Известия Саратовского университета. Новая серия. Серия: Социология. Политология. 2025. Т. 25, вып. 4. С. 440–446
Izvestiya of Saratov University. Sociology. Politology, 2025, vol. 25, iss. 4, pp. 440–446
https://soziopolit.sgu.ru https://doi.org/10.18500/1818-9601-2025-25-4-440-446, EDN: UPMYMT

Научная статья
УДК 327.7

Обеспечение информационной безопасности в формате ОДКБ как региональный ответ на вызовы и угрозы в сфере ИКТ

К. Ю. Голуб[1]

Секретариат Организации Договора о коллективной безопасности, Россия, 101000, г. Москва, Сверчков пер., д. 3/2

Голуб Кирилл Юрьевич, кандидат юридических наук, начальник правового отдела, kirillgoloub@mail.ru, https://orcid.org/0009-0003-2677-6210

Аннотация. Бурное развитие информационно-коммуникационных технологий приводит к качественному и количественному увеличению новых вызовов и угроз, связанных с информационной сферой. Их трансграничный характер предопределяет продолжающееся расширение межгосударственного сотрудничества в этой сфере, в том числе и в рамках Организации Договора о коллективной безопасности. В этой связи цель работы заключается в системном рассмотрении коллективных механизмов обеспечения информационной безопасности в формате ОДКБ в контексте общемировых усилий в этой сфере. В ОДКБ осуществляется комплексное противодействие вызовам и угрозам информационной безопасности. Государства-члены вырабатывают согласованные позиции, координируют свое участие в существующих глобальных переговорных форматах, а представители Секретариата присутствуют на соответствующих международных площадках. Готовятся совместные шаги с другими региональными организациями. Политическое взаимодействие дополняется совместной практической работой правоохранительных органов и специальных служб на базе институализированных механизмов сотрудничества. Заложены правовые и организационные основы для противодействия враждебным действиям (Консультационный координационный центр по вопросам реагирования на компьютерные инциденты), проведения совместных специальных мероприятий (операция «ПРОКСИ»), борьбы с преступностью, а также подготовки кадров. Однако в современной международной обстановке нарастающие потребности обеспечения информационной безопасности требуют расширения сотрудничества за пределы существующего политического и практического взаимодействия. По мере готовности государств представляются актуальными выработка коллективных мер и координация их сотрудничества на основе концепции когнитивной безопасности.

Ключевые слова: ОДКБ, ИКТ, МИБ, РГОС, информационная безопасность, операция «ПРОКСИ», когнитивная безопасность

Для цитирования: *Голуб К. Ю.* Обеспечение информационной безопасности в формате ОДКБ как региональный ответ на вызовы и угрозы в сфере ИКТ // Известия Саратовского университета. Новая серия. Серия: Социология. Политология. 2025. Т. 25, вып. 4. С. 440–446. https://doi.org/10.18500/1818-9601-2025-25-4-440-446, EDN: UPMYMT

Article

Ensuring information security within the CSTO framework as a regional response to the IT related challenges and threats

K. Yu. Golub

The Collective Security Treaty Organization Secretariat, 3/2 Sverchkov pereulok, Moscow 101000, Russia

Kirill Yu. Golub, kirillgoloub@mail.ru, https://orcid.org/0009-0003-2677-6210

Abstract. The rapid development of information technology leads to qualitative and quantitative increase in new challenges and threats related to the information domain. Their transboundary nature predetermines the ongoing expansion of international cooperation in this area, including activities within the Collective Security Treaty Organization. In this regard, the work objective is to make a systemic study of the collective mechanisms for ensuring information security in the framework of the CSTO in the context of global efforts in this area. The CSTO implements a comprehensive response to challenges and threats to information security. Member states develop agreed positions, coordinate their participation in existing global negotiation formats. The CSTO Secretariat staff representatives are present at relevant international venues. Joint steps are being prepared with other regional organizations. Political interaction is complemented by joint practical work of law enforcement agencies and special services based on institutionalized cooperation mechanisms. The legal and organizational foundations have been laid for countering hostile cyber actions (Consultative Coordination Center for Response to Computer Incidents), conducting joint

[1] Статья отражает личное мнение автора и не является официальной позицией Организации Договора о коллективной безопасности или ее органов.

special operation (“PROKSI”), combating crime, and training personnel. However, in the current international situation, the growing needs for ensuring information security require expanding cooperation beyond current political and practical interaction. As states become ready, it seems relevant to develop collective measures and coordinate international cooperation based on the concept of cognitive security.
Keywords: CSTO, IT, IIS, OEWG, information security, PROKSI operation, cognitive security

For citation: Golub K. Yu. Ensuring information security within the CSTO framework as a regional response to the IT related challenges and threats. *Izvestiya of Saratov University. Sociology. Politology,* 2025, vol. 25, iss. 4, pp. 440–446 (in Russian). https://doi.org/10.18500/1818-9601-2025-25-4-440-446, EDN: UPMYMT

Последние десятилетия ознаменовались бурным развитием информационно-коммуникационных технологий (далее – ИКТ), которые глубоко укоренились в повседневной жизни значительной части человечества. Их широкое распространение закономерно привело к качественному и количественному увеличению вызовов и угроз в информационной сфере. В зависимости от их характера задачи по обеспечению информационной безопасности стоят перед широким спектром субъектов: от отдельных граждан и организаций до государств и их объединений.

Закономерным образом указанная проблематика становится предметом сотрудничества и в формате Организации Договора о коллективной безопасности (далее – ОДКБ или Организация). С 2012 г. взаимодействие государств-членов в сфере информационной безопасности является одной из ее уставных задач. В ОДКБ выстроена и постоянно совершенствуется система механизмов противодействия вызовам и угрозам в области информационной безопасности. В этой связи рассмотрение проблем и перспектив становления коллективных механизмов обеспечения информационной безопасности Организации представляется весьма актуальным. Тем не менее, несмотря на большой массив публикаций о деятельности Организации, значительная часть мероприятий ОДКБ и ее органов на этом направлении не получает должного научного изучения, которое и предполагается в известной мере развить настоящей работой. Ее цель заключается в системном рассмотрении коллективных механизмов обеспечения информационной безопасности в формате ОДКБ в контексте общемировых усилий в данной сфере. Для этого предполагается прежде всего рассмотреть предпринятые Организацией политические шаги по обеспечению международной информационной безопасности, проанализировать практические меры ОДКБ по парированию вызовов и угроз в сфере ИКТ и обозначить дальнейшие усилия Организации на этом направлении.

В основу работы положен структурно-функциональный метод, позволяющий определить цели, задачи и позиции субъектов взаимодействия в сфере обеспечения информационной безопасности. Системный подход используется для того, чтобы оценить потенциал ОДКБ в противодействии вызовам и угрозам информационной безопасности и подчеркнуть взаимосвязь созданных механизмов в рамках системы коллективной безопасности.

В соответствии со Стратегией коллективной безопасности ОДКБ на период до 2025 года (далее – Стратегия)[2] формирование безопасного информационного пространства государств-членов ОДКБ является одной из стратегических задач Организации в сфере противодействия транснациональным вызовам и угрозам. Для решения указанной задачи, равно как и других, определенных руководящими установками ОДКБ, Организация реализует комплекс мероприятий, из которых в соответствии с принципами Устава ОДКБ приоритет отдается политическим средствам.

При этом нужно отметить, что подходы ОДКБ следуют за сложившимся русскоязычным словоупотреблением, в котором термин «информационный» и термины с приставкой «кибер-» несут в себе содержательные оттенки смысла. Как отмечает С. А. Себекин, в то время как западная приставка «кибер-» подразумевает под собой сугубо технические аспекты воздействия (в отношении конкретных устройств, систем, сетей, технологических процессов, цифровой инфраструктуры), термин российского происхождения «информационный»

[2] Решение Совета коллективной безопасности ОДКБ от 14 октября 2016 г. «О Стратегии коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года» // Документы по вопросам формирования и функционирования системы коллективной безопасности государств-членов Организации Договора о коллективной безопасности (далее – «Документы…»). Вып. 17. М., 2017. С. 153.

носит амбивалентный характер: под ним понимаются как информационно-технические, так и информационно-психологические воздействия [1, с. 171].

Практические мероприятия по укреплению межведомственной координации в сфере обеспечения информационной безопасности, проведение совместных мероприятий по противодействию и нейтрализации противоправной деятельности в информационно-телекоммуникационном пространстве государств-членов ОДКБ основываются на обсуждении и выработке согласованных правил взаимодействия в информационной сфере, их продвижении на глобальном уровне[3].

Такие общие для государств-членов ОДКБ нормы закреплены в Соглашении о сотрудничестве государств-членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г. (далее – Соглашение), которое является основополагающим международно-правовым документом, определяющим термины, принципы и направления совместной работы государств-членов ОДКБ в этой сфере[4].

Принципиальным аспектом, зафиксированным в Соглашении, является указание в его преамбуле на приоритетность государственного суверенитета в вопросах обеспечения информационной безопасности. На этом подходе базируется коренное отличие согласованных действий государств-членов ОДКБ от политики руководства западных стран по размыванию государственных суверенитетов, нашедших свое выражение, например, в Глобальном цифровом договоре[5], в котором проводится линия на вовлечение в вопросы регулирования информационной сферы «частного сектора, гражданского общества, международных организаций, технических и научных кругов и всех других заинтересованных сторон»[6].

Другие узловые для государств-членов ОДКБ элементы политики обеспечения информационной безопасности и глобального регулирования информационного пространства изложены в цикле заявлений министров иностранных дел государств-членов ОДКБ,[7] в которых последовательно отстаивается несколько общих подходов.

Во-первых, с точки зрения государств-членов ОДКБ, информационно-коммуникационные технологии не должны применяться для вмешательства во внутренние дела суверенных государств и осуществления любых посягательств на территориальную целостность, государственный суверенитет и независимость государств.

Во-вторых, поддерживается деятельность Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 (далее – РГОС) в качестве единого межгосударственного переговорного механизма под эгидой ООН по данной тематике.

В-третьих, государства-члены ОДКБ выступают за выработку и принятие универсального международно-правового инструмента, регулирующего поведение государств в информационном пространстве в соответствии с общепризнанными принципами и нормами международного права.

В-четвертых, подчеркивается важность развития взаимодействия по тематике между-

[3] Документы... Вып. 17. М., 2017. С. 158.

[4] Соглашение о сотрудничестве государств-членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г. // Документы… Вып 18. М., 2018. С. 84.

[5] Резолюция Генеральной Ассамблеи ООН. Пакт во имя будущего. 22 сентября 2024 г. A/RES/79/1 // Секретариат ООН. URL: https://documents.un.org/doc/undoc/gen/n24/272/24/pdf/n2427224.pdf (дата обращения: 28.10.2024).

[6] Интервью заместителя министра иностранных дел Российской Федерации С. В. Вершинина газете «Комсомольская правда» // МИД России. 23.09.2024. URL: https://www.mid.ru/ru/foreign_policy/news/1970834/ (дата обращения: 28.10.2024).

[7] Заявление министров иностранных дел государств-членов Организации Договора о коллективной безопасности о совместных мерах по обеспечению информационной безопасности от 17 июля 2017 г. // Документы… Вып. 18. М., 2018. С. 9–10 ; Заявление министров иностранных дел государств-членов Организации Договора о коллективной безопасности о координации совместных усилий в сфере информационной безопасности, включая противодействие использованию информационно-коммуникационных технологий в террористических и иных преступных целях от 15 сентября 2021 г. // Документы… Вып. 22. М., 2021. С. 47–48 ; Совместное заявление министров иностранных дел государств-членов Организации Договора о коллективной безопасности об активизации сотрудничества в области обеспечения международной информационной безопасности от 23 ноября 2022 г. // Документы… Вып. 23. М., 2022. С. 53–54 ; Заявление министров иностранных дел государств-членов Организации Договора о коллективной безопасности о расширении сотрудничества в области международной информационной безопасности от 21 июня 2024 г. // Организация Договора о коллективной безопасности. 24.06.2024. URL: https://odkb-csto.org/news/news_odkb/zayavlenie-ministrov-nostrannykh-delgosudarstv-chlenov-organizatsii-dogovora-o-kollektivnoy-bezopa/ (дата обращения: 28.10.2024).

народной информационной безопасности в рамках международных и региональных организаций.

Наличие общих, выработанных в рамках Организации, подходов позволяет государствам-членам занимать на площадке ООН согласованные позиции, становиться соавторами соответствующих резолюций [2, с. 85], а представителям Секретариата ОДКБ участвовать в мероприятиях РГОС, проводя линию, выработанную государствами-членами ОДКБ[8].

В целях углубления политического сотрудничества государств-членов ОДКБ в сфере международной информационной безопасности по инициативе Российской Федерации в 2023 г. утвержден перечень дополнительных мер государств-членов ОДКБ, направленных на обеспечение информационной безопасности[9]. Они предусматривают продолжение взаимных консультаций по проблематике обеспечения международной информационной безопасности в различных международных форматах, первый раунд которых состоялся 11 октября 2024 г. в Москве. Участники консультаций обменялись оценками современных вызовов в сфере информационной безопасности в зоне ответственности Организации и подходами к противодействию им, включая развертывание новых низкоорбитальных спутниковых систем интернет-связи[10].

В качестве следующих мер в указанный Перечень включены изучение возможностей гармонизации национальных режимов правового регулирования в области международной информационной безопасности, дальнейшее содействие выработке под эгидой ООН юридических обязывающих правил, норм и принципов ответственного поведения государств в информационном пространстве, а также запуск консультаций с внешними партнерами по вопросам международной информационной безопасности. К внешним партнерам, прежде всего, следует отнести Шанхайскую организацию сотрудничества и Содружество Независимых Государств, одним из направлений сотрудничества с которыми определено обеспечение информационной безопасности[11].

С точки зрения организации практического взаимодействия государств-членов ОДКБ в сфере обеспечения информационной безопасности в Соглашении определены три основные угрозы информационной безопасности государств-членов ОДКБ.

Во-первых, к ним отнесено деструктивное информационное воздействие, в которое вкладывается максимально широкое содержание – любое использование информационно-коммуникационных технологий в целях нарушения деятельности органов власти, ослабления национальной безопасности, нанесения ущерба информационно-коммуникационным системам, сетям и ресурсам, критически важным и другим структурам, ухудшения межгосударственных отношений, создания внутренней социально-политической напряженности, разрушения традиционных духовных и нравственных ценностей, установления контроля над национальными информационными ресурсами, формирования угрозы возникновения чрезвычайных ситуаций, причинения иного ущерба национальным интересам государств-членов ОДКБ.

Во-вторых, аналогичным образом рассматривается использование информационно-коммуникационных технологий террористическими и экстремистскими организациями, организованными преступными группами (сообществами). В-третьих, таким же статусом квалифицировано осуществление противоправной деятельности с использованием информационно-коммуникационных технологий (см. ст. 3 Соглашения).

[8] Выступление заместителя Генерального секретаря ОДКБ В. Семерикова на неформальной межсессионной встрече Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий // Организация Договора о коллективной безопасности. 7.12.2022. URL: https://odkb-csto.org/news/news_odkb/vystuplenie-zamestitelya-generalnogo-sekretarya-odkb-valeriya-semerikova-na-neformalnoy-mezhsessionn/?sphrase_id=137765 (дата обращения: 28.10.2024).

[9] Решение Совета министров иностранных дел и Комитета секретарей советов безопасности ОДКБ от 22 ноября 2023 г. «О Перечне дополнительных мер государств-членов Организации Договора о коллективной безопасности, направленных на обеспечение информационной безопасности Организации Договора о коллективной безопасности» // Документы… Вып. 24. М., 2023. С. 49–51.

[10] О мероприятиях, посвященных обсуждению вопросов в сфере международной информационной безопасности в рамках ОДКБ // Организация Договора о коллективной безопасности. 14.10.2024. URL: https://odkb-csto.org/news/news_odkb/o-meropriyatiyakh-posvyashchennykh-obsuzhdeniyu-voprosov-v-sfere-mezhdunarodnoy-informatsionnoy-bezo/ (дата обращения: 28.10.2024).

[11] Решение Совета коллективной безопасности ОДКБ от 23 ноября 2022 г. «О намерениях развивать сотрудничество Организации Договора о коллективной безопасности с Содружеством Независимых Государств и Шанхайской организацией сотрудничества» // Документы… Вып. 23. М., 2022. С. 95–99.

Практическим средством противодействия указанным угрозам стал комплекс мероприятий, направленных на противодействие преступлениям в сфере и с применением информационных технологий, который проводится в формате ОДКБ с 2008 г. под условным наименованием «операция «ПРОКСИ» (акроним от «ПРОтиводействие Криминалу в Сети Интернет»). С 2014 г. операции придан статус постоянного действия[12].

С 2008 по 2023 г. операция «ПРОКСИ» проведена 14 раз. За эти годы выявлено более 500 тыс. информационных ресурсов, направленных на разжигание национальной и религиозной розни, наносящих политический ущерб национальным и союзническим интересам, распространяющих идеи террористической и экстремистской направленности в интересах преступных групп, совершения различных преступлений в сфере информационных технологий.

При этом была приостановлена деятельность более 210 тыс. информационных ресурсов, выявлено более 630 тыс. фактов, свидетельствующих о совершении преступлений, и возбуждено более 400 тыс. уголовных дел[13].

Формальной основой для практического взаимодействия национальных уполномоченных органов служит Протокол о взаимодействии государств-членов ОДКБ по противодействию преступной деятельности в информационной сфере[14] (далее – Протокол), который регламентирует порядок и сроки обмена соответствующей информацией, а также процедуры направления и рассмотрения обращений о необходимости оказания содействия.

Помимо защиты информационного пространства государств-членов ОДКБ от деструктивного информационного воздействия, Протоколом предусматривается взаимодействие по признакам преступлений против основ конституционного строя и безопасности государства, против мира и безопасности, а также в сфере информационных технологий.

По мнению некоторых исследователей, например Н. О. Мороз, Протокол имеет целый ряд недостатков, обусловленных, в первую очередь, тем, что в его основу были заложены преимущественно положения Соглашения о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации, многие из которых нуждаются в совершенствовании как в силу неточностей содержательного характера, так и несоответствия современным потребностям международного сотрудничества компетентных органов в деле противодействия противоправному использованию информационных технологий [3, с. 81]. Не отвергая принципиальной необходимости постоянного совершенствования нормативной правовой основы для сотрудничества государств-членов ОДКБ, полагаем, что вопрос ее модернизации целесообразно рассматривать после подписания и вступления в силу Конвенции ООН против киберпреступности; укрепления международного сотрудничества в борьбе с преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимся к серьезным преступлениям (далее – Конвенция).

В рамках существующих механизмов защита критической информационной инфраструктуры в каждом из государств-членов ОДКБ осуществляется создаваемой и развиваемой национальной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы. Основным коллегиальным органом взаимодействия государств-членов ОДКБ в этой сфере является созданный в 2014 г. Консультационный координационный центр государств-членов ОДКБ по вопросам реагирования на компьютерные инциденты (далее – ККЦ).

Из числа задач, возложенных на ККЦ в целях координации взаимодействия нацио-

[12] Решение Совета коллективной безопасности ОДКБ от 23 декабря 2014 г. «О Положении об операции постоянного действия государств-членов Организации Договора о коллективной безопасности по противодействию преступлениям в сфере информационных технологий (операция “ПРОКСИ”)» // Документы… Вып. 15. М., 2015. С. 140–146.

[13] *Кузнецов А. В.* Система международной информационной безопасности. Коллективные усилия государств-членов ОДКБ по формированию региональной и национальной безопасности в сфере использования информационно-коммуникационных технологий. 21 августа 2023 г. // Текущий архив Секретариата ОДКБ.

[14] Протокол о взаимодействии государств-членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере от 23 декабря 2014 г. // Документы… Вып. 15. М., 2015. С. 63–68.

нальных уполномоченных органов по вопросам компьютерных инцидентов, следует выделить две ключевые. Во-первых, сбор и обмен информацией по компьютерным инцидентам между национальными уполномоченными органами, а также анализ угроз в данной сфере для государств-членов ОДКБ. Во-вторых, через ККЦ организуется оказание взаимной помощи в решении организационных, технических и нормативно-правовых вопросов, связанных с предотвращением компьютерных атак и чрезвычайных ситуаций, оперативным реагированием на них и ликвидацией последствий компьютерных инцидентов[15].

Третьим аспектом функционирования системы обеспечения информационной безопасности в формате ОДКБ, помимо рассмотренных выше политического сотрудничества государств-членов ОДКБ в сфере международной информационной безопасности и практического взаимодействия их уполномоченных органов, является недопустимость использования существующей информационной инфраструктуры для распространения информации, представляющей угрозу безопасности, что вытекает из рассмотренной выше всеобъемлющей трактовки деструктивного информационного воздействия.

В качестве угрозы национальной и коллективной безопасности государства-члены ОДКБ квалифицировали использование современных ИКТ для пропаганды нетерпимости на расовой, этнической и религиозной почве, идеологии экстремистских и террористических организаций, в том числе с целью вербовки рекрутов, а также деструктивного идеологического и морально-психологического воздействия с целью искажения нравственно-ценностных ориентиров молодежи[16]. Такое деструктивное информационное воздействие может оказываться через электронные информационные сети и медиаресурсы в форме манипулирования общественным сознанием в целях воздействия на общественно-политическую и социально-экономическую обстановку (см. п. 3.2 Стратегии).

Для координации соответствующих усилий создана рабочая группа при Комитете секретарей советов безопасности ОДКБ по вопросам информационной политики и информационной безопасности. В практику Организации введено планирование совместных шагов в этой сфере. В 2011 г. согласован План первоочередных мероприятий по формированию основ скоординированной информационной политики в интересах государств-членов ОДКБ[17] до 2015 г., в 2018 г. – План мероприятий по развитию скоординированной информационной политики в интересах государств-членов ОДКБ до 2025 г.[18]

При этом следует признать, что указанные документы во многом носят формальный характер. На практике общие мероприятия включают обмен опытом в сфере противодействия угрозам в информационной сфере и пресечение пропаганды идей, разжигающих те или иные виды розни, различных форм содействия террористической деятельности и незаконному обороту наркотиков.

Представляется, что соответствующая сфера сотрудничества требует наращивания привлекаемого инструментария. Как отмечает А. И. Возженников, для противодействия внешнему информационно-психологическому воздействию необходимо привлечение как информационно-коммуникационных, так и информационно-идеологических средств. По его мнению, приоритетное значение имеет определение целевой международной аудитории для деятельности в форме превентивных или просветительских акций и мероприятий [4, с. 141].

В этом смысле требует осмысления опыт последнего десятилетия, связанный с влиянием, прежде всего, социальных сетей

[15] См.: Решение Совета коллективной безопасности ОДКБ от 23 декабря 2014 г. «О Консультационном координационном центре Организации Договора о коллективной безопасности по вопросам реагирования на компьютерные инциденты» // Документы… Вып. 15. М., 2015. С. 147–152.

[16] См.: Заявление министров иностранных дел государств-членов Организации Договора о коллективной безопасности о совместных мерах по обеспечению информационной безопасности от 17 июля 2017 г.

[17] Решение Совета коллективной безопасности ОДКБ от 20 декабря 2011 г. «О Плане первоочередных мероприятий по формированию основ скоординированной информационной политики в интересах государств-членов Организации Договора о коллективной безопасности» // Документы… Вып. 12. М., 2012. С. 156–157.

[18] Решение Совета коллективной безопасности ОДКБ от 8 ноября 2018 г. «О Плане мероприятий по развитию скоординированной информационной политики в интересах государств-членов Организации Договора о коллективной безопасности» // Документы… Вып. 19. М., 2018. С. 164–170.

на сохранение социальной стабильности в экстремальных условиях (включая события «Арабской весны» и пандемию коронавируса). Значительный потенциал видится в дальнейшей разработке концепции когнитивной безопасности с выходом на предложения по координации межгосударственного сотрудничества в этой сфере [5, с. 295].

Вместе с тем задача выработки коллективных идеологических и когнитивных средств противодействия в международном информационном противостоянии не видится решаемой в среднесрочной перспективе. С учетом наметившегося прорыва в создании международно-правовой основы для межгосударственного сотрудничества в форме Конвенции решение информационно-технических вопросов обеспечения информационной безопасности в среднесрочной перспективе превратится в рутину, в значительной степени лишенную нынешней остроты политического противостояния. В таких условиях особую роль приобретет информационно-психологическая сторона информационной безопасности, которая в условиях отсутствия просматривающихся возможностей по ее правовой регламентации может превратиться в бескомпромиссную битву нарративов противоборствующих государств и их объединений.

В этих рамках управление информационной сферой в целях реализации национальной информационной политики становится критически важным элементом национального суверенитета. От государств потребуется особая готовность к объединению усилий для сотрудничества в этой сфере.

Таким образом, Организация Договора о коллективной безопасности является востребованным инструментов ее государств-членов по координации усилий в сфере обеспечения национальной и коллективной информационной безопасности. Поскольку в соответствии с Уставом ОДКБ в достижении своих целей Организация отдает приоритет политическим средствам, для решения соответствующих задач соединяются мероприятия как политического, так и практического характера. При этом подход ОДКБ к обеспечению информационной безопасности основывается на многоаспектном ее понимании и включает в себя не только согласование политических подходов к регулированию соответствующих вопросов на глобальном уровне и обеспечение технической стороны информационной безопасности, но и недопустимость использования существующей информационной инфраструктуры для распространения информации, представляющей угрозу безопасности. Вместе с тем противодействие злоупотреблению возможностями информационной инфраструктуры требует выработки и внедрения новых коллективных методов межгосударственного взаимодействия, в том числе наращивания координации национальных информационных политик.

Список литературы

1. *Себекин С. А.* Система международной информационной безопасности в условиях политической турбулентности // Вестник Санкт-Петербургского университета. Международные отношения. 2023. Т. 16, вып. 2. С. 170–190. https://doi.org/10.21638/spbu06.2023.205, EDN: JQHKPU
2. *Бойко С. М.* Международная информационная безопасность: Россия в ООН. Начало нового этапа (2020–2021 гг.) // Международная жизнь. 2024. № 6. С. 82–99. EDN: DQDQEO
3. *Мороз Н. О.* Особенности участия Республики Беларусь в международном сотрудничестве в сфере обеспечения информационной безопасности // Вестник Марийского государственного университета. Серия: Исторические науки. Юридические науки. 2017. № 2 (10). С. 79–84. EDN: ZEWNPF
4. *Возженников А. В.* Современные приоритеты политики защиты информационного пространства ОДКБ // Вестник ОрелГИЭТ. 2020. № 4 (54). С. 139–141. https://doi.org/10.36683/2076-5347-2020-4-54-139-141, EDN: PROIKV
5. Информационно-психологическая и когнитивная безопасность / под ред. И. Ф. Кефели, Р. М. Юсупова. СПб. : Петрополис, 2017. 300 с. EDN: TGFHSZ

Поступила в редакцию 20.01.2025; одобрена после рецензирования 05.09.2025; принята к публикации 17.09.2025
The article was submitted 20.01.2025; approved after reviewing 05.09.2025; accepted for publication 17.09.2025