DOI 10.35775/PSI.2024.109.9.009
УДК 32

З.Е. АБДУРАГИМОВ
соискатель Департамента политологии
Финансового университета при Правительстве РФ,
Россия, г. Москва

«МЯГКИЕ» ПОЛИТИЧЕСКИЕ ТЕХНОЛОГИИ ПО ПРОФИЛАКТИКЕ И ПРОТИВОДЕЙСТВИЮ ТЕРРОРИЗМУ

Статья посвящена актуальной на сегодняшний день проблеме противодействия международному терроризму посредством политических технологий. Исследование раскрывает содержание понятий «профилактика терроризма», «экстремизм», «радикализация», «мягкая сила»; также в нем представлены типологии терроризма и различные способы его предотвращения.

Выделяются и описываются характерные особенности новых механизмов взаимодействия террористических групп в киберпространстве с использованием перспективных технологий и платформ социальных сетей. Особое внимание уделяется предотвращению радикализации в социальных сетях и Интернете в эпоху цифровых технологий, рассматриваются соответствующие методы и подходы, которые террористы используют для распространения своей пропаганды и вербовки в Интернете.

Рассмотрены существующие международные инструменты и механизмы для выявления и предотвращения финансирования терроризма, а также описаны и проанализированы роли органов, участвующих в противодействии данного вида преступлений. Значительное внимание уделяется понятию «мягкая сила» в контексте политических технологий и методов.

Данная статья представляет собой попытку проанализировать роль дипломатии, как важного и незаменимого инструмента в борьбе против терроризма.

Ключевые слова: *политические технологии, международный терроризм, противодействие, «мягкая сила», радикализация, экстремизм, дипломатия, финансирование терроризма.*

В эпоху глобализации и цифровизации, помимо трансформационных изменений, происходит ряд более мелких преобразований и более тонких тенденций, каждая из которых может радикально изменить возможности и успехи мировых государств в продолжающейся войне с терроризмом. Эти изменения, от растущей известности террористических манифестов до доминирования одиночных субъектов и конвергенции экстремистских идеологий, вероятно, будут усиливаться в течение следующего десятилетия, создавая новые проблемы и препятствия для разведывательных и правоохранительных органов, которым поручено

противодействовать этому весьма динамичному и развивающемуся виду преступлений [9. С. 80].

Стирание различий между внутренним и международным терроризмом повлияет на существующее разделение между внешней и внутренней разведкой, разведкой и правоохранительными органами, а также на то, как правительство организует реагирование на такие пересекающиеся угрозы. В мире, который становится все более сетевым, связанным социальными и цифровыми сетями, любое практическое различие между внутренним и международным терроризмом полностью исчезает.

Экстремистские движения, которые традиционно были сосредоточены на местных проблемах, парадоксальным образом становятся все более интернациональными.

Следует подчеркнуть, что в работах российских и зарубежных авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [1; 5; 6; 8; 10; 11; 16; 18; 21; 22; 23; 24; 25].

Однако проблему искоренения экстремизма и терроризма в контексте применения политических технологий нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

Необходимость в профилактике и искоренения мирового терроризма не нуждается в обосновании, так как доминирующий подход в борьбе с терроризмом, основанный в основном на жестких военных действиях, как мы можем видеть, например, на Ближнем Востоке, потерпел неудачу. Статистика показывает, что большинство террористических группировок не только не прерывают свою преступную деятельность, встретив военный отпор со стороны государства, но и приумножают радикальные настроения внутри своих незаконных образований. Поэтому при анализе данной проблематики следует отслеживать и учитывать, как качественные изменения в террористическом сообществе, так и факторы, способствующие вербовке новых «рекрутов».

Традиционный военный инструмент сдерживания не работает против противников, которые в большинстве случаев не имеют фиксированной территориальной базы, а обезглавливание террористических организаций путем убийства их лидеров приводит к росту желающих отомстить, и в результате для многих стран «лекарство» от военизированной борьбы с терроризмом оказывается хуже, чем сама «болезнь» терроризма [17. С. 208-210].

Современные террористические группы представляют собой поколение, активно использующее Всемирную Сеть, поэтому неудивительно, что онлайн-платформы становятся все более эффективными инструментами пропаганды, подстрекательства, запугивания и радикализации гораздо более обширной и ранее недоступной аудитории.

Не вызывает сомнения тот факт, что, в связи с меняющимся характером и огромным разнообразием онлайн-платформ, а также широтой используемых

методов применения, современным исследователям и аналитикам необходимо применять более широкий подход при изучении деятельности террористов в киберпространстве. С ростом технологических преобразований для политиков ведущих государств разумно более пристально взглянуть на возникающее влияние технологий как инструментов для предотвращения террористических движений и помощи в защите сообществ от опасностей экстремизма во всем мире [19. С. 217].

Террористические организации представляют собой динамичные системы, которые адаптируются и развиваются с течением времени. Несмотря на это, на сегодняшний день существует ряд «мягких» законодательных и политических мер для решения этой проблемы, в том числе: блокировка онлайн-контента и доступа; фильтрация и удаление контента; расширение прав и возможностей онлайн-сообществ для противодействия нарративам насильственного экстремизма и терроризма; продвижение позитивных и альтернативных посланий; а также повышение цифровой устойчивости и медиаграмотности населения [20. С. 15-17].

Нужно отметить, что часть законодательных мер ориентирована на контроль за тем, как частный пользователь должен предотвращать террористический контент на своих платформах. Эти механизмы взаимосвязаны, поскольку законодательство о цифровой профилактике может быть адаптировано и изменено только по мере появления новых технологических инструментов в сфере профилактики.

При этом существует множество проблем, связанных с законодательством и политическими методами предотвращения распространения террористического контента в Интернете. При принятии решений иногда возникает неправильное понимание того, как работают интернет-компании и компании, занимающиеся социальными сетями, и какие новые технологии доступны на сегодняшний день.

Еще меньше известно о том, как модерировать или регулировать эти платформы для предотвращения террористического контента в Интернете. В этом отношении обеспечение того, чтобы правительства и частный сектор работали вместе и в партнерстве, является еще более важным фактором для профилактики мирового терроризма.

Другими словами, отсутствуют доказательства того, что предлагаемые инструменты действительно эффективны для успешного предотвращения распространения террористического контента, а последствия такого агрессивного удаления могут привести к непреднамеренным нарушениям прав человека (например, ограничению свободы слова), если те методы не доказали свою эффективность или действенность.

Один из «мягких» подходов к предотвращению онлайн-терроризма, предпринятый рядом правительств, заключался в блокировании доступа террористических группировок к Интернету и каналам социальных сетей. Это варьировалось

от блокировки отдельных веб-сайтов и страниц в социальных сетях до блокировки целых платформ социальных сетей [20. С. 15].

Например, после пасхальных атак 2019 года на церкви, отели и популярные туристические объекты в Шри-Ланке правительство временно заблокировало весь доступ к популярным соцсетям и мессенджерам. Это временно ограничило каналы связи перед лицом непосредственной угрозы новых нападений по всей стране, но также ограничило цифровые возможности жителей Шри-Ланки, эмигрантов и туристов. Аналогичным образом, Индонезия также заблокировала популярное приложение социальных сетей Telegram в 2017 году после растущей обеспокоенности по поводу влияния ИГИЛ в регионе и использования Telegram, в частности, для распространения своих сообщений по частным каналам [13. С. 73].

Можно сделать вывод о том, что, с одной стороны, блокировка веб-сайтов, страниц в социальных сетях и целых платформ социальных сетей замедляет распространение террористических сообщений в Интернете, она также замедляет работу обычных каналов связи для остального населения. То есть, хотя временная блокировка доступа к контенту может быть эффективной в краткосрочных кризисных ситуациях, таких как последствия многоплановых атак джихадистов в Шри-Ланке, долгосрочная блокировка в конечном итоге вынудит как террористические группы, так и население в целом искать альтернативные формы общения.

Таким образом, если WhatsApp будет заблокирован в одной стране, его место, скорее всего, займет другое приложение с аналогичными функциями, а население и террористы вновь получат возможность общаться.

В этом отношении правительствам, возможно, придется рассмотреть возможность сочетания своих усилий по блокировке веб-сайтов с обеспечением основных прав человека в соответствии с международным правом.

Важно упомянуть об еще одном способе предупреждения распространения контента террористической направленности в Сети – удаление отдельных публикаций или веб-сайтов самими технологическими компаниями или третьими лицами. Это можно сделать несколькими способами: запросы государственных органов на удаление частей контента; саморегулирование технологических компаний по удалению контента; искусственный интеллект, такой как «фильтры загрузки»; посредством отдельных хакеров и удаления контента по инициативе гражданского общества.

Нужно подчеркнуть, что особенностью мягких политических технологий является то, что они сосредоточены, прежде всего, на профилактике криминализации финансирования терроризма, установлении международных норм по противодействию терроризма и предоставлении технической помощи странам для выполнения этих рекомендаций на многосторонних встречах и конференциях.

В этой связи инициативы по противодействию финансированию терроризма в некоторой степени направлены на обеспечение так называемой

«промежуточной» профилактики, например, ограничение финансирования террористической группы снижает риск того, что группа или организация смогут подготовить террористическую кампанию. Действия террористических групп ограничены из-за нехватки средств или отсутствия возможности перемещать, хранить, управлять или скрывать эти средства [20. С. 45].

Терроризм является прямой асимметричной угрозой безопасности граждан всего мира, а также международной стабильности и процветанию. Терроризм, как постоянная глобальная проблема, не знающая границ, национальности и религии, является задачей, которую международное сообщество должно решать сообща [7. С. 399].

Развитие потенциала и работа над инновационными технологиями являются частью основной деятельности НАТО, а методы борьбы с асимметричными угрозами, включая терроризм и использование нетрадиционных вооружений, имеют особое значение. Большая часть этой работы проводится в рамках программы работы по защите от терроризма, которая способствует развитию возможностей защиты сил НАТО, гражданского населения и территории от нападений террористов, в том числе с использованием беспилотников и самодельных взрывных устройств [14. С. 441-442]. Большинство проектов в рамках программы направлены на поиск решений, которые можно применить в краткосрочной перспективе и которые отвечают военным потребностям альянса.

Как было сказано ранее, современные террористы стали использовать и манипулировать различными технологиями в своих операциях, в том числе легкодоступными технологиями. В частности, в качестве угрозы были признаны дроны, в связи с чем в феврале 2019 года министры обороны стран НАТО согласовали практические рамки противодействия беспилотным авиационным системам. Новая программа работы по координации подходов и определению дополнительных шагов по устранению этой угрозы была согласована в 2023 году и в настоящее время успешно реализуется.

Точно также реализуется политика в отношении биометрических данных, она является особенно актуальной для защиты сил и угроз от иностранных террористических группировок.

Мягкие политические технологии в области гражданской готовности, защиты критически важных объектов инфраструктуры и кризисного регулирования предоставляет ресурс, который по запросу может служить как союзникам, так и партнерам. Эта область может быть напрямую связана с борьбой с терроризмом, повышением устойчивости и обеспечением надлежащего планирования и подготовки к реагированию на террористические акты и восстановлению после них [12. С. 420].

Политики всех стран, занимающиеся проблемами терроризма, должны активно сотрудничать и быть в постоянном диалоге с учеными и экспертами, тем самым способствуя лучшему пониманию террористической угрозы, разработке мер по обнаружению и реагированию, а также развитию сети экспертов. Мероприятия, координируемые программой, включают семинары, учебные

курсы и многолетние проекты исследований и разработок, которые способствуют определению методов защиты критически важной инфраструктуры, материалов и персонала; технологии обнаружения взрывных устройств и незаконной деятельности; а также управление рисками, передовой опыт и использование новых технологий в ответ на терроризм [9. С. 78].

Приоритет жесткой силы, которая включает в себя применение силы, по сравнению с мягкой силой, препятствует возможности граждан и организаций гражданского общества участвовать в укреплении своих сообществ. Тактика мягкой силы, такая как расширение прав и возможностей граждан и сообществ, должна быть признана важным инструментом в установлении стабильности и предотвращении насильственного экстремизма. Эффективный обмен информацией между правоохранительными, судебными и разведывательными органами имеет решающее значение для борьбы с терроризмом, отслеживания иностранных боевиков.

Нужно отметить, что Евросоюз, на сегодняшний день приняли ряд мер по улучшению обмена информацией между странами, в том числе, определил структуру взаимодействия между информационными системами ЕС, которые помогают управлять границами, безопасностью и миграцией, обновил Шенгенскую информационную систему, используемую полицией и пограничниками для обмена оповещениями о разыскиваемых или пропавших без вести лицах и объектах, создал европейский антитеррористический центр для поддержки обмена информацией между национальными полицейскими органами, а также разработал ИТ-системы для борьбы с преступностью и обеспечения безопасности границ ЕС.

Нужно отметить, что все больше преступников и террористов используют цифровые технологии для планирования и совершения преступлений. В результате власти все больше полагаются на электронные доказательства при выслеживании и осуждении преступников. ЕС в настоящее время работает над новыми правилами, чтобы обеспечить более эффективный механизм трансграничного доступа к электронным доказательствам [9. С. 77-79].

Использование цифровых инструментов в уголовных процессах, связанных с террористическими преступлениями, на всей территории ЕС имеет решающее значение в свете меняющейся картины угроз безопасности и быстрых темпов технологического развития.

Терроризм, постоянная глобальная проблема, не знающая границ, национальности и религии, является проблемой, которую международное сообщество должно решать сообща.

Дипломатия, как мягкая сила политтехнологии, является важным инструментом в борьбе против современного терроризма. То, что мы считаем основными навыками дипломатии, вероятно, появились в самом начале человеческой цивилизации при создании первых организованных человеческих сообществ. Хотя война и применение оружия были важнейшим средством внешней

политики на протяжении тысячелетий, появление национальных государств привело к дипломатическому общению между ними.

Эти проблемы будут сохраняться, поскольку экстремистские сети стремятся внедрить своих членов в правоохранительные органы и активно вербовать действующих и вышедших на пенсию сотрудников.

Российское правительство также признало, что эти группы могут быть уязвимы для экстремистских идеологий, и нацелилось на военнослужащих, резервистов, ветеранов и полицию посредством агрессивной кибер-кампании и дезинформационной кампании на цифровых платформах. Военные и сотрудники правоохранительных органов обладают ценными навыками, необходимыми экстремистским сетям, например, тактикой небольших подразделений, коммуникацией, логистикой, разведкой и наблюдением. Они также могут иметь доступ к оружию и взрывчатым веществам [3. С. 27]. Любые усилия по пресечению экстремизма в вооруженных силах должны охватывать все этапы службы.

Военные и полиция должны также уделять больше внимания образованию в области противодействия экстремизму, а также понимать четкие процессы отчетности и надзора для нынешних военнослужащих и сотрудников полиции [4. С. 69].

«Мягкие», но эффективные политические технологии позволяют повысить результативность военных операций, а также могут использоваться как отдельные формы борьбы с терроризмом. Во многих случаях методы «мягкой силы» гораздо более продуктивны, чем их жесткие варианты, в ответ на которые велика вероятность возникновения новой волны террористической активности [2. С. 140].

Борьба с терроризмом состоит из сложных и разнообразных стратегий и тактик, направленных на разработку целостного ответа на угрозу терроризма, включая принятие антитеррористического законодательства, использование разведки и тактики противодействия финансированию терроризма, а также активное сотрудничество с другими странами [14. С. 440-441].

Со стороны политических технологий это предполагает принятие либо подхода прямого действия, такого как замораживание активов, массовые аресты, разрушение тренировочных лагерей, сбор разведданных и ответные меры против государственного спонсора, либо принятие защитных/превентивных мер, таких как обеспечение безопасности границ или усиление технологических барьеров.

Многие исследователи приходят к выводу о том, что природа государства существенно влияет на историю насилия, а также на политические меры и тактику, принятые в ответ на такое насилие. Например, в случае Алжира, где полный контроль осуществляют военные, стратегии борьбы с терроризмом существенно отличаются от стратегий, принятых государством с гражданским правлением, таким как Турция, или монархией, такой как Саудовская Аравия или Марокко [2. С. 140].

Эти различия важны для измерения изменений, происходящих во времени в результате национальных, региональных или международных кризисов или конфликтов, а также для оценки того, как страны реагируют на эти кризисы. Форма правления государства играет роль в том, выберет ли правительство более жесткие или более мягкие меры [15. С. 37].

Целостный подход к борьбе с угрозой терроризма, затрагивающий не только аспекты безопасности проблемы, но и ее экономические, социальные, культурные, образовательные аспекты и аспекты развития, а также идеологические и интеллектуальные коренные причины, мы можем видеть на примере Саудовской Аравии. Он включает в себя программы и действия, направленные на улучшение работы органов безопасности путем реструктуризации деятельности Министерства внутренних дел по предотвращению террористических атак, обмен разведывательной информацией. Мягкий подход включает дерадикализацию и другие превентивные стратегии, инициативы в этом отношении включают реализацию тюремной программы, оказание поддержки семьям задержанных и реализацию программы последующего контроля за освобожденными заключенными в рамках правительственной стратегии профилактики и реабилитации [14. С. 440].

На опыте большинства стран, можно говорить о том, что правительствам следует воздерживаться от принятия репрессивных законов о борьбе с терроризмом и использования их в качестве инструментов для продвижения политических интересов и подавления оппозиционных групп. Факты говорят о том, что, хотя репрессии могут быть формой сдерживания в краткосрочной перспективе, они контрпродуктивны в долгосрочном прогнозе, поскольку способствуют вербовке и радикализации молодежи и маргинализированных людей.

Подводя итог вышесказанному, для эффективной борьбы с угрозой терроризма правительствам необходимо направить больше усилий и ресурсов на превентивные меры и меры по дерадикализации, направленные на потенциальные коренные причины терроризма, такие как бедность, маргинализация и безработица. Также странам необходимо активизировать свои усилия по развитию партнерства, демократизации общества [14. С. 440-441].

Разработка новых антитеррористических законов и внесение поправок в существующие с малой долей вероятности предотвратят терроризм или преодолеют его, а могут даже оказаться контрпродуктивными. Фактически, приведение политики и стратегий в соответствие с измеримыми показателями и опора на целостные и всеобъемлющие тактики борьбы с терроризмом дадут возможность политикам всех стран меньше полагаться на драконовские подходы и улучшить свою превентивную и ответную тактику в отношении терроризма.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Акопян Г.А.** Современный терроризм: ключевые особенности развития и проблемы его искоренения // Вопросы национальных и федеративных отношений. 2024. № 4.
2. **Багнычев М.Ю.** Профилактика терроризма на ранней стадии: противодействие терроризму и экстремизму / Пенитенциарная система и общество: опыт взаимодействия: Сборник материалов VII Международной научно-практической конференции, Пермь, 02 апреля 2020 года / Составитель В.А. Овченков. Том I. Пермь: Пермский институт Федеральной службы исполнения наказаний, 2020.
3. **Боднар Э.Л.** Психология терроризма: учеб.-метод. Пособие. Екб.: Изд-во Урал. федер. ун-та, 2013.
4. **Будаева С.В., Дегтярева Н.В.** Международное сотрудничество в области борьбы с терроризмом // Вестник ЗабГУ. 2014. № 5.
5. **Буданцев Э.В.** Информационная безопасность как фактор стратегического суверенитета на пространстве Большой Евразии // Евразийский Союз: вопросы международных отношений. 2024. № 6.
6. **Габриелян Г.Р.** Развитие национальных интернет-платформ как фактор обеспечения информационной безопасности КНР // Вопросы национальных и федеративных отношений. 2024. № 6.
7. **Гасилин Н.А.** Понятие и сущность «мягкой силы» // Молодой ученый. 2019. № 22 (260).
8. **Голубов М.А.** Факторы улучшения системы предотвращения угроз международной безопасности при соотношении организованной экономической и транснациональной преступности // Вопросы национальных и федеративных отношений. 2024. № 5.
9. **Джавиш Р.** Практика применения системы политических технологий противодействия терроризму на примере Сирии: специфика, динамика, результативность // Теории и проблемы политических исследований. 2021. Т. 10. № 5А.
10. **Залысин И.Ю., Старцева С.Г.** Современный терроризм: специфика, динамика, тенденции // Евразийский Союз: вопросы международных отношений. 2024. № 5.
11. **Ермаков К.А.** Экстремизм как основа «новой религии» «глобального либерализма» в мировой политике // Вопросы национальных и федеративных отношений. 2023. № 5.
12. **Ефанова Е.В.** Инструменты «мягкой силы» во внешней политике государства // Вестник РУДН. Сер. Политология. 2018. № 3.
13. **Излученко Т.В.** Особенности профилактики экстремизма в высших учебных заведениях // Перспективы Науки и Образования. 2019. № 3 (39).

14. **Киреев М.П., Баклицкий К.А.** Организация предупреждения терроризма и экстремизма в современной России // Пробелы в российском законодательстве: юрид. журн. 2008. № 2.
15. **Миронова Т.А.** Развитие политических коммуникаций студенчества в целях профилактики экстремизма и терроризма в среде вузовской молодежи // Этносоциум и межнациональная культура. 2022. № 1 (163).
16. **Муамар Ф.** Root-Causes and Solutions of the Islamic Extremism Kind of Terrorism in the Scholarly Local-Literature of the MENA Region/Корень-причины и способы устранения исламского экстремизма, приводящего к терроризму в местной научной литературе Ближнего Востока и Северной Африки // Евразийский Союз: вопросы международных отношений. 2023. № 5.
17. **Ниточкин Ф.В.** «Мягкая сила», «цветная революция» и гибридная война: публичная дипломатия vs политическая технология // Дипломатическая служба. 2023. № 3.
18. **Павлов Н.Р., Слабов Е.А.** Противодействие сетевому терроризму в контексте становления информационного общества // Вопросы политологии. 2023. № 8-2.
19. Политический экстремизм и терроризм: причины, критерии и вопросы специальной профилактики для обеспечения национальной безопасности: монография / С.Е. Бакулев, В.И. Сигов, А.А. Смирнов, Э.П. Теплов; Национальный государственный университет физической культуры, спорта и здоровья им. П.Ф. Лесгафта, Санкт-Петербург. Санкт-Петербург: без издательства, 2018.
20. Профилактика и противодействие терроризму: исторические, политические, психологические, правовые аспекты / Н.В. Савчук, Е.Г. Воронцова, Б.Ф. Чечет, А.И. Сорокина. Ангарск: Ангарский государственный технический университет, 2017.
21. **Рахимов К.Х., Сабиров Б.Т., Хайдаров Б.К.** Проблема терроризма в Республике Узбекистан // Вопросы национальных и федеративных отношений. 2023. № 9.
22. **Рузавина А.К.** Молодежный экстремизм – угрозы и вызовы современной России // Вопросы национальных и федеративных отношений. 2023. № 7.
23. **Старостин А.М., Тованчова Е.Н.** Криптоинновации как концепт и практический инструментарий современного терроризма // Вопросы национальных и федеративных отношений. 2023. № 7.
24. **Цогоев Д.А.** Роль СМИ в политическом механизме противодействия экстремизму в современной России // Вопросы политологии. 2024. № 3.
25. **Чжао Лэй.** Сотрудничество в области кибербезопасности и борьбы с кибертерроризмом в рамках ШОС // Евразийский Союз: вопросы международных отношений. 2024. № 5.

Z.E. ABDURAGIMOV
Applicant of the Department of Political Science
Financial University under the Government of the Russian Federation, Moscow, Russia

«SOFT» POLITICAL TECHNOLOGIES FOR PREVENTING AND COUNTERING TERRORISM

The article is devoted to the current problem of countering international terrorism with the help of political technologies. The study reveals the content of the concepts «prevention of terrorism», «extremism», «radicalization», soft power»; typologies of terrorism and its prevention are presented.

The characteristic features of new mechanisms of interaction between terrorist groups in cyberspace using promising technologies and social networking platforms are identified and described. Particular attention is paid to preventing radicalization on social media and the Internet in the digital age, examining the relevant methods and approaches that terrorists use to disseminate their propaganda and recruit online.

The existing international instruments and mechanisms for identifying and preventing the financing of terrorism are reviewed, and the roles of the authorities involved in combating this type of crime are described and analyzed. Considerable attention is paid to the concept of «soft power» in the context of political technologies and methods.

This article is an attempt to address the issue of the role of diplomacy as an important and indispensable tool in the fight against terrorism.

Key words: *political technologies, international terrorism, counteraction, «soft power», radicalization, extremism, diplomacy, terrorist financing.*