий в целях, подрывающих международную стабильность и безопасность.

3. Углубление и расширение (2010–2020 гг.). В этот период сотрудничество стало более предметным. Страны ШОС не только осознали общность угроз, но и начали вырабатывать конкретные механизмы взаимодействия.

   Принятие дополнительных протоколов и соглашений, а также регулярный обмен мнениями на площадках Совета глав государств и Совета министров иностранных дел позволили синхронизировать национальные подходы к международной информационной безопасности (МИБ).

4. Стратегическая консолидация (после 2020 г.). Современный этап характеризуется растущей интеграцией вопросов МИБ в общую экономическую и транспортно-логистическую повестку ШОС.

   Безопасность цифровой инфраструктуры стала рассматриваться как необходимое условие для реализации масштабных проектов, таких как развитие международных транспортных коридоров.

[1] Хартия Шанхайской организации сотрудничества. URL: http://www.kremlin.ru/supplement/3450

[2] Екатеринбургская декларация глав государств – членов Шанхайской организации сотрудничества. URL: http://www.kremlin.ru/supplement/66

Расширение организации за счет включения новых членов (в том числе Беларусь) еще больше усиливает потребность в выработке единых стандартов и координированной политики в информационной сфере.

Основным инструментарием ШОС в сфере международной информационной безопасности является формирование комплексной нормативно-правовой базы. Этот процесс реализуется через принятие ключевых документов на регулярных саммитах, которые задают стратегические ориентиры.

К таким документам относятся совместные декларации (Екатеринбургская 2009 г., Уфимская 2015 г., Астанинская 2017 и 2024 г.), заявления и концепции, последовательно закрепляющие принципы уважения государственного суверенитета и невмешательства во внутренние дела как основу безопасного информационного пространства [3].

В этих документах государства – члены ШОС координируют свои позиции для продвижения инициатив по разработке универсальных норм поведения в киберпространстве и всеобъемлющей конвенции по борьбе с киберпреступностью на площадке ООН.

Важным механизмом оперативного взаимодействия выступают постоянно действующие рабочие группы и экспертные советы [4]. Эти структуры, такие как Группа экспертов по МИБ или рабочие группы при Региональной антитеррористической структуре (РАТС), обеспечивают координацию на техническом и профильном уровнях.

Их функционал включает мониторинг новых киберугроз, выработку мер противодействия, гармонизацию национальных законодательств и разработку совместных позиций для международных форумов [5].

Заседания этих органов, проводящиеся на регулярной основе, позволяют детально прорабатывать конкретные аспекты сотрудничества, включая противодействие использованию ИКТ в преступных и террористических целях.

Третьим направлением деятельности является реализация образовательных программ и мероприятий по повышению квалификации, нацеленных на преодоление кадрового дефицита в сфере информационной безопасности [6]. Ключевую роль в этой работе играет Университет ШОС, объединяющий вузы стран – участниц ШОС.

В его рамках осуществляется подготовка высококвалифицированных IT-специалистов, проводятся международные конференции, семинары и тренинги, в том числе для сотрудников правоохранительных органов, занимающихся расследованием киберпреступлений. Это способствует не только обмену передовым опытом, но и созданию общего профессионального поля и укреплению доверия между государствами–членами.

Наконец, сотрудничество в рамках ШОС включает разработку и внедрение согласованных технических мер и международных стандартов. Государства совместно создают системы мониторинга и раннего предупреждения кибератак, внедряют технологии шифрования и аутентификации для защиты критической информационной инфраструктуры.

Оперативное взаимодействие обеспечивается через специализированные каналы связи и базы данных для обмена информацией о киберинцидентах и вредоносном ПО [7–9]. Параллельно ведется работа по гармонизации национальных законодательств, направленная на создание единого правового пространства в сфере МИБ, что делает взаимодействие между странами более предсказуемым и эффективным.

Современные вызовы и приоритеты в сфере информационной безопасности в странах ШОС формируются под влиянием роста цифровых угроз и стремления государств–членов противостоять милитаризации киберпространства.

Основные усилия организации направлены на создание архитектуры безопасности, способной эффективно противодействовать как традиционным, так и новым вызовам [10]. В *табл. 1* представлены ключевые вызовы и соответствующие им приоритеты деятельности ШОС в области информационной безопасности.

Стоит отметить, что помимо глобальных вызовов, которые стоят перед странами ШОС, существует комплекс структурных проблем и внутренних ограничений, которые оказывают глубокое влияние на темпы и глубину интеграции в рамках организации.

Одним из фундаментальных ограничителей является сама архитектура принятия решений в ШОС. Организация функционирует на основе многоуровневой системы, высшим звеном которой является Совет глав государств. Ключевые решения требуют консенсуса всех стран – участниц ШОС [11].

Такой подход, с одной стороны, гарантирует учет мнения каждого суверенного государства, но с другой – выступает серьезным тормозом в процессе принятия оперативных и смелых стратегических решений. В условиях, когда состав ШОС расширился до десяти очень разных членов, достижение консенсуса по чувствительным вопросам становится все более сложной задачей.

Кроме того, внутри ШОС сосуществуют государства, имеющие глубокие двусторонние противоречия, что создает постоянный источник напряженности. Наиболее яркий пример – соперничество между Индией и Пакистаном[3]. Их конфликт не остается лишь внешнеполитическим фоном, а напрямую влияет на работу организации.

Например, в 2025 г. Индия заблокировала вступление Азербайджана в ШОС, поскольку та поддерживает Пакистан[4]. Подобные действия демонстрируют то, как двусторонние споры могут парализовать процесс принятия решений и препятствовать дальнейшему расширению организации.

Государства–члены ШОС существенно различаются по уровню своего инновационного развития, что напрямую влияет на их восприятие угроз и приоритеты политики. Россия и Китай являются бесспорными технологическими лидерами в организации [12].

Для них характерна комплексная позиция, которая делает акцент на развитии киберсуверенитета, установлении общих международных стандартов в области информационной безопасности и развитии многостороннего сотрудничества для противодействия трансграничным угрозам. Их подход сочетает защиту национального информационного пространства с активными действиями на международной арене.

Такие государства, как Индия, Иран и Казахстан демонстрируют значительные успехи в инновационном развитии. В частности, Казахстан позиционируется как технологический лидер в Центральноазиатском регионе, а потому вопросы построения информационной безопасности являются для него стратегическим фокусом. Эти страны стремятся не только решать внутренние задачи, но и активно участвовать в формировании региональной повестки дня [13–15].

Менее технологически развитые члены ШОС, такие как Кыргызстан, Таджикистан и Узбекистан, в большей степени концентрируются на предотвращении и устранении угроз внутренней политической стабильности, исходящих из информационного пространства.

Несмотря на это, они также выдвигают собственные инициативы в рамках Организации, что свидетельствует о растущем понимании важности данной проблематики.

[3] Что такое ШОС и для чего она России. URL: https://trends.rbc.ru/trends/social/6683b2469a7947835daa1763

[4] Там же.

Еще одной проблемой является необходимость координации масштабных инициатив, продвигаемых разными членами организации. В научной среде звучат предостережения о потенциальной противоречивости параллельного развития китайского проекта Экономического пояса Шелкового пути и Евразийского экономического союза, инициированного Россией [16].

Создание конкурирующих зон свободной торговли может осложнять выработку единой политической стратегии для государств Центральной Азии и, как следствие, гармонизацию подходов к информационной безопасности.

Таким образом, вместо универсального применения термина «киберсуверенитет» данное исследование предлагает концепцию «дифференцированного киберсуверенитета».

Эта модель позволяет систематизировать подходы государств–членов не по формальному признаку «развитый – развивающийся», а по глубине и инструментам осуществления суверенитета в цифровой сфере, что напрямую определяет их приоритеты в рамках ШОС.

Модель включает три ключевых типа.

1. Киберсуверенитет как технологический и правовой барьер (Российская Федерация, Китай). Для этих стран киберсуверенитет – это активная проекция государственной власти в цифровое пространство.

   Он реализуется через создание автономной технологической экосистемы (национальных сегментов интернета, импортозамещения ПО и оборудования), жесткое правовое регулирование (создание законов о локализации данных, КИИ, «суверенном интернете») и активное продвижение этих норм в качестве международных стандартов.

   Их запрос к ШОС – это институционализация данных подходов в формате юридически обязывающих многосторонних соглашений. Успешным примером является лоббирование через ШОС (с опорой на соглашения 2009 и 2015 г.) концепции государственного суверенитета в киберпространстве в рамках Группы правительственных экспертов ООН. Таким образом, для РФ и КНР ШОС выступает как платформа для легитимации и глобализации национальных стандартов цифровой автаркии.

2. Киберсуверенитет как обеспечение внутренней политической безопасности (Центральноазиатские государства – члены ШОС). Для Узбекистана, Таджикистана, Кыргызстана и Казахстана суверенитет в информационной сфере – это прежде всего защита государственной власти и общественной стабильности от внутренних угроз, таких как экстремистская пропаганда, организация массовых протестов через социальные сети, информационно-психологическое воздействие.

   Их фокус находится на контроле контента, мониторинге социальных медиа и укреплении потенциала правоохранительных органов. Их ключевой запрос к ШОС – получение технической помощи, обмен опытом и нормативными шаблонами для решения этих задач.

   В этом контексте они активно участвуют в образовательных программах ШОС и используют площадку для заимствования успешных практик (например, элементов российского и китайского законодательства о регулировании интернета).

3. Киберсуверенитет как обеспечение стратегической автономии и экономического развития (Индия). Подход Индии – страны с либеральным политическим режимом, но стремящейся к стратегической самостоятельности – является уникальным в рамках ШОС.

   Здесь киберсуверенитет понимается не как барьер, а как способность самостоятельно обеспечивать безопасность критической инфраструктуры и данных, не ограничивая при этом интеграцию в глобальные технологические цепочки и рост IT-экспорта.

Индийская политика сочетает развитие национального потенциала (защиту КИИ, программы типа «Цифровая Индия») с прагматичным партнерством с западными технологическими компаниями.

В рамках ШОС Индия выступает в роли «внутреннего критика», блокируя и смягчая инициативы, которые могут привести к фрагментации интернета или избыточному регулированию. Яркий пример – сдержанная позиция Индии по вопросам всеобъемлющей конвенции ООН по киберпреступности, активно продвигаемой Россией и Китаем.

Эта дифференцированная модель показывает, что ШОС функционирует не как механизм унификации, а как сложная арена переговоров между разными моделями киберсуверенитета.

Именно это противоречие, а не просто «разный уровень развития», генерирует «размытые» формулировки итоговых документов – они являются не недостатком, а закономерным результатом поиска консенсуса между этими тремя парадигмами.

Для формирования полной картины необходимо обратиться к данным международных индексов, которые однако следует учитывать с определенной долей критичности, поскольку они могут отражать западную точку зрения.

Среди членов ШОС Индия стабильно показывает наиболее высокие результаты в рейтингах, таких как Индекс демократии (The Economist Intelligence Unit, 41-е место из 167), Freedom on the Net (Freedom House, 41-е место из 70) и Freedom in the World (92-е место из 210)[5]. Это указывает на несколько иной, более либеральный подход к регулированию интернета и информационной среды по сравнению с другими участниками Организации.

Большинство государств – членов ШОС занимают низкие позиции в этих рейтингах. Например, Китай стабильно оказывается на последних местах в индексе Freedom on the Net, а в World Press Freedom Index (Reporters Without Borders) он находится на 176-м месте из 180, опережая только Иран.

Схожие низкие показатели демонстрируют Беларусь, Россия и другие центральноазиатские страны. Эти данные подчеркивают, что для многих членов ШОС концепция информационной безопасности тесно связана с защитой государственного суверенитета и стабильности, что отражается в соответствующем нормативно-правовом регулировании.

Одним из самых значительных шагов в укреплении безопасности стало решение, принятое на саммите в Тяньцзине в сентябре 2025 г., о создании Универсального центра по противодействию вызовам и угрозам безопасности[6].

Этот центр, размещающийся в Ташкенте, заменит РАТС и получит значительно более широкие полномочия. В его функции будет входить противодействие не только «трем силам зла» (терроризму, сепаратизму, экстремизму), но и их проявлениям в информационном пространстве, а также транснациональной организованной преступности и финансированию незаконной деятельности.

В рамках этого Универсального центра будет учрежден специализированный Центр информационной безопасности, также базирующийся в Ташкенте. Его работа будет сосредоточена непосредственно на киберугрозах, что свидетельствует о глубоком понимании ШОС специфики современных рисков.

Данные инициативы свидетельствуют о переходе ШОС от общих деклараций к созданию конкретных механизмов противодействия гибридным угрозам, в которых киберпространство играет ключевую роль.

[5] SCO: Unfree, Undemocatic, Dangerous for the Press? URL: https://www.statista.com/chart/32537/ranking-of-shanghai-cooperation-organization-member-states-on-selected-indices/

[6] Об участии в Глобальном форуме по сотрудничеству в области общественной безопасности. URL: https://rus.sectsco.org/20250917/1988715.html

Чтобы предложить рекомендации по дальнейшему развитию данного направления в рамках деятельности ШОС, обратимся к конкретным эмпирическим данным для сравнения эффективности и уникальности подхода ШОС.

Согласно данным, публикуемым РАТС, основной акцент в деятельности организации в информационной сфере сделан на противодействии использованию интернета в террористических, сепаратистских и экстремистских целях.

Доклады РАТС регулярно освещают проведение совещаний экспертов, конференций и учений, таких как «Киберщит-антитеррор», которые направлены на выработку общих подходов. Однако в открытых официальных отчетах и коммюнике, включая итоговые декларации саммитов ШОС, отсутствуют упоминания о конкретных случаях совместной нейтрализации трансграничных кибератак или детали оперативных совместных расследований киберинцидентов, проведенных под эгидой организации после 2015 г.

В отличие от ШОС, в рамках БРИКС был создан и функционирует конкретный практический инструмент – Рабочая группа по безопасности в сфере использования информационно-коммуникационных технологий. Важным эмпирическим фактом является заявление о запуске в 2024 г. под эгидой этой рабочей группы «специального электронного реестра для обмена данными о компьютерных атаках и инцидентах».

Существование такого реестра указывает на переход от политических дискуссий к созданию инфраструктуры для практического обмена технической информацией. Финансовым инструментом, поддерживающим подобные инициативы в БРИКС, является Новый банк развития БРИКС, который, согласно своему уставу, может финансировать проекты, связанные с устойчивым развитием и инфраструктурой, что потенциально включает и проекты в сфере цифровой безопасности.

Это доказывает тезис о том, что принцип консенсуса в разнородной ШОС является более серьезным барьером для создания глубоких оперативных механизмов, чем более гибкий формат БРИКС, который, как отмечает эксперт Алексей Маслов, является объединением без жесткого членства и с более прагматичными задачами[7].

Отличия от ОДКБ очевидны: ОДКБ – это военно-политический блок с четкой иерархией и обязательствами по коллективной обороне, не ставящий информационную безопасность в центр своей повестки. ШОС же – организация, где военная безопасность не является центральной.

Ее уникальность состоит в том, что она позволяет странам с глубокими историческими противоречиями (Индия и Пакистан, Киргизия и Таджикистан) поддерживать диалог на менее официальных параллельных встречах, когда прямые официальные контакты затруднены. Это делает ШОС не аналогом НАТО, а уникальной платформой для управления соперничеством.

В отличие от АСЕАН, которая работает по принципу консультаций и мягкой силы, ШОС сочетает консенсусную модель с активным продвижением государствами–лидерами (РФ, КНР) жестких концепций цифрового суверенитета на глобальном уровне. АСЕАН же, как правило, избегает столь идеологизированных подходов, фокусируясь на практическом сотрудничестве.

Предложенная нами концепция «дифференцированного киберсуверенитета» предоставляет не только аналитическую рамку для понимания внутренних противоречий ШОС, но и служит основой для разработки конкретных, прагматичных и многоуровневых рекомендаций. Эти предложения учитывают расхождения в подходах и национальных интересах, превращая разнообразие из источника слабости в потенциал для гибкой и поэтапной кооперации.

[7] Алексей Маслов рассказал о различиях БРИКС и ШОС.
URL: https://bigasia.ru/aleksej-maslov-rasskazal-o-razlichiyah-briks-i-shos/

Активизация роли РАТС как центрального оперативного узла. Данная структура определена как ключевой орган ШОС по обеспечению безопасности, который уже координирует практические действия, включая сферу кибербезопасности. Поэтому логичным развитием является не создание новых структур «с нуля», а целевое расширение мандата и технических возможностей РАТС.

Конкретно, это может означать разработку в рамках РАТС специализированного протокола обмена техническими индикаторами компрометации (IoC) и тактиками, техниками и процедурами (TTPs) киберугроз, но строго в контексте борьбы с «тремя силами зла» – терроризмом, сепаратизмом и экстремизмом.

Такой подход, фокусирующийся на бесспорно общей угрозе, имеет наибольшие шансы на консенсус и соответствует духу документов ШОС, где угрозы в киберпространстве рассматриваются через эту призму [17].

Институционализация экспертных платформ на базе успешных прецедентов. Анализ показывает, что ШОС уже проводит успешные совместные образовательные мероприятия, такие как онлайн-семинары по борьбе с киберпреступностью, объединяющие экспертов из многих стран.

Рекомендация заключается в превращении подобных разовых мероприятий в постоянно действующую рабочую группу экспертов по техническим и правовым аспектам кибербезопасности под эгидой Совета национальных координаторов.

Эта группа могла бы заниматься не только обменом опытом, но и гармонизацией национальных подходов к расследованию киберинцидентов, что соответствует целям, обсуждавшимся на семинарах.

Развитие сотрудничества с профильными международными и отраслевыми партнерами. Официальные источники подчеркивают заинтересованность ШОС в установлении контактов с другими организациями, например, Консультативно-координационным центром ОДКБ по вопросам реагирования на компьютерные инциденты.

Поэтому перспективным направлением является создание совместных рабочих групп с такими партнерами по конкретным темам, таким как защита критической информационной инфраструктуры. Это позволит ШОС не изолироваться, а стать частью более широкой сети региональной кибербезопасности, используя свой уникальный подход к международной информационной безопасности.

Создание целевых программ в рамках Университета ШОС. Следует предложить разработку сетевых магистерских программ по международной информационной безопасности и правовым аспектам киберпространства.

Такие программы могли бы совместно реализовываться ведущими вузами стран–членов, с акцентом на сравнительный анализ национальных законодательств и подходов ШОС к вопросам цифрового суверенитета, что является предметом научного интереса и обсуждения [18–20].

Превращение учений в регулярную комплексную практику. Известно, что Совет РАТС еще в 2015 г. достиг договоренности о проведении совместных учений по борьбе с кибертерроризмом. Рекомендацией является регуляризация этих учений и расширение их формата.

Помимо силового блока, к ним следует привлекать специалистов по защите критической инфраструктуры (энергетики, транспорта, финансов), учитывая, что эти объекты являются мишенями для атак.

Также можно рассмотреть привлечение к учениям компетентных органов стран ШОС, не входящих в другие военно-политические союзы, что соответствует заявленной позиции руководства РАТС.

Разработка отраслевых стандартов кибербезопасности для совместных проектов. Учитывая, что логистическая и транспортная инфраструктуры являются приоритетом экономического сотрудничества в ШОС, логичной рекомендацией является инициирование разработки «Рамочных требований по кибербезопасности для международных транспортно-логистических коридоров на пространстве ШОС».

Этот документ мог бы устанавливать минимальные стандарты защиты систем управления, протоколы оповещения об инцидентах и порядок взаимодействия национальных CERT-команд. Защита именно этой общей инфраструктуры от киберугроз становится практической необходимостью, а не идеологической декларацией.

Создание тематических альянсов для защиты критических секторов. Опасность атак на критическую инфраструктуру (энергетику, водоснабжение, здравоохранение) признается экспертами ШОС.

Поэтому можно рекомендовать формирование тематических групп быстрого реагирования и обмена информацией для ключевых секторов экономики на добровольной основе. Такие группы могли бы работать под эгидой профильных совещаний министров (например, транспорта или по чрезвычайным ситуациям), используя уже существующую институциональную сеть организации.

Коллективные усилия стран Шанхайской организации сотрудничества в сфере информационной безопасности демонстрируют последовательную эволюцию – от формирования основ взаимного доверия к созданию сложной архитектуры противодействия современным киберугрозам.

Несмотря на внутренние вызовы, такие как необходимость достижения консенсуса среди разнородных членов и наличие двусторонних противоречий, ШОС подтверждает свою роль ключевой платформы для выработки общих подходов к безопасности в цифровую эпоху.

Принятые на саммите в Тяньцзине в 2025 г. решения о создании Универсального центра и специализированного Центра информационной безопасности в Ташкенте знаменуют собой переход от деклараций к практической реализации совместных механизмов защиты.

В то же время сохраняется фундаментальное напряжение между стремлением к единой региональной политике и объективно существующей дифференциацией государств–членов. Технологические лидеры, такие как Россия и Китай, продвигают концепцию киберсуверенитета и многостороннего регулирования.

При этом другие участники (например, Индия) могут придерживаться более либеральных взглядов, а менее развитые страны фокусируются на вопросах внутренней стабильности. Это разнообразие подходов, с одной стороны, обогащает дискуссию, а с другой – затрудняет выработку универсальных протоколов и быстрых решений.

Таким образом, будущее сотрудничества в рамках ШОС будет определяться способностью организации превратить свое многообразие из ограничения в преимущество. Реализация предложенных мер – внедрение гибких форматов диалога, создание платформ для обмена данными, реализация совместных образовательных программ и концентрация на непримиримых угрозах – может стать тем путем, который позволит укрепить коллективную киберустойчивость.

Успех в этой области станет не только гарантией безопасности каждого государства–члена, но и весомым вкладом в формирование более стабильной и предсказуемой системы глобальной информационной безопасности.

Таблица 1
Ключевые вызовы и соответствующие им приоритеты деятельности ШОС в области информационной безопасности

Table 1
Key challenges and corresponding priorities of SCO activities in the field of information security

Современные вызовы	Приоритеты и ответные меры ШОС
Милитаризация сферы ИКТ	Категорическое противодействие милитаризации, продвижение мирного использования технологий
Угрозы критической информационной инфраструктуре	Защита критической инфраструктуры государств-членов от внешних угроз
Использование интернета и даркнета для дестабилизации обстановки, вовлечения молодежи в преступную деятельность	Борьба с киберпреступностью, терроризмом и экстремизмом в информационном пространстве
Использование цифровых технологий (ИИ, шифрование) преступными и террористическими группировками	Разработка механизмов противодействия с использованием искусственного интеллекта и работы с цифровыми доказательствами

Источник: авторская разработка по данным Агентства экономической информации ПРАЙМ. URL: https://1prime.ru/20250901/shos-861570168.html

Source: Authoring, based on the PRIME Economic Information Agency data. URL: https://1prime.ru/20250901/shos-861570168.html

Список литературы

1. Цзэкунь Гу. Сотрудничество и вызовы в области обеспечения информационной безопасности в рамках шанхайской организации сотрудничества // Информационные войны. 2023. № 4. С. 37–41. EDN: BCDWWY
2. Лепешкина О.И. Международное сотрудничество государств СНГ по противодействию киберпреступности // Евразийская интеграция: экономика, право, политика. 2023. Т. 17. № 4. С. 82–91. DOI: 10.22394/2073-2929-2023-04-82-91 EDN: BCZVQY
3. Рахимов К.Х., Салимзода К.Х. Взаимодействие БРИКС и ШОС в сфере обеспечения информационной безопасности // Вопросы национальных и федеративных отношений. 2024. Т. 14. № 11. С. 3530–3544. DOI: 10.35775/PSI.2024.116.11.020 EDN: VMEKXK
4. Руденко М.Н. Национальная безопасность России в геополитических контурах // Экономическая безопасность. 2025. Т. 8. № 3. С. 643–664. DOI: 10.18334/ecsec.8.3.122980 EDN: SKBOZA
5. Андронова И.В., Гусаков Н.П., Завьялова Е.Б. Финансирование терроризма: новые вызовы для международной безопасности // Вестник международных организаций: образование, наука, новая экономика. 2020. Т. 15. № 1. С. 120–134. DOI: 10.17323/1996-7845-2020-01-05 EDN: ICJJPL
6. Завьялова Е.Б. Перспективы развития российского рынка образования в новых международных условиях: сценарные варианты // Международный научный журнал. 2023. № 3. С. 31–47. DOI: 10.34286/1995-4638-2023-90-3-31-47 EDN: XYFJFK
7. Мингаирова А.К. Эволюция подхода Китая к обеспечению международной информационной безопасности: значение для России // Вестник ученых-международников. 2023. № 2. С. 256–275. EDN: MKEMFA

8. Шарофзода Р.Ш. Деятельность современного государства в условиях усиления информационных вызовов и угроз // Юридическая наука: история и современность. 2021. № 10. С. 175–188. EDN: VQLKMZ

9. Лагуткина Ю.Н., Мадалимбеков Ж.И., Омарова Д.К. Противодействие Российской Федерации и Республики Казахстан информационному терроризму // Постсоветские исследования. 2022. Т. 5. № 8. С. 847–860. EDN: GHIIRB

10. Фатыхов Д.Р. Теоретические и практические аспекты международной информационной безопасности в текущих условиях // Право и управление. XXI век. 2024. Т. 20. № 2. С. 140–147. DOI: 10.24833/2073-8420-2024-2-71-140-147 EDN: RLHQXA

11. Поршнева О.С., Разинков С.Л. Институциональное становление и эволюция деятельности ШОС: опыт ретроспективного анализа // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2024. Т. 24. № 2. С. 264–279. DOI: 10.22363/2313-0660-2024-24-2-264-279 EDN: WQJPKJ

12. Помозова Н.Б., Ли Ч., Старикова Е.А. и др. Особенности экономического сотрудничества России и Китая на современном этапе: взгляд ученых и общества // Право и управление. XXI век. 2024. Т. 20. № 4. С. 94–103. DOI: 10.24833/2073-8420-2024-4-73-94-103 EDN: LJGFEE

13. Юй Т. Китайско-российское сотрудничество в области совместного обеспечения информационной безопасности: состояние, факторы влияния и принятые меры // Международный научно-исследовательский журнал. 2025. № 1. DOI: 10.60797/IRJ.2025.151.19

14. Констан П.Я. Субрегиональные организации, стоящие перед вызовами глобализации // Культура Мира. 2025. Т. 13. № 44. С. 247–255. EDN: PRGPIH

15. Болгов Р.В., Еременков А.А., Чернов С.И. Подходы международных организаций к защите прав человека в цифровом пространстве // Россия в глобальном мире. 2025. Т. 28. № 1. С. 7–29. DOI: 10.48612/rg/RGW.28.1.1 EDN: QMVNXN

16. Лу С. Достижения и проблемы сотрудничества в области информационной безопасности в рамках ШОС // Теории и проблемы политических исследований. 2023. Т. 12. № 1А. С. 169–178. DOI: 10.34670/AR.2023.87.56.019 EDN: HOBPJC

17. Дубень А.К. Стратегический вектор обеспечения международной информационной безопасности на пространстве международных организаций // Аграрное и земельное право. 2021. № 10. С. 154–158. DOI: 10.47643/1815-1329_2021_10_154 EDN: ZHWKEH

18. Сагымбаев А.А., Мамадалиева Ж.Б., Сагымбаев А.А. и др. Международная информационная безопасность: вызовы и возможности // Вестник Кыргызско-Российского Славянского университета. 2024. Т. 24. № 12. С. 101–105. DOI: 10.36979/1694-500X-2024-24-12-101-105 EDN: RWGITC

19. Гао Юе. Особенности и перспективы российско-китайского сотрудничества в сфере обеспечения информационной безопасности // ПОИСК: Политика. Обществоведение. Искусство. Социология. Культура. 2023. № 1. С. 87–97. EDN: IERGDY

20. Щербань А.В. Политика обеспечения информационной безопасности в государствах–членах ШОС // Евразийская интеграция: экономика, право, политика. 2025. Т. 19. № 1. С. 159–170. DOI: 10.22394/2073-2929-2025-01-159-170 EDN: DFBCZG

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

pISSN 2073-2872
eISSN 2311-875X

Economic Policy of the State

INFORMATION SECURITY OF SCO MEMBER COUNTRIES IN THE CURRENT GEOPOLITICAL REALITY

DOI: https://doi.org/10.24891/wcbuva
EDN: https://elibrary.ru/wcbuva

Oleg B. PICHKOV

Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation (MGIMO University),
Moscow, Russian Federation
e-mail: o.b.pichkov@yandex.ru
ORCID: 0000-0003-1210-2066

Elena A. BRENDELEVA

Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation (MGIMO University),
Moscow, Russian Federation
e-mail: e.brendeleva@inno.mgimo.ru
ORCID: not available

Mikhail S. GROMOV

Corresponding author, Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation (MGIMO University),
Moscow, Russian Federation
e-mail: gromovmikhailmgimo@yandex.ru
ORCID: 0000-0002-5552-0885

Article history:
Article No. 767/2025
Received 26 Nov 2025
Accepted 2 Feb 2026
Available online 30 Mar 2026

JEL Classification: F52

Keywords: SCO, information security, differentiated cyber sovereignty, cyber threats, challenges

Abstract

Subject. The state and prospects of cooperation in the field of information security within the Shanghai Cooperation Organization in the current geopolitical context.

Objectives. The study aims to identify the key challenges and policy priorities of the Shanghai Cooperation Organization, and develop practical recommendations for optimizing the mechanisms of this cooperation.

Methods. For the study, we used a historical-chronological analysis of the cooperation evolution, a comparative study of the member States positions, and a structural review of institutional mechanisms.

Results. The article identifies structural limitations of integration, systematizes contemporary threats, and formulates specific recommendations for strengthening interaction.

Conclusions. Despite existing internal contradictions and differences in approaches, the Shanghai Cooperation Organization demonstrates progress toward establishing mechanisms for ensuring information security.

Please cite this article as: Pichkov O.B., Brendeleva E.A., Gromov M.S. Information security of SCO member countries in the current geopolitical reality. *National Interests: Priorities and Security*, 2026, iss. 3, pp. 22–36. DOI: 10.24891/wcbuva EDN: WCBUVA

References

1. Zekun G. [Cooperation and challenges in the field of information security under the framework of the shanghai cooperation organization]. *Informatsionnye voiny*, 2023, no. 4, pp. 37–41. (In Russ.) EDN: BCDWWY
2. Lepeshkina O.I. [International cooperation of member nations of the CIS on counteracting cybercrime]. *Evraziiskaya integratsiya: ekonomika, pravo, politika*, 2023, vol. 17, iss. 4, pp. 82–91. (In Russ.) DOI: 10.22394/2073-2929-2023-04-82-91 EDN: BCZVQY
3. Rakhimov K.Kh., Salimzoda K.Kh. [Interaction between BRICS and the SCO in the sphere of information security]. *Voprosy natsional'nykh i federativnykh otnoshenii*, 2024, vol. 14, iss. 11, pp. 3530–3544. (In Russ.) DOI: 10.35775/PSI.2024.116.11.020 EDN: VMEKXK
4. Rudenko M.N. [Russia's national security in geopolitical terms]. *Ekonomicheskaya bezopasnost'*, 2025, vol. 8, iss. 3, pp. 643–664. (In Russ.) DOI: 10.18334/ecsec.8.3.122980 EDN: SKBOZA
5. Andronova I.V., Gusakov N.P., Zav'yalova E.B. [Terrorism financing: New challenges for international security]. *Vestnik mezhdunarodnykh organizatsii: obrazovanie, nauka, novaya ekonomika*, 2020, vol. 15, iss. 1, pp. 120–134. (In Russ.) DOI: 10.17323/1996-7845-2020-01-05 EDN: ICJJPL
6. Zav'yalova E.B. [The Russian education market in the new international environment]. *Mezhdunarodnyi nauchnyi zhurnal*, 2023, no. 3, pp. 31–47. (In Russ.) DOI: 10.34286/1995-4638-2023-90-3-31-47 EDN: XYFJFK
7. Mingairova A.K. [Evolution of China's approach to maintaining international information security: Meaning for Russia]. *Vestnik uchenykh-mezhdunarodnikov*, 2023, no. 2, pp. 256–275. (In Russ.) EDN: MKEMFA
8. Sharofzoda R.Sh. [The activity of the modern State in the context of increased information challenges and threats]. *Yuridicheskaya nauka: istoriya i sovremennost'*, 2021, no. 10, pp. 175–188. (In Russ.) EDN: VQLKMZ
9. Lagutkina Yu.N., Madalimbekov Zh.I., Omarova D.K. [Counteraction of the Russian Federation and the Republic of Kazakhstan to information terrorism]. *Postsovetskie issledovaniya*, 2022, vol. 5, iss. 8, pp. 847–860. (In Russ.) EDN: GHIIRB
10. Fatykhov D.R. [Theoretical and practical aspects of international information security under current conditions]. *Pravo i upravlenie. XXI vek*, 2024, vol. 20, iss. 2, pp. 140–147. (In Russ.) DOI: 10.24833/2073-8420-2024-2-71-140-147 EDN: RLHQXA
11. Porshneva O.S., Razinkov S.L. [Institutional formation and development of sco activities: Experience of retrospective analysis]. *Vestnik Rossiiskogo universiteta druzhby narodov. Seriya: Mezhdunarodnye otnosheniya*, 2024, vol. 24, iss. 2, pp. 264–279. (In Russ.) DOI: 10.22363/2313-0660-2024-24-2-264-279 EDN: WQJPKJ
12. Pomozova N.B., Li Ch., Starikova E.A. et al. [The particularities of Russian–Chinese economic cooperation at the present stage: Scientists and society's opinions]. *Pravo i upravlenie. XXI vek*, 2024, vol. 20, iss. 4, pp. 94–103. (In Russ.) DOI: 10.24833/2073-8420-2024-4-73-94-103 EDN: LJGFEE
13. Yui T. [Chinese-Russian co-operation in the field of joint provision of information security: State, influencing factors and measures taken]. *Mezhdunarodnyi nauchno-issledovatel'skii*

zhurnal, 2025, no. 1. DOI: 10.60797/IRJ.2025.151.19

14. Konstan P.Ya. [Subregional organizations facing the challenges of globalization]. *Kul'tura Mira*, 2025, vol. 13, iss. 44, pp. 247–255. (In Russ.) EDN: PRGPIH
15. Bolgov R.V., Eremenkov A.A., Chernov S.I. [Approaches of international organizations to the protection of digital human rights]. *Rossiya v global'nom mire*, 2025, vol. 28, iss. 1, pp. 7–29. (In Russ.) DOI: 10.48612/rg/RGW.28.1.1 EDN: QMVNXN
16. Lu S. [Achievements and challenges of cooperation in the field of information security within the SCO framework]. *Teorii i problemy politicheskikh issledovanii*, 2023, vol. 12, iss. 1A, pp. 169–178. DOI: 10.34670/AR.2023.87.56.019 EDN: HOBPJC
17. Duben' A.K. [The strategic vector of ensuring international information security in the space of international organizations]. *Agrarnoe i zemel'noe pravo*, 2021, no. 10, pp. 154–158. (In Russ.) DOI: 10.47643/1815-1329_2021_10_154 EDN: ZHWKEH
18. Sagymbaev A.A., Mamadalieva Zh.B., Sagymbaev A.A. et al. [International information security: Challenges and opportunities]. *Vestnik Kyrgyzsko-Rossiiskogo Slavyanskogo universiteta*, 2024, vol. 24, iss. 12, pp. 101–105. (In Russ.) DOI: 10.36979/1694-500X-2024-24-12-101-105 EDN: RWGITC
19. Gao Yu. [Features and prospects of Russian–Chinese cooperation in the field of information security]. *POISK: Politika. Obshchestvovedenie. Iskusstvo. Sotsiologiya. Kul'tura*, 2023, no. 1, pp. 87–97. EDN: IERGDY
20. Shcherban' A.V. [Information security policy in the SCO member states]. *Evraziiskaya integratsiya: ekonomika, pravo, politika*, 2025, vol. 19, iss. 1, pp. 159–170. (In Russ.) DOI: 10.22394/2073-2929-2025-01-159-170 EDN: DFBCZG

Conflict-of-interest notification

We, the authors of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.