

ОДКБ – платформа по кибербезопасности

Противодействие использованию ИКТ в террористических целях

Виталий ФИЛИПОВИЧ

Стремительное развитие и распространение новейших цифровых средств коммуникации всё отчетливее определяет современную картину глобального мира, в котором наряду с благами научно-технического прогресса серьезно повышается уровень угроз, обусловленных лавинообразным распространением информационно-коммуникационных технологий (ИКТ) и систем искусственного интеллекта (ИИ) как их разновидности.

Множащиеся угрозы их неконтролируемого использования, в том числе в террористических и иных преступных целях, подрывают устойчивость действующих международных институтов, трансформируют ландшафт международных отношений. Современные террористические сообщества применяют ИКТ для:

- организации терактов;
- привлечения и вербовки новых сторонников;
- финансирования противоправной деятельности;
- распространения экстремистской идеологии, особенно среди молодого поколения как наиболее уязвимой части общества;
- подстрекательства граждан совершать теракты и диверсии;
- распространения ложных сообщений об актах терроризма в целях дестабилизации ситуации, насаждения страха.

Зачастую довольно сложно отделить факты использования информационных систем в террористических целях от их применения в

ФИЛИПОВИЧ Виталий Любомирович – аспирант Дипломатической академии МГИМО МИД России. E-mail: vlfilipovich@yandex.ru

Ключевые слова: ОДКБ, терроризм, ИКТ, ИИ, международное сотрудничество, безопасность.

иных преступных деяниях. Нередко террористические акты, задевающие ИКТ, маскируются под менее опасные киберпреступления¹. Масштабы и изощрённость транснациональной киберпреступности сегодня подрывает не только основы национального суверенитета и доверия между отдельными мировыми акторами, но и безопасности человечества в целом².

Распространение терроризма в современном мире обусловлено рядом факторов, которые имеют прямое отношение к внутренним проблемам государств (политическим, экономическим, межконфессиональным). Но вместе с тем крайне негативную роль играют и транснациональные угрозы, единые для всего мирового сообщества.

Усилению экстремистских тенденций способствует расширение региональных и международных конфликтов, формирующих социальную среду преступности. Прямым следствием таких конфликтов становится формирование крупных террористических центров с развитой инфраструктурой, их слияние с организованной преступностью транснационального характера³. Значительно возрастает и масштаб бедствий, причинённых ими: расширение географии терроризма, количества террористических актов и пострадавших от них лиц.

Одновременно с «классическими» способами террористических действий (взрывами, поджогами, применением взрывчатых веществ и горючих смесей кустарного производства) экстремисты всё чаще задействуют высокотехнологичное оборудование, включая ИКТ, которым свойственны автономность и возможность удалённого управления.

Так, Украина, например, при проведении террористических атак на российскую инфраструктуру активно применяет современные беспилотные летательные аппараты (БПЛА), нередко с ИИ, обладающие большим поражающим эффектом и представляющие реальную угрозу для гражданского населения.

Для оперативного обмена информацией, подготовки и совершения терактов применяются передовые ИКТ, включая американскую спутниковую систему *Starlink*⁴. В целях радикализации отдельных слоёв населения и координации действий при совершении терактов задействуются технологические возможности интернет-мессенджеров, как правило, располагающих функцией кодирования сообщений, социальных сетей и коммуникативных интернет-площадок.

На поток поставлено создание биодронов – людей, которых украинские кураторы используют для совершения преступлений диверсионной направленности. Они становятся дешёвым оружием киевского террора в российском тылу.

¹ Информационно-коммуникационные технологии для глобального мира / под общ. ред. О.А. Мельниковой; рук. проекта А.В. Крутских. М.: Аспект Пресс, 2024. С. 328.

² *Штоль В.В., Задохин А.Г.* Информационно-коммуникационные технологии и информационная безопасность России // Обозреватель—Observer. 2022. № 5–6. С. 66.

³ Концепция противодействия терроризму в Российской Федерации (утв. Президентом Российской Федерации 05.10.2009) // URL: https://rg.ru/documents/2009/10/20/zakon-dok.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F

⁴ Доклад Министерства иностранных дел Российской Федерации «О совершении киевским режимом преступлений террористической направленности» // URL: https://www.mid.ru/ru/foreign_policy/doklady/1969025/

Российская Федерация рассматривает терроризм, в том числе международный, как одну из самых серьёзных угроз миру и безопасности. Опираясь на собственный опыт, признаёт, что эффективная борьба с киберпреступностью возможна только усилиями всего международного сообщества. По этой причине Россия ведёт последовательную работу в рамках ООН по продвижению идеи согласования и принятия универсальных юридически обязывающих договорённостей в области противодействия терроризму и другим деструктивным действиям с использованием ИКТ, призывает все страны объединить усилия для отпора этому злу.

По инициативе Российской Федерации вопросы минимизации угроз от использования ИКТ в террористических акциях прошли обсуждение в Специальном комитете ООН (создан в 2019 г.) для разработки всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях (Спецкомитет). Внесённый Россией в Спецкомитет (июль 2021 г.) проект Конвенции ООН содержал варианты криминализации преступлений, связанных с террористической и экстремистской деятельностью. Однако из-за активного противодействия западных стран – регламентирующих деятельность Организации в сфере обеспечения информационной безопасности традиционных противников обсуж-

дения темы терроризма на площадке ООН – эти статьи не вошли в итоговый текст Конвенции ООН против киберпреступности*.

В настоящее время многие акторы мирового сообщества признают необходимость расширения и укрепления сотрудничества в области противодействия использованию ИКТ в террористических и иных преступных целях. Тот факт, что многие государства сегодня подписываются под соглашениями, ориентированными на борьбу с ИКТ-преступностью, свидетельствует о приоритете совместных усилий по организации борьбы с международным терроризмом и экстремизмом с сохранением координирующей роли ООН, на основе международного права, без политизации и двойных стандартов.

Попытки выработать на глобальном уровне, прежде всего в рамках ООН, универсальные юридически обязывающие нормы, пресекающие противоправное использование ИКТ, систематически блокируются. Обусловлено это глубокой политизацией вопроса, отсутствием доверия между основными геополитическими игроками и в значительной степени тем, что государства демонстрируют существенную разницу в подходах к регулированию ИКТ.

Так, если страны Евросоюза в целом ориентированы на защиту пользователей, то США предпочитают сохранять свободу распространения ИИ, тогда как Россия, страны Глобального Юга и Востока делают ставку на государственное регулирование⁵.

⁵ Салунов А. Почему искусственный интеллект вызывает споры: возможности, риски и мнение экспертов // URL: https://rg.ru/2025/08/22/pochemu-iskusstvennyj-intellekt-vyzyvaet-spyry-vozmozhnostiriski-i-mnenie-ekspertov.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F

* Документ был утверждён Генеральной Ассамблеей ООН 24 декабря 2024 г. и подписан 25–26 октября 2025 г. в Ханое (Вьетнам). Сегодня к нему присоединились 76 участников (75 государств и Евросоюз).

В этих условиях переговоры сменяются с выработки универсального договора в сторону более прагматичных, хотя и ограниченных по охвату, региональных форматов. На этом фоне усилия таких региональных структур, как СНГ, ОДКБ или ШОС, имеют ряд конкурентных преимуществ:

- более высокую степень доверия между участниками;
- упрощённые процедуры согласования решений;
- возможность оперативного реагирования на угрозы без необходимости преодолевать сопротивление других акторов.

Иными словами, в условиях современного геополитического противостояния и в ситуации, в которой универсальные институты оказываются не всегда способными адекватно реагировать на возникающие вызовы, решение задач по регулированию и организации противодействия киберугрозам берут на себя региональные структуры.

В этой связи важен опыт институциональной и практической деятельности по противодействию использованию ИКТ в террористических и иных преступных целях, который накоплен ОДКБ.

Свою историю Организация Договора о коллективной безопасности (ОДКБ) ведёт с 15 мая 1992 г., когда в Ташкенте (Узбекистан) главы шести государств – Армении, Казахстана, Киргизии, России, Таджикистана и Узбекистана – подписали Договор о коллективной безопасности. В сентябре 1993 г. к объедине-

нию присоединился Азербайджан, а в декабре того же года – Грузия и Белоруссия.

Первоначально планировалось, что на постсоветских просторах организация будет выполнять функции военно-политического союза.

В апреле 1999 г. Протокол о продлении Договора подписали шесть государств (кроме Азербайджана, Грузии и Узбекистана), а тремя годами позже, 14 мая 2002 г., Совет коллективной безопасности принял решение о придании Договору статуса международной региональной организации⁶.

7 октября 2002 г. на саммите СНГ в Кишинёве был утверждён Устав ОДКБ. В Секретариате ООН он был зарегистрирован в декабре 2003 г., годом позже получил статус наблюдателя в Генеральной Ассамблее ООН. Соответственно, юридическое оформление статуса ОДКБ как международной региональной организации, обеспечивающей коллективную безопасность своих членов на постсоветском пространстве, было завершено⁷.

На сегодняшний день ОДКБ представляет собой военный союз, членами которого являются Республика Беларусь, Республика Казахстан, Киргизская Республика, Российская Федерация и Республика Таджикистан. Узбекистан, возобновивший членство в 2006 г., вновь приостановил его в 2012-м, а в 2024 г. своё членство фактически приостановила Армения.

Одним из ключевых принципов, на которых основано членство в ОДКБ, является коллективная оборона. Кроме военной защиты к зада-

⁶ История. От Договора к Организации // URL: <https://odkb-csto.org/30-let-odkb/istoriya/>

⁷ Там же.

чам организации относится противодействие использованию ИКТ в преступных целях – терроризму, наркотрафику, другим угрозам безопасности в регионе. В этих целях ОДКБ проводит совместные учения и координирует действия своих участников в кризисных ситуациях.

В соответствии с Уставом ОДКБ координация совместных действий возложена на её постоянно действующие рабочие и вспомогательные органы, высшим из которых является Совет коллективной безопасности (СКБ)⁸. В его состав входят главы государств-членов. Совет рассматривает стратегические вопросы деятельности ОДКБ, принимает необходимые решения и координирует совместную работу стран-членов по достижению целей организации.

Консультативно-исполнительную функцию выполняют Совет министров иностранных дел (СМИД), Совет министров обороны (СМО) и Комитет секретарей советов безопасности (КССБ).

Постоянно действующими рабочими органами ОДКБ выступают Секретариат и Объединённый штаб (действует с января 2004 г.).

Последовательно отстаивая интересы государств-членов, ОДКБ начала активно заниматься вопросами обеспечения международной информационной безопасности (МИБ) в конце 2006 г. Тогда была учреждена Рабочая группа по вопросам информационной политики и информационной безопасности.

Важной вехой на этом пути стало создание в декабре 2014 г. Консультационного координационного центра ОДКБ по вопросам реагирования на компьютерные инциденты (ККЦ). Его задача – координировать взаимодействие уполномоченных органов при возникновении компьютерных инцидентов, создающих угрозу функционированию информационно-телекоммуникационных сетей и информационных систем любого из государств – членов ОДКБ⁹.

ККЦ находится в подчинении Комитета секретарей советов безопасности (КССБ) ОДКБ.

За прошедшие десятилетия было принято более 20 соглашений, регламентирующих деятельность ОДКБ в сфере МИБ.

Наиболее значительным среди них является Соглашение о сотрудничестве государств – членов ОДКБ в области обеспечения информационной безопасности от 30 ноября 2017 г. (Минск, Белоруссия). Для Российской Федерации этот документ вступил в силу 17 апреля 2019 г.

В Соглашении оговариваются следующие направления совместной деятельности стран:

- совершенствование механизмов противодействия информационным угрозам;
- организация совместных (в том числе практических) мероприятий по укреплению информационной безопасности и борьбе с противоправной деятельностью в информационном пространстве государств-членов;
- взаимодействие по вопросам обеспечения МИБ;
- содействие разработке и принятию под эгидой ООН универсальных правил, норм и принципов ответственного поведения государств в информационном пространстве;
- взаимная помощь в развитии технологической базы.

Наряду с этим в Соглашении зафиксированы основные угрозы информационной безопасности:

- деструктивное информационное воздействие на государства – члены ОДКБ и организацию в целом;
- использование ИКТ террористическими и экстремистскими организациями, а также организованными преступными группами;
- противоправная деятельность с применением ИКТ.

⁸ История. От Договора к Организации.

⁹ Организация Договора о коллективной безопасности (справка) // URL: https://www.mid.ru/ru/foreign_policy/integracionnye-struktury-prostranstva-sng/1710399/

Следует подчеркнуть, что формирование ККЦ и принятие в рамках организации собственного Соглашения по информационной безопасности означает, что с 2017 г. ОДКБ фактически создала важный региональный механизм по вопросам МИБ.

Государства – члены ОДКБ, демонстрируя приверженность совместным действиям по формированию системы информационной безопасности и выполняя договорённости о недопущении использования ИКТ для дестабилизации обстановки на их территориях, в 2019 г. подписали Протокол о взаимодействии по противодействию преступной деятельности в информационной сфере (для России он вступил в силу 17 апреля 2019 г.).

Согласно этому документу страны ОДКБ обязались совместно обеспечивать защиту информационного пространства от деструктивного влияния и противодействовать использованию национальных сегментов сети Интернет в целях, запрещенных национальным законодательством. Взаимодействие осуществляется, в частности, в отношении деяний, совершаемых с применением ИКТ и признаваемых национальным правом преступными.

К ним относятся преступления против:

- основ конституционного строя и безопасности государства;
- мира и безопасности человечества, а также преступления в сфере информационных технологий.

В число последних входят:

- разжигание национальной и религиозной розни;
- деятельность террористических и экстремистских преступных групп;
- незаконный оборот наркотиков;
- незаконная миграция и торговля людьми;
- мошенничество;
- создание, распространение и использование вредоносных программ, а также изготовление и распространение детской порнографии;
- нарушение авторских и лицензионных прав;
- финансирование терроризма, наркоторговли и легализация преступных доходов;
- иные виды преступлений (пропаганда суицида, непристойные действия и др.);
- распространение контрафакта, рекламы товаров и услуг, которые могут причинить вред жизни и здоровью человека;
- сбыт специальных технических средств;
- использование информационных технологий в целях совершения противоправных действий в отношении государственных объектов информационно-коммуникационной инфраструктуры и электронных информационных ресурсов, в том числе разглашение государственной тайны и иных видов тайн¹⁰.

Одним из основных направлений сотрудничества в сфере МИБ в рамках ОДКБ является расширение мер доверия, сопровождаемое развитием технологий и отработкой практических механизмов реагирования на киберугрозы. Быстрыми темпами осуществляется формирование международно-правовой базы этой деятельности.

Так, в 2020 г. на Парламентской ассамблее ОДКБ была одобрена Концепция противодействия киберугрозам и разработаны рекомендации по выработке общих принципов в сфере развития искусственного интеллекта и робототехники.

¹⁰ Протокол о взаимодействии государств – членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере // URL: <https://docs.cntd.ru/document/561354812>

В декабре 2021 г. по инициативе России было озвучено Совместное заявление глав МИД ОДКБ «О профилактике и борьбе с использованием Интернета в террористических целях».

В ноябре 2023 г. решением СМИД и КССБ ОДКБ утверждён Перечень дополнительных мер государств – членов ОДКБ по обеспечению информационной безопасности; в 2022, 2024 и 2025 гг. принимались совместные заявления министров иностранных дел по вопросам МИБ.

Систематически ОДКБ реализует практические мероприятия по противодействию преступности в сфере информационных технологий в формате операции ПРОКСИ (противодействие криминалу в сфере информации). Основная цель проводимых мероприятий состоит в том, чтобы совместными усилиями предотвращать и пресекать использование национальных сегментов ИКТ-инфраструктуры для организации деяний, запрещённых законодательством государств-членов. В рамках сотрудничества осуществляется взаимодействие по выявлению и расследованию преступлений, совершаемых с применением ИКТ.

В рамках ОДКБ развивается и аналитическая деятельность по исследованию ИКТ-угроз. В частности, в Стратегии коллективной безопасности ОДКБ на период до 2025 г. к основным факторам, их порождающим, отнесены:

– стремление отдельных акторов добиваться стратегических целей с

применением силы (в том числе посредством информационного давления);

– использование ИКТ для деструктивного воздействия на общественно-политическую и социально-экономическую обстановку, манипулирование общественным мнением, а также применение так называемых комплексных или гибридных цифровых технологий¹¹.

Совместными усилиями государств – членов ОДКБ в рамках ООН были возобновлены переговоры по проблематике МИБ.

Эта работа ведётся в формате Группы правительственных экспертов ООН (ГПЭ) и Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ (РГОС), в каждую из которых входили эксперты от стран ОДКБ.

Цель переговоров – выработка правил, норм и принципов ответственного поведения государств в информационном пространстве¹².

Очередным этапом обсуждения всех аспектов МИБ стала работа Всемирного механизма по достижениям в области ИКТ, который призван содействовать ответственному поведению государств в информационной сфере и который будет действовать на постоянной основе. Его организационная сессия состоялась 30–31 марта 2026 г. в Нью-Йорке.

Таким образом, в рамках ОДКБ последовательно осуществляется

¹¹ Стратегия коллективной безопасности организации договора о коллективной безопасности на период до 2025 г. от 18 октября 2016 г. (утв. Решением Совета коллективной безопасности ОДКБ от 14 октября 2016 г. «О Стратегии коллективной безопасности организации договора о коллективной безопасности на период до 2025 г.») // URL: https://odkb-csto.org/documents/statements/strategiya_kollektivnoy_bezопасnosti_organizatsii_dogovora_o_kollektivnoy_bezопасnosti_na_period_do_/#loaded

¹² Жуковская Н.Ю., Калинина Е.В., Радолин А.М. Формирование правовых основ обеспечения международной информационной безопасности в формате ООН: этапы и результаты // Международное право и международные организации. 2024. № 4. С. 76. 74-86.

процесс, направленный на укрепление сотрудничества государств-членов в сфере информационной безопасности. При этом стратегической задачей является разработка юридически обязывающих инструментов обеспечения МИБ.

В контексте анализа эффективности деятельности ОДКБ в сфере предотвращения угроз кибертерроризма остаётся крайне актуальной задача дальнейшего укрепления практического сотрудничества и совершенствования деятельности профильных подразделений национальных органов государственной безопасности и внутренних дел, а также активизации совместной деятельности государств – членов ОДКБ по предотвращению актов кибертерроризма. В этой связи весьма важным представляется подписанный Секретариатом ОДКБ и фондом развития кибербезопасности «Сайберус» (апрель 2025 г.) меморандум о сотрудничестве, направленный на повышение уровня киберзащиты в государствах – членах ОДКБ. Документ предусматривает:

- совместную работу в области противодействия киберугрозам;
- обмен передовыми технологиями защиты критически важных объектов;
- подготовку квалифицированных кадров в сфере кибербезопасности;
- содействие совершенствованию законодательства в области информационной безопасности.

В июне 2025 г. в Киргизии (г. Чолпон-Ата) при участии делега-

ций всех государств – членов ОДКБ, а также представители СНГ и ШОС, состоялась первая Международная конференция ОДКБ по кибербезопасности, где, в частности, обсуждались вопросы противодействия и профилактики преступлений, совершаемых с использованием ИКТ.

Особое внимание было уделено приоритетам в сфере противодействия угрозам в информационном пространстве. Отмечено, что такие явления, как кибертерроризм и информационные войны, подрывают национальную безопасность государств, являются причиной возникновения международных конфликтов.

Все принятые в ходе конференции решения легли в основу выработки общей политики, направленной на обеспечение кибербезопасности в государствах ОДКБ. Акцент был сделан, в частности, на недопустимости использования ИКТ для вмешательства во внутренние дела суверенных государств и дестабилизации социально-политической обстановки в них. В то же время при обсуждении основных направлений взаимодействия участники форума отметили необходимость согласования вопросов функционирования низкоорбитальных спутниковых систем интернет-связи, эксплуатация которых должна осуществляться с учётом национальных интересов и безопасности государств¹³.

Одним из важнейших элементов укрепления регионального сотрудничества является гармонизация национального законодательства государств – членов ОДКБ, что обеспе-

¹³ Заявление министров иностранных дел государств – членов Организации Договора о коллективной безопасности о международной информационной безопасности. 30.06.2025 // URL: https://www.mid.ru/ru/foreign_policy/integracionnye-struktury-prostranstva-sng/2033300/

чивает единообразную правовую основу для согласованных действий в военно-политической сфере. В условиях внешнего давления сближение правовых систем государств становится залогом обеспечения суверенитета и безопасности участников, создания единого правового пространства для оперативного реагирования на кризисные ситуации, унификации процедур использования сил и средств коллективной безопасности.

Основную роль в гармонизации законодательства государств-членов играет уставной орган межпарламентского сотрудничества – Парламентская Ассамблея ОДКБ (ПА ОДКБ), которую образуют парламентские делегации государств-членов.

ПА ОДКБ принимает модельные законодательные акты, направленные на регулирование отношений в зоне ответственности ОДКБ. Цель этой деятельности состоит в том, чтобы обеспечить соответствие, законодательства государств-членов положениям международных договоров, заключённых партнёрами в рамках ОДКБ*. В настоящее время ведётся активная работа по адаптации правовых систем к современным вызовам, включая вопросы:

- обеспечения информационной безопасности;
- реализации соглашений, направленных на защиту информационного пространства;
- унификацию законов в сфере противодействия терроризму и экстремизму (в том числе – противоправному использованию ИКТ).

Программа ПА ОДКБ на ближайшие пять лет предполагает разработку 45 модельных актов, в том числе направленных на совершенствование законодательства в области кризисного реагирования и укрепление информационной безопасности, защиту электоральных процессов¹⁴. Реализация подобной стратегии осуществляться с учётом стоящей перед организацией задачи укрепления блоковой координации, повышения степени доверия внутри ОДКБ и создания единого контура кибербезопасности. В частности, для непрерывного обмена данными о цифровых угрозах уровень доверия и политической солидарности между странами-участницами должен быть беспрецедентно высоким.

Таким образом, нормативная система противодействия использованию ИКТ в террористических и иных преступных целях, разработанная к настоящему времени в рамках ОДКБ, является одной из наиболее основательных региональных систем подобной направленности. В то же время невозможность распространения установленных правил на государства, которые не являются членами ОДКБ и которые зачастую становятся источником угроз, том числе в сфере использования ИКТ, требует постоянного и пристального реагирования со стороны государств – членов организации.

Одновременно укрепление партнёрских отношений с внешними субъектами актуально для эффективной борьбы с имеющими транс-

¹⁴ Страны ОДКБ будут работать над укреплением информационной безопасности // Парламентская газета. 20.04.2026 // URL: <https://www.pnp.ru/politics/strany-odkb-budut-rabotat-nad-ukrepleniem-informacionnoy-bezopasnosti.html>

* Действующая программа деятельности по сближению национальных законодательств на 2026–2030 гг. включает 11 проектов модельных законов и рекомендаций.

национальный характер терроризмом, экстремизмом и преступностью с использованием ИКТ. В этом контексте крайне важно, что в рамках первой Международной конференции ОДКБ по кибербезопасности (2025 г.) члены организации вновь обратились к мировому сообществу с призывом выработать универсальные, юридически обязывающие механизмы обеспечения МИБ, включая предотвращение и урегулирование межгосударственных конфликтов, продолжить предметные дискуссии по этому вопросу в рамках ООН¹⁵.

Рост киберугроз и совершенствование взятых на вооружение террористами цифровых инструментов, с одной стороны, существенно повышает для ОДКБ значение совместных способов реагирования, а с другой – делает крайне актуальной задачу быстрой и своевременной выработки коллективного ответа на новые вызовы.

С 1 января 2026 г. в ОДКБ председательствует Российская Федерация. Определяя приоритеты российского председательства, которое проходит под девизом «Коллективная безопасность в многополярном мире»¹⁶, непосредственно в сфере борьбы с кибертерроризмом президент России В.В. Путин указал следующие задачи:

- разработку новой антитеррористической стратегии ОДКБ;
- более тесную координацию деятельности спецслужб стран-членов;

- совместную подготовку подразделений;

- работу по выявлению террористических ячеек и пресечению каналов их финансирования.

В числе приоритетных направлений деятельности президент России выделил обеспечение информационной безопасности, в том числе противодействие распространению радикальных идей, особенно в молодёжной среде, и защиту общего информационного пространства стран ОДКБ¹⁷. В данном контексте предусматривается обмен опытом и лучшими практиками в сфере противодействия отмыванию доходов, полученных преступным путём, анализ влияния новых технологий на борьбу с финансированием терроризма и экстремизма¹⁸, противодействие угрозе использования ИКТ в экстремистских целях.

Принимая во внимание множасьщиеся вызовы и угрозы безопасности, активизация сотрудничества в сфере МИБ предполагает:

- дальнейшую координацию по вопросам совершенствования международно-правовой основы в области обеспечения информационной безопасности, регулирования в сфере ИИ;

- укрепление взаимодействия национальных компетентных органов;

- обмен передовым опытом, обучение, подготовка, переподготовка, повышение квалификации специалистов.

¹⁵ Роль ОДКБ в противодействии терроризму. 02.10.2023 // URL: https://odkb-csto.org/analytics/?ELEMENT_ID=22538#loaded

¹⁶ Приоритеты председательства Российской Федерации в Организации Договора о коллективной безопасности. 09.12.2025 // URL: https://odkb-csto.org/priorities_rf/?ELEMENT_ID=24449#loaded

¹⁷ Саммит ОДКБ: от киберугроз до боевой готовности – что обсуждают главы государств // Onliner. 27.11.2025 // URL: <https://people.onliner.by/2025/11/27/sammit-odkb?ysclid=mj75klrznt27679954>

¹⁸ Там же.

Таким образом, российское председательство в ОДКБ субстантивно и практически обеспечивает сотрудничество государств-членов во всех сферах их взаимодействия и достойно подводит организацию к её предстоящим юбилеям, которые будут отмечаться в 2027 г.: 25-летию Организации Договора о коллективной безопасности и 35-летию подписания Договора о коллективной безопасности.

Предпринимаемые меры в совокупности будут способствовать реальному повышению эффективности усилий государств-членов в сфере информационной безопасности и противодействия угрозам использования ИКТ в террористических и иных преступных целях.

Библиография

- Жуковская Н.Ю., Калинина Е.В., Радолин А.М.* Формирование правовых основ обеспечения международной информационной безопасности в формате ООН: этапы и результаты // *Международное право и международные организации*. 2024. № 4. С. 74-86.
- Информационно-коммуникационные технологии для глобального мира* / под общ. ред. О.А. Мельниковой; рук. проекта А.В. Крутских. М.: Аспект Пресс, 2024. – 542 с.
- История. От Договора к Организации* // URL: <https://odkb-csto.org/30-let-odkb/istoriya/>
- Концепция противодействия терроризму в Российской Федерации* (утв. Президентом Российской Федерации 05.10.2009) // URL: https://rg.ru/documents/2009/10/20/zakon-dok.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F
- Протокол о взаимодействии государств – членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере* // URL: <https://docs.cntd.ru/document/561354812>
- Стратегия коллективной безопасности организации договора о коллективной безопасности на период до 2025 г. от 18 октября 2016 г.* (утв. Решением Совета коллективной безопасности ОДКБ от 14 октября 2016 г. «О Стратегии коллективной безопасности организации договора о коллективной безопасности на период до 2025 г.») // URL: https://odkb-csto.org/documents/statements/strategiya_kollektivnoy_bezопасnosti_organizatsii_dogovora_o_kollektivnoy_bezопасnosti_na_period_do_/#loaded
- Штоль В.В., Задохин А.Г.* Информационно-коммуникационные технологии и информационная безопасность России // *Обозреватель—Observer*. 2022. № 5-6. С. 66-78.

Статья поступила в редакцию 14 мая 2026 г.

Статья принята к публикации 20 мая 2026 г.