DOI 10.35775/PSI.2025.70.5.019
УДК 32.327

И.В. СУРМА
кандидат экономических наук,
начальник отдела НАМИБ, доцент кафедры
международной и национальной безопасности
Дипломатической академии МИД РФ,
профессор Академии Военных Наук,
Россия, г. Москва

ВЗАИМОДЕЙСТВИЕ ГОСУДАРСТВ-ЧЛЕНОВ ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА В ОБЛАСТИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье рассматривается роль и значение действующих и потенциальных механизмов и инструментов взаимодействия государств-членов Шанхайской организации сотрудничества (ШОС) по вопросам обеспечения международной информационной безопасности. Исходя из основных целей ШОС, включая совместное противодействие новым вызовам и угрозам и поощрение эффективного и взаимовыгодного сотрудничества в различных областях, показаны ключевые задачи, стоящие перед государствами-членами ШОС в сфере обеспечения международной информационной безопасности такие как, защита критической информационной инфраструктуры, информационное взаимодействие в области предотвращения и реагирования на инциденты в киберпространстве и борьба с киберпреступностью, а также подготовка специалистов в области международной информационной безопасности. Автор отмечает, что несмотря на успехи государств-членов ШОС в укреплении сотрудничества в сфере международной информационной безопасности еще остаются серьезные вызовы, связанные с различиями во взглядах на приоритетность тех или иных аспектов международной информационной безопасности, с ограниченностью финансовых и технических возможностей некоторых государств-членов ШОС и влиянием геополитических факторов.

Ключевые слова: *ШОС, международная информационная безопасность, Университет ШОС, киберпреступность, Хартия ШОС, ИКТ, РАТС ШОС.*

В основу деятельности ШОС согласно Хартии [23] положены принципы взаимного уважения суверенитета, независимости, территориальной целостности государств и нерушимости государственных границ, ненападения, невмешательства во внутренние дела, неприменения силы или угрозы силой в международных отношениях, отказа от одностороннего военного превосходства в сопредельных районах, что вошло в международный политический лексикон под названием «шанхайского духа». Этот «дух» как раз и определил тот факт, что сегодня Шанхайская организация сотрудничества (ШОС) является

одним из основных участников формирования международного диалога в области информационной безопасности. Играя важную роль в создании условий для взаимодействия государств-членов в сфере международной информационной безопасности (МИБ), ШОС предоставляет платформу для обсуждения актуальных вопросов, выработки совместных решений и координации действий по противодействию глобальным вызовам и угрозам, обусловленным стремительным развитием информационно-коммуникационных технологий.

Исходя из основных целей ШОС, определенных в базовом уставном документе [23], таких как укрепление взаимного доверия, дружбы и добрососедства; упрочение разностороннего взаимодействия в деле поддержания и укрепления мира, безопасности и стабильности в регионе; совместное противодействие новым вызовам и угрозам; поощрение эффективного и взаимовыгодного сотрудничества в различных областях и содействие экономическому росту, социальному и культурному развитию, перед государствами-членами ШОС в сфере обеспечения международной информационной безопасности стоят следующие задачи:

1. Защита критической информационной инфраструктуры. Государства-члены ШОС заинтересованы в создании механизмов защиты объектов жизненно важной национальной информационной инфраструктуры от компьютерных атак.

2. Борьба с киберпреступностью. Государства-члены ШОС заинтересованы в разработке международных стандартов и правовых норм для противодействия преступной деятельности в информационной сфере и всячески способствуют этому.

3. Информационное взаимодействие. Государства-члены ШОС заинтересованы в комплексном обмене информацией и опытом в области предотвращения и реагирования на инциденты в киберпространстве.

4. Обучение и подготовка кадров. Сегодня важную роль играют программы подготовки специалистов в области МИБ, проводимые государствами-членами ШОС.

5. Создание доверительной информационной среды. Государства-члены ШОС стремятся сформировать взаимное доверие через диалог и координацию усилий в вопросах обеспечения МИБ.

При этом основными механизмами и потенциальными инструментами, используемыми для достижения целей в сфере международной информационной безопасности, являются:

1. **Совместные декларации и заявления.** Государства-члены ШОС регулярно принимают совместные документы, направленные на укрепление сотрудничества, в том числе в области международной информационной безопасности. Так, в Екатеринбурге в 2009 году были подписаны Екатеринбургская декларация глав государств-членов Шанхайской организации сотрудничества и Соглашение о сотрудничестве в области обеспечения международной

информационной безопасности [5]. В Пекине в 2012 году принята Декларация о построении в регионе долгосрочного мира и совместного процветания, в которой определено, что страны ШОС будут активно участвовать в построении мирного, безопасного, справедливого и открытого информационного пространства, основываясь на принципах уважения государственного суверенитета и невмешательства во внутренние дела других государств [6]. В 2015 году в Уфе была подписана Уфимская декларация глав государств-членов Шанхайской организации сотрудничества и утверждена Стратегия развития ШОС до 2025 года, в которой были определены приоритетные направления деятельности по всем основным направлениям сотрудничества, включая вопросы МИБ на базе разработанного ШОС проекта «Правила поведения государств в области обеспечения международной информационной безопасности» [2].

Следует отметить важность Астанинской декларации (2017) [7], которая определила в рамках ШОС форматы совместного сотрудничества, а главы государств выступили за подготовку в рамках ООН универсального кодекса правил, принципов и норм ответственного поведения государств в информационном пространстве. Этому предшествовало распространение в качестве официального документа ООН новой редакции Правил поведения в области обеспечения международной информационной безопасности еще в январе 2015 г. от государств-членов ШОС.

В 2018 году в Циндао была подписана декларация ШОС [24], в которой лидеры государств-членов призвали разработать под эгидой ООН документ по борьбе с использованием информационных технологий в преступных целях. Еще одним важным документом явилась Концепция сотрудничества государств-членов ШОС в сфере цифровизации и ИКТ (Бишкек, 2019 год) [16], определяющая принципы взаимодействия государств-членов в этой области.

Важной вехой явился План по реализации Стратегии развития ШОС до 2025 года, утвержденный в Москве в 2020 году, где также было принято Заявление Совета глав государств-членов ШОС о всеобъемлющей реализации Соглашения между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. [9]. В 2021 году подписана Душанбинская декларация ШОС, отражающая основные итоги двадцатилетней деятельности Организации, и принят разработанный по инициативе Узбекистана и России План взаимодействия государств-членов ШОС по вопросам обеспечения международной информационной безопасности на 2022-2023 годы [17]. В План взаимодействия включено три основных направления. Во-первых, совершенствование нормативно-правовой базы в сфере международной информационной безопасности, куда входили, в частности определение компетентных органов государств-членов ШОС по разработке терминологии в сфере обеспечения МИБ и изучение национального законодательства государств-членов ШОС в области МИБ для выработки терминологии и определений в данной сфере. Во-вторых, обеспечение организационно-информационного

взаимодействия и, в-третьих, повышение квалификации кадров в области информационной безопасности.

По итогам саммита ШОС, прошедшего в Самарканде 16 сентября 2022 г., было принято 44 документа, среди которых Программа сотрудничества между уполномоченными органами государств-членов по развитию цифровой грамотности [13] и Программа сотрудничества между уполномоченными органами государств-членов по развитию искусственного интеллекта [14], в которых определены основные направления, формы и принципы сотрудничества, а также механизмы их реализации.

В развитие этих документов 1 ноября 2022 г. Совет глав правительств государств-членов ШОС утвердил Программу сотрудничества государств-членов Шанхайской организации сотрудничества по развитию цифровой экономики [18].

В следующем, 2023 году на саммите Совета глав государств в Нью-Дели было принято Заявление по сотрудничеству в области цифровой трансформации, в котором лидеры государств-членов поддержали интеграцию цифровых решений в финансовой сфере и широкое распространение цифровых услуг с целью обеспечения их доступности для населения государств-членов ШОС с учетом требований информационной безопасности [3].

Важным документом в сфере МИБ явилась подписанная в 2024 году в Казахстане Астанинская декларация, определяющая основные направления развития Организации и сотрудничества между ее членами [1], где отмечена ключевая роль ООН в противодействии угрозам в информационной сфере и создании безопасного информационного пространства, построенного на принципах уважения государственного суверенитета и невмешательства во внутренние дела других стран. Государства-члены призвали международное сообщество добиваться консенсуса по вопросу принятия в рамках ООН всеобъемлющей Конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Было отмечено, что важным вкладом в эти усилия будет документ ШОС о сотрудничестве в борьбе с преступлениями в сфере информационных технологий. Подчеркнуто, что серьезным шагом в этом направлении должно стать обеспечение равных для всех стран прав на регулирование сети Интернет в своем национальном сегменте.

2. **Совещания, рабочие группы и экспертные советы.** Для эффективного взаимодействия, в том числе на экспертном уровне в области МИБ, используются различные форматы: совещания секретарей советов безопасности, совещания министров внутренних дел и общественной безопасности, совещания генеральных прокуроров, совещания министров по ИКТ и др. Кроме того, создаются специализированные рабочие группы, основные функции которых состоят в исследовании новых угроз в информационной сфере и выработке мер противодействия им и разработке международных стандартов и рекомендаций для государств-членов ШОС.

Примерами таких рабочих групп являются: рабочая группа Региональной антитеррористической структуры (РАТС) ШОС для борьбы с терроризмом в Интернете, рабочая группа экспертов компетентных органов государств-членов ШОС по борьбе с киберпреступлениями, специальная рабочая группа государств-членов ШОС по современным ИКТ и т.п.

Практическое сотрудничество государств-членов ШОС в области обеспечения международной информационной безопасности началось еще в 2006 году. Тогда по решению министров государств-членов ШОС, отвечающих за внешнеторговую и внешнеэкономическую деятельность, была создана Специальная рабочая группа по современным ИКТ. В тот же период главы государств приняли решение о создании группы экспертов государств-членов ШОС по МИБ с участием представителей Секретариата Организации и Исполкома РАТС для выработки плана действий по обеспечению международной информационной безопасности и определению возможных путей и средств решения в рамках ШОС проблемы МИБ во всех ее аспектах [4].

18-19 апреля 2024 г. в Москве под председательством российской стороны в гибридном формате состоялось очередное заседание Группы экспертов государств-членов ШОС по международной информационной безопасности, где особое внимание было уделено вопросам активизации многостороннего взаимодействия в сфере обеспечения информационной безопасности, включая взаимодействие на профильных многосторонних площадках, прежде всего в рамках ООН, для создания безопасного, справедливого и открытого информационного пространства. Также обсуждались реализация и продление сроков Плана взаимодействия государств-членов ШОС по вопросам МИБ на 2022-2023 годы и были озвучены предложения по противодействию использованию информационно-коммуникационных технологий в преступных целях, по налаживанию диалога в финансовой сфере по линии центральных (национальных) банков государств-членов ШОС [12].

3. **Образовательные программы и тренинги.** Одной из важных составляющих международного сотрудничества ШОС является регулярное проведение учебных мероприятий и тренингов для специалистов в области информационной безопасности. Такие мероприятия способствуют повышению квалификации кадров и внедрению современных методик защиты информационных систем. Образовательные программы включают курсы по защите информационных систем государственных органов, по корпоративной безопасности и управлению рисками информационной безопасности.

Кроме того, для ШОС стоит задача повышения общего уровня информационной безопасности и удовлетворения растущего кадрового дефицита в этой сфере. На саммите в Бишкеке 16 августа 2007 г. Президентом Российской Федерации В.В. Путиным была выдвинута идея создания Университета ШОС [21; 22], одобренная государствами-членами. Соглашение об учреждении и функционировании Университета ШОС подписали Казахстан, Китай, Россия, Киргизия, Таджикистан. Соглашение открыто для присоединения для всех государств-членов ШОС.

В настоящее время в Университете ШОС (1) осуществляется подготовка высококвалифицированных специалистов по наиболее приоритетным областям знаний (в том числе по ИТ-технологии, нанотехнологии), на регулярной основе организуются международные семинары, конференции и курсы повышения квалификации для специалистов в области кибербезопасности. Также осуществляется поддержка правоохранительных органов стран-участниц в целях повышения уровня профессионализма сотрудников правоохранительных структур, занимающихся расследованием киберпреступлений, через проведение тренингов и образовательных курсов и поддерживаются исследования и разработки новых методов анализа цифровых следов и выявления источников компьютерных атак.

Как было отмечено в 2024 году в Астанинской декларации [1], государства-члены ШОС подчеркивают важность дальнейшего углубления сотрудничества в области образования, расширения межвузовского сотрудничества и изучения передового опыта в сфере цифрового образования, включая внедрение инновационных образовательных технологий.

4. **Технические меры и регламенты.** В рамках деятельности ШОС разрабатываются стандарты и технические регламенты, обеспечивающие защиту информационных систем и сетей от внешних угроз. Государства-члены ШОС совместно создают системы раннего предупреждения и мониторинга киберугроз, что позволяет быстро реагировать на потенциальные атаки в информационной среде. Также активно внедряются технологии шифрования и аутентификации для защиты данных и сетей от несанкционированного доступа. Особое внимание уделяется развитию технологий для защиты критически важной информационной инфраструктуры в таких отраслях, как энергетика, транспорт, финансы и банковская сфера, и др. Страны ШОС осуществляют противодействие распространению вредоносного программного обеспечения (ПО). Для этого организации и эксперты государств-членов ШОС сотрудничают в области разработки программного обеспечения и инструментов для обнаружения и удаления вирусов, троянов и другого вредоносного ПО, осуществляется мониторинг активности хакеров и их группировок, чтобы своевременно реагировать на угрозы в информационной сфере. Отметим, что согласованные технические меры, в частности использование одинаковых или совместимых технологических решений для защиты информации, делают взаимодействие между странами ШОС более предсказуемым и надежным. Кроме того, создание специализированных каналов связи и баз данных позволяет оперативно обмениваться информацией о киберинцидентах и новых угрозах, способах их предотвращения и расследованиях. Это помогает снизить уровень недоверия, так как страны видят, что партнеры готовы делиться важными сведениями.

5. Разработка международных стандартов и правовых норм. Государства-члены ШОС работают над гармонизацией национальных законодательств в области МИБ, стремясь создать единую нормативно-правовую базу и единое правовое пространство. Важным шагом в этом направлении стало Соглашение

между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности [19], в котором были определены основные направления сотрудничества, начиная от создания системы мониторинга и совместного реагирования на возникающие в этой области угрозы, выработки совместных мер по развитию норм международного права в области ограничения распространения и применения информационного оружия, создающего угрозы обороноспособности, обеспечения национальной и общественной безопасности, противодействия угрозам использования информационно-коммуникационных технологий в террористических целях и до противодействия информационной преступности в целом.

Разработка и внедрение общих стандартов и правил в области информационной безопасности, безусловно, должны способствовать созданию гармонизированной правовой среды, что уменьшит вероятность разногласий и конфликтов. Для формирования такой среды необходимо прежде всего создание списка согласованных терминов, связанных с киберпреступлениями, а также проведение унификации правовых процедур для расследования киберпреступлений и преследования киберпреступников. Так, в Приложении № 1 к Соглашению между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности представлен Перечень основных понятий в области обеспечения международной информационной безопасности [19].

Одним из важнейших механизмов в сфере международной информационной безопасности является работа по унификации законодательства в области кибербезопасности. Для этого необходимо определить основные виды угроз, их источники и признаки, поэтому в Приложении 2 к рассматриваемому Соглашению представлен Перечень основных видов угроз в области международной информационной безопасности, их источников и признаков [19].

Государства-члены ШОС пытаются гармонизировать национальные законы таким образом, чтобы они позволяли эффективно бороться с трансграничными киберпреступлениями. При этом, как подчеркивается в Астанинской декларации [1], безопасность киберпространства должна строиться на принципах уважения государственного суверенитета.

Таким образом, совместные правовые акты помогают государствам-членам ШОС координировать свои действия и обмениваться информацией в борьбе с киберпреступностью.

6. Регулярный обмен информацией и опытом, координация антитеррористической деятельности и создание объединенных центров реагирования государств-членов ШОС. Организация поддерживает активное взаимодействие между правоохранительными органами и спецслужбами государств-членов ШОС для оперативного обмена информацией о выявленных угрозах и методах их нейтрализации. Также проводятся регулярные совещания экспертов, которые позволяют делиться передовыми практиками и новейшими технологиями, применяемыми для борьбы с противоправным использованием ИКТ. Созданы

специальные платформы и базы данных, позволяющие странам ШОС оперативно получать данные о новых угрозах, тактике преступников и успешных мерах противодействия. При этом важную роль играют аналитические центры, которые ведут мониторинг киберпространства и предупреждают о потенциальных рисках в сети Интернет.

В рамках ШОС был инициирован процесс создания национальных и межгосударственных центров реагирования на компьютерные инциденты (CERT), где специалисты разных стран будут взаимодействовать в режиме реального времени для отслеживания и ликвидации последствий кибератак, а 13 сентября 2023 г. в Алматы (Казахстан) состоялись межведомственные консультации государств-членов ШОС по вопросу создания Центра по информационной безопасности на базе Региональной антитеррористической структуры Шанхайской организации сотрудничества в Ташкенте (Узбекистан) [8]. Выступая на саммите ШОС в Астане в июле 2024 г. Президент Российской Федерации В.В. Путин заявил, что поддержание безопасности участников ШОС остается приоритетной задачей [15] и на базе антитеррористической структуры ШОС создается Универсальный центр реагирования на угрозы в сфере безопасности с отделением в Бишкеке – Центром по противодействию международной организованной преступности. Кроме того, в Душанбе будет создан антинаркотический центр.

Поскольку киберпреступники часто связаны с террористическими организациями, ШОС усиливает интеграцию между антитеррористическими структурами и подразделениями, и службами обеспечения информационной безопасности. Также проводятся учения и совместные кибероперации по выявлению и пресечению деятельности террористических группировок, использующих цифровые каналы для планирования и осуществления терактов. Периодическое проведение киберучений и моделирование реальных ситуаций [20] позволяет членам ШОС тестировать готовность своих информационных систем к актуальным и потенциальным угрозам и улучшать взаимодействие между уполномоченными ведомствами. Кроме того, такие мероприятия демонстрируют надежность партнеров и способность действовать сообща. В результате участники получают возможность оценить эффективность совместных планов действий и выявить слабые места в своей защите. Таким образом, ШОС применяет комплексный подход к борьбе с киберпреступностью, сочетая законодательные, научно-технические и образовательные меры. Эта многоуровневая стратегия направлена на обеспечение безопасного цифрового пространства для всех государств-членов Организации.

6. Межведомственное сотрудничество государств-членов ШОС и сотрудничество с международными структурами. Организация активно сотрудничает с ООН, Интерполом и другими международными структурами, занимающимися вопросами обеспечения информационной безопасности. Обмен опытом и информацией с этими структурами позволяет усилить общую эффективность борьбы с киберпреступностью.

7. Интеграция сил правопорядка и спецслужб. Сотрудничество между правоохранительными органами и спецслужбами государств-членов ШОС на постоянной основе помогает укрепить доверие, поскольку участники понимают, что их партнеры готовы оказывать поддержку в сложных ситуациях. Делегация Исполнительного комитета Региональной антитеррористической структуры ШОС приняла 3 апреля 2025 г. участие в прошедших в Москве консультациях государств-членов ШОС [11]. В рамках обсуждения вопроса «Углубление внешнеполитической координации в целях дальнейшего укрепления международных позиций ШОС обеспечение стабильности и безопасности в регионе» было подчеркнуто, что терроризм, сепаратизм и экстремизм по-прежнему сохраняют актуальность, как серьезные угрозы и вызовы для мирового сообщества и региона ШОС. В этих условиях Исполкомом РАТС на постоянной основе проводится работа по усилению взаимодействия компетентных органов стран ШОС по противодействию «силам трех зол». На заседании Совета глав государств ШОС была представлена одобренная Советом РАТС отдельная Программа сотрудничества стран ШОС в противодействии экстремистской идеологии на пространстве Шанхайской организации сотрудничества на 2026-2030 годы.

8. Общественная дипломатия и культурные обмены. Повышение осведомленности населения государств-членов ШОС и участие гражданского общества в повышении культуры информационной безопасности. Помимо официальных контактов, важны и общественные инициативы, такие как научные конференции, культурные обмены и молодежные программы. Они способствуют установлению личных связей и укреплению дружеских отношений между гражданами государств-членов ШОС. Также важным направлением является просветительская деятельность среди граждан государств-членов ШОС. Разрабатываются программы обучения и информирования, направленные на повышение киберграмотности населения, что помогает предотвратить массовое мошенничество и фишинговые атаки.

9. Научно-исследовательские программы и осуществление мониторинга, оценка эффективности мер в области МИБ. Исследования в области кибербезопасности становятся важным направлением международного сотрудничества ШОС. Научные коллективы из разных стран объединяют усилия для изучения перспективных технологий защиты данных, предотвращения утечек информации и повышения устойчивости критических информационных систем к внешним воздействиям [25]. Причем результаты этих исследований находят применение как в государственном секторе, так и в частных компаниях стран-членов ШОС. В этой связи интересен опыт Национального центра исследований ШОС (НЦИ ШОС) [10], который был создан в 2024 году на базе Института Китая и современной Азии РАН (ИКСА РАН) при поддержке МГИМО МИД России. После согласования с МИД России Центр стал членом экспертного Форума ШОС. Сегодня Центр публикует аналитические исследования по отдельным темам и отраслям, обзоры регулярных и предстоящих мероприятий, экспертные

заключения по отдельным вопросам, включая результаты анализа угроз и тенденций в области международной информационной безопасности.

Эффективность принимаемых государствами-членами ШОС мер постоянно оценивается с помощью независимых аудитов и отчетов. Анализ полученных результатов позволяет вносить коррективы и оперативно адаптироваться к новым условиям и динамичному развитию технологий.

Перечисленные инструменты и механизмы обеспечивают странам ШОС надежную основу для совместной работы в области международной информационной безопасности, позволяя минимизировать риски и защищать критически важные информационные ресурсы.

Используя эти механизмы, Шанхайская организация сотрудничества активно работает над укреплением доверия между государствами-членами в сфере международной информационной безопасности. Этот процесс имеет большое значение, поскольку доверие лежит в основе эффективного сотрудничества и координации действий в борьбе с киберугрозами. Укрепление доверия между странами в сфере МИБ требует комплексного подхода, который включает в себя как официальные, так и неофициальные формы взаимодействия. Сегодня Шанхайская организация сотрудничества активно развивает эти направления, создавая условия для конструктивного диалога, обмена знаниями и технологиями, а также для практической координации действий.

На сегодняшний день ШОС добилась значительных успехов в укреплении сотрудничества в сфере МИБ. Организация стала платформой для обмена передовым опытом и лучшими практиками в области международной информационной безопасности. Вместе с тем остаются серьезные вызовы, среди которых следует выделить наиболее важные, такие как:

1. Различия в подходах. Несмотря на общие интересы, государства-члены ШОС имеют разные взгляды на приоритетность тех или иных аспектов международной информационной безопасности.

2. Недостаток ресурсов. Ограниченность финансовых и технических возможностей некоторых государств-членов ШОС, обусловленная низким уровнем развития финансово-экономической и научно-технологической сфер, существенно снижает потенциал этих стран по реализации проектов в области МИБ.

3. Роль международного контекста. Влияние геополитических факторов и противоречий между ведущими державами, трансформация системы международных отношений затрудняет достижение консенсуса по ряду вопросов в области МИБ.

В заключение отметим, что Шанхайская организация сотрудничества играет одну из важных ролей в формировании современной архитектуры сотрудничества в сфере международной информационной безопасности. Благодаря своим усилиям она способствует укреплению доверия и взаимопонимания между странами-членами, создает условия для разработки и внедрения эффективных мер по защите информационного пространства. Важно продолжать работу

по устранению существующих вызовов и расширению сотрудничества в целях обеспечения устойчивого развития и безопасности в международном информационном пространстве.

ПРИМЕЧАНИЯ:

(1) В Университет ШОС входит 77 вузов:14 – из Казахстана, 24 – из Китая, 8 – из Киргизии, 20 – из России и 11 – из Таджикистана, а также один вуз из Белоруссии.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Астанинская декларация Совета глав государств-членов Шанхайской организации сотрудничества // ШОС. 4 июля 2024 г. // https://rus.sectsco.org/20240704/1420683.html.
2. Заседание Совета глав государств-членов ШОС // Уфа, Россия, 10.07.2015 // http://www.kremlin.ru/events/president/news/49907.
3. Заявление Совета глав государств-членов Шанхайской организации сотрудничества по сотрудничеству в области цифровой трансформации // 4 июля 2023 г., Нью-Дели // https://rus.sectsco.org/20230704/1597907.html.
4. Заявление глав государств-членов ШОС по международной информационной безопасности // 15 июня 2006 г., Шанхай // http://www.infoshos.ru/ru/?id=94.
5. Екатеринбургская декларация глав государств-членов Шанхайской организации сотрудничества // Екатеринбург, 16.06.2009 // http://www.kremlin.ru/supplement/66.
6. Информационное сообщение по итогам заседания Совета глав государств-членов ШОС // Пекин, Китай, 6-7 июня 2012 г. // https://rus.sectsco.org/20120606/47370.html.
7. Информационное сообщение по итогам заседания Совета глав государств-членов Шанхайской организации сотрудничества // Астана, Казахстан, 09.06.2017 // https://rus.sectsco.org/20170609/289250.html?ysclid=m8si0r2hvj139633021.
8. Межведомственные консультации государств-членов ШОС по вопросу создания Центра по информационной безопасности // Шанхайская организация сотрудничества // https://rus.sectsco.org/20230913/Mezhvedomstvennye-konsultatsii-gosudarstv-chlenov-ShOS-po-voprosu-sozdaniya-Tsentra-po-informatsionnoy-955808.html.
9. Московская декларация Совета глав государств-членов Шанхайской организации сотрудничества // Москва, Россия, 10.11.2020 (онлайн-формат) // http://www.kremlin.ru/supplement/5575.
10. Национальный центр исследований ШОС // Официальный сайт НЦИ ШОС // https://www.iccaras.ru/nczi-shos/.

11. Об участии в консультациях государств-членов ШОС // РАТС. 4 апреля 2025 г. // https://ecrats.org/ru/press/news/16993/.
12. О заседании Группы экспертов государств-членов ШОС по международной информационной безопасности // Официальный сайт ШОС. 20 апреля 2024 г. // https://rus.sectsco.org/20240420/1330429.html.
13. Программа сотрудничества между уполномоченными органами государств-членов Шанхайской организации сотрудничества по развитию цифровой грамотности // Самарканд, Узбекистан, 16.09.2022 // https://rus.sectsco.org/20220916/1602199.html.
14. Программа сотрудничества между уполномоченными органами государств-членов Шанхайской организации сотрудничества по развитию искусственного интеллекта // Самарканд, Узбекистан, 16.09.2022 // https://rus.sectsco.org/20220916/1602237.html.
15. Путин: в ШОС будет создан центр реагирования на угрозы в сфере безопасности // Шанхайская организация сотрудничества // https://www.kommersant.ru/doc/6806871.
16. Решение Совета глав государств-членов Шанхайской организации сотрудничества об утверждении Концепции сотрудничества государств-членов Шанхайской организации сотрудничества в сфере цифровизации и информационно-коммуникационных технологий // Бишкек. 14.06.2019 // https://rus.sectsco.org/20190614/1602432.html?ysclid=mbjbfhgz2t214213432.
17. Решение Совета глав государств-членов Шанхайской организации сотрудничества об утверждении Плана взаимодействия государств-членов ШОС по вопросам обеспечения международной информационной безопасности на 2022-2023 годы // Душанбе, Таджикистан, 16-17 сентября 2021 г. // https://rus.sectsco.org/20210917/1602962.html.
18. Решение заседания Совета глав правительств (премьер-министров) государств-членов Шанхайской организации сотрудничества о Программе сотрудничества государств-членов Шанхайской организации сотрудничества по развитию цифровой экономики // 1 ноября 2022 года, Пекин // https://rus.sectsco.org/20221101/1600422.html.
19. Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности // Официальный сайт МИД России, 16 июня 2009 г. // https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/multilateral_contract/50243/.
20. Спецслужбы стран-членов ШОС провели в Нью-Дели учения по отражению кибератак террористов // ТАСС. 19.12.2023 // https://tass.ru/mezhdunarodnaya-panorama/19575463.
21. Университет ШОС // Официальный сайт ШОС. 20 апреля 2024 г. // https://rus.sectsco.org/20190716/565375.html.
22. Университет Шанхайской организации сотрудничества // Официальный сайт Университета ШОС // https://uni-sco.ru/.

23. Хартия Шанхайской организации сотрудничества (7 июня 2002 г., вступила в силу 19 сентября 2003 г.) // Шанхай, 07.06.2002 // https://rus.sectsco.org/20020607/1608561.html.
24. Циндаоская декларация Совета глав государств-членов Шанхайской организации сотрудничества // Циндао, 09.06.2018 // https://rus.sectsco.org/20180609/442929.html.
25. 35 экспертов из 18 исследовательских институтов обсудили расширение экономической кооперации и сферу безопасности на пространстве ШОС // 1 октября 2020 г. // https://xs.uz/ru/post/ekspertnyj-forum-shos-nametil-perspektivy-sotrudnichestva.

I.V. SURMA
Candidate of Economic Sciences,
Head of the Department of the National Association for International Information Security, Associate Professor of the Department of International and National Security of the Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation;
professor of the Academy of Military Sciences,
Moscow, Russia

INTERACTION OF MEMBER STATES OF THE SHANGHAI COOPERATION ORGANIZATION IN THE FIELD OF INTERNATIONAL INFORMATION SECURITY

The article considers the role and significance of existing and potential mechanisms and instruments of interaction of the Shanghai Cooperation Organization (SCO) member states on the issues of ensuring international information security. Based on the main objectives of the SCO, including joint counteraction to new challenges and threats and promotion of effective and mutually beneficial cooperation in various areas, the article shows the key tasks facing the SCO member states in the field of ensuring international information security, such as protection of critical information infrastructure, information interaction in the field of prevention and response to incidents in cyberspace and combating cybercrime, as well as training of specialists in the field of international information security.

The author notes that despite the success of the SCO member states in strengthening cooperation in the field of international information security, there are still serious challenges associated with differences in views on the prioritization of certain aspects of international information security, the limited financial and technical capabilities of some SCO member states and the influence of geopolitical factors.

Key words: *SCO, international information security, SCO University, cybercrime, SCO Charter, ICT, SCO RATS.*