 оригинальная статья / original paper

DOI: 10.22394/2073-2929-2025-01-159-170

специальность: 5.5.4

EDN: DFBCZG

Политика обеспечения информационной безопасности в государствах — членах ШОС

Щербань А. В.
Санкт-Петербургский государственный университет, Санкт-Петербург, Россия
e-mail: n.shche@mail.ru

РЕФЕРАТ

Настоящее исследование посвящено изучению ключевых приоритетов государств — участников ШОС в сфере информационной безопасности, а также выявлению роли геополитических противоречий и их влияние на сотрудничество. **Цель и задачи.** На основании теоретического материала и практического анализа рейтинга и официальных документов выявить особенности взаимодействия государств — членов ШОС в вопросах обеспечения информационной безопасности. Проанализировать в Глобальном инновационном индексе показатели инновационного развития государств — членов ШОС, определить лидеров в этой области; исследовать уровень обеспечения информационной безопасности стран-участниц; выявить противоречия и рассмотреть общие приоритеты политики государств сотрудничества в сфере обеспечения информационной безопасности. **Методология.** Работа основана на анализе официальных документов, сравнительном методе количественных показателей, методе кейс-стади и синтезе. **Результаты.** Исследование показало, что в зависимости от уровня развития инноваций, государства ШОС по-разному видят угрозы в информационном пространстве. Так, для стран, обладающих технологическим лидерством, первостепенными являются вопросы обеспечения кибербезопасности, установления единых стандартов и развития международного сотрудничества. Менее развитые в технологиях государства заинтересованы в предотвращении и устранении угроз внутриполитического характера. Фактор геополитических противоречий оказывает влияние на сотрудничество отдельных государств внутри организации в вопросах развития сферы информационно-коммуникационных технологий (пример Пакистана и Китая). Однако в рамках ШОС государства стремятся к конструктивному диалогу и выработке единых подходов регулирования сферы информационной безопасности. **Выводы.** Результаты исследования демонстрируют значение уровня технологического развития государств — членов ШОС в построении собственной информационной политики и предложенных инициативах в рамках ШОС. Безусловными технологическими лидерами в организации являются Китай и Россия. Будучи их союзником, Республика Беларусь стремится к улучшению системы обеспечения информационной безопасности. В то же время Пакистан, являясь геополитическим противником Индии, в рамках программы «Один пояс — один путь» развивает сотрудничество с Китаем в вопросах совершенствования сферы информационно-коммуникационных технологий. Проанализировав тенденцию инновационного развития, можно отметить значительные успехи Индии, Ирана и Казахстана. В случае с Казахстаном важно указать, что республика является технологическим лидером в Центрально-Азиатском регионе, а потому вопросы построения информационной безопасности являются стратегическим направлением. Таджикистан, Киргизия и Узбекистан фокусируются на решении внутренних проблем в информационном пространстве, однако активно выдвигают свои инициативы по данному вопросу в рамках ШОС.

Ключевые слова: ШОС, информационная безопасность, киберпространство, информационно-психологическая безопасность, Глобальный инновационный индекс

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

Information Security Policy in the SCO Member States

Anastasia V. Shcherban
St. Petersburg State University, Saint Petersburg, Russia
e-mail: n.shche@mail.ru

ABSTRACT
This study is devoted to studying the key priorities of the SCO member states in the field of information security, as well as identifying the role of geopolitical contradictions and their impact on cooperation. **Aim and Tasks.** Based on the theoretical material and practical analysis of the rating and official documents, to identify the specifics of cooperation between the SCO member states in matters of information security. To analyze the indicators of innovative development of the SCO member states in the Global Innovation Index (GII), identify leaders in this field; to study the level of information security of the participating countries; to identify contradictions and to consider the general priorities of the policy of the states of cooperation in the field of information security. **Methods.** The work is based on the analysis of official documents, the comparative method of quantitative indicators, the case study method and synthesis. **Results.** The study showed that, depending on the level of innovation development, the SCO states see threats in the information space differently. Thus, for countries with technological leadership, cybersecurity, the establishment of common standards and the development of international cooperation are of paramount importance. Less technologically advanced states focus on preventing and eliminating threats of a domestic political nature. The factor of geopolitical contradictions has an impact on the cooperation of individual states within the organization in the development of the ICT sector (for example of Pakistan and China). However, within the framework of the SCO, states strive for constructive dialogue and the development of common approaches to regulating the field of information security. **Conclusions.** The results of the study demonstrate the importance of the level of technological development of the SCO member states in building their own information policy and proposed initiatives within the SCO. China and Russia are the undisputed technological leaders in the organization. As their ally, the Republic of Belarus strives to improve its information security system. At the same time, Pakistan, being a geopolitical opponent of India, has established cooperation with China on the development of the ICT sector within the framework of the "One Belt — One Road" project. Analyzing the trend of innovative development, we can note the significant successes of India, Iran and Kazakhstan. In the case of Kazakhstan, it is important to point out that the republic is a technological leader in the Central Asian region, and therefore the issues of building information security are a strategic focus. Tajikistan, Kyrgyzstan, and Uzbekistan are focusing on solving internal problems in the information space, but they are actively putting forward their initiatives in this area within the SCO.

***Keywords**:* SCO, information security, cyberspace, information and psychological security, Global Innovation Index
For citation: Shcherban A. V. Information Security Policy in the SCO Member States // Eurasian Integration: Economics, Law, Politics. 2025. Vol. 19. No. 1. P. 159–170. (In Russ.)
https://doi.org/10.22394/2073-2929-2025-01-159-170. EDN: DFBCZG

Введение

В докладе «Четвертая промышленная революция» (2016 г.) на Всемирном экономическом форуме в Давосе Клаус Шваб обозначил начало нового этапа индустриальной революции. Отличительной чертой этого витка технологического прогресса является слияние физического и виртуального миров. Международная нестабильность, связанная с борьбой за большие данные (колониализм данных), цифровое неравенство государств, возрастающий уровень безработицы, обусловленный автоматизацией производства, а также отсутствие этических норм и контроля являются нерешенной дилеммой международного уровня [2, с. 8; 15, с. 81].

В 1998 г. на уровне ООН министр иностранных дел России И. С. Иванов поднимал вопрос о регулировании международной сферы информационной безопасности. В том же году Москвой был представлен первый проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». США, в свою очередь, стремились сохранять гегемонию в вопросах регулирования данной сферы. Считая другие государства своими «цифровыми колониями», американцы отказывались от глобального сотрудничества. Поэтому за последнюю четверть века можно проследить формирование двух подходов к вопросам обеспечения международной информационной безопасности: российского и американского [8, с. 257; 18, p. 455].

В «Доктрине кибербезопасности США» 2023 г., в разделе «Злонамеренные акторы» (Malicious Actors), в качестве угроз национальной безопасности прописаны правительства Китайской Народной Республики (КНР), Российской Федерации, Ирана, Северной Кореи и других автократических режимов[1]. Кроме этого, в Стратегической концепции НАТО от 29 июня 2022 г. Российская Федерация значится государством, составляющим угрозу государствам — участникам альянса [14, с. 114–115]. В п. 13 документа отмечается негативный контекст сотрудничества России и Китая[2].

Исходя из вышеизложенного и учитывая поляризацию мира после февраля 2022 г., говорить об урегулировании сферы информационной безопасности на международном уровне не представляется возможным. Однако в данных обстоятельствах региональные организации и объединения являются хорошей площадкой для переговоров и законотворчества в вопросах регулирования данной сферы [21, p. 318; 22, p. 112].

Россия, будучи участницей Шанхайской организации сотрудничества (ШОС), может выдвигать собственные инициативы, способствующие защите национальной безопасности и укрепляющие отношения между государствами.

Материалы и методы

Проведение всестороннего анализа проблематики информационной безопасности в рамках ШОС основано на комплексном применении взаимодополняющих методов. Основной упор сделан на анализ официальных документов, теоретических концепций и рейтинговых показателей. Метод кейс-стади использовался для изучения текущего состояния политики информационной безопасности в государствах ШОС. Это позволило выявить национальные особенности и вызовы, с которыми сталкиваются страны организации. Благодаря методу синтеза удалось определить закономерности подходов государств ШОС к обеспечению информационной безопасности.

Основными источниками информации для исследования стали доктрины, концепции, стратегии, а также законодательные акты, регулирующие вопросы обеспечения информационной безопасности государств — членов ШОС. Кроме этого, использовались данные рейтинга Глобального инновационного индекса (ГИИ), а также проводился анализ отечественных и зарубежных исследований по данной проблематике.

---

[1] National Cybersecurity Strategy [Электронный ресурс]. URL: https://d-russia.ru/wp-content/uploads/2023/03/national-cybersecurity-strategy-2023.pdf (дата обращения: 12.01.2025).

[2] Стратегическая концепция НАТО 2022 года [Электронный ресурс]. URL: https://www.nato.int/cps/ru/natohq/topics_56626.htm (дата обращения: 16.01.2025).

Результаты

Уровень развития технологий государств — членов ШОС влияет на определение приоритетов обеспечения информационной безопасности. Ведущие экономики стран ШОС — Россия, Китай, Индия — заинтересованы в обеспечении кибербезопасности, установлении единых стандартов, а также развитии международного сотрудничества. Таджикистан, Киргизия и Узбекистан сосредоточены на предотвращении информационных угроз внутриполитического характера и привлечении зарубежных инвестиций в развитие сферы технологий.

Полученные данные демонстрируют наличие разных подходов в стратегиях информационной безопасности стран ШОС. Преодоление технологического разрыва и формирование единой нормативно-правовой базы являются первостепенной задачей в рамках диалога на площадке ШОС.

Обсуждение

Особенности развития области инноваций государств — членов ШОС

Формирование региональной системы информационной безопасности в рамках ШОС тесно переплетается с особенностями обеспечения собственной системы национальной безопасности государств-участников. Поэтому между странами могут возникать противоречия, в основе которых заложены разные взгляды понимания информационной безопасности[1].

Характеристика стратегий информационной безопасности ШОС невозможна без оценки уровня технологического развития стран-участниц. Всемирная организация интеллектуальной собственности ежегодно публикует ГИИ. Рейтинг 133 государств позволяет проследить развитие инноваций, охватывая показатели политической ситуации, системы образования и технологий в каждой стране. Практика оценки и сравнения государств по определенным критериям является достаточно спорной, ведь большинство рейтингов составлены западными компаниями. Поэтому необходимо критически относиться к результатам и учитывать фактор мировой нестабильности.

Для характеристики развития инноваций в государствах ШОС рассмотрим результаты позиции государств — членов ШОС в рейтинге в период 2019–2024 гг., где нижняя граница 2019 г. — последний год (допандемийный) стабильности мировых процессов, верхняя граница 2024 г. — конфронтация мира после начала специальной военной операции в феврале 2022 г.

Таблица

Рейтинг Глобального инновационного индекса государств — участников ШОС в период 2019–2024 гг.

Table. The Ranking of the Global Innovation Index of the SCO member states in the period 2019–2024

Страна / год	2019	2020	2021	2022	2023	2024
Российская Федерация	46	47	45	47	51	59
КНР	14	14	12	11	12	11
Республика Беларусь	72	64	62	77	80	85
Иран	62	67	60	53	62	64
Индия	52	48	46	40	40	39
Пакистан	105	107	99	87	88	91
Республика Казахстан	79	94	79	83	81	78
Республика Таджикистан	100	109	103	104	100	107
Республика Узбекистан	—	93	86	82	82	83
Кыргызская Республика	90	94	98	94	106	99

Источник: Глобальный инновационный индекс [Электронный ресурс]. URL: https://www.wipo.int/ru/web/global-innovation-index (дата обращения: 06.01.2025)

[1] О Шанхайской организации сотрудничества [Электронный ресурс] // Шанхайская организация сотрудничества URL: https://rus.sectsco.org/20151208/16789.html (дата обращения: 17.01.2025).

Исходя из данных таблицы, основанных на ежегодных рейтингах ГИИ, можно проследить положительную динамику роста Республики Индии, Исламской Республики Пакистан и Республики Узбекистан. Устойчивые позиции инновационного развития демонстрируют Китай, Иран, Казахстан и Киргизия. Однако Российская Федерация, Республика Беларусь и Республика Таджикистан теряют позиции в рейтинге, в среднем на десять строк. Для Российской Федерации утрата позиций обусловлена устаревшими данными, которые используют авторы рейтинга ГИИ. Как отмечает В. В. Власова, по 18 индикаторам из 78 используются результаты старше 2022 г., а по 3 индикаторам информация и вовсе отсутствует[1]. Тенденция снижения позиций Республики Беларусь и Республики Таджикистан обусловлена ухудшением позиций в индикаторах «институты», «человеческий капитал и развитие науки», «развитие инфраструктуры» и «уровня развития бизнеса».

Важно учитывать, что позиции стран в рейтинге ГИИ отражают уровень развития инноваций, который влечет появление новых вызовов и угроз. Анализ позиций государств в рейтинге демонстрирует, что обеспечение информационной безопасности является стратегическим приоритетом для Российской Федерации, КНР, Республики Индии и Исламской Республики Иран. Подвергаясь угрозам внешнего влияния и дестабилизации внутриполитической обстановки, Республика Беларусь и Республика Казахстан заинтересованы в обеспечении надежной системы информационной безопасности. Исходя из этого, коллективное сотрудничество в рамках ШОС в вопросах обеспечения информационной безопасности позволяет государствам выработать общие меры противодействия вызовам и угрозам в данной области.

Особенности системы информационной безопасности государств — участников ШОС

В Российской Федерации существуют два подхода к пониманию информационной безопасности. Кибербезопасность нацелена на защиту технических систем, критически важной сетевой инфраструктуры. Информационно-психологическая безопасность подразумевает защиту населения от деструктивного влияния извне. Достаточно широкая интерпретация термина «информационной безопасности» позволяет использовать его в стратегиях, доктринах и законах [16, с. 4]. В отечественной науке вопросы обеспечения информационной безопасности связаны с изучением теории информационного противоборства, которая охватывает весь спектр воздействия: как использование технологий, так и информационно-психологическое влияние на людей в межгосударственном противостоянии [1, с. 139].

По мнению И. Ф. Кефели, обеспечение информационной безопасности предотвращает военное и невоенное воздействие. Для государства наличие идеологии является главным элементом обеспечения информационно-психологической безопасности [4, с. 144].

Е. Н. Пашенцев под термином «информационно-психологической безопасности» понимает защиту системы международных отношений от негативного психологического воздействия, связанного с разнообразными объективными и субъективными факторами. Прежде всего он акцентирует внимание на проблеме злонамеренного использования искусственного интеллекта, который используется в политических и преступных целях [9, с. 286].

Подводя итог, можно отметить, что междисциплинарный подход изучения информационной безопасности позволяет выделить отдельные области, которые должны регулироваться на государственном уровне.

Вопросы обеспечения информационной безопасности в Российской Федерации закрепляет вторая редакция Доктрины информационной безопасности РФ от 5 декабря 2016 г.[2], кроме этого, основные положения содержатся в Концепции внешней политики РФ от 31 марта 2023 г.[3] и Стратегии

[1] Валерия Власова об оценке позиций России в ГИИ-2024 [Электронный ресурс] // Национальный исследовательский университет «Высшая школа экономики». 27.09.2024. URL: https://issek.hse.ru/news/967248155.html (дата обращения: 10.01.2025).

[2] Доктрина информационной безопасности РФ от 5 декабря 2016 г. [Электронный ресурс] // Российская газета. URL: https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 15.01.2025).

[3] Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В. В. Путиным 31 марта 2023 г.) [Электронный ресурс] // Министерство иностранных дел РФ. URL: https://www.mid.ru/ru/detail-material-page/1860586/ (дата обращения: 15.01.2025).

национальной безопасности РФ от 2 июля 2021 г.[1] Особенностью Доктрины информационной безопасности РФ являются:

- сотрудничество в сфере информационной безопасности и предоставление помощи своим союзникам;
- борьба с подрывом традиционных ценностей, фальсификацией истории и распространением ложных новостей;
- положения доктрины отмечают, что информационная безопасность распространяется на духовную жизнь граждан.

При этом необходимо понимание, что после начала острой конфронтации с Западом, а также бурным развитием цифровых технологий положения доктрины будут дополняться. Таким образом, политика информационной безопасности России направлена на сохранение традиционных семейных ценностей, исторической памяти, воспитание патриотизма, а также на духовно-нравственное развитие граждан [10, с. 155].

В Китайской Народной Республике сформировалась надежная система информационной безопасности, которая подразумевает защиту информации и сетей критически важной информационной инфраструктуры от взломов, утечек данных и уничтожения информации. На законодательном уровне вопросы обеспечения информационной безопасности регулируются законом «О кибербезопасности» от 2017 г., законом «О безопасности данных» от 2021 г. и законом «О защите персональной информации» от 2021 г. [13, с. 80; 19, p. 225–226]. Важной особенностью китайской системы сетевой безопасности (терминология для обозначения «кибербезопасности» в официальных документах) является концепция цифрового суверенитета. Она подразумевает защиту информационных потоков и больших данных от внешнего влияния. Уникальная техническая система «Золотой щит» позволяет осуществлять мониторинг и контроль в Интернете. Система подвергает цензуре нежелательный контент, контролирует китайские социальные сети и мобильные приложения, кроме этого, предоставляет большие данные государственным структурам и осуществляет видеонаблюдение для отслеживания правонарушений по всей стране [11, с. 58–59; 17, с. 38]. Среди основных принципов регулирования информационной безопасности в Китае можно выделить следующие: осуществление контроля в информационном и киберпространстве, строгая локализация данных и шифрование их при передаче за рубеж, а также обеспечение надежной защиты научно-технических открытий.

Для Республики Беларусь обеспечение защиты информационно-технологического пространства является стратегическим направлением государственной политики. Нормативно-правовая база Республики Беларусь (РБ) регулируется Концепцией информационной безопасности РБ от 18 марта 2019 г., законом «Об информации, информатизации и защите информации» от 2008 г. и законом «О защите персональных данных» от 2021 г. В концепции содержатся основные приоритеты государственной политики, направленные на устранение ключевых угроз в политическом, экономическом, социальном и техническом пространстве. Важно отметить, что в документе подчеркиваются угрозы распространения деструктивной информации, а также манипуляция общественным мнением в экстремистских и террористических целях. Попытки дестабилизации внутриполитической обстановки в стране, а также геополитическое положение вблизи военного конфликта подчеркивают необходимость серьезного подхода к обеспечению национальной безопасности [6, с. 8].

В Республике Индии вопросы обеспечения информационной безопасности регулируются законом «Об информационных технологиях» от 2000 г. Дополнением к нему служит закон «О персональных данных», принятый в 2023 г., в основе которого заложен европейский Общий регламент защиты персональных данных. Национальная политика кибербезопасности Индии от 2013 г. определяет области защиты киберпространства, однако в 2020 г. Совет по безопасности данных Индии анонсировал разработку новой Национальной программы, которая на момент конца 2024 г. находится в стадии утверждения[2].

[1] Указ Президента Российской Федерации от 02.07.2021 № 400 [Электронный ресурс] // Правительство России (дата обращения: 15.01.2025).
[2] Data Security Council of India Analysis of National Cyber Security Policy (NCSP–2013) [Электронный ресурс]. URL: https://www.dsci.in/blogs/national-cyber-security-policy-ncsp-2013/ (дата обращения: 16.01.2025).

На международном уровне Индия активно ведет сотрудничество в вопросах обеспечения информационной безопасности. В октябре 2024 г. состоялся первый «кибер-диалог» между Италией и Индией. По итогам диалога государства укрепили двустороннее сотрудничество в обеспечении безопасного киберпространства. В 2023 г., в рамках ШОС, Индия организовала практический семинар на тему «Противодействие неправомерному использованию Интернета и новых информационных технологий». Так, можно проследить многовекторный подход государства в установлении сотрудничества в данной области [7, с. 445–448; 20, p. 13].

Политика Исламской Республики Пакистан в вопросах обеспечения информационной безопасности регулируется Национальной политикой кибербезопасности, принятой в июле 2021 г. Документ регулирует защиту киберпространства, определяет сотрудничество между государством и частными предприятиями, а также закрепляет создание Комитета по киберуправлению. Напряженные отношения Индии, Китая и Пакистана побуждают Пекин и Исламабад к тесному сотрудничеству в области обеспечения кибербезопасности. По уровню развития ИКТ Пакистан серьезно уступает ключевому региональному противнику — Индии. Регулярные хакерские атаки со стороны Индии на инфраструктуру Исламабада привели к подписанию между Китаем и Пакистаном Китайско-пакистанского экономического коридора 2017–2030. Данное соглашение затрагивает вопросы сотрудничества в сфере информационной безопасности. Основными целями сотрудничества является улучшение информационной инфраструктуры в Пакистане, обеспечение защиты данных, а также сотрудничество в сфере обмена опытом и технологиями для предотвращения угроз [3, с. 110; 7, с. 442]. В рамках ШОС Пакистаном в 2024 г. была выдвинута идея о создании общего цифрового рынка. Так, создание единого пространства позволит свободно обмениваться цифровыми товарами и услугами, что послужит укреплению связей и преодолению существующих барьеров.

В Исламской Республике Иран политика информационной безопасности выстраивается на идеях Исламской революции 1979 г. Будучи клерикальным государством, Иран выстраивает информационную политику, направленную на поддержку шиитской ветви ислама. Приоритетной областью является выработка эффективных мер по защите культурного и духовно-нравственного наследия, традиций и норм общественной жизни страны. На площадке ШОС Иран активно предлагает инициативы, направленные на защиту от зарубежного влияния и информационных войн, развитие общих стандартов информационной безопасности, а также создание совместных центров по вопросам предотвращения угроз в информационном пространстве [5, с. 23–24].

Переходя к центральноазиатским республикам, необходимо упомянуть о существующих различиях в экономическом и технологическом потенциале развития государств. Геополитическая конкуренция и имеющиеся политические, территориальные претензии отражают разный взгляд на подходы регулирования сферы информационной безопасности.

Казахстан является ведущей экономикой в Центрально-Азиатском регионе. Привлечение иностранных инвестиций способствует совершенствованию многих областей, включая развитие инноваций. Имея хорошо развитую цифровую инфраструктуру, Астана заинтересована в создании устойчивой системы информационной безопасности. Разработав ряд законов и нормативных актов, государство стремится установить собственную модель цифрового суверенитета, а также контролировать деструктивные информационные потоки, направленные на расшатывание политической ситуации в стране. К основным недостаткам можно отнести нехватку специалистов, которые способны обеспечить открытия в области информационных технологий. Казахстан на площадке ШОС выдвигает инициативу создания Центра информационной безопасности по предотвращению киберугроз. В 2023 г. в Алматы казахская сторона представила разработанный проект центра.

Особенностью политики информационной безопасности в Таджикистане является разработка институциональных механизмов и выработка нормативно-правовой базы. Для противодействия угрозе распространения экстремистских материалов правительство строго контролирует информационное пространство, включающее цензурирование иностранных материалов. В июле 2024 г., выступая на заседании Совета глав государств — членов ШОС, президент Таджикистана отметил важность координации

усилий в борьбе с распространением деструктивной идеологии. Поэтому в вопросах обеспечения информационной безопасности Таджикистан больше ориентируется на предотвращение внутренних угроз, которые обусловлены высокой активностью экстремистских группировок.

В Кыргызской Республике информационная безопасность носит фрагментарный и декларативный характер. Среди основных угроз в информационном пространстве можно выделить распространение зарубежного контента, который может негативно влиять на политические убеждения граждан.

К особенностям информационной политики в Узбекистане можно отнести достаточно свободный подход ограничений в Интернете. В стремлении стать региональным лидером, Узбекистан развивает многовекторное сотрудничество. В вопросах обеспечения информационной безопасности в рамках ШОС республика активно выдвигает свои предложения и организует научно-экспертные мероприятия. Важной инициативой является разработка Плана взаимодействия по международной информационной безопасности [3, с. 110–115, 126].

Вопросы обеспечения информационной безопасности в повестке деятельности ШОС

История переговорного процесса в рамках Шанхайской организации сотрудничества по вопросам обеспечения информационной безопасности берет начало 15 июня 2006 г. В совместном заявлении главы государств — членов ШОС впервые затронули вопросы регулирования международной информационной безопасности (МИБ)[1].

В 2009 г. было подписано основополагающее Соглашение между Правительствами государств — членов ШОС о сотрудничестве в области обеспечения МИБ, которое вступило в силу 2 июня 2011 г.[2] В Соглашении определялась терминология и отмечались основные угрозы в области обеспечения МИБ. Кроме этого, указывались основные направления сотрудничества в рамках регулирования МИБ.

Во время саммита ШОС в Уфе в июле 2015 г. было утверждено решение о проекте «Стратегии развития ШОС до 2025 года», которая определила приоритеты деятельности организации в сфере обеспечения информационной безопасности на десятилетие[3]. Стратегия подчеркивает необходимость коллективного сотрудничества в вопросах укрепления мира, обеспечения информационной безопасности, а также расширения связей с региональными и международными организациями.

Важным шагом в вопросах регулирования информационной безопасности является принятая в 2019 г. Концепция сотрудничества государств — членов ШОС в сфере цифровизации и ИКТ[4]. В качестве приоритетов развития документ закрепляет развитие информационной инфраструктуры, обеспечение безопасности данных, цифровизацию государственных структур, сотрудничество в области науки и техники, а также равенство всех членов-партнеров. Среди положительных сторон документа можно отметить стремление к международному сотрудничеству, научному обмену и равному диалогу государств — участников ШОС в вопросах политики информационной безопасности. При этом разногласия могут возникать в связи с разным уровнем развития ИКТ в государствах — членах ШОС, а также пониманием вопросов регулирования сферы информационной безопасности [12, с. 280].

Не менее важными документами регулирования региональной системы информационной безопасности являются ежегодные декларации по итогам саммитов ШОС. Исходя из основных положений, можно прийти к выводу, что приоритетами политики в области обеспечения информационной безопасности являются:

---

[1] Декларация пятилетия Шанхайской организации сотрудничества [Электронный ресурс] // Президент России. URL: https://www.mid.ru/ru/foreign_policy/rso/1679413/ (дата обращения: 16.01.2025).

[2] О вступлении в силу Соглашения между правительствами государств — членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] // Министерство иностранных дел РФ. URL: https://www.mid.ru/ru/foreign_policy/rso/1725922/ (дата обращения: 16.01.2025).

[3] Уфимская декларация глав государств-членов [Электронный ресурс] // Официальный сайт председательства Российской Федерации в Шанхайской организации сотрудничества в 2014–2015 годах. URL: https://rus.sectsco.org/files/49097/49097 (дата обращения: 16.01.2025).

[4] Бишкекская декларация Совета глав государств — членов Шанхайской организации сотрудничества [Электронный ресурс] // Президент России. URL: http://kremlin.ru/supplement/5421 (дата обращения: 16.01.2025).

- обеспечение безопасности ИКТ-структур государств ШОС;
- разработка и реализация мероприятий в области обеспечения международной информационной безопасности согласно появлению новых типов информационных угроз, признание ООН в качестве главного органа международного регулирования;
- сотрудничество государств-членов в сфере борьбы с преступными группировками, использующими ИКТ.

Особую роль в определении приоритетов деятельности организации в сфере информационной безопасности играют Российская Федерация и Китай, которые стремятся к принятию общих правил и выработке информационного суверенитета.

Заключение

Вопросы обеспечения информационной безопасности являются приоритетной сферой развития диалога в рамках Шанхайской организации сотрудничества. Анализ уровня показателей рейтинга Глобального инновационного развития продемонстрировал разный уровень технического состояния стран ШОС. Занимая лидерские позиции, Россия и Китай активно продвигают инициативы, которые направлены на международное регулирование системы информационной безопасности, предотвращение угроз в киберпространстве, а также продвижение концепции цифрового суверенитета. Наличие геополитических противоречий между Индией, Пакистаном и Китаем влечет установление сотрудничества между Пекином и Исламабадом в вопросах развития и защиты ИКТ-систем. Различия в понимании информационной безопасности в центральноазиатских республиках обусловлены разным уровнем технологического развития. Так, Казахстан, являясь лидером в регионе, стремится к обретению цифрового суверенитета и развитию международного сотрудничества, в то время как действия Таджикистана направлены на устранение внутриполитических информационных угроз.

Однако, несмотря на перечисленные противоречия, страны серьезно относятся к разработке мер по выявлению и устранению угроз в информационном пространстве. Учитывая принципы равенства и суверенитета, государства стремятся укрепить прочную дипломатическую базу для развития сотрудничества государств-членов в области обеспечения информационной безопасности.

Список литературы

1. *Выходец Р. С., Панцерев К. А.* Сравнительный анализ современных концепций информационного противоборства // Евразийская интеграция: экономика, право, политика. 2022. Т. 16. № 4 (42). С. 139–148. EDN: SVTUJU. DOI: 10.22394/2073-2929-2022-04-139-148
2. *Галушкин А. А.* К вопросу о значении понятий «национальная безопасность», «информационная безопасность», «национальная информационная безопасность» // Правозащитник. 2015. № 2. С. 8.
3. *Ибрагимова Г. Р.* Подходы государств Центральной Азии к вопросам управления Интернетом и обеспечения информационной безопасности // Индекс безопасности. 2013. Т. 19. № 1 (104). С. 103–128. EDN: PILLVN
4. *Кефели И. Ф.* Асфатроника: на пути к теории глобальной безопасности: монография. СПб. : ИПЦ СЗИУ РАНХиГС, 2020. 228 с. ISBN: 978-5-89781-676-7. EDN: JSTIQP
5. *Майорова М. А.* Информационная безопасность Исламской Республики Иран // Гуманитарные науки. Вестник Финансового университета. 2024. Т. 14. № 3. С. 20–27. EDN: GGVAWQ. DOI: 10.26794/2226-7867-2024-14-3-20-27
6. *Масленченко С. В.* Реализация концепции информационной безопасности Республики Беларусь в государственной культурной политике // Вестник Белорусского государственного университета культуры и искусств. 2023. № 4 (50). С. 5–15. EDN: PITXSM

7. *Матюхина Е. Н.* Эволюция инфраструктуры информационной и кибербезопасности Индии // СибСкрипт. 2024. Т. 26. № 3 (103). С. 441–458. EDN: RPEGEY. DOI: 10.21603/sibscript-2024-26-3-441-458
8. Международная информационная безопасность: Теория и практика: В трех томах. Т. 2: Сборник документов (на русском языке) / под общ. ред. А. В. Крутских. М. : Аспект Пресс, 2019. 784 с. ISBN: 978–5–7567–1032–8 (т. 2).
9. *Пашенцев Е. Н.* Злонамеренное использование искусственного интеллекта: новые угрозы для международной информационно-психологической безопасности и пути их нейтрализации // Государственное управление. Электронный вестник. 2019. № 76. С. 279–300. EDN: CVLXTW. DOI: 10.24411/2070-1381-2019-10013
10. *Полыхань К. О.* Проблемы и особенности состояния информационной безопасности в соответствии с доктриной информационной безопасности Российской Федерации // Устойчивое развитие науки и образования. 2019. № 5. С. 154–160.
11. *Романовский В. Г., Абубекерова Д. А.* Права человека, кибербезопасность, борьба с терроризмом (опыт Китая) // Наука. Общество. Государство. 2021. Т. 9. № 3 (35). С. 57–67. EDN: PGIKQC. DOI: 10.21685/2307-9525-2021-9-3-6
12. *Себекин С. А.* Роль Шанхайской организации сотрудничества и БРИКС в обеспечении международной информационной безопасности в условиях продолжающегося конфликта на Украине // Российско-китайские исследования. 2022. Т. 6. № 4. С. 276–287. EDN: SPOIBR. DOI: 10.17150/2587-7445.2022.6(4).276-287
13. *Чекменева Т. Г., Ершов Б. А., Трубицын С. Д., Остапенко А. А.* Стратегия Китая по обеспечению информационной безопасности: политический и технический аспекты // Бюллетень социально-экономических и гуманитарных исследований. 2020. № 7 (9). С. 78–97. EDN: KBYJRD DOI: 10.5281/zenodo.3911320
14. *Филатов О. В.* Современная структура НАТО по обеспечению информационной безопасности // Этносоциум и межнациональная культура. 2022. № 9 (171). С. 112–121. EDN: EBLJAS
15. *Шваб К.* Глобализация 4.0. Новая архитектура для четвертой промышленной революции // Евразийская интеграция: экономика, право, политика. 2019. № 1. С. 79–84. EDN: QOGCGT
16. *Шерстюк В. П.* Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения информационной безопасности // Информационное общество. 1999. № 5. С. 3–5. EDN: HRNTDF
17. *Яковлева А. В.* Правовое обеспечение кибербезопасности в Китае // Информационное право. 2021. № 2. С. 37–40. EDN: NCYMDX. DOI: 10.18572/1999-480X-2021-2-37-40
18. *Denning D.* Information Warfare and Security. New York : ACM Press. 1999. 522 p.
19. *Kremer J., Müller B.* Cyberspace and International Relations: Theory, Prospects and Challenges. Ed. 1. New York : Springer. 2014. 284 p. DOI: 10.1007/978-3-642-37481-4
20. *Pk. Mallick.* Vivekananda International Foundation [Electronic resource]. URL: https://www.researchgate.net/publication/344336074_Cyber_Attack_on_Kudankulam_Nuclear_Power_Plant_-_A_Wake_Up_Call .2019. 36 p. (accessed: 18.04.2024)
21. Russia and the United States in the Evolving World Order / ed. by A. Torkunov, N. Noonan, T. Shakleina. Moscow : MGIMO University Press. 2018. 414 p.
22. *Winterfeld S., Andress J.* The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice. Syngress, 2012. 164 p. ISBN: 978-0-12-404737-2.

Об авторе:

Щербань Анастасия Владимировна, аспирант факультета международных отношений Санкт-Петербургского государственного университета (Санкт-Петербург, Россия);
e-mail: n.shche@mail.ru

References

1. Vykhodets, R. S., Pantserev, K. A. Comparative Analysis of Modern Concepts of Information Warfare // Eurasian Integration: Economics, Law, Politics. 2022. Vol. 16. No. 4 (42). P. 139–148. (In Russ.) EDN: SVTUJU. DOI: 10.22394/2073-2929-2022-04-139-148
2. Galushkin, A. A. On the Question of the Meaning of the Concepts “National Security”, “Information Security”, “National Information Security” // Human Rights Defender. 2015. No. 2. P. 8. (In Russ.)
3. Ibragimova, G. R. Approaches of the Central Asian States to the Issues of Internet Governance and Information Security // The Security Index. 2013. Vol. 19. No. 1 (104). P. 103–128. (In Russ.) EDN: PILLVN
4. Kefeli, I. F. Asphatronics: On the Way to the Theory of Global Security. St. Petersburg, 2020. 228 p. (In Russ.)
5. Mayorova, M. A. Information Security of the Islamic Republic of Iran // Humanities. Bulletin of the Financial University. 2024. Vol. 14. No. 3. P. 20–27. (In Russ.) EDN: GGVAWQ. DOI: 10.26794/2226-7867-2024-14-3-20-27
6. Maslenchenko, S. V. Implementation of the Concept of Information Security of the Republic of Belarus in State Cultural Policy // Bulletin of the Belarusian State University of Culture and Arts. 2023. No. 4 (50). P. 5–15. (In Russ.) EDN: PITXSM
7. Matyukhina, E. N. Evolution of India’s Information and Cybersecurity Infrastructure // SibSkript. 2024. Vol. 26, No. 3 (103). P. 441–458. (In Russ.) EDN: RPEGEY. DOI: 10.21603/sibscript-2024-26-3-441-458
8. International Information Security: Theory and Practice: in 3 volumes. Vol. 2: Collection of Documents. Under the general editorship / ed. by A. V. Krutskikh. Moscow : Aspect Press, 2019. 784 p. (In Russ.)
9. Pashentsev, E. N. Malicious use of Artificial Intelligence: New Threats to International Information and Psychological Security and Ways to Neutralize Them // Public Administration. Electronic Bulletin. 2019. No. 76. P. 279–300. (In Russ.) EDN: CVLXTW. DOI: 10.24411/2070-1381-2019-10013
10. Polyhan, K. O. Problems and Features of the State of Information Security in Accordance with the Doctrine of Information Security of the Russian Federation // Sustainable Development of Science and Education. 2019. No. 5. P. 154–160. (In Russ.)
11. Romanovsky, V. G., Abubekerova, D. A. Human Rights, Cybersecurity, and the Fight Against Terrorism (China’s Experience) // Science. Society. State. 2021. Vol. 9. No. 3 (35). P. 57–67. (In Russ.) EDN: PGIKQC. DOI: 10.21685/2307-9525-2021-9-3-6
12. Sobekin, S. A. The Role of the Shanghai Cooperation Organization and BRICS in Ensuring International Information Security in the Context of the Ongoing Conflict in Ukraine // Russian-Chinese Studies. 2022. Vol. 6. No. 4. P. 276–287. (In Russ.) EDN: SPOIBR. DOI: 10.17150/2587-7445.2022.6(4).276-287
13. Chekmeneva, T. G., Ershov, B. A., Trubitsyn, S. D., Ostapenko, A. A. China’s Strategy for Ensuring Information Security: Political and Technical Aspects // Bulletin of Socio-economic and Humanitarian Studies. 2020. No. 7 (9). P. 78–97. (In Russ.) EDN: KBYJRD. DOI: 10.5281/zenodo.3911320
14. Filatov, O. V. The Modern Structure of NATO to Ensure Information Security // Ethnosocium and Interethnic Culture. 2022. No. 9 (171). P. 112–121. (In Russ.) EDN: EBLYAS
15. Schwab, K. Globalization 4.0. A New Architecture for the Fourth Industrial Revolution // Eurasian Integration: Economics, Law, Politics. 2019. No. 1. P. 79–84. (In Russ.) EDN: QOGCGT
16. Sherstyuk, V. P. Information Security in the System of Ensuring National Security of Russia, Federal and Regional Aspects of Ensuring Information Security // Information Society. 1999. No. 5. P. 3–5. (In Russ.) EDN: HRNTDF
17. Yakovleva, A. V. Legal Provision of Cybersecurity in China // Information Law. 2021. No. 2. P. 37–40. (In Russ.) EDN: NCYMDX. DOI: 10.18572/1999-480X-2021-2-37-40
18. Denning, D. Information Warfare and Security. New York : ACM Press. 1999. 522 p.
19. Kremer, J., Müller, B. Cyberspace and International Relations: Theory, Prospects and Challenges. Ed. 1. New York : Springer. 2014. 284 p. DOI: 10.1007/978-3-642-37481-4
20. Pk., Mallick. Vivekananda International Foundation URL: https://www.researchgate.net/publication/344336074_Cyber_Attack_on_Kudankulam_Nuclear_Power_Plant_-_A_Wake_Up_Call 2019. 36 p. (accessed: 18.04.2024).

21. Russia and the United States in the Evolving World Order / ed. by A. Torkunov, N. Noonan, T. Shakleina. Moscow : MGIMO University Press. 2018. 414 p.
22. Winterfeld, S., Andress J. The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice. 2012. 164 p. ISBN: 978-0-12-404737-2.

About the author:

Anastasia V. Shcherban, PhD student at the Faculty of International Relations of St. Petersburg State University (Saint Petersburg, Russia);
e-mail: n.shche@mail.ru