

КОНЦЕПТУАЛЬНАЯ ЗАПИСКА

Почему Россия последовательно выступает за включение в конвенцию положений о противодействии использованию информационно-коммуникационных технологий (ИКТ) в террористических и экстремистских целях?

В большинстве случаев дела о терроризме на национальном уровне в той или иной степени связаны с использованием злоумышленниками Интернета. Однако национальное законодательство многих развивающихся стран, в отличие от развитых (Австралия, Великобритания, государства-члены Европейского союза, США, Новая Зеландия и др.), в этой области не достаточно продвинуто. Поэтому компетентные органы таких государств в целях привлечения к ответственности террористов применяют содержащиеся в их уголовных кодексах статьи о других преступлениях. Это не позволяет адекватно бороться с текущими угрозами.

Террористические группировки переводят работу в «Интернете» на качественно новый уровень. В частности, ИГИЛ в своей структуре использовало мощный медиахолдинг, производящий широкий перечень мультимедийной продукции: агитационные видеоролики, фильмы, аудиозаписи проповедей, электронные версии журналов, буклетов, постеров и т. д. В этих целях террористическая организация задействовала собственные интернет-ресурсы, а также многочисленные аккаунты в наиболее популярных социальных сетях (*Facebook, YouTube, Instagram* и др.).

Активно используют Интернет-ресурсы и для организации и подготовки терактов. Так, во Франции в 2015 и 2016 гг. прошла серия терактов, координация которых осуществлялась через мессенджер «Телеграм». Аналогичные случаи имели место в Индонезии и в Швеции в 2017 г.

Подготовка и координация терактов, в частности, в Индонезии в 2021 г., Турции в 2022 г., в России в 2023 г. также осуществлялась преимущественно посредством использования информационно-коммуникационных технологий.

Важной тенденцией является все более частое использование террористами для финансирования своей деятельности криптовалют, разнообразных «электронных кошельков», мобильного банкинга, краудфандинга. Все это значительно усложняет задачу по перекрытию каналов финансирования террористических группировок. При этом специалисты выделяют такой способ финансирования террористов в Интернете, как создание подставных благотворительных организаций для сбора пожертвований.

Важной площадкой для террористических организаций становятся онлайн-игры и индустрия Интернет-развлечений (экстремисты используют их для продвижения своей идеологии и вербовки уязвимых лиц).

Остро также стоит проблема сбора и хранения электронных доказательств совершения преступлений террористического характера. Правоохранительные органы большинства государств, прежде всего развивающихся, испытывают нехватку квалифицированных кадров, которые могли бы не только выявлять, но и вести расследование преступлений террористических группировок в информационном пространстве. Далеко не все действия террористов можно подвести под статьи законодательства либо получить необходимые доказательства из других государств. Часто такие запросы не могут быть исполнены, потому что этого не позволяет сделать местное законодательство либо данные уже удалены.

Эксперты обращают особое внимание на разработку террористами своих образцов искусственного интеллекта (создано несколько аналогов чат-бота ChatGPT, где отсутствовали ограничения на генерацию контента).

В этой связи государства приступили к разработке документов и механизмов по противодействию террористической деятельности в информационном пространстве на глобальном и региональном уровнях. Резолюция ГА ООН 74/247 о необходимости разработки всеобъемлющей конвенции, инициированная Россией, получила широкую поддержку государств-членов ООН. Задача — представить в ходе 78 сессии ГА ООН такой

документ, который бы обеспечивал эффективное международное правоохранительное сотрудничество в области противодействия использованию ИКТ в преступных целях.

Глобальный уровень

В резолюции Совета Безопасности **ООН 1617 (2005)** государства-члены выразили озабоченность по поводу того, что террористические организации, а также их сообщники используют различные средства массовой информации, включая Интернет, в том числе для террористической пропаганды и подстрекательства к террористическому насилию.

В резолюции Совета Безопасности **ООН 1624 (2005)** государства-члены признают важное значение того, чтобы государства совместно принимали меры к тому, чтобы террористы не могли использовать современную технологию, коммуникации и ресурсы для подстрекательства к поддержке преступных деяний.

В резолюции Совета Безопасности **ООН 2161 (2014)** выражается озабоченность по поводу того, что в глобализованном обществе террористы и их сторонники все шире используют новые информационно-коммуникационные технологии, в частности Интернет, для содействия террористическим актам, а также используют эти технологии в целях подстрекательства, вербовки, финансирования или планирования террористических актов.

В резолюции Совета Безопасности **ООН 2178 (2014)** государства-члены выражают озабоченность по поводу активизации использования террористами и их сторонниками коммуникационных технологий для целей доведения радикализации до уровня, порождающего терроризм, вербовки и подстрекательства других к совершению террористических актов, в том числе с использованием Интернета. Подчеркивается необходимость совместных действий государств-членов, направленных на недопущение использования террористами технологий, средств коммуникации и ресурсов для мобилизации

поддержки террористических актов. Осуждается насильственный экстремизм, который может стать питательной средой для терроризма.

К тому же в документе прямо прописан призыв государствам-членам сотрудничать при принятии национальных мер, призванных воспрепятствовать использованию террористами технологий, средств связи и ресурсов для подстрекательства к поддержке террористических актов.

Резолюция Совета Безопасности ООН **2354 (2017)** возлагает главную ответственность за противодействие террористическим актам и насильственному экстремизму, порождающему терроризм на государства-члены. В ней подчеркивается, что терроризм можно победить только при последовательном и комплексном подходе, предполагающем активное участие и сотрудничество всех государств и международных и региональных организаций с целью блокировать, ослабить, изолировать и обезвредить террористическую угрозу. Отмечается также, что террористы формируют искаженные идеи, которые основываются на неверном толковании и представлении в ложном свете религии с целью оправдать насилие и используются для вербовки сторонников и иностранных боевиков-террористов, мобилизации ресурсов и получения поддержки от сочувствующих им лиц, в частности за счет использования информационно-коммуникационных технологий, в том числе через «Интернет» и социальные сети.

В резолюции Генеральной Ассамблеи ООН **77/298 (2023)** подтверждается обязанность государств-членов предотвращать и пресекать финансирование террористических актов, воздерживаться от оказания любой формы активной или пассивной поддержки организациям или лицам, причастным к террористическим актам, в том числе путем пресечения вербовки членов террористических групп, и установить уголовную ответственность за умышленное предоставление или сбор любыми методами, прямо или косвенно, финансовых средств с намерением, чтобы они использовались (или при осознании того, что они будут использованы) полностью или частично для

совершения террористического акта, и выражается озабоченность по поводу злонамеренного использования Интернета и других информационно-коммуникационных технологий, включая виртуальные активы, мобильные платежные системы и краудфандинг, и иных форм финансирования терроризма.

В этом же документе отмечается озабоченность использованием Интернета и других информационно-коммуникационных технологий, включая платформы социальных сетей, в террористических целях, включая непрерывающееся распространение террористического контента, и рекомендуя государствам-членам работать друг с другом.

Региональный уровень

СНГ

В Стратегии обеспечения информационной безопасности государств-участников СНГ 2019 г. зафиксирована необходимость формирования механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в противоправных и террористических целях, а также повышение эффективности международного сотрудничества в области противодействия информационной преступности и информационному терроризму.

В Соглашении о сотрудничестве государств-участников СНГ 2018 г. в борьбе с преступлениями в сфере информационных технологий предусмотрено обязательство сторон признавать в соответствии с национальным законодательством в качестве уголовно наказуемого деяния, если оно совершено умышленно, распространение с использованием информационно-телекоммуникационной сети "Интернет" или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма.

ОБСЕ

В ОБСЕ накоплен солидный массив политических обязательств в контексте борьбы с терроризмом, в частности, содержащихся в решении Совета министров № 3/04 о борьбе с использованием Интернета в террористических целях, решении Совета министров № 7/06 о противодействии использованию Интернета в террористических целях и решении Совета министров № 5/07 о государственно-частном партнерстве в борьбе с терроризмом.

В Совместном заявлении министров иностранных дел Армении, Белоруссии, Казахстана, Кыргызстана, России и Таджикистана «О профилактике и борьбе с использованием Интернета в террористических целях» на 28-м заседании СМВД ОБСЕ (Стокгольм, 2 декабря 2021 г.) выражается серьезная озабоченность в связи с растущим использованием Интернета в террористических целях, включая прямые трансляции террористических нападений. Отмечается, что для вербовки новых сторонников и иностранных террористов-боевиков, мобилизации ресурсов используются информационно-коммуникационные технологии, в том числе Интернет и социальные сети. Выражается озабоченность распространением, в том числе через Интернет, языка ненависти и идей, подстрекающих к насилию и питающих терроризм.

АСЕАН

В рамках Регионального форума АСЕАН по безопасности (АРФ) в 2019 г. принято Заявление о противодействии терроризму и насильственному экстремизму, способствующему терроризму. В нем выражается обеспокоенность тем, что террористы продолжают использовать информационно-коммуникационные технологии (ИКТ), в частности Интернет и социальные сети, в террористических целях, в том числе для совершения, подстрекательства, радикализации и вербовки, финансирования или планирования террористических актов. Документ также призывает участников АРФ обратить внимание на онлайн-платформы с целью способствовать

принятию усилий ими по предотвращению потоковой передачи, загрузки или повторной загрузки террористического контента и контента, связанного с терроризмом и экстремизмом.

Таким образом, вышеизложенные документы универсального и регионального характера наглядно демонстрируют необходимость регламентации механизма противодействия использованию информационно-коммуникационных технологий в террористических и экстремистских целях в тексте разрабатываемой конвенции. Только детальное правовое регулирование данного вопроса позволит государствам-участникам осуществлять эффективное международное сотрудничество в борьбе с преступлениями террористической и экстремистской направленности.