

*Е. В. Данилова*

## **Правовые основы и практика обеспечения информационной безопасности в рамках ШОС**

**Аннотация.** Данная статья посвящена исследованию основных направлений деятельности государств — членов Шанхайской организации сотрудничества (ШОС), направленной на обеспечение информационной безопасности на национальном, региональном и глобальном уровне. Особое внимание уделено нормативной основе сотрудничества стран, которое представляется ключевым звеном для развития взаимодействия. Кроме того, анализируются практические шаги государств-членов, способствующие укреплению защиты информационного сектора. Делается акцент на проведении совместных киберучений, проведении конференций, расширении взаимодействия и обмене опытом между профильными структурами между государствами-членами, совершенствовании институциональной основы организации. Были сделаны выводы, что страны укрепляют сотрудничество в защите критической информационной инфраструктуры и противодействии киберугрозам, с особым упором на противодействии терроризму и экстремизму в сети Интернет. Организация оперативно адаптируется к изменениям в международной обстановке, развивает нормативную базу, совершенствует институциональную структуру и проводит совместные учения.

**Ключевые слова:** киберугрозы, киберпространство, международная информационная безопасность, Шанхайская организация сотрудничества, киберучения.

**Автор:** Данилова Евгения Вячеславовна, магистрант 1 курса, факультет международных отношений, Дипломатическая академия МИД России.  
ORCID: 0009-0005-0237-4668. E-mail: jane.dan02@mail.ru

*Evgeniia V. Danilova*

## **Legal framework and practices for ensuring information security within the SCO**

**Abstract.** This article is devoted to a study of the main activities of the member states of the Shanghai Cooperation Organization (SCO) aimed at ensuring information security at the national, regional and global levels. Particular attention is given to the normative framework of country cooperation, which appears to be a key link for promoting collaboration. The practical steps taken by Member States to strengthen the protection of the information sector are also analysed. Emphasis is placed on conducting joint cyber exercises, holding conferences, expanding interaction and exchange of experience between relevant structures among member states, improving the institutional framework of the organization. It was concluded that countries are strengthening cooperation in protecting critical information infrastructure and countering cyber threats, with special emphasis on countering terrorism and extremism on the Internet. The organization rapidly adapts to changes in the international environment, develops normative frameworks, improves institutional structures and conducts joint exercises.

**Keywords:** cyber threats, cyberspace, international information security, Shanghai Cooperation Organization, cyber-trainings.

**Author:** *Danilova Evgeniia V.*, 1st year master's student, faculty of international relations, the Diplomatic Academy of the Russian Foreign Ministry.  
ORCID: 0009-0005-0237-4668. E-mail: jane.dan02@mail.ru

Система международных отношений изменяется под влиянием различных факторов, ключевым из которых можно назвать экономические процессы и технологические революции. Обострение конкуренции государств и иных субъектов международных отношений за ресурсы и доминирование в цифровой сфере выступает значимым фактором дестабилизации глобальной системы. Кризис проявляется в нескольких взаимосвязанных вызовах: и геополитическая конкуренция за большие данные, что зачастую носит название колониализм данных, и становящееся более явным цифровое неравенство, и рост уровня безработицы, вызванный роботизацией, а также правовые и этические пробелы в регулировании этих процессов. Параллельно происходит становление и формирование многополярного мирового порядка, который в свою очередь сопровождается повышением уровня конфликтности на региональном и глобальном уровне, нарастанием конфронтации между государствами или же блоками стран.

На данном фоне увеличивается роль региональных организаций, которые объединяют и аккумулируют экономическую, политическую и в ряде случаев военную силу государств. Так, набирает вес Шанхайская организация сотрудничества, в которую в настоящее время входят Россия, Китай, Казахстан, Индия, Кыргызстан, Пакистан, Таджикистан, Узбекистан, Иран и Беларусь. Она основана на принципах «шанхайского духа»: взаимное доверие, взаимная выгода, равноправие, уважение к многообразию культур и стремление к совместному развитию. О росте авторитета на мировой арене свидетельствует увеличивающееся число стран-партнеров, в том числе из государств Персидского залива, что позволяет ШОС действовать за региональными рамками.

Шанхайская организация сотрудничества воспринимается в качестве объединения, одной из ключевых задач которого является обеспечение безопасности стран-членов. Если прежде угрозы носили более материальный характер, то сейчас фокус в том числе сместился на киберпространство. По данным РАТС ШОС, в 2024 г. более 60 % киберугроз в регионе имели целью использование интернет-пространства для распространения экстремистской идеологии и планирования террористической деятельности [В ШОС заявили о предотвращении].

## **Влияние информационных атак на государства — члены Шанхайской организации сотрудничества**

Каждый из десяти государств-членов региональной организации сталкивается с возрастающим количеством атак, наносящих вред критически важной инфраструктуре в области энергетики, финансов, обороны и ряде других. Более того, киберпространство может использоваться в качестве арены ведения инфор-

мационной войны. Так, по заявлению директора Департамента информации и печати Министерства иностранных дел Российской Федерации, Марии Захаровой, Коллективный запад ведет гибридную войну против России, одной из составляющей которой является дезинформация, распространение фейковой информации и атаки на российскую инфраструктуру с целью получения стратегических данных и нарушения функционирования государственных институтов [Сборов А.]. Кроме того, согласно результатам совместного исследования Экспертно-аналитического центра группы компаний InfoWatch и группы компаний ЦИРКОН, проведенного в 2024 г., субъекты коммерческой деятельности тоже подвержены значительным рискам в результате информационных атак. Так, средний прямой финансовый ущерб, наносимый российским компаниям за один день, оценивается приблизительно в 11,5 млн рублей [Средний ущерб компаний РФ].

Китайская Народная Республика рассматривает информационную безопасность в качестве одного из приоритетных направлений внутренней и внешней политики, что связано как с утечкой данных, так и с усилением государственного кибершпионажа. В 2025 г. был зафиксирован масштабный инцидент информационной безопасности, связанный с несанкционированным доступом и компрометацией приблизительно 4 млрд записей персональных данных на территории страны, что демонстрирует высокий уровень угроз и колоссальные объёмы информации, подвергающиеся риску в глобальном цифровом пространстве [NCSC Annual Review 2025].

Ключевой вызов для информационной безопасности Ирана связан с ростом геополитической конфронтации в регионе и сопровождающими её интенсивными кибероперациями. Наибольшему давлению подвержены стратегические объекты, такие как системы управления судами, АЗС и банкоматы, что не только приводит к экономическим убыткам, но и наносит урон двусторонним отношениям государства с партнёрами [Лаврова Д.]. Страны-участницы ШОС Центральной Азии также сталкиваются с такими вызовами, как фишинговые атаки, активизация вредоносного программного обеспечения для кражи данных, распространение деструктивной идеологии, что возводит вопрос обеспечения информационной безопасности в число проблем первостепенной важности [Авезова Я.]. Что касается Индии, то стоит отметить, что страна является одной из наиболее атакуемых в мире. В 2024 г. она заняла второе место по числу жертв кибератак после США [Индия стала главной целью]. В то же время основным источником проблем в сфере информационной безопасности в Беларуси являются внутренние факторы, такие как сбои программного обеспечения, технические неполадки, человеческий фактор [Матвеев А.].

Таким образом, государства-члены ШОС сталкиваются с растущим количеством угроз для их информационной безопасности. Более того, современные вызовы приобретают трансграничный характер, что наглядно демонстрируется распространением самореплицирующихся вредоносных программ, известных как «черви». В контексте региональной организации, участницы которой связаны общими транспортными, энергетическими и логистическими сетями, локальный киберинцидент способен в кратчайшие сроки привести к нарушению функ-

ционирования критически важной инфраструктуры на территории всего региона. Эффективное противодействие подобным вызовам требует не индивидуальных, а скоординированных действий, в связи с чем участники Шанхайской организации сотрудничества укрепляют взаимодействие по данному направлению.

Сотрудничество стран — членов ШОС осуществляется на двух основных уровнях: документальное закрепление позиций сторон, включая формулировку и закрепление основных вызовов и подходов; практическое взаимодействие, включающее как проведение совместных учений, так и взаимодействие профильных ведомств в рамках специализированных институтов организации.

### **Правовая база сотрудничества стран — участниц ШОС в области обеспечения информационной безопасности**

Актуальность проблемы информационной безопасности для стран-участниц ШОС подтверждается наличием правовой базы, закладывающей стратегические основы взаимодействия государств и определяющей направление их совместной деятельности. Это также свидетельствует о том, что несмотря на принимаемые меры на национальном уровне, государства признают необходимость развития международного взаимодействия по данному вопросу.

Так, еще в 2009 г. было принято «Соглашение между правительствами государств — членов ШОС о сотрудничестве в области международной информационной безопасности» [Соглашение]. В документе были обозначены основные угрозы для стран, среди которых можно выделить информационный терроризм, применение информационного оружия, информационную преступность. В отдельную категорию были выделены противоправные действия, направленные на нанесение ущерба или уничтожение критически важной инфраструктуры. Стороны отметили, что деятельность в международном информационном пространстве должна способствовать социально-экономическому развитию всех стран и международной безопасности и стабильности, а не служить деструктивным элементом. Политика акторов мировой арены в киберпространстве обязана соответствовать общепризнанным принципам международного права, включая мирное урегулирование споров, неприменение силы, невмешательство во внутренние дела и уважение прав человека. Но в то же время каждая сторона имеет суверенное право на защиту своих информационных ресурсов и критически важной инфраструктуры от вредоносных атак.

По мере стремительного возрастания количества угроз и их влияния на национальные интересы государства вопросы информационной безопасности стали подниматься на уровне встреч глав государств и министров иностранных дел, а стратегические шаги стали находить отражение в итоговых декларациях организации. Так, в 2016 г. по итогам саммита в Ташкенте был принят документ, в котором стороны среди прочих заявлений обозначили ключевые принципы деятельности стран в сфере МИБ. В целом, многие положения схожи с соглашением 2009 г., однако была особо отмечена необходимость наращивания сотрудничества в упомянутой сфере [Ташкентская декларация]. В 2017 г. проблематика ин-

формационной безопасности в рамках региональной организации приняла качественно иной характер. В Астанинской декларации глав государств-членов была выражена готовность выстраивания сотрудничества со всеми заинтересованными сторонами: странами, организациями, объединениями и структурами ООН. Содержался призыв к международному сообществу сосредоточить усилия на мерах по укреплению доверия, отказу от применения силы и предотвращению конфликтов в информационной среде [Астанинская декларация].

Следующим этапом развития правового аспекта сотрудничества стран ШОС, направленного на обеспечение региональной информационной безопасности, стало подписание в 2018 г. «Циндаоской декларации Совета глав государств-членов Шанхайской организации сотрудничества» [Циндаоская декларация]. Документ подчеркивает первостепенную роль ООН в создании архитектуры международной информационной безопасности, так как только данная организация наделена полномочиями принятия общеобязательных для всех государств норм и принципов, гарантирующих их ответственное поведение в информационном пространстве. Важно также отметить, что данное положение свидетельствует о том, что страны — участницы ШОС стали осознавать взаимозависимость всех государств в киберпространстве вне зависимости от географического расположения, поэтому достижение консенсуса на региональном уровне недостаточно для обеспечения информационной безопасности государства. Не менее важным пунктом, упомянутом в рассматриваемом документе служит тезис о необходимости создания общей системы мониторинга угроз в цифровом пространстве, что говорит о возрастающей готовности подписавшихся сторон переходить к практическим действиям.

В 2019 г. в рамках Шанхайской организации сотрудничества была принята «Концепция сотрудничества государств — членов ШОС в сфере цифровизации и информационно-коммуникационных технологий», в 2021 был создан специальный механизм, регулирующий развитие ИКТ в странах. Согласно Концепции, в его задачи входит разработка межгосударственных соглашений, принятие мер, направленных на стимулирование обмена знаниями, проведение совместных исследований и привлечение экспертов, и повышение квалификации работников в сфере цифровизации в государствах-членах. Кроме того, среди задач Совещания входит создание условий для партнерства между компаниями, реализация высокотехнологичных проектов на базе инновационных кластеров, а также обмен опытом в поддержке стартапов [Совещание].

Серьезным вызовом для мирового сообщества стала милитаризация информационного пространства, ставшая следствием использования ИКТ с целью нанесения ущерба другой стороне. В связи с этим страны — участницы ШОС приняли Самаркандскую декларацию по итогам встречи глав государств-членов в 2022 г. [Самаркандская декларация]. В ней отмечается, что стороны выступают против милитаризации информационного пространства, а также поддержали запуск разработки под эгидой Организации Объединенных Наций международной конвенции о противодействии использованию ИКТ в преступных целях. Более того, в Тяньцзиньской декларации, принятой по итогам XXV заседания Совета глав государств — членов ШОС, также отмечается кристально ясная отрицатель-

ная позиция стран относительно превращения информационного пространства в новую арену геополитического противостояния и начала новой гонки кибервооружения [Тяньцзиньская декларация].

Одним из направлений сотрудничества государств — членов Шанхайской организации сотрудничества является противодействие терроризму. С развитием ИКТ, способствующим более быстрой передаче информации вне зависимости от территориального расположения, террористическая идеология и агитация стали настоящей угрозой для национальной, региональной и международной безопасности. В ответ на данную тенденцию страны наращивают сотрудничество по предотвращению распространения деструктивных нарративов в сети Интернет, важной основой для которого, бесспорно, является нормативная база. Так, основополагающим является «Соглашения о сотрудничестве в области выявления и перекрытия каналов проникновения на территории государств — членов ШОС лиц, причастных к террористической, сепаратистской и экстремистской деятельности» от 2006 года» [Соглашение о сотрудничестве]. В данном документе основной упор делается на единогласном стремлении сторон противодействовать терроризму, в то время как в уже упомянутом «Соглашении о сотрудничестве в области обеспечения международной информационной безопасности» от 2009 г. отмечаются новые механизмы и инструменты для использования в противоправной деятельности.

### **Практическое сотрудничество по обеспечению безопасности в информационном пространстве**

Оформление политической воли открывает возможности для принятия конкретных действий, направленных на непосредственное обеспечение информационной безопасности. Так, в сфере практической реализации принятых нормативно-правовых актов особого внимания заслуживают проводимые совместные учения в киберпространстве. В 2015 г. прошли первые киберучения, «Сямынь-2015». В рамках мероприятия компетентным органам было предложено выполнить задания, направленные на повышение квалификации в области планирования, подготовки и реализации специальных миссий по обезвреживанию террористических группировок в киберпространстве [Штабные киберучения стран ШОС по борьбе с терроризмом].

В 2023 г. Специальные службы стран — членов Шанхайской организации сотрудничества провели в Нью-Дели в четвертый и на данный момент последний раз совместное антитеррористическое учение. Его целью являлась отработка навыков выявления и пресечения использования сети Интернет в террористических, сепаратистских и экстремистских целях, а также повышение качества взаимодействия спецслужб в условиях кибератак на объекты критически важной информационной инфраструктуры. В рамках мероприятия участники осуществили обмен опытом по противодействию использованию цифровых активов для финансирования запрещенной деятельности [Спецслужбы стран — членов ШОС провели в Нью-Дели].

Таким образом, проведение совместных киберучений свидетельствует о готовности стран ШОС не только декларировать необходимость сотрудничества для обеспечения национальной и региональной информационной безопасности, но и предпринимать для этого конкретные шаги. Более того, совместные учения всегда являются показателем не только военной мощи государств, но и их единства и сплоченности. Не менее важным является практический результат данного направления деятельности, так как создают условия для отработки совместных действий специалистами из различных государств, имеющих различия в техническом оснащении, правовых системах и языковой среде, что способствует повышению уровня координации государств — членов ШОС при реагировании на реальные кибератаки трансграничного характера.

Развивается сотрудничество и по направлению обмена информацией и опытом между профильными ведомствами государств-членов. На Международной конференции по противодействию терроризму в странах ШОС, которая проводится в ноябре 2025 г. в Ташкенте, Директор исполнительного комитета Региональной антитеррористической структуры ШОС Уларбек Шаршеев заявил, что в целях противодействия террористической деятельности отмечается интенсификация обмена сведениями о физических лицах с признаками вовлеченности в террористическую и экстремистскую деятельность, а также аналитической информацией о новых методах использования ресурсов сети Интернет нелегальными преступными структурами [Спецслужбы стран ШОС].

Важным событием в области сотрудничества по обеспечению информационной безопасности является решение о создании Универсального центра по противодействию вызовам и угрозам безопасности государств-членов ШОС, который будет располагаться в Ташкенте. Данное решение было принято на саммите Шанхайской организации сотрудничества, состоявшемся 31 августа — 1 сентября 2025 г. в Китае. Под эгидой Универсального центра будет сформирован Центр информационной безопасности ШОС, который станет координирующим инструментом, направленным на оптимизацию усилий по защите информационного пространства [ШОС против киберугроз]. Пекин сыграл ключевую роль в данном событии, так как в ходе своего председательства призвал ускорить создание специализированных центров по борьбе с традиционными и новыми угрозами.

Данное событие стало закономерным шагом в развитии работы Региональной антитеррористической структуры ШОС, которая функционирует с 2004 г. Базируясь в Ташкенте, РАТС обеспечивает координацию совместных усилий государств-членов в противодействии «трем силам зла» — так в терминологии ШОС обозначаются терроризм, сепаратизм и экстремизм.

## **Развитие сотрудничества с другими акторами международных отношений**

ШОС стремится выйти за региональные рамки и расширить сотрудничество с другими акторами мировой арены. Одним из таких партнеров является БРИКС, который по праву считается проводником формирующегося многополярного порядка, основанного на нормах международного права, уважении на-

ционального суверенитета, взаимовыгоде и решении вопросов дипломатическим путем.

Важным направлением взаимодействия БРИКС и ШОС в области информационной безопасности выступает реализация совместных инициатив, ориентированных на обучение и повышение квалификации профильных специалистов. Проведение в данном формате учебных курсов, семинаров и тренингов создает условия для эффективного обмена знаниями о современных методах защиты информации и противодействия киберугрозам. Указанная деятельность направлена на развитие человеческого капитала как ключевого ресурса обеспечения национальной и региональной безопасности.

Кроме того, формирование платформы для совместного мониторинга и анализа киберугроз представляет собой фундамент стратегического партнерства двух объединений в рассматриваемой сфере. Институционализированный обмен оперативными данными об инцидентах и уязвимостях между государствами-членами создаст условия для своевременного реагирования на возникающие вызовы и позволит минимизировать потенциальный ущерб. Это не только повысит уровень глобальной безопасности, но и выполнит объединяющую функцию, способствуя укреплению отношений между членами БРИКС и ШОС [Взаимодействие БРИКС и ШОС].

## **Заключение**

Таким образом, в условиях активной цифровой трансформации границы между физической и виртуальной реальностью становятся все более проницаемыми. Интернет превратился из средства коммуникации в глобальную среду, порождающую новые вызовы, включая киберпреступность и атаки на критически важную инфраструктуру. Для защиты своих национальных интересов государства обращают особое внимание на совершенствование законодательной базы, регулирующей деятельность в информационном пространстве, а также на внедрение специальных механизмов, защищающих как критически важную инфраструктуру, так и социально-психологическое состояние их населения.

Однако, в сфере информационной безопасности возможно достичь успехов только при сотрудничестве с другими игроками мировой арены. Основой такого сотрудничества может служить схожее видение основ деятельности стран в киберпространстве, а также общие подходы к регулированию данной политики. Государства-члены ШОС, которые придерживаются принципов «шанхайского духа», достигли значительных результатов в области обеспечения набирающего актуальность вида безопасности.

Стороны стремятся к налаживанию конструктивного диалога для выработки взаимовыгодных и взаимоприемлемых подходов к регулированию информационного пространства и созданию безопасного киберпространства. Среди основополагающих направлений взаимодействия можно выделить создание нормативно-правовой базы, на основе которой в последующем создаются профильные ко-

митеты, совещания, или же институты в рамках организации. Кроме того, документальное оформление видения ШОС проблемы безопасности в информационном поле стимулирует подписавшиеся стороны предпринимать практико-ориентированные действия.

Уникальным является проведение совместных военных учений в киберпространстве, что позволяет странам — участницам ШОС готовить свой состав к предотвращению ново возникающих угроз. Геополитические амбиции организации, особенно в сфере международной информационной безопасности, возрастают, о чем свидетельствует создание Универсального центра по противодействию вызовам и угрозам безопасности. Из первоначально пограничного формата по укреплению доверия ШОС трансформировалась в площадку для построения единой и неделимой системы евразийской безопасности. А приверженность ШОС идеалам многополярного мира, базирующегося на нормах международного права и центральной роли ООН, красной нитью проходит по всем официальным документам объединения.

В то же время стоит иметь в виду, что существует ряд препятствий, не позволяющих странам достичь полной интеграции по данному направлению. Одной из наиболее острых проблем являются различия в уровне технологического и инновационного развития участников, что определяет не только внутреннюю политику государства, но и влияет на его действия при взаимодействии с другими странами. Так, Китай и Россия, будучи наиболее технически развитыми участниками делают упор на принятие единых общеобязательных стандартов, в то время как их партнеры в качестве приоритета рассматривают создание инфраструктуры и подготовку высококвалифицированных специалистов, которые бы могли развивать экосистему информационной безопасности в стране. Не менее важную роль играют политические разногласия между участниками, что не позволяет организации выйти на более высокий уровень военно-стратегического сотрудничества.

---

## Библиографический список

Авезова Я. Актуальные киберугрозы в странах СНГ 2023—2024 // Positive Technologies. URL: <https://www.ptsecurity.com/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/> (дата обращения: 01.12.2025).

Астанинская декларация глав государств — членов Шанхайской организации сотрудничества // Президент России. URL: <http://special.kremlin.ru/supplement/5206> (дата обращения: 22.11.2025).

В ШОС заявили о предотвращении 181 теракта в 2023 году. URL: <https://ria.ru/20240523/shos-1947842604.html> (дата обращения: 22.11.2025).

Взаимодействие БРИКС и ШОС в сфере обеспечения информационной безопасности // Информационный портал СНГ. URL: <https://e-cis.info/news/566/122331/#2> (дата обращения: 22.11.2025).

Индия стала главной целью хакеров в начале 2025 года, Россия удерживает место в топ-10 // Cyber Media. URL: <https://securitymedia.org/news/indiya-stala-glavnoy-tselyu-khakerov-v-nachale-2025-goda-rossiya-uderzhivaet-mesto-v-top-10.html> (дата обращения: 01.12.2025).

Лаврова Д. Ландшафт киберугроз в Иране: 2021 — H1 2024 // Positive Technologies. URL: <https://www.ptsecurity.com/research/analytics/landshaft-kiberugroz-v-irane-2021-h1-2024/#id1> (дата обращения: 01.12.2025).

Матвеев А. Какие общие проблемы и вызовы в сфере инфобеза в России и Беларуси // Proway. URL: <https://www.google.com/amp/s/companies.rbc.ru/amp/news/9b24ece8-4a56-49bf-813f-28efb2e869a2/> (дата обращения: 01.12.2025).

Самаркандская декларация Совета глав государств — членов Шанхайской организации сотрудничества // Президент России. URL: <http://www.kremlin.ru/supplement/5841> (дата обращения: 22.11.2025).

Сборов А. Мария Захарова: «Информационная война идет одновременно за прошлое, настоящее и будущее» // Эксперт. URL: <https://expert.ru/mnenie/informatsionnaya-voyna-idet-odno-vremennno-za-proshloe-nastoyashchee-i-budushchee/> (дата обращения: 01.12.2025).

Совещание руководителей министерств и ведомств государств — членов ШОС, ответственных за развитие информационно-коммуникационных технологий // Шанхайская организация сотрудничества. URL: <https://rus.sectsc.org/20240208/1268009.html> (дата обращения: 22.11.2025).

Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности // Электронный фонд правовых и нормативно-технических документов. URL: <https://docs.cntd.ru/document/902289626> (дата обращения: 22.11.2025).

Соглашения о сотрудничестве в области выявления и перекрытия каналов проникновения на территории государств-членов ШОС лиц, причастных к террористической, сепаратистской и экстремистской деятельности // Электронный фонд правовых и нормативно-технических документов. URL: <https://docs.cntd.ru/document/902320010> (дата обращения: 22.11.2025).

Спецслужбы стран ШОС усиливают сотрудничество в киберпространстве для блокирования доступа к террористическому и экстремистскому контенту // Sputnik. URL: <https://uz.sputniknews.ru/20251127/kak-vyrastit-zdorovogo-rebenka-53766387.html> (дата обращения: 22.11.2025).

Спецслужбы стран — членов ШОС провели в Нью-Дели учения по отражению кибератак террористов // ТАСС. URL: <https://tass.ru/mezhdunarodnaya-panorama/19575463> (дата обращения: 22.11.2025).

Ташкентская декларация 15-летия Шанхайской организации сотрудничества // Президент России. URL: <http://special.kremlin.ru/supplement/5094> (дата обращения: 22.11.2025).

Тяньцзиньская декларация Совета глав государств — членов Шанхайской организации сотрудничества // Президент России. URL: <http://kremlin.ru/supplement/6376> (дата обращения: 22.11.2025).

Циндаоская декларация Совета глав государств — членов Шанхайской организации сотрудничества // Президент России. URL: <http://www.kremlin.ru/supplement/5315> (дата обращения: 22.11.2025).

ШОС против киберугроз: Ташкент примет Центр информационной безопасности // Stan Radar. URL: <https://stanradar.com/news/full/58196-shos-protiv-kiberugroz-tashkent-primet-tsentr-informatsionnoj-bezopasnosti.html> (дата обращения: 22.11.2025).

Штабные киберучения стран ШОС по борьбе с терроризмом проходят в Китае // РИА Новости. URL: <https://ria.ru/20151014/1301603766.html> (дата обращения: 22.11.2025).

NCSC Annual Review 2025 // National Cyber Security Centre. URL: <https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025/chapter-01-cyber-threat-to-the-uk> (дата обращения: 01.12.2025).

---

## References

Astaninskaya deklaratsiya glav gosudarstv — chlenov Shankhayskoy organizatsii sotrudnichestva // Prezident Rossii. URL: <http://special.kremlin.ru/supplement/5206> (accessed: 22 November 2025). (In Russian).

Avezova Ya. Aktual'ny'e kiberugrozy` v stranax SNG 2023—2024 // Positive Technologies. URL: <https://www.ptsecurity.com/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/> (accessed: 1 December 2025). (In Russian).

Indiya stala glavnoj cel'yu xakerov v nachale 2025 goda, Rossiya uderzhivaet mesto v top-10 // Cyber Media. URL: <https://securitymedia.org/news/indiya-stala-glavnoy-tselyu-khakerov-v-nachale-2025-goda-rossiya-uderzhivaet-mesto-v-top-10.html> (accessed: 1 December 2025). (In Russian).

Lavrova D. Landshaft kiberugroz v Irane: 2021 — H1 2024 // Positive Technologies. URL: <https://www.ptsecurity.com/research/analytics/landshaft-kiberugroz-v-irane-2021-h1-2024/#id1> (accessed: 1 December 2025). (In Russian).

Matveev A. Kakie obshhie problemy` i vy'zovy` v sfere infobeza v Rossii i Belarusi // Proway. URL: <https://www.google.com/amp/s/companies.rbc.ru/amp/news/9b24ece8-4a56-49bf-813f-28efb2e869a2/> (accessed: 1 December 2025). (In Russian).

NCSC Annual Review 2025 // National Cyber Security Centre. URL: <https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025/chapter-01-cyber-threat-to-the-uk> (accessed: 22 November 2025).

Samarkandskaya deklaratsiya Soveta glav gosudarstv-chlenov Shankhayskoy organizatsii sotrudnichestva // Prezident Rossii. URL: <http://www.kremlin.ru/supplement/5841> (accessed: 22 November 2025). (In Russian).

ShOS protiv kiberugroz: Tashkent primet Tsentr informatsionnoy bezopasnosti // Stan Radar. URL: <https://stanradar.com/news/full/58196-shos-protiv-kiberugroz-tashkent-primet-tsentr-informatsionnoy-bezopasnosti.html> (accessed: 22 November 2025). (In Russian).

Shtabnyye kiberucheniya stran ShOS po bor'be s terrorizmom prokhodyat v Kitaye // RIA Novosti. URL: <https://ria.ru/20151014/1301603766.html> (accessed: 22 November 2025). (In Russian).

Soglasheniya o sotrudnichestve v oblasti vyyavleniya i perekrytiya kanalov proniknoveniya na territorii gosudarstv-chlenov ShOS lits, prichastnykh k terroristicheskoy, separatistskoy i ekstremistskoy deyatel'nosti // Elektronnyy fond pravovykh i normativno-tekhnicheskikh dokumentov. URL: <https://docs.cntd.ru/document/902320010> (accessed: 22 November 2025). (In Russian).

Soglasheniye mezhdru pravitel'stvami gosudarstv — chlenov Shankhayskoy organizatsii sotrudnichestva o sotrudnichestve v oblasti obespecheniya mezhdunarodnoy informatsionnoy bezopasnosti // Elektronnyy fond pravovykh i normativno-tekhnicheskikh dokumentov. URL: <https://docs.cntd.ru/document/902289626> (accessed: 22 November 2025). (In Russian).

Soveshchaniye rukovoditeley ministerstv i vedomstv gosudarstv-chlenov ShOS, otvetstvennykh za razvitiye informatsionno-kommunikatsionnykh tekhnologiy // Shankhayskaya organizatsiya sotrudnichestva. URL: <https://rus.sectso.org/20240208/1268009.html> (accessed: 22 November 2025). (In Russian).

Spetssluzhby stran ShOS usilivayut sotrudnichestvo v kiberprostranstve dlya blokirovaniya dostupa k terroristicheskomu i ekstremistskomu kontentu // Sputnik. URL: <https://uz.sputniknews.ru/20251127/kak-vyrastit-zdorovogo-rebenka-53766387.html> (accessed: 22 November 2025). (In Russian).

Spetssluzhby stran-chlenov ShOS proveli v N'yu-Deli ucheniya po otrazheniyu kiberatak terroristov // TASS. URL: <https://tass.ru/mezhdunarodnaya-panorama/19575463> (accessed: 22 November 2025). (In Russian).

Srednij ushherb kompanij RF ot odnoj utechki informacii sostavlyaet okolo 11,5 mln rub // Finmarket. URL: <https://www.finmarket.ru/news/6324665> (accessed: 1 December 2025). (In Russian).

Tashkentskaya deklaratsiya 15-letiya Shankhayskoy organizatsii sotrudnichestva // Prezident Rossii. URL: <http://special.kremlin.ru/supplement/5094> (accessed: 22 November 2025). (In Russian).

Tsindaoskaya deklaratsiya Soveta glav gosudarstv-chlenov Shankhayskoy organizatsii sotrudnichestva // Prezident Rossii. URL: <http://www.kremlin.ru/supplement/5315> (accessed: 22 November 2025). (In Russian).

Тьян'тзин'ская декларация Совета глав государств-членов Шанхайской организации сотрудничества // Президент России. URL: <http://kremlin.ru/supplement/6376> (accessed: 22 November 2025). (In Russian).

V ShOS zayavili o predotvrashchenii 181 terakta v 2023 godu. URL: <https://ria.ru/20240523/shos-1947842604.html> (accessed: 22 November 2025). (In Russian).

Vzaimodeystviye BRIKS i ShOS v sfere obespecheniya informatsionnoy bezopasnosti // Informatsionnyy portal SNG. URL: <https://e-cis.info/news/566/122331/#2> (accessed: 22 November 2025). (In Russian).

---

Поступила в редакцию: 14.11.2025  
Принята к публикации: 20.11.2025

Received: Nov 14, 2025  
Accepted: Nov 20, 2025