УДК 33 **10.34670/AR.2023.87.56.019**

Достижения и проблемы сотрудничества в области информационной безопасности в рамках ШОС

Лу Сюаньтун

Магистрант,
Университет Китайской академии общественных наук,
102488, Китайская Народная Республика, Пекин, ул. Чанъюй, 11;
e-mail: luxuantong919@163.com

Аннотация

По мере развития Шанхайской организации сотрудничества (ШОС) фокус ее взаимодействия в области безопасности сместился с традиционного сотрудничества в приграничных районах на противодействие нетрадиционным угрозам безопасности, и сотрудничество в области информационной безопасности стало одним из приоритетных направлений. В условиях более серьезной ситуации в киберпространстве, начиная с 2005 года, сотрудничество в области информационной безопасности в рамках ШОС перешло от консенсуса к действиям и достигло положительных результатов, включая подписание ряда официальных документов, улучшение институционального строительства, проведение учений по борьбе с кибертерроризмом и участие в управлении международной информационной безопасностью (МИБ) в рамках ООН. Однако в то же время такие проблемы, как киберсуверенитет, цифровой разрыв и вмешательство внешних сил, также создают вызовы для развития сотрудничества в области информационной безопасности. В будущем мудрость и мужество государств-членов ШОС будут проверены на то, как решить вышеупомянутые проблемы и углубить взаимодействие в данной сфере.

Для цитирования в научных исследованиях

Лу Сюаньтун. Достижения и проблемы сотрудничества в области информационной безопасности в рамках ШОС // Теории и проблемы политических исследований. 2023. Том 12. № 1А. С. 169-178. 10.34670/AR.2023.87.56.019

Ключевые слова

Шанхайская организация сотрудничества (ШОС), сотрудничество в рамках ШОС, информационные технологии, информационная безопасность, экономика.

Введение

С развитием и применением информационных технологий человеческое общество вступило в цифровую эпоху. Информационные технологии меняют весь мир, делая нашу повседневную жизнь быстрее и удобнее. В то же время, в связи с открытым, виртуальным и интерактивным характером сетевой информации, проблемы информационной безопасности становятся все более актуальным и превращаются в важный фактор, влияющий на национальную безопасность всех стран. Пандемия коронавирусной инфекции ускорила процессы цифровизации, которая проводилась зачастую без учета соображений безопасности, и, таким образом, обострила угрозы международной информационной безопасности (далее – МИБ) [Международная информационная безопасность…, www]. Поддержание информационной безопасности все больше требует международного сотрудничества.

С момента создания Шанхайской организации сотрудничества (далее — ШОС) сотрудничество в области безопасности является ее приоритетом. Более 20 лет в соответствии с реалистичными потребностями ШОС постоянно расширяет масштабы сотрудничества для устранения новых нетрадиционных угроз безопасности в регионе на основе совместных контртеррористических действий [邓浩, 2021, 21]. Участницы организации придают большое значение информационной безопасности для политической стабильности, экономического развития и глобального престижа, осуществили ряд мероприятий по сотрудничеству в области информационной безопасности и достигли плодотворных результатов. Сегодния мир переживает невиданные за столетие большие перемены, обзор достижений и обобщение опыта сотрудничества между государствами-членами ШОС в области информационной безопасности поможет углубить дальнейшее сотрудничество в данной сфере, решить новые проблемы и обеспечить стабильность региона.

Основные достижения сотрудничества в области информационной безопасности в рамках ШОС

Информационная безопасность определена официальным документом ШОС как состояние защищенности личности общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве [Соглашение…, www]. Защиту информации можно рассматривать как совокупность тесно связанных между собой задач в области международной этики, права, организации управления, разработки технических средств, программирования и математики [Ромашкина, 2015, 77]. С 2005 года сотрудничество в области информационной безопасности в рамках ШОС перешло от консенсуса к действиям и достигло плодотворных результатов.

1. Ряд официальных документов представляет собой руководство к действию.

В 2005 году на Пятом саммите главы государств-членов ШОС подписали «Декларацию глав государств-членов Шанхайской организации сотрудничества» [Декларация…, www], в которой впервые был упомянут информационный терроризм, что положило начало сотрудничеству в области информационной безопасности в рамках ШОС.

По случаю пятой годовщины создания ШОС, важность информационной безопасности была разъяснена на Шестом саммите в 2006 году, по итогам которого была подписано «Заявление глав государств-членов ШОС по международной информационной безопасности» [Заявление…, www]. В документе говорится, что транснациональный характер

информационно-коммуникационных технологий (далее — ИКТ) делают необходимым сотрудничество по обеспечению информационной безопасности. Данное заявление является первым официальным документом ШОС в области информационной безопасности и постановило создать группу экспертов по МИБ.

В 2009 году на 9-м саммите ШОС участницы организации подписали «Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности». Уникальность документа заключается в том, что он впервые на международно-правовом уровне зафиксировал наличие конкретных угроз в области информационной безопасности, а также определил основные направления, принципы, формы и механизмы сотрудничества в этой сфере [Гайнетдинова, Сизых, 2019, 174].

За прошедшее десятилетие ШОС неоднократно выдвигала рекомендации по укреплению сотрудничества в декларациях саммитов, демонстрируя твердую решимость всех сторон поддерживать международную и региональную информационную безопасность. В 2020 году на 20-м саммите в Москве утверждены «Заявление Совета глав государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности» и «Заявление Совета глав государств-членов Шанхайской организации сотрудничества о противодействии распространению террористической, сепаратистской и экстремистской идеологии, в том числе в сети Интернет» [Документы…, www]. В вышеупомянутых заявлениях всесторонне изложены цели, принципы и задачи организации по обеспечению МИБ, выражена воля к дальнейшему укреплению взаимодействия, высказана поддержка по созданию сообщества единой судьбы в киберпространстве.

Таким образом, в рамках ШОС был издан и обновлен ряд официальных документов, обеспечивающих важные ориентиры для сотрудничества в области информационной безопасности, которое постепенно поднимается на стратегический уровень.

2. Создание механизмов находится в центре внимания сотрудничества в области информационной безопасности.

Для эффективного осуществления сотрудничества в области информационной безопасности государства-члены ШОС намеренны совершенствовать соответствующие механизмы. Региональная антитеррористическая структура (далее – РАТС), созданная в 2004 году, является одним из двух постоянных органов ШОС и отвечает за обмен информацией и координацию действий по борьбе с экстремизмом, транснациональной преступностью и незаконным оборотом наркотиков. В последние годы из-за появления новых угроз в киберпространстве, РАТС предприняли шаги по координации действий между государствами-членами. В 2016 году были приняты структурой «Совместные меры по предотвращению актов терроризма» и «Совместные меры по распространению экстремистских идеологий на территории государств-членов», которые эффективно помогли сторонам в предотвращении распространения кибертерроризма в регионе.

В июне 2006 года по решению Совета глав государств-членов ШОС была создана Группа экспертов (ГЭ) по МИБ. Эксперты из разных стран оценивают скрытые угрозы в области информационной безопасности, изучают возможные пути сотрудничества и дают рекомендации на основе международного права, а также способствуют достижению консенсуса между государствами-членами по вопросам, связанным с МИБ. В 2021 году Группа экспертов разработала «План взаимодействия государств-членов ШОС по вопросам обеспечения международной информационной безопасности на 2022-2023 годы», который был включен в «Душанбинская декларация двадцатилетия ШОС» [Душанбинская декларация…, www].

В августе 2006 года была создана Специальная рабочая группа (СРГ) по современным информационным и телекоммуникационным технологиям государств-членов ШОС. Ее основными обязанностями являются: изучение и разработка приоритетных проектов сотрудничества в области ИКТ; содействие взаимодействию и обмену между информационно-коммуникационными секторами государств-членов; обеспечение безопасности и равных прав государств-членов в области ИКТ. По инициативе Узбекистана в 2021 году состоялась первая встреча руководителей ведомств государств-членов ШОС, ответственных за развитие ИКТ, на которой стороны рассмотрели ряд документов по сотрудничеству в области ИКТ и обсудили перспективы углубления взаимодействия в рамках существующих рабочих групп [Состоялась первая встреча…, www].

3. Учения по борьбе с кибертерроризмом воплощают достигнутый консенсус в конкретную практику.

С 2015 года провели ряд учений по борьбе с кибертерроризмом при координации РАТС, которые эффективно повысили способность сторон к совместной работе по борьбе с кибертерроризмом.

В 2015 году в Сямыне (Китай) организовано учение по борьбе с кибертерроризмом «Сямынь-2015» – совместное штабное учение компетентных органов государств-членов ШОС [В Китае…, www]. В ходе учения стороны обменялись своими рабочими процессами, правовыми процедурами и техническими возможностями в борьбе с террористической деятельностью, при дальнейшем совершенствовании механизма сотрудничества между соответствующими ведомствами государств-членов и создании совместной технической платформы для противодействия кибертерроризму.

На этой основе в 2017 и 2019 годах были проведены еще два совместных учения по борьбе с кибертерроризмом, которые полностью проверили эффективность механизма сотрудничества в рамках ШОС, укрепили многостороннее взаимное доверие и продемонстрировали твердую уверенность государств-членов ШОС в поддержании безопасности регионального информационного пространства.

4. ШОС продвигает сотрудничество в области МИБ в рамках ООН.

Масштаб и технологический уровень деструктивного использования ИКТ неуклонно возрастает, при этом отсутствие необходимой международно-правовой базы, регулирующей деятельность государств в сфере их использования, является сегодня одной из ключевых проблем безопасности [Полякова, 2016, 17]. ШОС выступает за то, чтобы международное сообщество укрепляло координацию через ООН и другие международные платформы, совместно разрабатывало соответствующие международные правила, поддерживало равные права всех стран на участие в управлении международным информационным пространством.

В 2011 году во время 66-й сессии Генеральной Ассамблеи (ГА) ООН четыре страны — Китай, Россия, Таджикистан и Узбекистан — представили на рассмотрение «Правила поведения в области международной информационной безопасности» [Правила поведения…, www], который привлек широкое внимание международного сообщества и способствовал процессу выработки международных правил в киберпространстве.

После скандала США с программой PRISM в 2013 году больше стран призывают к созданию международных правил поведения в области информационной безопасности. На этом фоне шесть государств-членов ШОС, включая Китай и Россию, вновь представили обновленный «Правила поведения в области обеспечения международной информационной безопасности (МИБ)» на 69-й сессии ГА ООН в 2015 году. Новая версия документа является более

сбалансированной и включает в себя расширенное содержание по вопросам управления интернетом, преодоления цифрового разрыва и наращивания потенциала, а также новые меры по укреплению доверия в области кибербезопасности [Письмо постоянных представителей…, www]. Инициатива ШОС заслужила единодушную похвалу от международного сообщества.

Проблемы сотрудничества в области информационной безопасности между государствами-членами ШОС

В последние годы в связи с быстрым развитием информационных технологий и переменами в международной обстановке, ШОС столкнулась с рядом проблем, которые должны быть решены государствами-членами надлежащим образом.

1. Споры о киберсуверенитете ослабляют готовность государств-членов к сотрудничеству

«Шанхайский дух», с его акцентом на национальный суверенитет и равные консультации, является краеугольным камнем сотрудничества в области безопасности между государствами-членами ШОС, но он в определенной степени также создает неудобства для углубления сотрудничества [蒋也好,刘雪迪, 2021, 33]. Являясь новыми независимыми государствами после распада Советского Союза, страны Центральной Азии придают большое значение своей суверенной безопасности и предъявляют высокие требования к киберсуверенитету. В сочетании с специфическим и чувствительным характером самой информационной безопасности, проблемы киберсуверенитета стали препятствием для дальнейшего сотрудничества. Исходя из уважения суверенных интересов государств-членов, ШОС использует консенсусный подход к принятию решений, что затрудняет принятие обязательных документов и делает форму сотрудничества более важной, чем содержание. Например, в ходе предыдущих учений по борьбе с кибертерроризмом, хотя стороны проводили совместные операции под координацией РАТС, они по-прежнему осуществляли обработку информации, расследование и сбор доказательств в соответствии с своими национальными законами и правилами, и возможности совместного реагирования были ограничены.

В этом контексте председатель КНР Си Цзиньпин на саммите ШОС 2018 года выдвинул инициативу о «совместном создании сообщества единой судьбы ШОС» в качестве будущего направления сотрудничества [Си Цзиньпин…, www]. Перед лицом споров о киберсуверенитете государства-члены должны полностью осознать важность и актуальность информационной безопасности со стратегической высоты сообщества единой судьбы, чтобы достичь большего консенсуса.

2. Цифровой разрыв между государствами-членами увеличился после расширения организации.

В настоящее время совокупная мощь и возможности в области ИКТ государств-членов ШОС сильно различаются, что делает устойчивость стран к рискам информационной безопасности разной. В организации есть как державы с развитыми IT-технологиями, такие как Россия, Китай и Индия, так и малые и средние страны, чье развитие сетевой инфраструктуры относительно отстает. Кроме того, между законодательством государств-членов имеются значительные расхождения в части установления ответственности за противоправные деяния, совершаемые в сфере информационной безопасности. Эти различия касаются методов регулирования (уголовно-правовой или административный), количества и признаков составов наказуемых деяний, а также характера и размера установленных за них санкций [Додонов, Карабанова, 2019, 124].

Еще надо отметить, что различные позиции основных участниц организации по управлению киберпространством в определенной степени затрудняют многостороннее сотрудничество. Китай и Россия выступают за создание межправительственной структуры сотрудничества в области МИБ под эгидой ООН, которая обеспечит равенство и демократию в управлении интернет-ресурсами. Однако с 2015 года Индия стала ближе к позиции развитых стран, поддерживая модель управления с участием многих заинтересованных сторон, за которую ратовали США, пытаясь сформировать модель таким образом, чтобы укрепить свои позиции в глобальном киберуправлении. Это полностью отражает прагматические тенденции индийской политики [白联磊, 2021, 90].

Для того чтобы сократить цифровой разрыв, государства-члены ШОС должны сформировать импульс для сотрудничества в информационной индустрии, повысить технический уровень путем создания программного обеспечения, ускорить создание системы безопасности сетевой инфраструктуры, разработать и внедрить программы обучения молодых специалистов, усилить обмен опытом в данной области и повысить практические способности совместного реагирования на кибертерроризм.

3. Западные силы мешают сотрудничеству между государствами-членами ШОС.

С момента зарождения Интернета в США в конце 1960-х годов западные страны всегда доминировали в международном информационном пространстве, монополизируя право устанавливать международные правила Интернета. После окончания холодной войны США, как единственная сверхдержава, приступили к сдерживанию России и Китая в области ИКТ, чтобы защитить свои интересы глобальной кибергегемонии. Они преувеличивают так называемый «российский и китайский цифровой авторитаризм» и «теорию цифровой угрозы», что заставляет некоторые государства-члены ШОС с подозрением и осторожностью относиться к сотрудничеству в рамках организации [邓浩,李天毅, 2021, 76].

В последние годы США использовали свое преимущество в кибертехнологиях для вмешательства во внутренние дела других стран, осуществляя такие действия, как подслушивание телефонных переговоров, манипулирование в избирательных кампаниях и контроль общественного мнения, а также собрали альянс «Пять глаз» и начали кибервойну против других стран. Наращивание США ударного киберпотенциала вкупе с нежеланием обсуждать юридически обязывающие международн-правовые акты в рамках борьбы с киберугрозами тормозит выход мирового сообщества из латентного состояния войны всех против всех по Томасу Гоббсу, перенесенной в киберпространство [Демидов, 2013, 162]. На этом фоне возрастает риск международной гонки кибервооружений, что оказывает большее давление на ШОС в этой области.

В целях противодействия милитаризации глобального информационного пространства, Россия и Китай, являющиеся ведущими силами в ШОС, активно выстраивают практическое взаимодействие. В 2015 году подписано обеими сторонами «Соглашение между Правительством РФ и Правительством КНР о сотрудничестве в области обеспечения международной информационной безопасности» [Соглашение…, www], в котором четко обозначены конкретные угрозы МИБ и определены направления, принципы и механизмы сотрудничества в данной сфере. В будущем эффективное сотрудничество между двумя странами не только поможет разрушить информационную монополию западных держав, но и укажет путь для дальнейшего участия ШОС в управлении безопасностью глобального информационного пространства.

Заключение

На сегодняшний день мир переживает небывалые за последнее столетие серьезные перемены, на первый план выходят нетрадиционные угрозы безопасности. Несмотря на то, что меняющиеся информационные технологии дали толчок бурному развитию общества, они также породили кибертерроризм и информационную войну. Являясь важным субъектом управления безопасностью, ШОС постоянно работает над поддержанием информационной безопасности на глобальном и региональном уровнях. В будущем участницы организации будут и дальше укреплять чувство солидарности, ускорять реализацию инициатив по сотрудничеству в области информационной безопасности и совершенствовать механизмы взаимодействия, поддерживая при этом дружественные отношения с ООН и активно участвуя в управлении МИБ. Сотрудничество государств-членов ШОС в этой сфере не только внесет еще больший вклад в продвижение международной и региональной информационной безопасности, но и станет полезным поиском для формирования нового типа международных отношений и построения сообщества единой судьбы человечества.

Библиография

1. В Китае проходит 1-е совместное штабное учение компетентных органов государств-членов ШОС «Сямынь-2015». URL: https://knews.kg/2015/10/14/v-kitae-prohodit-1-e-sovmestnoe-shtabnoe-uchenie-kompetentnyih-organov-gosudarstv-chlenov-shos-syamyin-2015
2. Гайнетдинова А.К., Сизых Е.Ю. Перспективы развития сотрудничества в сфере противодействия кибертерроризму в рамках ШОС // Global and Regional Research. 2019. Т. 1. № 1. С. 171-175.
3. Декларация глав государств-членов Шанхайской организации сотрудничества. URL: http://www.kremlin.ru/supplement/3666
4. Демидов О.В. Обеспечение международной информационной безопасности и российские национальные интересы // Индекс безопасности. 2013. Т. 19. № 1 (104). С. 129-168.
5. Додонов В.Н., Карабанова Е.Н. Законодательство государств-членов ШОС, направленное на противодействие преступлениям и иным нарушениям, совершаемым в сфере или с использованием информационно-коммуникационных технологий (информационно-аналитический обзор) // Вестник Университета прокуратуры Российской Федерации. 2019. № 6 (74). С. 113-124.
6. Документы, принятые по итогам заседания Совета глав государств – членов Шанхайской организации сотрудничества. URL: http://www.kremlin.ru/supplement/5574
7. Душанбинская декларация двадцатилетия ШОС. URL: http://www.kremlin.ru/supplement/5699
8. Заявление глав государств-членов ШОС по международной информационной безопасности. URL: http://rus.sectsco.org/load/44842/
9. Международная информационная безопасность: подходы России. URL: https://mgimo.ru/upload/iblock/047/01fgupojoj7ka0tw75bw19li4bmurfse/Доклад%20русский.pdf
10. Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря. URL: https://www.mid.ru/ru/foreign_policy/un/organs/1582262/
11. Полякова Т.А. Базовые принципы правового обеспечения информационной безопасности // Труды Института государства и права РАН. 2016. № 3. С. 17-40.
12. Правила поведения в области обеспечения международной информационной безопасности: письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при ООН от 12 сентября 2011 г. на имя Генерального секретаря. A/66/359. URL: http://rus.rusemb.org.uk/data/doc/internationalcoderus.pdf
13. Ромащкина Н.П. Международная деятельность по обеспечению информационной безопасности в XXI веке // Информационные войны. 2015. № 2(34). С. 75-88.
14. Си Цзиньпин призывает к построению сообщества единой судьбы ШОС. URL: http://russian.news.cn/2018-06/10/c_137244095.htm
15. Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности. URL: http://rus.sectsco.org/documents/20090616/203974.html
16. Соглашение между Правительством РФ и Правительством КНР о сотрудничестве в области обеспечения международной информационной безопасности. URL: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/43921

17. Состоялась первая встреча руководителей ведомств государств-членов ШОС, ответственных за развитие ИКТ. URL: http://rus.sectsco.org/news/20211126/802096.html

18. 白联磊. 印度参与上合组织网络合作的特点和前景 // 中国信息安全. 2021. № 8. С. 89-91.

19. 邓浩. 上海合作组织安全合作的进程、动力与前景 // 当代世界. 2021. № 9. С. 20-25.

20. 邓浩, 李天毅. 上合组织信息安全合作：进展、挑战与未来路径 // 中国信息安全. 2021. № 8. С. 73-76.

21. 蒋也好, 刘雪迪. 上海合作组织与网络恐怖主义区域治理 // 区域与全球发展. 2021. № 2. С. 20-33.

Achievements and challenges of cooperation in the field of information security within the SCO framework

Lu Xuantong

Master's Student,
University of Chinese Academy of Social Sciences,
102488, 11, Changyu str., Beijing, People's Republic of China;
e-mail: luxuantong919@163.com

Abstract

As the Shanghai Cooperation Organisation (SCO) has evolved, the focus of its security cooperation has shifted from traditional cooperation in border areas to countering non-traditional security threats, and cooperation in the field of information security has become one of the priority areas. With the more serious situation in cyberspace since 2005, information security cooperation within the SCO framework has moved from consensus to action and has achieved positive results, including the signing of several official documents, improving institution building, conducting exercises against cyberterrorism and participating in international information security governance within the UN. At the same time, however, issues such as cyber sovereignty, the digital divide, and the interference by external forces also pose challenges to developing information security cooperation within the SCO framework. In the future, the wisdom and courage of the SCO members will be tested on how to solve the above-mentioned problems and deepen cooperation in this field. Today, the world is undergoing major changes unprecedented over the past century, with non-traditional security threats coming to the fore. Although changing information technologies have given impetus to the rapid development of society, they have also given rise to cyberterrorism and information warfare. Being an important subject of security management, the SCO is constantly working to maintain information security at the global and regional levels. In the future, the members of the organization will further strengthen the sense of solidarity, accelerate the implementation of initiatives for cooperation in the field of information security and improve the mechanisms of interaction.

For citation

Lu Xuantong（2023）Dostizheniya i problemy sotrudnichestva v oblasti informatsionnoi bezopasnosti v ramkakh SHOS [Achievements and challenges of cooperation in the field of information security within the SCO framework]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 12 (1A), pp. 169-178. 10.34670/AR.2023.87.56.019

Keywords

Shanghai Cooperation Organisation (SCO), cooperation within the SCO framework, information technology, information security, economics.

References

1. *Deklaratsiya glav gosudarstv – chlenov Skhankhaiskoi organizatsii sotrudnichestva* [Declaration of the Heads of the Member States of the Skhangkhai Cooperation Organization]. Available at: http://www.kremlin.ru/supplement/3666 [Accessed 08/01/23].
2. Demidov O.V. (2013) Obespechenie mezhdunarodnoi informatsionnoi bezopasnosti i rossiiskie natsional'nye interesy [Ensuring international information security and Russian national interests]. *Indeks bezopasnosti* [Security Index], 1 (104), pp. 129-168.
3. Dodonov V.N., Karabanova E.N. (2019) Zakonodatel'stvo gosudarstv-chlenov SHOS, napravlennoe na protivodeistvie prestupleniyam i inym narusheniyam, soverskhaemym v sfere ili s ispol'zovaniem informatsionno-kommunikatsionnyh tekhnologii (informacionno-analiticheskii obzor) [Legislation of SCO Member States to counter crimes and other offences committed in or involving the use of information and communication technologies (information and analytical review)]. *Vestnik Universiteta prokuratury Rossiiskoi Federatsii* [Bulletin of the University of the Public Prosecutor's Office of the Russian Federation], 6 (74), pp. 113-124.
4. *Dokumenty, prinyatye po itogam zasedaniya Soveta glav gosudarstv – chlenov Shankhaiskoi organizatsii sotrudnichestva* [Documents adopted following the meeting of the Council of Heads of State of the Skhangkhai Cooperation Organisation]. Available at: http://www.kremlin.ru/supplement/5574 [Accessed 08/01/23].
5. *Duskhanbinskaya deklaratsiya dvadtsatiletiya SHOS* [Duskhanbe Declaration on the 20th Anniversary of the SCO]. Available at: http://www.kremlin.ru/supplement/5699 [Accessed 08/01/23].
6. Gainetdinova A.K., Sizyh E.YU. (2019) Perspektivy razvitiya sotrudnichestva v sfere protivodeistviya kiberterrorizmu v ramkah SHOS [Prospects for cooperation in countering cyberterrorism within the SCO framework]. *Global and Regional Research*, 1, pp. 171-175.
7. *Mezhdunarodnaya informatsionnaya bezopasnost': podkhody Rossii* [International Information Security: Russia's Approaches]. Available at: https://mgimo.ru/upload/iblock/047/01fgupoioi7ka0tw75bw19li4bmurfse/Доклад%20русский.pdf [Accessed 08/01/23].
8. *Pis'mo postoyannykh predstavitelei Kazakhstana, Kitaya, Kyrgyzstana, Rossiiskoi Federatsii, Tadzhikistana i Uzbekistana pri Organizatsii Ob"edinennykh Natsii ot 9 yanvarya 2015 goda na imya General'nogo sekretarya* [Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Taiikistan and Uzbekistan to the United Nations addressed to the Secretary-General]. Available at: https://www.mid.ru/ru/foreign_policy/un/organs/1582262/ [Accessed 08/01/23].
9. Polyakova T.A. (2016) Bazovye printsipy pravovogo obespecheniya informatsionnoi bezopasnosti [Basic principles of legal provision for information security]. *Trudy Instituta gosudarstva i prava RAN* [Proceedings of the Institute of State and Law of the RAS], 3, pp. 17-40.
10. *Pravila povedeniya v oblasti obespecheniya mezhdunarodnoi informatsionnoi bezopasnosti: pis'mo postoyannykh predstavitelei Kitaya, Rossiiskoi Federatsii, Tadzhikistana i Uzbekistana pri OON ot 12 sentyabrya 2011 g. na imya General'nogo sekretarya. A/66/359* [The Code of Conduct in the Field of Ensuring International Information Security: Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Taiikistan and Uzbekistan to the United Nations addressed to the Secretary-General. A/66/359.]. Available at: http://rus.rusemb.org.uk/data/doc/internationalcoderus.pdf [Accessed 08/01/23].
11. Romashchkina N.P. (2015) Mezhdunarodnaya deyatel'nost' po obespecheniyu informatsionnoi bezopasnosti v XXI veke [International action for information security in the twenty-first century]. *Informatsionnye voiny* [Information wars], 2(34), pp. 75-88.
12. *Si Tsizn'pin prizyvaet k postroeniyu soobshchestva edinoi sud'by SHOS* [Xi Jinping calls for building a SCO community with a skhared future]. Available at: http://russian.news.cn/2018-06/10/c_137244095.htm [Accessed 08/01/23].
13. *Soglashenie mezhdu pravitel'stvami gosudarstv-chlenov SHOS o sotrudnichestve v oblasti obespecheniya mezhdunarodnoi informatsionnoi bezopasnosti* [Agreement among the Governments of the SCO Member States on Cooperation in Ensuring International Information Security]. Available at: http://rus.sectsco.org/documents/20090616/203974.html [Accessed 08/01/23].
14. *Soglashenie mezhdu Pravitel'stvom RF i Pravitel'stvom KNR o sotrudnichestve v oblasti obespecheniya mezhdunarodnoi informatsionnoi bezopasnosti* [Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in the field of ensuring international information security]. Available at: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/43921/ [Accessed 08/01/23].

15. *Sostoyalas' pervaya vstreckha rukovoditelei vedomstv gosudarstv-chlenov SHOS, otvetstvennykh za razvitie IKT* [The first meeting of the heads of the departments of the SCO member states responsible for the development of ICT takes place]. Available at: http://rus.sectsco.org/news/20211126/802096.html [Accessed 08/01/23].
16. *V Kitae prokhodit 1-e sovmestnoe shtabnoe uchenie kompetentnykh organov gosudarstv-chlenov SHOS «Syamyn'-2015»* [China hosts the 1st joint staff exercise of the competent authorities of the SCO member states «Xiamen-2015»]. Available at: https://knews.kg/2015/10/14/v-kitae-prohodit-1-e-sovmestnoe-shtabnoe-uchenie-kompetentnyih-organov-gosudarstv-chlenov-shos-syamyin-2015/ [Accessed 08/01/23].
17. *Zayavlenie glav gosudarstv-chlenov SHOS po mezhdunarodnoi informatsionnoi bezopasnosti* [Statement by the Heads of the SCO Member States on International Information Security]. Available at: http://rus.sectsco.org/load/44842/ [Accessed 08/01/23].
18. 白联磊. (2021) 印度参与上合组织网络合作的特点和前景. *中国信息安全*, 8, pp. 89-91.
19. 邓浩. (2021) 上海合作组织安全合作的进程、动力与前景. *当代世界*, 9, pp. 20-25.
20. 邓浩, 李天毅. (2021) 上合组织信息安全合作：进展、挑战与未来路径. *中国信息安全*, 8, pp. 73-76.
21. 蒋也好, 刘雪迪. (2021) 上海合作组织与网络恐怖主义区域治理. *区域与全球发展*, 2, pp. 20-33.