Инициатива «Иностранные тербойцы»
((ИТ) (FTF))

Гаагско-марракешский меморандум о надлежащей практике для более эффективного реагирования на феномен ИТ

Введение

Угроза, представляемая «иностранными тербойцами» ((ИТ) (FTF))[1] – индивидами, совершающими поездки за границу, в государства, в которых не проживают и чьими гражданами не являются, для участия, организации, планирования, подготовки, осуществленияили иных действий, поддерживающих террористическую активность, или для проведения или прохождения обучения для осуществления этих действий (часто именуемого «обучением террористов») – является серьезной проблемой для международной и национальной безопасности. Правительства по-прежнему пытаются решить проблему работы со сложным комплексом вызовов, создаваемых этой угрозой. Многие страны озабочены тем, что все большее количество людей, особенно молодежи, вовлеченных в радикализацию и насильственный экстремизм и совершающих поездки в целях борьбы или прохождения обучения совместно с террористическими группами в конфликтных и неконфликтных областях, подвергнется дальнейшей радикализации и создаст новую террористическую угрозу для собственной страны или третьих стран, включая страны транзита.

ИТ могут оказать влияние на страны происхождения, транзита и назначения, включая планирование операций и увеличение потока новых членов организаций и оружия, а также возрастание угрозы терроризма после их возвращения в родную страну или третьи страны, куда они приезжают потенциально индоктринированными и/или связанными с насильственными экстремистскими группами, знания оперативной деятельности или опыт участия в терактах и обучении. После их возвращения, безотносительно к тому, действуют ли они самостоятельно («одиночные действующие лица») или в составе группы, существует риск совершения ИТ терактов или популяризации насилия, предоставления консультаций и экспертных знаний по оперативным вопросам, сбора средств и/или вербовки, радикализации или широких мер побуждения других лиц участвовать в насилии в государстве, где они проживают или чьими гражданами являются, или в других государствах.

Сознавая этот долгосрочный и серьезный вызов, в сентябре 2013 г. Марокко и Нидерланды под эгидой ГКТФ начали инициативу по работе с феноменом ИТ. Цель этой инициативы – объединить практикующих специалистов и разработчиков политики из широкого круга стран и разных областей для обмена полученными знаниями, надлежащими практиками и

[1] Настоящий Меморандум и инициатива ГКТФ по ИТ в более широком смысле не задуманы и не должны толковаться в качестве утверждающих определенный правовой статус ИТ согласно национальному или международному праву, в частности международному гуманитарному праву, международным правам человека или закону о беженцах.

вызовами в рамках ответных мер, связанных с этой угрозой во всех ее проявлениях[2]. Надлежащие практики, содержащиеся в этом не имеющем обязательной силы меморандуме, предназначены для информирования и руководства деятельностью правительств в рамках их усилий по разработке политики, программ и подходов к решению феномена ИТ. Настоящие надлежащие практики также могут использоваться для формирования любых двусторонних или многосторонних мер технического содействия или содействия в сфере развития потенциалов, предоставляемого в данной области. Любые программы, политика, законы или действия, реализуемые в качестве продолжения настоящей надлежащей практики, должны полностью учитывать обязательства соответствующего государства в области релевантного международного права и норм.

Настоящий Меморандум представляет собой комплекс надлежащих практик, направленных на работу с феноменом ИТ, под четырьмя основными заголовками: (1) радикализация и вовлечение в насильственный экстремизм; (2) вербовка и содействие; (3) поездки и участие в борьбе и (4) возвращение и реинтеграция. Все государства приглашаются к изучению настоящих надлежащих практик, в то же время сознавая, что реализация любых мер должна быть согласована с применимым международным правом, а также с национальным законодательством и нормативными правовыми актами, с учетом многообразия историй, культур и правовых систем среди государств.

Надлежащие практики

A. Выявление и реагирование на насильственный экстремизм

Радикализация и вовлечение населения в насильственный экстремизм – сложный процесс, для реагирования на который необходимы комплексные средства. Тогда как радикализация и вовлечение населения в насильственный экстремизм – более широкий феномен с потенциалом ускорения процесса радикализации ИТ, не все индивиды, подверженные радикализации и вовлечению в насильственный экстремизм, становятся ИТ. Сходным образом, тогда как одни ИТ подвергаются радикализации и вовлечению в насильственный экстремизм до отъезда из своих стран, другие подвергаются этому процессу в ходе участия в борьбе или после возвращения. Поскольку ИТ могут происходить из всех сегментов населения государства и обычно поддерживают контакты с лицами из разных стран, эффективные программы по противодействию насильственному экстремизму (ПНЭ) с фокусом на ИТ требуют подхода, охватывающего правительство в целом, с проактивным взаимодействием с местными сообществами и международным сотрудничеством.

Надлежащая практика №1 *– Инвестирование в долгосрочное культивирование доверительных отношений с местными сообществами, подверженными вовлечению в насильственный экстремизм, изучение широкого круга проблем и угроз, затрагивающих сообщество.* Взаимодействие по вопросу феномена ИТ и радикализации и вовлечения в насильственный экстремизм – крайне болезненная тема. Государственные органы, взаимодействующие с сообществами, чьи члены уязвимы с точки зрения превращения в ИТ, могут обратиться к более широкому кругу проблем, таких, как национальная политика в области иностранных дел, культивировать доверие и решать главные

[2] Стартовое заседание по этой инициативе состоялось в Гааге 19-20 февраля 2014 г., на нем были выявлены ключевые вопросы к экспертам. Первое совещание экспертов прошло в Марракеше 14-15 мая 2014 г. и было посвящено правоохранительной деятельности, правосудию и обмену информацией, за ним последовало второе совещание про противодействию насильственному экстремизму (ПНЭ (CVE)), проведенное центром передовых знаний «Хедайя» (*Hedayah*) по ПНЭ 16-17 июня 2014 г. в Абу-Даби.

потребности и проблемы сообщества. Это может включить в себя усилия по ликвидации условий, стимулирующих радикализацию и насильственный экстремизм. Государственные органы должны быть честны относительно своей роли и обязанностей, последующего использования информации и возможности или невозможности раскрытия определенной информации членам сообщества.

Надлежащая практика №2 *– Разработка широкого спектра проактивных, положительных дискурсов, противопоставленных дискурсам экстремизма, и альтернативных действий, предлагающих ненасильственные, продуктивные альтернативы, чтобы помочь нуждающимся, а также средств канализации разочарования, раздражения и озабоченности без обращения к насилию*[3]. Вместо создания исключительно отрицательных информационных сообщений важно в сотрудничестве с сообществами обеспечить положительные альтернативы индивидам, собирающимся в страны назначения для оказания поддержки террористическим группам или совершения терактов иным способом. Положительные альтернативы могут включать предложение ненасильственных вариантов канализации разочарования, раздражения и озабоченности, таких, как благотворительность в пользу жертв конкретного конфликта. Систематические, адаптированные менторские программы могут оказаться высокоэффективными, особенно для молодежи, подверженной риску радикализации, поскольку предлагают индивидуальное внимание. Далее, эффективные дискурсы, противопоставленные дискурсам экстремизма, должны поощрять проверку утверждений, критическое мышление и выполнение анализа лицами, которые могут стать целевой аудиторией вербовки. Эти альтернативные дискурсы также могут послужить в качестве инструментов подверженным риску сообществам для противодействия информационным сообщениям насильственного экстремизма. Оценку эффективности таких кампаний следует проводить регулярно, в том числе с учетом ответов, полученных от представителей целевой аудитории.

Надлежащая практика №3 *– Объединение усилий социальных СМИ, экспертов-аналитиков и инноваторов в области технологий для разработки и создания убедительного содержания, противопоставленного экстремистскому.* Террористические организации и лица, осуществляющие вербовку ИТ, часто используют социальные СМИ в целях вербовки и распространения информационных сообщений. Сочетая большой объем профессионального содержания и мощное обращение к аудитории и призывая к действиям, эти организации могут создать убедительное информационное сообщение для индивидов, подверженных вовлечению в насильственный экстремизм. Одновременно с продолжением работы по устранению незаконного содержания, связанного с терроризмом, с онлайн-площадок правительства должны рассмотреть возможность уделить равное внимание созданию собственных стратегических коммуникационных продуктов, распространяемых через адекватные каналы, проактивного взаимодействия с социальными СМИ таким же образом, как это делают террористические и насильственные экстремистские организации. Мощное онлайн-содержание может оказать большое, положительное влияние на деятельность по ПНЭ в связи с феноменом ИТ. В этом отношении могут быть особенно эффективны дискурсы, противопоставленные дискурсам экстремизма и создаваемые жертвами терроризма и бывшими террористами.

Надлежащая практика №4 *– Расширение возможностей лиц, обладающих наилучшим потенциалом по инициированию изменений, включая молодежь, семьи, женщин и*

[3] См. надлежащую практику №9 «Анкарского меморандума о надлежащей практике многосекторного подхода к противодействию насильственному экстремизму» (*Ankara Memorandum on Good Practices for a Multi-Sectoral Approach to Countering Violent Extremism)* ГКТФ для более подробной информации о создании дискурсов, противопоставленных дискурсу экстремизма, и альтернатив насилию.

гражданское общество, для активной и ответственной разработки и распространения положительных дискурсов, противопоставленных дискурсам насильственного экстремизма. Лица, наиболее подверженные вероятности стать целевой аудиторией вербовки, должны быть в центре внимания при разработке программ ПНЭ в связи с вызовом ИТ. Противопоставленные дискурсы, исходящие из соответствующей возрастной группы лица, получат отклик с большей вероятностью, чем дискурсы, исходящие из источников, воспринимаемых как внешние по отношению к сообществу. Правительствам следует изучить возможность непрерывного взаимодействия с молодежью, женщинами, семьями и гражданским обществом, обеспечивая им релевантное и оперативное обучение по вопросам создания содержания, противопоставленного дискурсам экстремизма, деятельности по развитию связей и коммуникации.

Надлежащая практика №5 *– Предупреждение отождествления феномена ИТ или насильственного экстремизма с какой бы то ни было религией, культурой, этнической группой, национальностью или расой.* Тогда как связанный с безопасностью риск, исходящий от ИТ, нельзя игнорировать, злонамеренное использование неуместного внимания или неверно направляемое освещение проблемы ИТ в СМИ могут дополнительно стимулировать радикализацию ИТ. Программы по ПНЭ должны избегать и стремиться предотвращать отождествление ИН или насильственного экстремизма с какой бы то ни было религией, культурой, этнической группой, национальностью или расой; в контексте ИТ существует особенно большая вероятность, что произойдет подобное отождествление в области религии. Такой предвзятый подход к насильственному экстремизму ограничит кругозор лиц, ответственных за разработку инициатив по ПНЭ, может привести к отчуждению тех членов сообществ, чье сотрудничество важно для успеха мероприятий, и может быть использован насильственными экстремистскими группами в целях пропаганды для нейтрализации соответствующих мероприятий.

Б. Предупреждение, выявление и реагирование на вовлечение населения в насильственный экстремизм и содействие насильственному экстремизму

В некоторых пространствах могут работать традиционные сети вовлечения населения в насильственный экстремизм и содействия насильственному экстремизму, создаваемые стабильными террористическими организациями, которые могут быть нацелены на определенные сообщества, тогда как в других радикализация может осуществляться на основе интернет-технологий. Между этими двумя полюсами находятся гибридные модели, которые пользуются преимуществом масштабности и анонимности интернета, при этом сохраняя некоторые элементы традиционной модели, такие, как концентрация на определенной этнической или языковой принадлежности. Нижеприведенные надлежащие практики обеспечивают рамки для реагирования на сложные вызовы, создаваемые разными техниками вовлечения населения в насильственный экстремизм и содействие насильственном экстремизму. Следует отметить, что не все лица, вовлекаемые в экстремизм в качестве ИТ, подвержены радикализации до перемещения – некоторые могут подвергаться радикализации в продолжение нахождения в конфликтных или неконфликтных зонах или после возвращения.

Надлежащая практика №6 *– Коммуникация с местными сообществами для обеспечения информированности об угрозе ИТ и создания устойчивости к информационным сообщениям насильственного экстремизма.* Члены сообществ, становящихся целевой аудиторией вербовки, могут быть не осведомлены об основанных на интернет-технологиях или личном контакте техниках вербовки ИТ. Инструктаж для повышения информированности сообществ и базовые упражнения позволят сообществам самостоятельно разработать эффективные ответные меры для решения проблемы вербовки

ИТ помогут создать доверие, необходимое членам сообществ для обмена информацией об ИТ с государственными органами. В этом отношении важно вести последовательную работу по созданию, совершенствованию методологии и подходов к разработке политики в отношении сообществ, чтобы обеспечить высочайший уровень доверия между государственными органами и сообществами. Вовлечение специалистов, обладающих чувствительностью к культуре, таких, как психологи и поставщики социальных услуг, в инициативы по взаимодействию с сообществами и повышению информированности может оказаться высокоэффективным с учетом болезненности затрагиваемой темы. В конечном итоге следует мотивировать сообщества вести диалог с другими, в сотрудничестве с участниками из социальной, образовательной и медицинской сфер. В частности следует продвигать межконфессиональный и внутриконфессиональный диалог. Следует поддерживать разработку сообществами инициатив по предупреждению радикализации и вовлечения населения в насильственный экстремизм. В данном контексте следует тщательно избегать стигматизации религиозных или культурных сообществ.

Надлежащая практика №7 *– Сбор и объединение подробной информации из государственных организаций, от специалистов, работающих на местах, сообществ и социальных СМИ для выявления вовлечения населения в насильственный экстремизм и содействия насильственному экстремизму с соблюдением верховенства закона и прав человека***.** Государства могут получать информацию об известных и подозреваемых ИТ за счет проверенных временем техник правоохранительной деятельности, таких, как прослушивание телефонных разговоров, защищенные информаторы и проактивное взаимодействие с сообществом, а также за счет законного мониторинга платформ социальных СМИ и допросов семей и членов сообществ. Для обеспечения их легитимности эти механизмы должны подвергаться соответствующему надзору и предусматривать механизмы привлечения к ответственности за незаконное злоупотребление. Там, где это возможно, государствам рекомендуется делиться этой информацией с местными властями или национальными организациями и, поскольку большинство сетей вовлечения населения в насильственный экстремизм и содействия насильственному экстремизму являются мультинациональными – с партнерами на двусторонней или многосторонней основе для облегчения выявления и запрета этих сетей. Во многих случаях это означает просто усовершенствованное использование существующих платформ обмена информацией[4].

Надлежащая практика №8 *– Объединение ресурсов, обмен информацией и сотрудничество с частным сектором для ограничения онлайн-вербовки ИТ*. Государства, имеющие правовые органы и ресурсы для мониторинга онлайн-вербовки ИТ и содействия насильственному экстремизму, должны объединять свои ресурсы и осуществлять обмен информацией и анализом путем заслуживающих доверия механизмов, таких, как Интерпол и Европол, там, где это целесообразно. Более того, государствам следует сотрудничать с интернет-компаниями для содействия компаниями, принимающим быстрые и эффективные меры в отношении веб-сайтов и пользователей социальных СМИ, нарушающих условия предоставления услуг этими компаниями в плане преступного поведения; например, указывая этим компаниям на веб-сайты и пользователей социальных СМИ, чье содержание и деятельность могут быть приравнены к преступному поведению. Когда это целесообразно, результаты интернет-мониторинга также могут предоставляться семьям и лидерам сообществ для повышения их информированности о действиях их детей до того, как они подвергнутся радикализации или вовлечению в

[4] Государства также должны эффективно использовать режим санкций ООН, установленный согласно резолюции 1267 ООН и последующим резолюциям, и поощрять составление ООН списков – параллельно с составлением национальных списков – лиц, содействующих в перемещении ИТ.

насильственный экстремизм, и для укрепления отношений «сообщества/семьи – государственные органы».

Надлежащая практика №9 *– Принятие адаптированных и целенаправленных подходов, основанных на специфических факторах мотивации и целевой аудитории, для ответных мер в области ПНЭ в качестве реагирования на радикализацию и вовлечение населения в насильственный экстремизм.* Эффективные ответные меры в области ПНЭ учитывают конкретные потребности, культуру, озабоченность и недовольство – как реальные, так и субъективно воспринимаемые – соответствующих сообществ. Они также учитывают особый(ые) фактор(ы) мотивации, имеющие место в решении о получении статуса ИТ, которые могут быть политическими, экономическими, идеологическими, религиозными, гуманитарными или отражать тенденцию подверженности насилию. Успешные ответные меры в области ПНЭ с большой вероятностью включают многосекторный подход, привлекающий к участию образовательные системы, религиозные сообщества и организации, гражданское общество, организации внутри сообществ, специалистов, работающих на местах, семьи и молодежь.

B. Выявление и реагирование на перемещение и участие в борьбе

Хотя многие государства в последнее время сделали существенные шаги, по-прежнему необходимо приложить много усилий к развитию потенциалов как правоохранительных органов, так и разведывательных служб для выявления известных или подозреваемых ИТ до их перемещения. К сожалению, существенный процент ИТ не известен государственным органам до перемещения, что осложняет выявление момента их вхождения в систему международных поездок или обеспечение государствам других признаков, которые позволят пресечь их деятельность в процессе перемещения. ИТ могут совершать прямые поездки в страны назначения или скрыть свои намерения путем транзита через третьи страны. Нижеприведенные надлежащие практики обеспечивают эффективные меры ликвидации этих вызовов и выявления и принятия мер против перемещения и участия в борьбе.

Надлежащая практика №10 *– Увеличение объема обмена местной публичной, правоохранительной и разведывательной информацией и анализом и соответствующими лучшими практиками посредством двусторонних отношений и многосторонних форумов для предупреждения перемещения ИТ.* Государства должны разработать механизмы защиты уязвимой правоохранительной и разведывательной информации для поощрения объема информацией, полученной от разведслужб и правоохранительных органов, внутри страны[5]. Государства должны отдать приоритет обмену конкретной, своевременной и дающей основание для принятия мер информацией об известных или подозреваемых ИТ, как посредством официального обмена информацией о преступниках, так и посредством стабильных каналов для общего обмена разведывательной и иной уязвимой информацией или посредством указаний или уведомлений, касающихся определенных лиц, вызывающих опасения. Государства также должны обеспечить лучшее использование существующих многосторонних информационных систем, таких, как система распространения уведомлений и базы данных Интерпола, включая базу данных об интербойцах, а также шенгенскую информационную систему второго поколения (SIS II) Европейского союза (ЕС) и систему данных о пассажирах в фокусе внимания (Focal Point Travelers) Европола, там,

[5] См. надлежащую практику №6 «Рабатского меморандума о надлежащей практике эффективного противодействия терроризму в секторе уголовного правосудия» (*Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector)* ГКТФ или более подробный материал об обмене разведывательной информации с правоохранительными органами.

где это применимо. Наконец, государствам рекомендуется разработка новых инструментов, соответствующих национальному праву и политике, для своевременного обмена предварительной информаций о пассажирах (ПИП (API)) и списками имен пассажиров (СИП) (PNR)), который позволит другим государствам транзита принять меры в отношении подозреваемых ИТ. Помимо информации о пассажирах, государства должны поддерживать обмен любой информацией для включения надлежащей практики в меры противодействия ИТ.

Надлежащая практика №11 – *Разработка и внедрение адекватных правовых режимов и административных процедур для эффективного преследования и снижения риска, создаваемого ИТ*[6]. Государства должны оценить пробелы в мерах противодействия, учитывая широкий спектр потенциальных уязвимых мест, и постараться снизить угрозу посредством координирования усилий правительства в целом, а когда это возможно, также рассмотреть возможность создания комплексных контртеррористических правовых режимов, криминализирующих подготовительную террористическую деятельность. Особое значение имеет изучение эффективности внутренних уголовных законов в отношении поездок в зарубежные страны для присоединения к террористической группе, или участия в террористической деятельности, или предоставления поддержки (сюда должна быть включена финансовая и кадровая поддержка) террористической группе, в том числе в связи с вооруженным конфликтом. Государства также должны рассмотреть – там, где это совместимо с внутренним правом и политикой – широкий спектр административных мер и мер в области регулирования, например, лишение социальных льгот и заграничного паспорта. Все механизмы должны координироваться между разными организациями внутри правительства и, если это целесообразно и соответствует национальному праву – с иностранными партнерами и гражданским обществом или неправительственными партнерами для обеспечения комплексного подхода.

Надлежащая практика №12 – *Применение адекватных мер досмотра, направленных на невозможность перемещения ИТ, с особым вниманием к воздушному транспорту.* Государства должны разработать и совершенствовать меры безопасности в области воздушного транспорта, а также списки разыскиваемых лиц, учитывающие специфические характеристики перемещения ИТ и связанных угроз. Это может включать в себя: больший объем международного сотрудничества в области безопасности авиаперевозок, например, обмен данными, включая СИП, использование специальных протоколов допроса[7]; просвечивание/досмотр багажа с целью детекции при выезде из страны; просвечивание багажа на предмет наличия оружия, взрывчатых веществ и иных средства совершения нападения на авиационную или иную транспортную инфраструктуру. Далее, государства должны рассмотреть возможность использования сложных и специализированных инструментов, таких, как поведенческий анализ и анализ характеристик поездок, для выявления пассажиров-ИТ и их предполагаемых маршрутов,

---

[6] См. надлежащие практики 12 и 13 «Рабатского меморандума о надлежащей практике эффективного противодействия терроризму в секторе уголовного правосудия» (*Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector)* ГКТФ для более подробной информации о криминализации террористической деятельности и подготовительной террористической деятельности.

[7] Такие протоколы включают разработку техник ведения допроса и содержание, разработанное для выявления таких данных, как цель поездки, средства к существованию в течение поездки и т.д., и используются систематически в отношении лиц, соответствующих определенным характеристикам, во всех видах транспорта. При необходимости некоторые утверждения лиц следует проверять. Представляющая интерес информация, полученная в ходе таких допросов, после которых пассажирам разрешается дальнейшее следование, должна предоставляться компетентным органам в пунктах транзита и назначения. Эти протоколы должны соответствовать международному праву в области прав человека.

как при выезде в страну, так и при возвращении. Государства также могут создать более эффективное партнерство с организациями частного сектора в аэропортах, в том числе с частными охранными компаниями.

Надлежащая практика №13 *– Использование всех доступных инструментов для предупреждения незаконного использования дорожных документов для перемещения ИТ.* Государства должны использовать все доступные инструменты – в том числе административные действия и действия судебной власти там, где это целесообразно, и больший объем обмена информацией, особенно о лицах с двойным гражданством – для предупреждения перемещения и участия подозреваемых ИТ в террористической деятельности. В то же время государства должны предпринять все возможные шаги для предупреждения использования полученных незаконным путем, украденных, подделанных или используемых иным незаконным образом заграничных паспортов, в том числе более активно пользуясь базой данных Интерпола об утерянных и украденных паспортах и применяя международные стандарты контроля заграничных паспортов и использования биометрической информации. Технологии ФСБДИ (FIND) и МБДИ (MIND) также могут помочь государствам в проведении эффективных систематических проверок. Службы по борьбе с терроризмом и организованной преступностью должны осуществлять объединение и обмен информацией и данными, связанными с нелегальной иммиграцией, выпуском фальсифицированных документов и контрабандой оружия.

Надлежащая практика №14 *– Развитие потенциалов государств по предупреждению перемещения ИТ через наземные пограничные пункты и шире – принятие адекватных мер предупреждения планирования или подготовки терактов внутри страны или за границей, осуществляемого ИТ с их территории.* Все государства происхождения, транзита или назначения должны использовать все адекватные правоохранительные средства для обеспечения того, чтобы террористы с их территории не использовались при осуществляемом ИТ планировании или подготовке терактов внутри страны или за границей. В отношении пассажирских перевозок государства должны развивать свои потенциалы по предупреждению пересечения наземных границ ИТ. В дополнение к высокотехнологичным мерам, таким, как объединенные в сеть камеры и воздушное наблюдение, государства могут применить большое количество эффективных, низкотехнологичных подходов, таких, как плавающее время патрулирования границ; использование всех доступных источников информации, в том числе из местных сообществ, для определения стандартных маршрутов и времени поездок ИТ и иных правонарушителей. Наконец, способность препятствовать ИТ в целом повышается за счет своевременного предоставления информации о перемещении ИТ государствами происхождения и транзита.

Г. Выявление и реагирование при возвращении ИТ

Наличие спектра факторов мотивации создает сложности для выявления, реагирования и взаимодействия с ИТ при возвращении. Также правительства часто сталкиваются с трудностями при преследовании ИТ при их возвращении и/или включении их в программы профилактики, выхода из экстремистских организаций и реабилитации. Нижеприведенные надлежащие практики перечисляют зарекомендовавшие себя техники выявления и реагирования при возвращении ИТ как с точки зрения правоохранительной деятельности, так и с точки зрения ПНЭ.

Надлежащая практика №15 *– Использование максимально широкого набора источников информации для предвосхищения и выявления возвращающихся ИТ.* ИТ часто заранее планируют возвращение, обсуждают его на открытых платформах СМИ и

принимают меры для собственной «реинтеграции», такие, как встреча в аэропорту, запись на прием к врачу и трудоустройство. Таким образом, государства должны осуществлять законное использование источников информации – в том числе социальных СМИ, лидеров сообществ, семей, друзей и знакомых, поставщиков социальных услуг и работодателей из частного сектора – для предвосхищения и выявления возвращающихся ИТ. Кроме того, возвращающиеся ИТ также могут разбить свои поездки на части или отправиться в другую страну в попытке предупредить выявление или преследование, что также несет в себе долгосрочную угрозу для соответствующих стран. Международные базы данных и информационные системы, такие, как система распространения уведомлений Интерпола, также могут обеспечить полезную информацию для предвосхищения и выявления возвращающихся ИТ. Наконец, больший объем предоставления информации о выезде подозреваемых ИТ третьими странами может помочь государствам происхождения выявить «не идентифицированных возвращенцев».

Надлежащая практика №16 *– Создание и использование основанных на данных, индивидуальных рамок проведения оценки возвращающихся ИТ, оценка их состояния и соответствующее инициирование адекватных подходов к взаимодействию.*
Эффективная оценка рисков, основанная на разнообразных факторах, в том числе на мотивированности индивида совершать поездки в целях участия в борьбе, поведение в продолжение перемещения и в определенной зоне, которые могут быть получены в ходе допросов семьи и друзей, позволяет государственным органам принять индивидуально адаптированные ответные меры. Эти ответные меры могут варьироваться от преследования до мониторинга, мер по предупреждению насилия и/или программ по реинтеграции в общество. Оценка рисков также может помочь государственным органам обеспечить соответствие мер реагирования угрозам и избежать дальнейшей радикализации возвращающихся ИТ или членов их сообществ. Государства-партнеры должны обмениваться рамками оценки рисков, когда это целесообразно, для содействия созданию комплексного подхода, отражающего надлежащую практику.

Надлежащая практика №17 *– Усиление расследования и преследования деятельности ИТ, когда это целесообразно, посредством усовершенствованного обмена информацией и сбора данных.* Государства должны рассмотреть возможность обновления своего законодательства для криминализации вербовки ИТ и участия в террористической деятельности за границей. В целом данные, необходимые для преследования ИТ за их преступления, могут находиться более чем в одной стране, вызывая необходимость во взаимной правовой помощи (ВПП), которая может быть значительно расширена путем неофициального сотрудничества между следователями и прокурорами – например, путем предоставления другой стране упреждающего уведомления об направлении запроса на ВПП для обеспечения сохранности временно-зависимых данных[8]. Командирование сотрудников по связям и прокуроров за границу также является надлежащей практикой совершенствования обмена информацией и также может быть использовано для укрепления потенциалов партнеров из третьих стран по адекватному сбору данных, приемлемых для внутреннего преследования. Многие государства также имеют специальные пограничные органы досмотра, которые могут использоваться для законного сбора не только данных о подозреваемых ИТ, но и информации о лицах, осуществляющих вербовку ИТ и осуществляющих содействие в данной области; следует

[8] См. надлежащую практику №9 «Рабатского меморандума о надлежащей практике эффективного противодействия терроризму в секторе уголовного правосудия» (*Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector)* ГКТФ для более подробной информации об официальном и неофициальном международном сотрудничестве.

вести масштабный обмен этими данными. Наконец, там, где это применимо, расследование деятельности ИТ, осуществляемое органами, специализирующимися на работе с лицами, подозреваемыми в террористической деятельности, может усовершенствовать сбор данных и повысить вероятность успешного преследования.

Надлежащая практика №18 *– Подготовка и применение ответных мер в отношении тех типов терактов, для которых ИТ имеют специальные навыки.* Некоторые ИТ могли пройти подготовку по использованию переносных зенитно-ракетных комплексов (ПЗРК), самодельных взрывных устройств (СВУ) и автоматического оружия высокой мощности. Таким образом, планирование и выполнение ответных мер и мер управления последствиями, отражающие координированные меры реагирования на уровне правительства в целом, должны отдельно рассматривать проблемы дорожных мин, мародерских вооруженных нападений на особо важные или обладающие символической ценностью статичные цели и авиаатак с земли.

Надлежащая практика №19 *– Разработка комплексных программ реинтеграции ИТ после возвращения.* Комплексные программы реинтеграции – включая программы в пенитенциарных учреждениях – являются критически важной частью реагирования на потенциальные угрозы, создаваемые ИТ после возвращения. Действия ИТ мотивированы разными факторами, побуждающими их совершать заграничные поездки с целью участия в борьбе – включая религиозные, гуманитарные, идеологические, экономические или политические соображения – и радикализация и вовлечение в насильственный экстремизм могут произойти в процессе пребывания за границей, а не в качестве первичного мотивационного фактора перемещения. Соответственно программы реинтеграции должны учитывать разные факторы мотивации и включать индивидуальную оценку возвращающихся ИТ для определения наиболее адекватного подхода. Ключевые принципы, которые следует рассмотреть в качестве руководящих при взаимодействии и разработке таких программ включают: (1) потребность в формулировании цели мероприятий по снижению риска совершения терактов возвращающимися ИТ; (2) важность разработки целенаправленных и адаптированных стратегий взаимодействия, основанных на специфических факторах мотивации; (3) потребность в привлечении мультидисциплинарных участников в правоохранительные службы, сообщества и организации, основанные на религиозной принадлежности. Другие ключевые вопросы включают способы вовлечения семей и членов сообщества, имеющих контакт с возвращающимися ИТ, поощрение критического мышления и оспаривание логики и информационных сообщений ИТ и понимание и признание как реальных, так и субъективно воспринимаемых поводов для недовольства в ходе продуктивной дискуссии. Следует тесно взаимодействовать с сообществами для предоставления поддержки индивидам, создания рамок программ реинтеграции и нейтрализации возможных усилий по радикализации в будущем.

Заключение: ***Обмен информацией: комплексные интегрированные подходы, развитие потенциалов***

Как указано выше, государства должны участвовать в правоохранительной и пресекающей деятельности, а также в деятельности по профилактике и реинтеграции для противодействия угрозе, создаваемой ИТ. Этого можно добиться только путем применения подходов, охватывающих правительство в целом, тесно связанных с усилиями иностранных и неправительственных партнеров. Эта угроза безопасности может быть ликвидирована только путем коллективной работы, в первую очередь путем обмена информацией и надлежащими практиками.

ГКТФ может послужить вспомогательной платформой для долгосрочного диалога между государствами в отношении применения настоящей надлежащей практики и связанных с ним усилий по развитию потенциалов. Государствам рекомендуется адресовать предложения и запросы о сотрудничестве в административный отдел ГКТФ. Организаторы инициативы по ИТ будут делиться запросами и предложениями о сотрудничестве со всеми членами ГКТФ своевременно и регулярно. ГКТФ признает, что ни одно государство не несет обязательств по предоставлению или получению сотрудничества. Эти предложения или запросы должны быть основаны на собственном решении каждого государства на базе его правовой системы, приоритетов, потребностей и текущих обстоятельств.