КОНТРТЕРРОРИСТИЧЕСКОЕ УПРАВЛЕНИЕ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ
Контртеррористический центр ООН (КТЦ ООН)

INTERPOL

При финансовой поддержке Европейского союза

Кибербезопасность и новые технологии

Разработка мер реагирования в рамках национальной контртеррористической политики для противодействия использованию новых технологий в террористических целях

Выражение признательности

Настоящий доклад является результатом совместной инициативы Контртеррористического центра Организации Объединенных Наций (КТЦ ООН) при Контртеррористическом управлении Организации Объединенных Наций (КТУ ООН) и Интерпола, направленной на укрепление потенциала правоохранительных органов и органов уголовного правосудия в области противодействия использованию новых технологий в террористических целях. Реализация этой совместной инициативы стала возможной благодаря щедрой финансовой поддержке Европейского союза.

Контртеррористическое управление Организации Объединенных Наций

Центральные учреждения Организации Объединенных Наций

New York, NY 10017

www.un.org/counterterrorism

200, Quai Charles de Gaulle
69006 Lyon, France

www.interpol.int/en

Содержание

Совместное предисловие

Достижения в области информационно-коммуникационных технологий и их доступность сделали привлекательным для террористических и насильственных экстремистских групп их использование для совершения широкого спектра противоправных действий, включая подстрекательство, радикализацию, вербовку, обучение, планирование, сбор информации, коммуникацию, подготовку, пропаганду и финансирование. Террористы постоянно осваивают новые технологические рубежи, и государства-члены выражают все большую озабоченность относительно использования новых технологий в террористических целях.

В ходе седьмого обзора Глобальной контртеррористической стратегии Организации Объединенных Наций государства-члены попросили Контртеррористическое управление Организации Объединенных Наций и другие соответствующие структуры в рамках Глобального договора по координации контртеррористической деятельности «совместно поддерживать инновационные меры и подходы в том, что касается наращивания у государств-членов (по их запросу) способности учитывать в деле предупреждения терроризма и борьбы с ним те вызовы и возможности, которые порождаются новыми технологиями, включая аспекты, относящиеся к правам человека».

В своем докладе Генеральной Ассамблее о деятельности системы Организации Объединенных Наций по осуществлению Глобальной контртеррористической стратегии Организации Объединенных Наций (A/77/718) Генеральный секретарь подчеркивает, что «[...] новые и новейшие технологии открывают беспрецедентные возможности для улучшения благополучия человека и предлагают новые инструменты для борьбы с терроризмом. [...] Несмотря на активизацию усилий и усиление координации, ответные меры международного сообщества часто запаздывают. Иногда такие ответные меры неоправданно ограничивают права человека, в частности право на неприкосновенность частной жизни и свободу выражения мнений, включая право на поиск и получение информации».

Подготовив семь докладов, представленных в этом сборнике, который выпускается при сотрудничестве Контртеррористического центра Организации Объединенных Наций с Международной организацией уголовной полиции в рамках совместной инициативы CT TECH, финансируемой Европейским союзом, мы стремимся поддержать правоохранительные органы и органы уголовного правосудия государств-членов в их противодействии использованию новых и новейших технологий в террористических целях и задействовать такие технологии для борьбы с терроризмом в рамках проводимой работы при полном соблюдении прав человека и верховенства права.

Наши ведомства готовы и впредь оказывать поддержку государствам-членам и другим нашим партнерам в области предотвращения терроризма и борьбы с ним во всех его формах и проявлениях, а также в использовании положительного влияния технологий в борьбе с терроризмом.

Владимир Воронков
Заместитель Генерального секретаря,
Контртеррористическое управление
Организации Объединенных Наций,
Исполнительный директор,
Контртеррористический центр
Организации Объединенных Наций

Стивен Кавана
Исполнительный директор,
Полицейская служба Интерпола

Выражение признательности

Настоящий документ был разработан и подготовлен при участии широкого круга заинтересованных сторон. В частности, Контртеррористическое управление Организации Объединенных Наций (КТУ ООН) хотело бы выразить признательность следующим лицам:

- **Виктору Кипкоечу** — младшему специалисту по программам, Глобальный центр по вопросам сотрудничества в области безопасности (ГЦСБ);
- **Мариане Гонсалес Кэмпбелл** — консультанту по вопросам противодействия насильственному экстремизму, Организация американских государств (ОАГ);
- **Майклу О'Кифу** — специалисту по борьбе с терроризмом, Сектор по предупреждению терроризма Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН);
- **Уинтропу Уэллсу** — руководителю программ, Международный институт правосудия и верховенства права (IIIJ).

Термины и определения

Безопасность по умолчанию	Программа/политика, которая предоставляется потребителю, уже обладая необходимыми мерами для обеспечения безопасности (вместо того, чтобы потребителю приходилось отдельно реализовывать меры по обеспечению безопасности)[1].
Виртуальные активы	Термины «виртуальные активы» или «криптоактивы» означают цифровые формы валюты и других активов[2].
Даркнет/дарквеб	Зашифрованная часть сети Интернет, доступ к которой осуществляется с помощью специального программного обеспечения, которое само по себе не является криминальным, например браузера Tor. Однако общепризнанным является тот факт, что даркнет содержит в себе множество криминальных веб-сайтов и сервисов, размещенных в этих сетях[3].
Действия правоохранительных органов	Этот термин, как правило, описывает действия правоохранительных органов, предпринимаемые для противодействия угрозе, которые могут включать задержание отдельных лиц, пресечение деятельности злоумышленников (например, удаление контента, арест активов) и т. д.
Дерадикализация	Процесс, в ходе которого человек, проявляющий признаки радикализации, убеждается в необходимости отказа от радикальной идеологии[4].

1 Агентство по кибербезопасности и защите инфраструктуры США и соавт., («Изменение баланса рисков кибербезопасности: принципы и подходы к проектируемой безопасности и безопасности по умолчанию»), April 13, 2023, 5–6, URL: https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_ security-by-design-default_508_0.pdf

2 Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ), «Виртуальные активы», URL: https://www.fatf-gafi.org/ en/topics/virtual-assets.html (дата обращения: 1 июля 2024 г.).

3 Европейский центр киберпреступности (EC3),«Оценка угроз организованной преступности в Интернете за 2019 год» (Европол, 2019 г.), 4, URL: https://www.europol.europa. eu/cms/sites/default/files/documents/iocta_2019.pdf

4 Lorenzo Vidino and Clifford Bennett, "A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism", («Обзор трансатлантического передового опыта по противодействию радикализации в тюрьмах и рецидиву терроризма», 3-я конференция Консультативной сети Европейского контртеррористического центра (ECTC) по терроризму и пропаганде, Гаага, Нидерланды: Европол, 2019 г.), 8, URL: https://www.europol.europa.eu/cms/sites/default/files/documents/a_review_of_transatlantic_best_practices_for_countering_radicalisation_in_prisons_and_terrorist_recidivism.pdf

Доказательная практика (ДП)	Использование конкретных качественных данных как основы для формирования политики и ее реализации[5].
Доказательства	Официальный термин для обозначения информации, являющейся частью судебного процесса, которая используется для подтверждения или опровержения совершения предполагаемого преступления. Все доказательства являются информацией, но не вся информация является доказательством. Таким образом, информация — это первоначальная, исходная форма доказательств[6].
Зеттабайт	Один зеттабайт равен одному миллиарду терабайтов.
Зона ответственности (ЗО)	Область или регион, которые находятся под ответственностью или юрисдикцией практикующего специалиста.
Искусственный интеллект	Под этим термином обычно понимают дисциплину, занимающуюся разработкой технологических инструментов, позволяющих имитировать когнитивные функции человеческого мозга, такие как планирование, обучение, рассуждение и анализ.
Новые технологии	Термин «Новые технологии» охватывает широкий спектр различных технологий[7], однако для целей данного документа под новыми технологиями понимается использование и злоупотребление такими новыми технологиями, как Интернет, социальные сети, криптовалюты, системы распознавания лиц и даркнет[8].
Обнаружение аномалий	Процесс интеллектуального анализа данных, направленный на выявление единиц данных, которые выходят за рамки или отклоняются от нормы.
Обработка естественного языка (ОЕЯ)	Подмножество искусственного интеллекта (ИИ), которое занимается способностью машинного анализа человеческих языков и работы с ними как в качестве источника входных данных, так и в качестве результатов обработки (вместо, например, данных или программного кода)[9].
Оперативная информация	Информация, являющаяся результатом сбора, разработки, распространения, анализа и интерпретации данных, полученных из широкого круга источников, которая используется лицами, принимающими решения, в целях планирования последующих решений или действий на стратегическом, оперативном или тактическом уровнях. Сбор, хранение, использование и обмен оперативной информацией должны осуществляться с соблюдением обязательств государств-членов по международному праву прав человека.
Оперативная информация из открытых источников (OSINT)	Оперативная информация, полученная из общедоступных источников[10].

5 Rebecca Freese, Evidence-Based Counter-terrorism or Flying Blind? How to Understand and Achieve What Works («Борьба с терроризмом, основанная на фактических данных, или полет вслепую? Как понять и достичь того, что работает»), *Perspectives on Terrorism* 8, no. 1 (2014): 37.

6 Руководство ИДКТК по содействию в использовании и обеспечении допустимости в качестве доказательства в национальных уголовных судах информации, собранной, обработанной, сохраненной и предоставленной вооруженными силами для привлечения к ответственности за преступления террористического характера (2021 г.).

7 Искусственный интеллект, интернет вещей, блокчейн-технологии, криптоактивы, дроны и беспилотные летательные системы, ДНК, отпечатки пальцев, кибертехнологии, системы распознавания лиц, 3D-печать.

8 Проектный документ CT TECH — Приложение I. Описание действий, URL: https://www.interpol.int/Crimes/Terrorism/Counter-terrorism-projects/Project-CT-Tech

9 Ross Gruetzemacher, The Power of Natural Language Processing («Сила обработки естественного языка»), *Harvard Business Review*, April 19, 2022, URL: https://hbr.org/2022/04/the-power-of-natural-language-processing; Ben Lutkevich and Ed Burns, What Is Natural Language Processing? An Introduction to NLP («Что такое обработка естественного языка? Введение в ОЕЯ»), Enterprise AI, URL: https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP (дата обращения: 1 июля 2024 г.).

10 Rob Flanders et al., Cyber Threat Intelligence in Government: A Guide for Decision Makers and Analysts («Сбор и анализ оперативной информации о киберугрозах на государственном уровне: руководство для лиц, ответственных за принятие решений, и аналитиков»), 2nd ed. (United Kingdom, 2019), 22–24, URL: https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf

Оперативная информация из социальных сетей (SOCMINT)	Оперативная информация, собранная с помощью социальных сетей.
Отстранение	Процесс, в ходе которого человек, проявляющий признаки радикализации, убеждается в необходимости либо «покинуть свою группу, либо отвергнуть насилие, при этом не обязательно целью ставится изменение его основополагающей экстремистской точки зрения или идеологии»[11].
Проектная безопасность	Установка средств обеспечения безопасности на этапе строительства объекта для его надлежащей защиты от угроз в рамках существующей структуры/конфигурации/конструкции[12].
Реабилитация	Комплексный процесс, в идеале приводящий к тому, что реабилитированный человек будет вести самостоятельную и самодостаточную жизнь, не придерживаясь экстремистских взглядов и не участвуя в экстремистской деятельности (включая насилие).
Реинтеграция	Комплексный процесс возвращения человека в социальную и (или) функциональную среду.
Стандартные операционные процедуры (СОП)	Заранее определенная последовательность шагов, которые предпринимаются для реализации соответствующей политики.
Терроризм	Преступные деяния, в том числе против гражданского населения, совершаемые с намерением причинить смерть или серьезные телесные повреждения, или акты захвата заложников, которые призваны вызвать состояние ужаса у широких слоев населения, группы лиц или отдельных лиц, запугать население или заставить правительство или международную организацию совершить или воздержаться от совершения какого-либо действия, и которые являются преступлениями в рамках и в соответствии с определениями международных конвенций и протоколов в области противодействия терроризму[13].
Уголовное расследование	Процесс сбора информации (или доказательств) для установления факта совершения преступления, выявления преступника и представления доказательств в поддержку обвинения в судебном разбирательстве.
Уголовное правосудие	Юридический процесс, который предусматривает предъявление обвинений в совершении уголовно наказуемого деяния физическому или юридическому лицу, проведение судебных слушаний, разрешение дела, назначение наказания, а также исправление и реабилитацию осужденных.

11 Vidino and Bennett, 8.

12 Европейская комиссия, «Проектируемая безопасность: защита общественных мест от террористических атак» (Люксембург: Европейский союз, 2022 г.), 23, URL: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC131172/JRC131172_01.pdf

13 См. S/RES/1566 (2004), пункт 3.

Краткое содержание

Настоящий документ, «Разработка мер реагирования в рамках национальной контртеррористической политики для противодействия использованию новых технологий в террористических целях», представляет собой всеобъемлющую основу, призванную помочь разработчикам политики и заинтересованным сторонам в области борьбы с терроризмом понять влияние новых технологий на терроризм и сформулировать эффективные меры реагирования в рамках национальной контртеррористической политики. Он охватывает широкий спектр ключевых соображений при разработке мер реагирования в рамках национальной контртеррористической политики в ответ на использование новых технологий в террористических целях и предоставляет примеры передовой практики и практические идеи, которые призваны помочь разработчикам политики и практикующим специалистам в разработке эффективной контртеррористической политики и стратегии. В данном руководстве рассматриваются существующие меры политики и стратегии по борьбе с терроризмом и выявляются пробелы в том, как они решают проблему использования новых технологий в террористических целях.

В качестве информационных источников при разработке и составлении настоящего руководства был использован широкий спектр материалов, включая исследования, анализ и консультации с соответствующими заинтересованными сторонами и экспертами. Исследование было сосредоточено на выявлении ключевых проблем и возможностей, предоставляемых новыми технологиями в контексте террористической деятельности, а также существующих мер реагирования в рамках контртеррористической политики и стратегии. Оно включало в себя анализ существующей литературы, тематических исследований и передовой практики, а также определение на основе этих источников ключевых компонентов и эффективных стратегий для разработки мер реагирования в рамках контртеррористической политики. В данном руководстве представлен подробный анализ проблем, возникающих в результате использования террористами новых технологий, и предлагаются практические рекомендации по мерам реагирования. Оно включает в себя примеры передовой практики и успешных мер реагирования государств-членов. Терминология, касающаяся новых технологий, охватывает широкий спектр различных технологий, однако в данном руководстве более конкретно рассматриваются использование и злоупотребление новыми технологиями, такими как Интернет, социальные сети, криптовалюта, технология распознавания лиц и даркнет.

В руководстве признается, что технологии развиваются быстрее, чем может измениться национальная политика, и поэтому в нем предлагается основа для оценки эффективности политики и разработки поправок, которые позволят сохранить ее актуальность. В нем также подчеркивается, что многие существующие примеры контртеррористической политики не учитывают такие технологические возможности, как искусственный интеллект, даркнет, приложения со сквозным шифрованием и цифровые активы. В руководстве уделяется особое внимание использованию новых технологий в террористических целях и освещаются потенциальные возможности использования новых технологий в борьбе с терроризмом. Данное руководство построено вокруг четырех основных аспектов: осведомленность, вмешательство в отношении угроз, национальные возможности и сотрудничество, каждый из которых включает перекрестные компоненты, участвующие в процессе разработки политики, позволяющей эффективно реагировать на использование новых технологий в террористических целях.

В руководстве подчеркивается важность комплексной политики, определяющей институциональные мандаты, организационные обязанности, механизмы сотрудничества и координации между организациями, а также распределение ресурсов для развития национального потенциала. Далее в документе говорится о том, что важность разработки новой практики, инструментов и методов является одной из наиболее серьезных проблем, стоящих перед правоохранительными органами. Таким образом, необходимы скоординированные усилия различных государственных ведомств, правоохранительных органов, вооруженных сил и других заинтересованных сторон для обеспечения национальной безопасности параллельно с обеспечением защиты прав и свобод человека.

Одно из основных допущений, применяемых в настоящем документе, заключается в том, что динамичный ландшафт новых технологий требует, чтобы при разработке мер контртеррористической политики также учитывалась оценка эффективности стратегии по борьбе с терроризмом. Эта оценка необходима для корректировок, основанных на механизме постоянной обратной связи и сотрудничества между государственными

ведомствами, частным сектором и гражданским обществом. В руководстве предполагается, что в рамках контртеррористической политики необходимо решить ключевые вопросы для оценки технологических угроз и реагирования на них, включая понимание технологических возможностей и террористических мотивов, а также уделить особое внимание сбору оперативной информации об угрозах.

Разработка мер реагирования в рамках национальной контртеррористической политики, направленных на противодействие использованию новых технологий в террористических целях, является важным ресурсом для правительств, разработчиков политики и практикующих специалистов в создании эффективной и всеобъемлющей контртеррористической политики и стратегии. В данном руководстве представлена комплексная основа, которая рассматривает проблемы, возникающие в результате использования террористами новых технологий, и предлагает практические рекомендации по мерам реагирования. Ориентируясь на использование новых технологий в террористических целях, оно помогает странам сохранять контроль над ситуацией и эффективно реагировать на новые угрозы.

[I]

Базовая информация

1.1 Обзор

Государства — члены Организации Объединенных Наций придают большое значение вопросу влияния новых технологий в борьбе с терроризмом. В ходе седьмого обзора Глобальной контртеррористической стратегии Организации Объединенных Наций (A/RES/75/291)[14] в июле 2021 года государства-члены выразили глубокую озабоченность «использованием Интернета и других информационно-коммуникационных технологий, включая платформы социальных сетей, в террористических целях, в том числе непрекращающимся распространением террористического контента», и попросили Контртеррористическое управление и другие соответствующие структуры в рамках Глобального договора по координации контртеррористической деятельности «совместно поддерживать инновационные меры и подходы в том, что касается наращивания у государств-членов (по их запросу) способности учитывать в деле предупреждения терроризма и борьбы с ним те вызовы и возможности, которые порождаются новыми технологиями, включая аспекты, относящиеся к правам человека». Резолюции 2178 (2014)[15] и 2396 (2017)[16] Совета Безопасности призывают государства-члены сотрудничать при принятии национальных мер, призванных воспрепятствовать использованию террористами технологий и средств связи для совершения террористических атак. Резолюция 2396 (2017) Совета Безопасности также призывает государства-члены **расширять сотрудничество с частным сектором, особенно с компаниями, работающими в секторе информационно-коммуникационных технологий (ИКТ)**, в деле сбора цифровых данных и доказательств по делам, связанным с терроризмом.

В своем 30-м докладе Совету Безопасности Организации Объединенных Наций[17] Группа по аналитической поддержке и наблюдению за санкциями отметила, что «многие государства-члены подчеркнули растущую роль социальных сетей и других онлайн-технологий в финансировании терроризма и распространении пропаганды». Платформы, на которые ссылаются государства-члены, включают Telegram, Rocket.Chat, Hoop и TamTam, среди прочих. В докладе также говорится о том, что **сторонники ИГИЛ используют платформы в даркнете** для хранения учебных материалов, размещать которые другие сайты отказываются, и доступа к ним, а также **для приобретения новых технологий**.

Противодействие использованию новых и новейших технологий в террористических целях обсуждалось на специальном заседании Контртеррористического комитета (КТК) Совета Безопасности Организации Объединенных Наций, которое состоялось 28–29 октября 2022 года в Нью-Дели и завершилось принятием документа, не имеющего обязательной силы и известного как Делийская декларация[18].

14 Глобальная контртеррористическая стратегия Организации Объединенных Наций: седьмой обзор (A/RES/75/291), URL: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F75%2F291&Language=E&DeviceType=Desktop&LangRequested=False

15 Резолюция 2178 (2014) Совета Безопасности, URL: http://undocs.org/S/RES/2178(2014)

16 Резолюция 2396 (2017) Совета Безопасности, URL: http://undocs.org/S/RES/2396(2017)

17 Тридцатый доклад Группы аналитической поддержки и наблюдения за санкциями, представленный во исполнение резолюции 2610 (2021) по «Исламскому государству Ирака и Леванта» (ИГИЛ), «Аль-Каиде» и связанным с ними лицам, группам, предприятиям и организациям, S/2022/547 (undocs.org)

18 Делийская декларация, URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_special_meeting_outcome_document.pdf

КТК **«с озабоченностью отметил расширение использования в глобализованном обществе террористами и их сторонниками Интернета и других информационно-коммуникационных технологий,** включая платформы социальных сетей, в террористических целях» и признал **«необходимость обеспечения баланса между стимулированием инноваций и предотвращением использования новых и новейших технологий — по мере расширения их применения — в террористических целях, а также противодействием такому их использованию»**, особо отметив **«необходимость сохранения глобальной цифровой связности и свободного, надежного потока информации,** что способствовало бы экономическому развитию, коммуникации, участию и доступу к информации».

1.2 Инициатива CT TECH

CT TECH — это совместная инициатива КТУ ООН/КТЦ ООН и Интерпола, реализуемая в рамках Глобальной контртеррористической программы КТУ ООН/КТЦ ООН по кибербезопасности и новым технологиям. Она направлена на укрепление потенциала правоохранительных органов и органов уголовного правосудия в отдельных государствах-партнерах для противодействия использованию новых и новейших технологий в террористических целях, а также на оказание поддержки правоохранительным органам государств-партнеров в использовании новых и новейших технологий в борьбе с терроризмом.

Для достижения общей цели предусмотрена реализация инициативы CT TECH по двум направлениям, состоящим из шести компонентов.

РИСУНОК 1

ТАБЛИЦА 1. **Направления и компоненты CT TECH**

Направление 1: принятие эффективных мер реагирования в рамках контртеррористической политики в ответ на вызовы и возможности новых технологий в борьбе с терроризмом при полном соблюдении прав человека и принципа верховенства права.	
 Компонент 1.1	Подготовка информационных материалов для разработки мер реагирования в рамках национальной контртеррористической политики в ответ на вызовы и возможности новых технологий в борьбе с терроризмом при полном уважении прав человека и принципа верховенства права.
 Компонент 1.2	Повышение уровня осведомленности и знаний о передовой практике в области идентификации рисков и преимуществ, связанных с новыми технологиями в контексте борьбы с терроризмом, при полном уважении прав человека и принципа верховенства права.
 Компонент 1.3	Укрепление потенциала отдельных государств-партнеров в сфере разработки эффективных мер реагирования в рамках национальной контртеррористической политики для противодействия использованию террористами новых технологий и применения новых технологий в деле борьбы с терроризмом при полном уважении прав человека и принципа верховенства права.
Направление 2: укрепление оперативного потенциала правоохранительных органов и органов уголовного правосудия для противодействия использованию новых технологий в террористических целях и применения новых технологий в деле предотвращения терроризма и борьбы с ним при полном соблюдении прав человека и принципа верховенства права.	
 Компонент 2.1	Предоставление практических инструментов и руководства для правоохранительных органов в целях противодействия использованию новых технологий в террористических целях и применения новых технологий в деле предотвращения терроризма и борьбы с ним при полном уважении прав человека и принципа верховенства права.
 Компонент 2.2	Развитие у специалистов правоохранительных органов и органов уголовного правосудия государств-партнеров навыков, направленных на противодействие использованию новых технологий в террористических целях и применение новых технологий в деле предотвращения терроризма и борьбы с ним при полном уважении прав человека и принципа верховенства права.
 Компонент 2.3	Расширение международного сотрудничества и обмена информацией между органами полиции государств-партнеров по вопросам противодействия использованию террористами новых технологий и применения новых технологий в борьбе с терроризмом.

1.3 Цель и назначение документа

Цель настоящего документа состоит в том, чтобы обеспечить наличие у государств-членов необходимого понимания и инструментов для эффективной оценки и снижения угроз, а также реагирования на угрозы в их зонах ответственности (ЗО). Этот документ призван дать рекомендации по проведению оценки угроз на национальном уровне, повысить уровень осведомленности и стать необязательным руководством по передовому опыту в контексте разработки и реализации процесса оценки угроз и рисков, связанных с использованием новых технологий в террористических целях. Содержащиеся в нем материалы помогут разработчикам политики повысить эффективность планируемых мер реагирования на террористические угрозы, в особенности потому, что они касаются использования новых технологий в целях совершения злоумышленных действий.

1.3.1 Сфера охвата

В данном руководстве представлен подробный анализ проблем, возникающих в результате использования террористами новых технологий, и предлагаются практические рекомендации по мерам реагирования. Оно включает в себя примеры передовой практики и успешных мер реагирования государств-членов. Терминология, касающаяся новых технологий, охватывает широкий спектр различных технологий, однако в данном руководстве более конкретно рассматриваются использование и злоупотребление новыми технологиями, такими как Интернет, социальные сети, криптовалюта, технология распознавания лиц и даркнет.

1.3.2 Целевая аудитория

Настоящий документ предназначен в первую очередь для политиков, государственных чиновников, специалистов по борьбе с терроризмом, правоохранительных органов, спецслужб и соответствующих заинтересованных сторон, участвующих в борьбе с терроризмом. Целью данного руководства является предоставление всеобъемлющей информации и рекомендаций по формулированию эффективной политики и стратегий для решения проблем, возникающих в результате использования новых технологий в террористических целях. В нем рассматриваются конкретные потребности и обязанности целевой аудитории. Оно также предоставляет практические рекомендации и примеры передовой практики для других соответствующих заинтересованных сторон, таких как международные организации, дипломаты, разработчики политики, исследователи и ученые, специализирующиеся в таких областях, как борьба с терроризмом, технологии и разработка политики, эксперты, участвующие в международном сотрудничестве и сотрудничестве в борьбе с терроризмом, а также представители частного сектора и технологических компаний.

1.3.3 Преимущества

Настоящий документ отражает потребности и перспективы широкого круга заинтересованных сторон, включая экспертов в области борьбы с терроризмом, правительственных чиновников, правоохранительных и разведывательных органов, ученых и организаций гражданского общества. Целью данного документа является повышение способности разработчиков политики по взаимодействию с новыми технологиями в рамках стратегического планирования контртеррористической деятельности, будь то посредством реагирования на использование новых технологий в террористических целях или посредством их использования для реагирования на террористическую деятельность.

Данное руководство представляет собой всеобъемлющую основу и охватывает широкий спектр ключевых соображений при разработке мер реагирования в рамках национальной контртеррористической политики для противодействия использованию новых технологий в террористических целях. Оно также включает описание передовой практики, которая показывает, каким образом разные государства-члены либо использовали новые технологии для борьбы с терроризмом, либо реагировали на использование новых технологий в террористических целях. Это описание дает практическую информацию, которая призвана помочь разработчикам политики и практикующим специалистам в разработке эффективной политики и стратегии борьбы с терроризмом. В руководстве уделяется особое внимание использованию новых технологий, которые стремительно развиваются и тем самым создают новые вызовы и угрозы, в террористических целях. В нем также освещаются некоторые потенциальные возможности использования новых технологий в борьбе с терроризмом. Рекомендации по решению этих проблем, представленные в руководстве, призваны помочь государствам-членам оставаться на шаг впереди и эффективно реагировать на новые угрозы.

1.3.4 Ограничения

Разработка мер реагирования в рамках национальной контртеррористической политики для противодействия использованию новых технологий в террористических целях имеет ряд ограничений. Несмотря на то что данное руководство разработано таким образом, чтобы обеспечить его гибкость и адаптируемость к различным национальным контекстам, в нем учитывается разный уровень зрелости возможностей государств-членов по разработке мер реагирования, разные потребности и приоритеты, а также содержатся рекомендации для разработчиков политики и практикующих специалистов по адаптации разрабатываемых подходов. Данное руководство основано на уровне технологического развития и имеющихся сведениях об известных угрозах на момент его публикации. По мере появления новых и развития уже существующих технологий может возникнуть необходимость разработки новой стратегии, учитывающей фактические потребности и обстоятельства в соответствии с будущими особенностями новых технологий, которые не были учтены в данном руководстве.

[III]

Подход

2.1 Обзор

Цель настоящего доклада заключается в том, чтобы предоставить государствам-членам поддержку и возможности для эффективной разработки мер реагирования на уровне контртеррористической политики в рамках усилий по противодействию использованию новых технологий в террористических целях, которые соответствуют Глобальной контртеррористической стратегии Организации Объединенных Наций и реализуются при полном уважении прав человека и принципа верховенства права.

2.2 Руководящая основа

РИСУНОК 2

Руководящей основой является концептуальная модель, которая выступает в качестве направляющего, синхронизирующего и информационного ориентира при подготовке Доклада. Она призвана обеспечить согласованность Глобальной контртеррористической стратегии (ГКТС) Организации Объединенных Наций с национальной контртеррористической политикой и стратегией государства-члена на всех этапах — от разработки до реализации — на уровне целей и результатов, механизмов и потенциала правоохранительных органов и органов уголовного правосудия в отношении новых технологий.

ГКТС Организации Объединенных Наций, принятая Генеральной Ассамблеей, определяет широкий спектр действий государств-членов по борьбе с террористическими угрозами в рамках четырех основных направлений:

Направление I:	Меры по устранению условий, способствующих распространению терроризма
Направление II:	Меры по предотвращению терроризма и борьба с ним
Направление III:	Меры по укреплению потенциала государств по предотвращению терроризма и борьбе с ним и укреплению роли системы Организации Объединенных Наций в этой области
Направление IV:	Меры по обеспечению всеобщего уважения прав человека и верховенства права в качестве фундаментальной основы для борьбы с терроризмом

Государствам-членам рекомендуется выработать собственные политико-правовые основы борьбы с терроризмом в соответствии с ГКТС Организации Объединенных Наций. Они должны обеспечить, чтобы принятые ими контртеррористические законы, политики, стратегии и меры отвечали их обязательствам по международному праву, включая международное право прав человека, международное беженское право и международное гуманитарное право. Политико-правовые основы борьбы с терроризмом государств-членов должны быть направлены на предотвращение и устранение насильственного экстремизма, который может способствовать терроризму, предотвращение террористической деятельности или ограничение возможностей для ее осуществления, принятие соответствующих мер по защите граждан, находящихся под юрисдикцией государства, а также служб и инфраструктуры от обоснованно предсказуемых угроз совершения террористических атак и привлечение террористов к ответственности за их деяния.

Для достижения намеченных результатов и целей в борьбе с терроризмом в распоряжении национальных правоохранительных органов и органов уголовного правосудия государств-членов имеется целый ряд инструментов. К ним относятся, среди прочего, следующие:

ТАБЛИЦА 2. **Механизмы национальных правоохранительных органов и органов уголовного правосудия высокого порядка в борьбе с терроризмом**

Механизмы	Описание
Уголовное правосудие	Юридический процесс, который предусматривает предъявление обвинений в совершении уголовно наказуемого деяния физическому или юридическому лицу, проведение судебных слушаний, разрешение дела и назначение наказания, а также исправление и реабилитацию осужденных.
Оперативная информация	Результат сбора, разработки, распространения, анализа и интерпретации данных, полученных из широкого круга источников, для информирования лиц, принимающих решения, в целях планирования последующих решений или действий на стратегическом, оперативном или тактическом уровнях. Сбор, хранение, использование и обмен оперативной информацией должны осуществляться в соответствии с обязательствами государств-членов по международногму праву прав человека.
Уголовное расследование	Процесс сбора информации (или доказательств) для установления факта совершения преступления, выявления преступника и представления доказательств для уголовного преследования.
Действия правоохранительных органов	Этот термин, как правило, описывает действия правоохранительных органов, предпринятые для противодействия угрозе, которые могут включать задержание отдельных лиц, пресечение деятельности злоумышленников (например, удаление контента, арест активов) и т. д.
Реабилитация	В контексте уголовного правосудия термин «реабилитация» используется для обозначения мероприятий, проводимых исправительной системой с целью изменения взглядов или поведения правонарушителей, для того чтобы снизить вероятность повторного совершения ими преступления, а также подготовить и обеспечить их реинтеграцию в общество.
Реинтеграция	Комплексный процесс возвращения человека в социальную и (или) функциональную среду.

Эффективное использование и развертывание указанных механизмов и инструментов зависит от имеющихся возможностей. Нередко возможности, требуемые для обеспечения реализации механизмов, определяют и представляют с помощью модели возможностей. Модель возможностей состоит в распределении ключевых функций по логическим детализированным группам в процессе осуществления механизмов и мер. Модель возможностей определяет требования к персоналу (структуре и навыкам), процессам, технологиям, инфраструктуре и финансам.

Руководящая основа служит для обеспечения максимальной согласованности между стратегией и ее реализацей в обоих направлениях — «сверху вниз» и «снизу вверх».

2.3 Методология

РИСУНОК 3

В качестве информационных источников при разработке и составлении настоящего документа, «Разработка мер реагирования в рамках национальной контртеррористической политики для противодействия использованию новых технологий в террористических целях», был использован широкий спектр материалов, включая документы проекта CT TECH, консультации с заинтересованными сторонами, данные внутреннего анализа, кабинетные исследования, совещания экспертных групп, сотрудничество с различными структурами в рамках Глобального договора по координации контртеррористической деятельности, а также руководящая основа, описанная выше в разделе 2.2. Исследование было сосредоточено на выявлении ключевых проблем и возможностей, предоставляемых новыми технологиями в контексте террористической деятельности, а также существующих мер реагирования на уровне контртеррористической политики и стратегии.

Первый шаг включал проведение обширных исследований проблем и возможностей, которые предоставляют новые технологии в контексте борьбы с терроризмом. Данное кабинетное исследование включало в себя анализ существующей литературы, тематических исследований и передовой практики с целью выявления ключевых компонентов и эффективных стратегий разработки мер реагирования в рамках контртеррористической политики, включая анализ новых технологий и их возможного использования в террористических целях, равно как и потенциала их использования практикующими специалистами для борьбы с терроризмом. Второй шаг включал выявление передовой практики в области мер реагирования в рамках контртеррористической политики и стратегии, направленных на решение проблемы использования новых технологий в террористических целях. Третий этап включал разработку предварительной версии руководства, которая была

передана соответствующим заинтересованным сторонам и экспертам для получения отзывов. Полученные отзывы были включены в окончательную версию руководства, где были определены ключевые соображения и перекрестные компоненты, что позволило отразить в нем новейшие идеи и примеры передовой практики в данной области. На основе исследований, анализа и консультаций была разработана всеобъемлющая основа для разработки мер реагирования в рамках национальной контртеррористической политики для противодействия использованию новых технологий в террористических целях.

Эта основа включает в себя несколько соображений, направленных на устранение пробелов в контртеррористических стратегиях в отношении новых технологий. Она также призвана предоставить примеры передовой практики для разработки контртеррористической политики и протоколов для устранения угроз, исходящих от новых технологий, которые могут быть использованы террористами.

Источниками информации для кабинетного исследования послужили национальные оценки угроз и рисков государств-членов, данные межправительственных организаций, документы государственного и частного секторов об оценке угроз, а также научные материалы. Поскольку настоящий документ посвящен проведению оценки угроз и рисков применительно к новым технологиям, важно отметить, что некоторые модели, которые использовались в качестве источников информации, также были разработаны на базе систем оценки угроз в области кибербезопасности.

2.3.1 Совещания экспертных групп и консультации

Данное руководство было разработано при участии экспертов в рамках совещаний экспертных групп (СЭГ), а также по результатам индивидуальных консультаций и обзоров. СЭГ объединили экспертов и практиков из контртеррористических служб и правоохранительных органов, правозащитных организаций, частного сектора, научных кругов и гражданского общества для обсуждения вопросов, связанных с противодействием использованию новых технологий в террористических целях, применением новых технологий в рамках проводимой работы, определением передовых практик в этой области, а также для обсуждения рисков, проблем и неудачного опыта, требующих внимания и осторожности. Руководство было доработано в ходе взаимодействия со структурами Глобального договора по координации контртеррористической деятельности Организации Объединенных Наций и его Рабочей группой по новым угрозам и защите критически важной инфраструктуры, которая содействует координации и согласованности усилий, прилагаемых государствами-членами для предотвращения возникающих террористических угроз и реагирования на них с соблюдением прав человека и принципа верховенства права в качестве фундаментальной основы в соответствии с международным правом, включая право прав человека, беженское право и гуманитарное право.

2.3.2 Обзор справочных материалов

При разработке настоящего руководства были задействованы, приняты во внимание, дополнены и использованы в качестве основы данные многочисленных исследований, руководств и публикаций, среди которых:

ТАБЛИЦА 3. Справочные материалы

1	Amritt, Carl, Eliot Bradshaw, and Alyssa Schulenberg. "Threat Assessment and Management: Practices Across the World" («Оценка угроз и управление ими: обзор мировой практики»). Domestic Preparedness, February 1, 2023. https://www.domesticpreparedness.com/preparedness/threat-assessment-and-management-practices-across-the-world
2	Bloom, Mia, Hicham Tiflati, and John Horgan. "Navigating ISIS's Preferred Platform: Telegram" («Обзор предпочтительной платформы ИГИЛ: Telegram»). *Terrorism and Political Violence* 31, no. 6 (November 2, 2019): 1242–54. https://doi.org/10.1080/09546553.2017.1339695
3	"Counter Terrorism Legal Framework: Lessons Learned from IDLO Policy Dialogues in Collaboration with UNODC" («Правовая основа борьбы с терроризмом: уроки, извлеченные из политических диалогов МОПР в сотрудничестве с УНП ООН») *Development Law Update*, no. 2 (2007). https://www.files.ethz.ch/isn/138640/14.pdf
4	Агентство по кибербезопасности и защите инфраструктуры США, Федеральное бюро расследований, Агентство национальной безопасности, Австралийский центр кибербезопасности, Канадский центр кибербезопасности, Группа реагирования на компьютерные чрезвычайные ситуации Новой Зеландии, Национальный центр кибербезопасности Великобритании, Федеральное управление по информационной безопасности Германии (BSI) и Национальный центр кибербезопасности Нидерландов. «Изменение баланса рисков кибербезопасности: принципы и подходы к проектируемой безопасности и безопасности по умолчанию»), April 13, 2023. https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf
5	Европейская комиссия. «Контртеррористическая повестка ЕС: предвидеть, предупреждать, защищать, реагировать». Сообщение Комиссии Европейскому парламенту, Совету, Европейскому экономическому и социальному комитету и Комитету по делам регионов. Брюссель, Бельгия: Европейская Комиссия, 2020 г. https://home-affairs.ec.europa.eu/system/files/2020-12/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf
6	Европейская комиссия. «Закон о киберустойчивости», 15 сентября 2022 г. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
7	Европейская комиссия. «Проектируемая безопасность: защита общественных мест от террористических атак». Люксембург: Европейский союз, 2022 г. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC131172/JRC131172_01.pdf
8	Европейская комиссия: Информационная служба общественных исследований и разработок (CORDIS). «Обнаружение и анализ онлайн-контента и финансовой деятельности, связанных с терроризмом». https://cordis.europa.eu/project/id/700367 (дата обращения: 1 июля 2024 г.)
9	Европейская комиссия: Информационная служба общественных исследований и разработок (CORDIS). «Поиск и анализ гетерогенного онлайн-контента для распознавания террористической деятельности». https://cordis.europa.eu/project/id/700024 (дата обращения: 1 июля 2024 г.)
10	Европейский центр по борьбе с киберпреступностью (EC3). «Оценка угроз организованной преступности в Интернете за 2019 год». Европол, 2019 г. https://www.europol.europa.eu/cms/sites/default/files/documents/ioc-ta_2019.pdf
11	Европейский союз. «Директива (ЕС) 2017/541 Европейского парламента и Совета от 15 марта 2017 г. о борьбе с терроризмом и замене рамочного решения Совета 2002/475/JHA и внесении изменений в Решение Совета 2005/671/JHA»), Публичный закон № 2002/475/JHA, 088 OJ L 6 (2017 г.). http://data.europa.eu/eli/dir/2017/541/oj/eng
12	Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ). «Виртуальные активы». https://www.fatf-gafi.org/en/topics/virtual-assets.html (дата обращения: 1 июля 2024 г.)
13	Министерство внутренних дел Финляндии. «Национальная контртеррористическая стратегия на 2022–2025 гг.», Публикации Министерства внутренних дел, 2022:38. Хельсинки, Финляндия: Министерство внутренних дел Финляндии, 2022 г. https://julkaisut.valtioneuvosto.fi/handle/10024/164447

ТАБЛИЦА 3. **Справочные материалы**

14 Flanders, Rob, Lucy Johnson, Matthew Trevelyan, Anna Whitmore, Lisa Lesowiec, and Rajinder Tumber. "Cyber Threat Intelligence in Government: A Guide for Decision Makers and Analysts" («Сбор и анализ оперативной информации о киберугрозах на государственном уровне: руководство для лиц, ответственных за принятие решений, и аналитиков»), 2nd ed. United Kingdom, 2019. https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf

15 Freese, Rebecca. "Evidence-Based Counter-terrorism or Flying Blind? How to Understand and Achieve What Works" («Борьба с терроризмом, основанная на фактических данных, или полет вслепую? Как понять и достичь того, что работает»). *Perspectives on Terrorism* 8, no. 1 (2014): 37–56. http://www.jstor.org/stable/26297099

16 Правительство Австралии. «Защищаем наше сообщество вместе: контртеррористическая стратегия Австралии до 2022 года». Австралия: Содружество Австралии, 2022 г. https://www.nationalsecurity.gov.au/what-australia-is-doing-subsite/Files/safeguarding-community-together-ct-strategy-22.pdf

17 Gruetzemacher, Ross. "The Power of Natural Language Processing" («Сила обработки естественного языка»). *Harvard Business Review*, April 19, 2022. https://hbr.org/2022/04/the-power-of-natural-language-processing

18 Министерство внутренних дел Испании. «Национальная контртеррористическая стратегия, 2019 г.». https://www.dsn.gob.es/eu/file/4271/download?token=-K6uOf-C

19 Объединенная группа по оценке борьбы с терроризмом (JCAT). «Руководство по борьбе с терроризмом для сотрудников органов общественной безопасности». Правительство. Директор Национальной разведки. https://www.dni.gov/nctc/jcat/index.html (дата обращения: 1 июля 2024 г.)

20 Lutkevich, Ben, and Ed Burns. "What Is Natural Language Processing? An Introduction to NLP" («Что такое обработка естественного языка? Введение в ОЕЯ»). Enterprise AI. https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP (дата обращения: 1 июля 2024 г.)

21 Национальный центр кибербезопасности. «Концепция проектируемой безопасности». Национальный центр кибербезопасности, 7 марта 2018 г. https://www.ncsc.gov.uk/information/secure-default

22 Служба безопасности и разведки Новой Зеландии. «Как можно помочь: форма участия общественности». https://providinginformation.nzsis.govt.nz/ (дата обращения: 1 июля 2024 г.)

23 Транспортное агентство Новой Зеландии. «Реестр рисков». Правительство. Транспортное агентство Новой Зеландии. https://www.nzta.govt.nz/roads-and-rail/rail/operating-a-railway/risk-management/risk-register (дата обращения: 1 апреля 2023 г.)

24 Департамент ОБСЕ по транснациональным угрозам. «Статус универсальных контртеррористических конвенций и протоколов, а также других международных и региональных правовых инструментов, касающихся терроризма и сотрудничества по уголовным делам в регионе ОБСЕ». Организация по безопасности и сотрудничеству в Европе (ОБСЕ), июль 2018 г. https://www.osce.org/files/f/documents/5/8/17138_0.pdf

25 Romyn, David, and Mark Kebbell. "Terrorists' Planning of Attacks: A Simulated 'Red-Team' Investigation into Decision-Making" («Планирование террористами нападений: моделирование процесса принятия решений силами «красной команды»). *Psychology, Crime & Law 20*, no. 5 (May 28, 2014): 480–96. https://doi.org/10.1080/1068316X.2013.793767

26 Schneier, Bruce, and Tarah Wheeler. "Hacked Drones and Busted Logistics Are the Cyber Future of Warfare" («Взломанные дроны и разрушенная логистика — кибербудущее войны»). Brookings. Tech Stream (блог), June 4, 2021. https://www.brookings.edu/techstream/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/

27 Spulak, Robert G. "Science Technology and Innovation in Combating Terrorism" («Наука, технологии и инновации в борьбе с терроризмом»), февраль 2015 г. https://www.osti.gov/

28 Talley, Ian. "Islamic State Turns to NFTs to Spread Terror Message" («Исламское государство» обращается к использованию NFT-токенов для распространения террористических посланий»). *Wall Street Journal*, September 4, 2022, sec. Politics. https://www.wsj.com/articles/islamic-state-turns-to-nfts-to-spread-terror-message-11662292800

29 Terrell Hanna, Katie. "What Is the Dark Web (Darknet)?" WhatIs.com. [«Что такое даркнет (даркнет)?»). Веб-сайт WhatIs.com.] https://www.techtarget.com/whatis/definition/dark-web (дата обращения: 1 июля 2024 г.)

30 Содружество Австралии. «Белая книга внешней политики за 2017 год», в ред. Morris Walker Pty Ltd. Австралия, 2017 г. https://www.dfat.gov.au/sites/default/files/2017-foreign-policy-white-paper.pdf

ТАБЛИЦА 3. **Справочные материалы**

31	Объединение киберкластеров Великобритании (UKC3). «Операционная основа киберкластеров». UK Cyber Cluster Collaboration (блог). https://ukc3.co.uk/cyber-cluster-operating-framework/ (дата обращения: 1 июля 2024 г.)
32	Соединенное Королевство, «CONTEST: Контртеррористическая стратегия Соединенного Королевства». Соединенное Королевство: Британская корона, 2018 г. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf
33	Министерство бизнеса, энергетики и промышленной стратегии Соединенного Королевства. Законопроект о национальной безопасности и инвестициях, Публичный закон № BEIS006(F)-20-CCP (2020 г.) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/934276/nsi-impact-assessment-beis.pdf
34	Контртеррористический центр Организации Объединенных Наций (КТЦ ООН). «Итог обсуждений: международная конференция по национальным и региональным стратегиям борьбы с терроризмом — 31 января — 1 февраля 2013 г.», Краткое содержание конференции. Богота, Колумбия, 2013 г. https://www.un.org/counterterrorism/sites/www.un.org.counter-terrorism/files/bogota_jan-feb2013.pdf
35	Контртеррористический центр Организации Объединенных Наций и Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия. «Борьба с терроризмом в Интернете с помощью искусственного интеллекта: обзор для правоохранительных и контртеррористических органов в Южной и Юго-Восточной Азии». Совместный доклад. Организация Объединенных Наций, 2021 г. https://unicri.it/sites/default/files/2021-06/Countering%20Terrorism%20Online%20with%20AI%20-%20UNCCT-UNICRI%20Report.pdf
36	Контртеррористическое управление Организации Объединенных Наций. «Международные правовые документы». https://www.un.org/counter-terrorism/international-legal-instruments (дата обращения: 1 июля 2024 г.)
37	Управление Организации Объединенных Наций по наркотикам и преступности. «Ключевые вопросы модуля 12 по борьбе с терроризмом: подотчетность, надзор за методами сбора оперативной информации». Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН), июль 2018 г. https://www.unodc.org/e4j/en/terrorism/module-12/key-issues/accountability-oversight-of-intelligence-gathering-methods.html
38	Управление Организации Объединенных Наций по наркотикам и преступности. «Международная правовая основа». https://www.unodc.org/unodc/en/terrorism/expertise/international-legal-framework.html (дата обращения: 1 июля 2024 г.)
39	Исполнительный директорат Контртеррористического комитета Совета Безопасности Организации Объединенных Наций (ИДКТК). «Аналитическая записка ИДКТК: противодействие террористическим нарративам онлайн и офлайн». Организация Объединенных Наций, 2020 г. https://www.un.org/securitycouncil/ctc/content/cted-analytical-brief-%E2%80%93-countering-terrorist-narratives-online-and-offline
40	Соединенные Штаты Америки, «Национальная контртеррористическая стратегия Соединенных Штатов Америки». Вашингтон, округ Колумбия: Белый дом, 2018 г. https://purl.fdlp.gov/GPO/gpo109871
41	Vidino, Lorenzo, and Clifford Bennett. "A Review of Transatlantic Best Practices for Countering Radicalization in Prisons and Terrorist Recidivism" («Обзор трансатлантического передового опыта противодействия радикализации в тюрьмах и террористическому рецидивизму»). Гаага, Нидерланды: Европол, 2019 г. https://www.europol.europa.eu/cms/sites/default/files/documents/a_review_of_transatlantic_best_practices_for_countering_radicalisation_in_prisons_and_terrorist_recidivism.pdf

[III] Введение

3.1 Обзор

По мере ускорения технологического прогресса террористы все чаще злоупотребляют инновациями в этой сфере для реализации своих разрушительных планов. Быстрое распространение коммуникационных платформ, социальных сетей, шифровальных методов и новейших технологий создает серьезные проблемы для правоохранительных органов. Включение новых технологий в арсенал террористических группировок создает беспрецедентные проблемы, требуя от правительств переоценки своих стратегий и адаптации своих подходов.

При разработке контртеррористической политики государства-члены должны признать острую необходимость понимания, предвидения и эффективного реагирования на использование террористами новых технологий. Такая политика ориентирована на целый ряд аспектов, включая информированность, противодействие угрозам, национальный контртеррористический потенциал, сотрудничество и инициативы по наращиванию потенциала. Принимая комплексную и гибкую национальную контртеррористическую политику, правительства стремятся опережать события, активно снижая риски, связанные с использованием новых технологий в террористических целях, и одновременно обеспечивая безопасность, неприкосновенность частной жизни, а также соблюдение основных прав и гражданских свобод своих граждан.

3.2 Новые технологии и борьба с терроризмом

Развитие цифровых технологий, инноваций в области обработки и передачи данных и Интернета привело к созданию гиперсвязанного мира, в котором доступ к информации, обмен ею и ее получение происходят практически мгновенно. По состоянию на 2022 год почти 70 процентов населения мира пользуется Интернетом,[19] из которых более 93 процентов — это пользователи социальных сетей[20]. По оценкам, в 2022 году в мире будет создано более 97 зеттабайт[21] информации[22]. В то время как подобные технологические достижения способствуют преобразованию общества во имя всеобщего блага, террористы используют эти технологии в своих злонамеренных целях. Применение новых технологий в террористических целях ставит перед государствами-членами серьезные задачи по борьбе с терроризмом, в частности, по противодействию использованию технологий, которые обеспечивают анонимность и позволяют координировать действия и действовать удаленно.

С другой стороны, новые технологии открывают широкие возможности для укрепления потенциала контртеррористических и правоохранительных органов. Например, с их помощью правоохранительные органы смогут выполнять большие объемы работы с меньшими затратами, принимать своевременные решения в ускоренном порядке, генерировать новые знания и осуществлять противодействие удаленно.

19 Отчет МСЭ о глобальной возможности установления соединений за 2022 год, URL: https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/index/

20 Инфографика Data Never Sleeps от компании Domo, Data Never Sleeps 10.0 | Domo

21 Один зеттабайт равен одному миллиарду терабайтов.

22 Statista, Total data volume worldwide 2010-2025 (отчет «Общий объем данных по всему миру за 2010–2025 годы») | Statista

Противодействие использованию террористами новых технологий зависит от понимания механизмов такого использования, разработки эффективной правовой основы и мер реагирования на уровне политики, а также наращивания оперативного потенциала для противодействия применению таких технологий в террористических целях, включая освоение и использование новых технологий.

3.2.1 Вызовы: использование новых технологий в террористических целях

Достижения в области информационно-коммуникационных технологий (ИКТ) и их доступность сделали привлекательным для террористических и насильственных экстремистских групп использование Интернета и социальных сетей для совершения широкого спектра противоправных действий, включая подстрекательство, радикализацию, вербовку, обучение, планирование, сбор информации, коммуникацию, подготовку, пропаганду и финансирование. Кроме того, в своих целях террористические группировки умело используют гендерный фактор — неравенство, нормы и роли, включая агрессивную маскулинность, — и манипулируют им. Так, ИГИЛ эффективно вербует женщин через социальные сети, адаптируя свои послания для обращения к лицам женского пола, говорящим на разных языках и живущим в разных социальных, экономических и культурных условиях в Западной Европе, Центральной Азии, на Ближнем Востоке и в Северной Африке, и нередко эксплуатируя опыт женщин в области гендерного неравенства. Террористы также используют зашифрованные коммуникации и дарквеб для обмена террористическим контентом и опытом, например, разработками самодельных взрывных устройств и стратегиями нападений, а также для координации нападений и содействия их совершению, приобретения оружия и поддельных документов. Между тем развитие технологий в области искусственного интеллекта, машинного обучения, телекоммуникаций 5G, робототехники, больших данных, алгоритмической фильтрации, биотехнологий, беспилотных автомобилей и летательных аппаратов может привести к тому, что, как только эти технологии станут коммерчески доступными, недорогими и удобными в использовании, их также смогут применять террористы для расширения диапазона и повышения уровня смертоносности своих атак.

3.2.2 Возможности: контртеррористическая деятельность правоохранительных органов

Новые технологии открывают перед правоохранительными органами безграничные возможности для эффективного противодействия терроризму с соблюдением положений международного права прав человека. Правоохранительные органы могут применять новые технологии для выявления, расследования, судебного преследования и разрешения дел о террористической деятельности новыми и более эффективными способами.

Использование оперативной информации из открытых источников обеспечивает быстрый сбор данных об интересующих объектах, что может повысить эффективность действий правоохранительных органов. Передовые технологии анализа данных и искусственного интеллекта (ИИ) позволяют обрабатывать и анализировать огромные объемы информации, благодаря чему правоохранительные органы имеют возможность выявлять закономерности, обнаруживать потенциальные угрозы и принимать превентивные меры реагирования на террористическую деятельность. Новейшие системы наблюдения, включая распознавание лиц и биометрические технологии, помогают идентифицировать и отслеживать перемещения подозреваемых, повышая эффективность расследований, предотвращая потенциальные атаки и привлекая террористов к ответственности. Кроме того, с помощью инструментов цифровой криминалистики можно получать важные доказательства путем извлечения данных из электронных устройств, что позволяет правоохранительным органам выявлять скрытые связи, разрушать террористические сети и привлекать террористов к ответственности.

Использование новых технологий может способствовать более эффективному распределению ограниченных ресурсов правоохранительных органов. При этом крайне важно, чтобы эти технологии использовались с учетом этических норм и при строгом соблюдении права на неприкосновенность частной жизни, прав человека и принципа верховенства права. Необходимо обеспечить прозрачность и подотчетность действий и их результатов, чтобы гарантировать ответственное использование новых технологий и предотвратить потенциальное злоупотребление этими мощными инструментами. Кроме того, рекомендуется внедрить комплексные программы обучения, для того чтобы сотрудники правоохранительных органов могли овладеть необходимыми навыками с целью эффективного применения новых технологий в рамках правовых и этических норм. Ответственно подходя к использованию новых технологий, правоохранительные органы могут значительно расширить свои усилия по борьбе с терроризмом и обеспечить безопасность и защиту населения.

3.2.3 Права человека и новые технологии

Терроризм бросает серьезный вызов самим принципам верховенства права, защиты прав человека и их эффективного осуществления. Он может дестабилизировать законно сформированные правительства, подорвать плюралистическое гражданское общество, поставить под угрозу мир и безопасность и иметь отрицательные последствия для социально-экономического развития. Государства обязаны принимать надлежащие меры для защиты лиц, находящихся под их юрисдикцией, от обоснованно предсказуемых угроз совершения террористических атак. Обязанность государств защищать права человека предполагает принятие необходимых и адекватных мер для предотвращения, пресечения и привлечения к ответственности за совершение действий, ставящих под угрозу эти права, таких как угроза национальной безопасности или насильственные преступления, включая терроризм. Все подобные меры должны отвечать стандартам международного права прав человека и принципа верховенства права.

В контексте использования новых и новейших технологий в контртеррористической деятельности государства должны обеспечить, чтобы соответствующие законы, политики и практики гарантировали соблюдение таких прав, как право на неприкосновенность частной жизни, право на свободу выражения мнений, свободу ассоциации, свободу мысли, совести, убеждений и религии, право на свободу и личную неприкосновенность, право на справедливое судебное разбирательство, включая презумпцию невиновности, а также принцип недискриминации. Кроме того, государства должны строго соблюдать принцип абсолютного запрета пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения и наказания.

ООН, Интерпол и ЕС неоднократно подчеркивали взаимосвязь между новыми технологиями, борьбой с терроризмом и правами человека, включая гендерное равенство. В Глобальной контртеррористической стратегии ООН и различных резолюциях Генеральной Ассамблеи и Совета Безопасности подчеркиваются обязательства государств-членов по соблюдению международного права прав человека, международного беженского права и международного гуманитарного права в деле противодействия терроризму. В частности, согласно Глобальной контртеррористической стратегии ООН «действенные меры по борьбе с терроризмом и защита прав человека являются целями, которые не противоречат, а дополняют и взаимно подкрепляют друг друга», в связи с чем необходимо принять меры по обеспечению всеобщего уважения прав человека и принципа верховенства права в качестве фундаментальной основы борьбы с терроризмом. В связи с этим в

Стратегии государствам-членам предлагается бороться с использованием Интернета и других информационно-коммуникационных технологий, включая платформы социальных сетей, в террористических целях, в том числе с непрекращающимся распространением террористического контента, при соблюдении международного права, включая международное право прав человека, а также право на свободу выражения мнений.

3.2.4 Гендер, технологии и меры реагирования в рамках политики

Понятие «гендер» охватывает роли, поведение, занятия и качества, которые в конкретном обществе в определенный период времени считаются подходящими для мужчин и женщин, девочек и мальчиков. Помимо социальных атрибутов и возможностей, ассоциируемых с принадлежностью к мужскому или женскому полу, гендер связан с отношениями между женщинами и мужчинами, девочками и мальчиками. Гендер является частью более широкого социокультурного контекста и пересекается с другими факторами идентичности, включая пол, социальный класс, расовую принадлежность, уровень бедности, этническую принадлежность, половую ориентацию, возраст и т. д. Мужчины, женщины, девочки и мальчики, а также лица с другими гендерными идентичностями и моделями самовыражения чувствуют себя в безопасности по-разному и в соответствии со своими особыми потребностями, уязвимостями и возможностями[23]. В частности, несмотря на отсутствие иерархических структур в Интернете, которое позволяет устранить гендерные ограничения и создает возможности для расширения прав и возможностей женщин, использование новых технологий также повышает вероятность их вербовки или активного участия в деятельности насильственных экстремистских и террористических групп в Интернете[24]. По имеющимся данным, террористические группы умело используют гендерные аспекты в своих онлайн-коммуникациях; например, ИГИЛ построило свою стратегию вербовки и общения в Интернете на противоречивых гендерно ориентированных сообщениях, меняя свой дискурс в зависимости от целевой группы[25]. Еще один важный аспект, касающийся гендера и новых технологий, связан с цифровым гендерным разрывом, согласно которому во всем мире доступ женщин к Интернету оценивается в 85 процентов по сравнению с мужчинами, при этом около 1,7 млрд женщин из стран Глобального Юга вообще не имеют доступа к нему. Это неравенство создает проблему прав человека, лежащую в основе всех аспектов кибербезопасности, включая потенциальное воздействие, отсутствие безопасности или участие в управлении[26].

Таким образом, интеграция гендерных аспектов имеет решающее значение в рамках национальной контртеррористической политики, а также для разработки соответствующих мер реагирования, учитывающих особые потребности и уязвимости лиц разной гендерной идентичности, принимая во внимание пересекающиеся факторы, такие как возраст, инвалидность, этническую принадлежность, язык, национальность, расовую принадлежность, религию, сексуальную ориентацию или любой другой фактор идентичности и их сочетание.

---

23 ДКВС, ОБСЕ/БДИПЧ и Структура «ООН-женщины», «Инструментарий по гендерным вопросам и безопасности» (Женева: ДКВС, 2008 г.) URL: https://www.dcaf.ch/gender-and-security-toolkit

24 CTED, 'Gender Dimensions of The Response to Returning Foreign Terrorist Fighters - Research Perspectives', February 2019. («Гендерные аспекты мер реагирования, принимаемых в связи с возвращением иностранных боевиков-террористов: перспективы исследований»)

25 Nelly Lahoud, 'Empowerment or Subjugation: An Analysis of ISIL's Gendered Messaging, («Расширение прав и возможностей или подчинение: анализ гендерно ориентированных сообщений ИГИЛ», Структура «ООН-женщины», июнь 2018 г.).

26 ДКВС, «Гендерное равенство, кибербезопасность и управление сектором безопасности: понимание роли гендера в управлении кибербезопасностью», январь 2023 г.

[IV] Обзор национальной контртеррористической стратегии

4.1 Обзор

Цель создания документа для разработки национальной контртеррористической политики по противодействию использованию новых технологий в террористических целях заключается в том, чтобы дать возможность разработчикам политики разрабатывать и (или) обновлять контртеррористические стратегии и политику так, чтобы это позволяло учитывать текущее состояние научно-технического прогресса. Новые технологии открывают такие возможности, как способность определять приоритеты и инвестировать в инновации, модернизировать контртеррористический потенциал с помощью новых технологий, а также расширять сотрудничество между частным и государственным секторами. Террористы могут использовать новые технологии в злонамеренных целях. Террористические организации используют технологии, сочетая деятельность в Интернете с деятельностью в реальном мире. Вызовы, создаваемые новыми технологиями, включают использование Интернета, социальных сетей и даркнета, а также использование и злоупотребление виртуальными активами в террористических целях (например, для отмывания денег). Использование новых технологий в террористических целях также открывает возможность для кибератак со стороны террористов.

Поскольку развитие новых технологий происходит гораздо быстрее, чем темпы изменения национальной политики, данный документ призван обеспечить основу для оценки эффективности политики в борьбе с угрозами, связанными с использованием новых технологий в террористических целях. Кроме того, именно оценка эффективности существующей политики позволит разработать новые поправки к ней, чтобы сохранить ее актуальность. Национальная контртеррористическая политика важна для создания общего, целостного государственного подхода к террористическим угрозам с четким мандатом на высоком уровне. Такая политика важна для целей координации внутри государства, а также необходима ее интеграция с соответствующими мерами политики в области национальной безопасности, кибербезопасности и киберпреступности. В рамках такой политики должны быть определены институциональные мандаты, обязанности организаций, а также механизмы сотрудничества и координации между ними. В ней также должно быть предусмотрено выделение ресурсов для развития национального потенциала. Наличие национальной контртеррористической политики также необходимо для сотрудничества с неправительственными заинтересованными сторонами и организациями. Политика должна поддерживать координацию, коммуникацию и сотрудничество с частным сектором, общественностью и международными партнерами.

4.2 Новые технологии: использование террористами и применение для борьбы с терроризмом

Для разработки контртеррористической политики, отражающей актуальное состояние развития новых технологий, важно понимать обе стороны использования новых технологий — как в террористических целях, так и для борьбы с терроризмом; практикующие специалисты должны понимать, как технологии могут быть использованы в террористических целях, а также как они могут быть использованы в качестве инструмента для борьбы с терроризмом. В приведенной ниже таблице представлены новые технологии и их потенциальное использование в террористических целях, а также возможности их применения практикующими специалистами для борьбы с терроризмом. Понимание того, как новые технологии могут быть использованы для борьбы с терроризмом, может помочь практикам интегрировать их использование в меры реагирования в рамках контртеррористической политики.

Важно отметить, что таблица содержит точные сведения на момент составления настоящего документа, однако ее содержание подлежит регулярному пересмотру для обеспечения его точности и актуальности в случае использования. В связи с постоянным развитием новых технологий будут появляться новые способы их использования в террористических целях, а также новые способы применения технологий для борьбы с терроризмом.

ТАБЛИЦА 4. **Примеры злонамеренного использования технологий и возможностей для правоохранительных органов**

Тип технологии	Использование в террористических целях	Использование правоохранительными органами в контртеррористических целях
Интернет	• Вербовка в террористические организации через пропаганду, распространяемую в Интернете • Публикация в Интернете информации о том, как совершать террористические акты[27] • Финансирование терроризма • Радикализация, ведущая к терроризму • Сбор оперативной информации о потенциальных объектах террористических атак • Распространение террористического контента и искаженных представлений • Коммуникации, координация и иная поддержка террористических актов или деятельности • Информационные операции с применением кибертехнологий	• Противодействие насильственному экстремизму и террористическим установкам[28] • Сбор и анализ OSINT • Платформа для обмена информацией между заинтересованными сторонами • Выявление террористического контента в Интернете и пресечение его распространения • Группы по оценке интернет-контента, которые перенаправляют сообщения об экстремистском контенте в технологические компании, призванные бороться с ним на своих платформах • Выявление новых террористических групп и их намерений

27 Европейский союз, «Директива (ЕС) 2017/541 Европейского парламента и Совета от 15 марта 2017 г. о борьбе с терроризмом и замене рамочного решения Совета 2002/475/JHA и внесении изменений в Решение Совета 2005/671/JHA»), Публичный закон № 2002/475/JHA, 088 OJ L 6 (2017 г.), 88/7-8, URL: http://data.europa.eu/eli/dir/2017/541/oj/eng

28 Исполнительный директорат Контртеррористического комитета Совета Безопасности Организации Объединенных Наций (ИДКТК), «Аналитическая записка ИДКТК: противодействие террористическим нарративам онлайн и офлайн» (Организация Объединенных Наций, 2020 г.), URL: https://www.un.org/securitycouncil/ctc/content/cted-analytical-brief-%E2%80%93-countering-terrorist-narratives-online-and-offline

ТАБЛИЦА 4. Примеры злонамеренного использования технологий и возможностей для правоохранительных органов

Тип технологии	Использование в террористических целях	Использование правоохранительными органами в контртеррористических целях
Социальные сети	• Вербовка в террористические организации через пропаганду, распространяемую в социальных сетях • Дезинформационные кампании • Распространение террористического контента и искажающих реальность сведений, пропаганды и (или) материалов для размещения в качестве пропаганды в социальных сетях по зашифрованному каналу[29] (см. резолюцию 2396 Совета Безопасности) • Радикализация, ведущая к терроризму • Службы обмена зашифрованными сообщениями позволяют вести переписку, которую сложнее отследить тем, кто не является ее участником	• Сбор/мониторинг SOCMINT • Противодействие насильственному экстремизму и террористическим установкам • Перенаправление сообщений об экстремистском контенте в технологические компании • Предотвращение создания террористами новых аккаунтов
Даркнет	• Хакерские форумы, на которых можно приобрести вредоносное ПО, вирусы-вымогатели и другие вредоносные программы для совершения кибератак • Приобретение оружия • Вербовка • Зашифрованные сообщения между членами террористической группы	• Сбор и анализ OSINT
Виртуальные активы (криптовалюты, NFT, электронные платежные системы и т. д.)	• Использование криптовалют/NFT-токенов для финансирования терроризма • Использование криптовалют/NFT-токенов в деятельности по отмыванию денег	• NFT-токены могут использоваться для организации контрпропаганды в области борьбы с терроризмом (известен пример использования NFT-токенов ИГИЛ для распространения пропаганды)[30] • Сбор средств/краудфандинг в виртуальных активах может поддержать низовые усилия по борьбе с терроризмом (например, приобретение оборудования, необходимого на местах)
Распознавание лиц	• В настоящее время нет данных (н/д)	• Обнаружение аномалий (процесс интеллектуального анализа данных для выявления единиц данных, которые выходят за рамки или отклоняются от нормы) • Международная база данных террористов

29 Mia Bloom, Hicham Tiflati, and John Horgan, Navigating ISIS's Preferred Platform: Telegram («Обзор предпочтительной платформы ИГИЛ: Telegram»), *Terrorism and Political Violence* 31, no. 6 (November 2, 2019): 1242–54, URL: https://doi.org/10.1080/09546553.2017.1339695

30 Ian Talley, Islamic State Turns to NFTs to Spread Terror Message («Исламское государство» обращается к использованию NFT-токенов для распространения террористических посланий»), *Wall Street Journal*, September 4, 2022, sec. Politics, URL: https://www.wsj.com/articles/islamic-state-turns-to-nfts-to-spread-terror-message-11662292800

ТАБЛИЦА 4. **Примеры злонамеренного использования технологий и возможностей для правоохранительных органов**

Тип технологии	Использование в террористических целях	Использование правоохранительными органами в контртеррористических целях
3D-печать	• Создание оружия/частей оружия	• 3D-печать может быть использована для борьбы с терроризмом, например, печати деталей БПЛА, которые, в свою очередь, можно использовать для разведки, наблюдения и рекогносцировки (ISR)
Искусственный интеллект и машинное обучение	• Дезинформационные кампании и кибератаки с использованием искусственного интеллекта[31] • Оружие, управляемое искусственным интеллектом[32] • Кампании социальной инженерии[33] • Может использоваться для обновления эксплойтов или написания вредоносного ПО для сложных кибератак	• Использование ИИ/машинного обучения для автоматизации мониторинга и анализа в контртеррористической деятельности (например, автоматическая сортировка сообщений в социальных сетях/на онлайн-форумах)[34] • Анализ больших данных с помощью искусственного интеллекта[35] • Использование методов обработки естественного языка (ОЕЯ) для обнаружения символов и шаблонов, используемых террористическими группами в Интернете • Мониторинг распространения ложных сведений и дезинформации[36]

4.3 Эталонный образец

Данный документ призван помочь в использовании существующих передовых практик в области контртеррористической политики для дальнейшего развития использования новых технологий в борьбе с терроризмом, а также мер реагирования на их использование в террористических целях. При создании данного документа были рассмотрены многочисленные программные документы контртеррористической стратегии и политики как представителей государственного, так и частного секторов. Целью этого обзора было как оценить, имеются ли в текущей политике передовая практика, которую следует использовать в дальнейшем, так и обеспечить лучшее понимание состояния контртеррористической политики в контексте использования новых технологий. Изучение общедоступных документов по борьбе с терроризмом дает возможность еще больше усилить меры реагирования по борьбе с использованием новых технологий в террористических целях в рамках соответствующей национальной политики.

31 Контртеррористический центр Организации Объединенных Наций и Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия, «Алгоритмы и терроризм: злонамеренное использование искусственного интеллекта в террористических целях», совместный доклад (Организация Объединенных Наций, 2021 г.), 39–40, URL: https://unicri.it/News/Algorithms-Terrorism-UNICRI-UNOCCT

32 См. например, там же, 33–35.

33 Там же, 45.

34 Контртеррористический центр Организации Объединенных Наций и Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия, «Борьба с терроризмом в Интернете с помощью искусственного интеллекта: обзор для правоохранительных и контртеррористических органов в Южной и Юго-Восточной Азии», совместный доклад (Организация Объединенных Наций, 2021 г.), 20–21 и 23–30, URL: https://unicri.it/News/-Countering-Terrorism-Online-with-Artificial-Intelligence

35 Там же, 17.

36 Там же, 27–28.

4.4 Общие выводы

Во многих контртеррористических стратегиях, изученных при подготовке данного документа, при обсуждении новых технологий зачастую затрагивались такие вопросы, как использование Интернета и социальных сетей в террористических целях. Несмотря на это, многие стратегии не затрагивают технические возможности, которые используются или потенциально могут быть использованы террористами для новых типов операций, например, использование искусственного интеллекта, даркнета, приложений со сквозным шифрованием и цифровых активов. Это можно объяснить тем, что многие из этих стратегий обновлялись недостаточно быстро, чтобы идти в ногу с развитием и потенциально растущим использованием этих технологий.

Изучая опубликованные контртеррористические стратегии и политику разных стран, можно заметить, что в них признается наступление цифровой эпохи и существование связанных с ней сложностей. С другой стороны, многие из этих стратегических документов не обеспечивают четкой и более детальной основы для борьбы с угрозами, которые создает использование новых технологий в террористических целях, а также не затрагивают возможности использования новых технологий правоохранительными органами и другими заинтересованными сторонами в борьбе с терроризмом. Несмотря на то, что в этих стратегических документах обсуждается важность обмена информацией, в некоторых из них существует пробел относительно передовой практики обмена информацией; например, отсутствие описания их эффективности, безопасности (с точки зрения информационной/операционной безопасности) и законности (в контексте обмена данными).

4.4.1 Ключевые вопросы, требующие рассмотрения

При разработке комплексной контртеррористической стратегии и политики, направленной на решение проблемы использования новых технологий в террористических целях, необходимо решить несколько ключевых вопросов, чтобы гарантировать, что страны в достаточной степени подготовлены к противодействию текущим и будущим угрозам.

В рамках контртеррористической политики большое значение имеет способность оценивать угрозы и реагировать на них. Это включает в себя понимание технических возможностей, влияния технологий в экономике и социальной сфере, которое может быть использовано, и мотивов террористов. В рамках этого процесса оценки необходимо также уделить особое внимание процессу сбора оперативных данных об угрозах [например, с помощью таких средств, как сбор оперативной информации путем перехвата сигналов и сообщений (SIGINT), сбор оперативной информации из открытых источников (OSINT) и сбор оперативной информации из социальных сетей (SOCMINT)], чтобы практикующие специалисты могли упреждать угрозы и эффективно реагировать на них.

В этом контексте одним из ключевых вопросов является межсекторальное сотрудничество (с акцентом на обмен информацией) между заинтересованными сторонами, включая взаимодействие с национальными, субнациональными и местными заинтересованными сторонами. В эпоху цифровых и новых технологий межсекторальное сотрудничество между государственными правоохранительными органами и частным сектором, научными и некоммерческими организациями имеет решающее значение, особенно в условиях непрекращающегося развития технологий. Несмотря на то что многие контртеррористические стратегии, изученные в рамках данного доклада, включают элемент обмена информацией, в них не говорится о том, каким образом он должен происходить.

Еще один ключевой вопрос, который рассматривается в данном документе, — как лучше обучить заинтересованные стороны использованию новых технологий для реагирования на террористическую деятельность. Способность заинтересованных сторон оставаться в курсе проблем и возможностей, которые несут в себе новые технологии, позволит им эффективнее реагировать на постоянно развивающийся и меняющийся ландшафт угроз.

4.4.2 Разработка новых практик, инструментов и методов

Одной из наиболее важных задач, стоящих перед правоохранительными органами, является разработка новых практик, инструментов и методов борьбы с использованием новых технологий в террористических целях, таких как получение информации, мониторинг и правоприменение в области использования социальных сетей, пресечение подстрекательства к терроризму и участие в упреждающих усилиях по предотвращению потенциальных атак. Для этого необходимо расширить инструментарий правоохранительных органов, чтобы обеспечить понимание, управление и осуществление деятельности правоохранительных органов в контексте новых технологий. Во многих странах отсутствуют четкие директивы по вопросам борьбы с террористической деятельностью в Интернете, и все еще предстоит внедрить значительные судебные и правоприменительные механизмы, в том числе разработать законодательство и кодексы обеспечения исполнения против радикализации и подстрекательства в Интернете.

Все это должно быть сделано таким образом, чтобы обеспечить защиту права на частную жизнь, свободы выражения мнений и объединений, права на недискриминацию и других фундаментальных прав, или, если необходимо, ограничить эти права в строгом соответствии с принципами законности и соразмерности.

[V]

Соображения по поводу мер реагирования в рамках национальной контртеррористической политики

5.1 Обзор

Цель данной публикации — устранить пробелы в контртеррористических стратегиях в отношении новых технологий и привести примеры передовой практики в области контртеррористической политики для разработки стратегии и протоколов по борьбе с угрозами, исходящими от новых технологий. Среди других целей — использование новых технологий для борьбы с терроризмом, а также оптимизация мер реагирования и мер противодействия террористической деятельности. Соображения, касающиеся мер реагирования в рамках национальной контртеррористической политики, основаны на многогранном подходе, охватывающем основные аспекты контртеррористической политики, с целью обеспечения эффективности национальной безопасности при осуществлении надзора, необходимого для защиты прав и свобод человека.

В целом национальная контртеррористическая политика требует скоординированных усилий различных государственных ведомств, правоохранительных органов, вооруженных сил и других заинтересованных сторон для обеспечения безопасности и защиты населения, а также защиты прав и свобод человека.

Права человека, подвергающиеся наибольшему риску в связи с борьбой с терроризмом и новыми технологиями, включают в себя: неприкосновенность частной жизни, свободу выражения мнений и риск дискриминации. Запрет на дискриминацию не может быть ограничен, поскольку дискриминация зачастую является одной из важнейших первопричин терроризма. Любые ограничения прав на частную жизнь и свободу выражения мнений должны быть установлены законом или в соответствии с законом согласно статьям 17 и 19 Международного пакта о гражданских и политических правах. Кроме того, любые ограничения должны быть признаны необходимыми и соразмерными преследуемой законной цели.

На схеме (Рисунок 4) представлена модель, на которой основываются ключевые соображения национальной контртеррористической политики. Верхние строки схемы — надзор и оценка воздействия и эффективности — отражают всеобъемлющие соображения, которые должны быть учтены как на уровне всей контртеррористической политики, так и в каждом из ее компонентов. За этими двумя «зонтичными» соображениями следуют четыре интегральных: осведомленность, вмешательства в отношении угроз, национальный потенциал и сотрудничество. Каждое из этих интегральных соображений служит руководящим принципом для пяти перечисленных ниже компонентов национальной контртеррористической политики, включая обмен информацией, инновации, управление данными, правовую основу и обучение и подготовку. Именно благодаря сочетанию всех ключевых компонентов можно достичь целей, изложенных в четырех интегральных соображениях.

РИСУНОК 4

5.1.1 Надзор

При разработке контртеррористической политики важно учитывать вопросы надзора за политикой, чтобы обеспечить выполнение требований в области управления данными, конфиденциальности и защиты прав человека в ходе реализации контртеррористической политики. Меры надзора должны быть встроены во множество этапов контртеррористической политики, чтобы обеспечить соблюдение соответствующих соображений на протяжении всего ее жизненного цикла, особенно на этапах сбора оперативной информации и управления данными.

В рамках контртеррористической политики рекомендуется осуществлять два вида надзора: судебный и внесудебный[37]. Судебный надзор предполагает задействование судов для контроля и привлечения заинтересованных сторон к ответственности за их действия как в рамках сбора оперативной информации, так и в рамках мер реагирования на полученную оперативную информацию[38]. Внесудебный надзор может осуществляться парламентскими комитетами, учреждениями по защите данных, внутренними правоохранительными органами или органами надзора за сбором оперативной информации[39]. Кроме того, международные организации и организации гражданского общества играют определенную роль в мониторинге соответствия мер реагирования, разработанных правительством, международно-правовым обязательствам. В обоих случаях орган, осуществляющий надзор, должен быть независимым от разработчиков политики[40].

В рамках усилий по надзору сотрудничество с частным сектором, особенно в отношении сбора данных и оперативной информации, должно предусматривать определенный уровень прозрачности для общественности в отношении усилий по онлайн-мониторингу[41].

37 Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН), «Ключевые вопросы модуля 12 по борьбе с терроризмом: подотчетность, надзор за методами сбора оперативной информации», июль 2018 г., URL: https://www.unodc.org/e4j/en/terrorism/module-12/key-issues/accountability-oversight-of-intelligence-gathering-methods.html

38 Там же.

39 Там же.

40 Там же.

41 Government of Australia, *Safeguarding Our Community Together: Australia's Counter-Terrorism Strategy 2022* (Australia: The Commonwealth of Australia, 2022), URL: 29, https://www.nationalsecurity.gov.au/what-australia-is-doing-subsite/Files/safeguarding-community-together-ct-strategy-22.pdf

5.1.2 **Измерение воздействия и эффективности**

Как продолжают развиваться технологии, так же должна развиваться и контртеррористическая политика, чтобы оптимальным образом реагировать на актуальные угрозы. В связи с этим в контртеррористическую политику должна быть встроена система оценки эффективности и влияния контртеррористической политики и связанных с ней мер на способность смягчать террористические угрозы и реагировать на них. Один из методов, предложенных в контртеррористической стратегии США, заключается в ежегодном анализе как эффективности стратегии в достижении целей борьбы с терроризмом, так и прогресса в достижении этих целей применительно к новым и существующим угрозам[42].

Прежде чем оценивать воздействие и эффективность контртеррористических мер, государствам-членам рекомендуется четко определить желаемые цели и стратегические результаты[43]. Одним из важнейших факторов оценки угрозы и мер реагирования является то, насколько существующая политика соответствует или не соответствует намеченным целям действий или политики. Государствам-членам следует учитывать как качественные, так и количественные показатели для оценки влияния и эффективности выбранной политики в борьбе с террористическими угрозами.

При рассмотрении воздействия и эффективности существуют и другие соображения, которые также должны быть оценены разработчиками политики. Одним из таких соображений являются ограничения конкретной политики относительно технических или других достижений со времени предыдущей оценки политики. При оценке воздействия и эффективности политики также следует учитывать затраты на ее реализацию (например, за счет рабочей силы и других ресурсов) по отношению к соответствующим выгодам и тому, что обеспечивает данная политика[44].

При оценке воздействия и эффективности контртеррористической политики рекомендуется использовать подход доказательной практики (ДП), который обеспечивает конкретные измерения воздействия и эффективности политики с использованием различных критериев, позволяющие принимать обоснованные решения в ходе дальнейшей разработки политики[45]. При разработке оценки контртеррористической политики, основанной на подходе ДП, необходимо учитывать два разных фактора: цели политики (и конкретные средства измерения того, как политика позволила или не позволила достичь конкретной цели) и потенциальные последствия политики (и частота, с которой проявляются эти последствия)[46]. Для того чтобы оценить эти факторы и политику в целом, необходимо применять оценочные методы исследования, в рамках которых оцениваются ресурсы, процессы и результаты политики в свете двух предыдущих факторов[47]. Именно на основе этих оценок разработчики политики узнают, где и как необходимо скорректировать контртеррористическую политику, чтобы она оставалась актуальной и эффективной.

---

42 United States, *National Strategy for Counter-terrorism of the United States of America* (Washington, DC: The White House, 2018), 11, URL: https://purl.fdlp.gov/GPO/gpo109871

43 United Kingdom Department for and Business, Energy and Industrial Strategy, "National Security and Investment Bill," Pub. L. No. BEIS006(F)-20-CCP (2020), 7, URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/934276/nsi-impact-assessment-beis.pdf

44 United Kingdom Department for and Business, Energy and Industrial Strategy, 30.

45 Freese, "Evidence-Based Counter-terrorism or Flying Blind? How to Understand and Achieve What Works," 37–38.

46 Freese, 41.

47 Freese, 45–46.

5.2 Основные соображения по поводу мер реагирования в рамках контртеррористической политики в отношении использования новых технологий

Приведенные ниже основные соображения охватывают важные факторы, необходимые для разработки комплексной контртеррористической политики. Сосредоточившись на этих основных соображениях, разработчики контртеррористической политики смогут разработать политику, которая позволит сбалансировать необходимость решения задач обеспечения безопасности и защиты прав человека, а также эффективно противостоять использованию новых технологий в террористических целях. В этом разделе рассматриваются основные соображения, которые необходимо учитывать при разработке контртеррористической политики в ответ на вызовы, создаваемые новыми технологиями. Понимая и принимая во внимание эти основные соображения, разработчики политики могут разработать надежную и адаптивную политику, которая опережает использование террористами новых технологий, обеспечивая безопасность и защиту обществ в эпоху цифровых технологий.

5.2.1 Осведомленность

Осведомленность о политике борьбы с терроризмом должна повышаться как на уровне заинтересованных сторон, так и через представителей общественности. Например, практикующие специалисты должны иметь глубокое понимание не только того, как выявлять угрозы и угрожающее поведение и реагировать на них, но и как информировать общественность и реагировать на обеспокоенность, высказанную общественностью в отношении угроз[48]. Применительно конкретно к контртеррористической политике осведомленность включает в себя информирование практикующих специалистов и представителей общественности, которое позволит им выявлять случаи использования новых технологий в террористической деятельности, а также предоставит практикующим специалистам способы, с помощью которых они смогут использовать новые технологии для эффективного реагирования на террористическую деятельность.

Повышение осведомленности о контртеррористической политике и мерах реагирования предполагает упрощение процесса передачи информации, особенно для представителей общественности, которые хотели бы сообщить важные сведения об угрозах[49]. Поэтому общественность должна быть проинформирована об угрожающем поведении или действиях, а также о том, куда можно обратиться, чтобы сообщить об инциденте, который в дальнейшем будет рассмотрен практикующими специалистами или другими заинтересованными сторонами, прошедшими соответствующую подготовку. Этого можно добиться с помощью обучения выявлению признаков угрожающего поведения или поведения, имеющего признаки подстрекательства к террористическим действиям. В ходе тренингов по этим вопросам необходимо тщательно разъяснять, что выявление угрожающего поведения не должно допускать дискриминации людей по признаку пола, расы, цвета кожи, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного, сословного или иного положения. Кроме того, платформа, с помощью которой представители общественности могут передавать информацию об угрозах соответствующим органам, должна быть легкодоступной и простой в использовании, чтобы предотвратить отсутствие сообщений из-за ее сложности.

Помимо информирования общественности, правоохранительные органы и другие заинтересованные стороны также должны пройти обучение по выявлению угрожающего поведения или поведения, имеющего признаки подстрекательства к террористическим действиям. Кроме того, они должны быть обучены тому, как правильно реагировать на поступающие к ним сообщения (например, от населения) или собранные оперативные дан-

48 Объединенная группа по оценке борьбы с терроризмом (JCAT), «Руководство по борьбе с терроризмом для сотрудников органов общественной безопасности». Правительство, Канцелярия директора Национальной разведки, URL: https://www.dni.gov/nctc/jcat/index.html (дата обращения: 1 июля 2024 г.).

49 Carl Amritt, Eliot Bradshaw, and Alyssa Schulenberg, "Threat Assessment and Management: Practices Across the World («Оценка угроз и управление ими: мировая практика»), Domestic Preparedness, February 1, 2023, URL: https://www.domesticpreparedness.com/preparedness/threat-assessment-and-management-practices-across-the-world

ные об угрожающем поведении или поведении, имеющем признаки подстрекательства к террористическим действиям. В рамках этих тренингов необходимо подчеркнуть, что сбор оперативной информации и разработка плана реагирования на обнаруженные угрозы должны осуществляться без дискриминации людей по признаку пола, расы, цвета кожи, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного, сословного или иного положения.

5.2.2 Вмешательства в отношении угроз

Под вмешательствами в отношении угроз подразумеваются различные меры и действия, предпринимаемые для предотвращения, обнаружения и реагирования на террористические угрозы, создаваемые использованием новых технологий. Эти вмешательства включают использование передовых технологий, инструментов и стратегий для выявления, отслеживания и нейтрализации потенциальных угроз. Например, вмешательства в отношении угроз могут включать использование искусственного интеллекта, машинного обучения и анализа больших данных для анализа и интерпретации больших объемов данных, а также выявления закономерностей и тенденций, которые могут указывать на потенциальные угрозы. Вмешательства в отношении угроз играют решающую роль в борьбе с терроризмом и требуют использования передовых технологий и инструментов. Крайне важно, чтобы эти вмешательства проводились с соблюдением прав и свобод человека и соответствовали правовым и этическим нормам, предусматривающим абсолютный запрет на дискриминацию, как минимум, по признаку пола, расы, цвета кожи, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного, сословного или иного положения.

Способность страны эффективно оценивать угрозы и реагировать на них тесно связана с ее способностью осуществлять контртеррористическую политику в отношении этих угроз. В рамках реагирования на угрозы практикующие специалисты и другие соответствующие заинтересованные стороны должны иметь возможность активно принимать меры по предотвращению реализации таких угроз.

Существует множество способов, с помощью которых заинтересованные стороны могут участвовать во вмешательствах в отношении угроз в различных секторах. Например, в партнерстве между частным и государственным секторами предотвращение угроз может быть достигнуто посредством работы государственного сектора по предотвращению и пресечению использования террористами онлайн-платформ в тандеме с технологическими компаниями. В государственном секторе вмешательства в отношении угроз могут осуществляться посредством координации между государствами-членами и правоохранительными органами в целях мониторинга и борьбы с использованием цифровых платформ в террористических целях.

Одним из подходов к реагированию на угрозы, который может быть реализован в рамках контртеррористической стратегии государств-членов, является реализация упреждающего реагирования на угрозы до того, как они материализуются. Этого можно достичь с помощью множества превентивных мер. Превентивные меры могут включать в себя конкретные меры безопасности, встроенные в саму политику (безопасность по умолчанию и проектная безопасность), или средства, с помощью которых можно бороться с террористами до того, как они смогут совершить атаку, посредством таких действий, как программы дерадикализации. Оба аспекта обсуждаются ниже[50].

5.2.3 Национальный потенциал

Национальный потенциал — способ измерения возможностей страны в ее усилиях по борьбе с терроризмом путем анализа ресурсов, которыми она располагает (финансовых, технических, людских и т. д.). При разработке мер реагирования в рамках национальной контртеррористической политики необходимо оценить потенциал страны, чтобы обеспечить соответствие политики имеющимся возможностям. Поскольку каждая страна обладает разными ресурсами и уровнями квалификации, единая модель политики не может быть осуществимой и эффективной во всех государствах-членах. Оценка национального потенциала сама по себе является неотъемлемой частью разработки контртеррористической политики, непосредственно отвечающей потребностям государства-члена, для которого она разрабатывается.

50 Агентство по кибербезопасности и защите инфраструктуры США и соавт., «Изменение баланса рисков кибербезопасности: принципы и подходы к проектируемой безопасности и безопасности по умолчанию»; Vidino and Bennett, A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism («Обзор трансатлантического передового опыта по противодействию радикализации в тюрьмах и рецидиву терроризма»).

При оценке национального потенциала страны учитываются как существующие ресурсы, так и ресурсы, которые государство может приобрести при помощи таких мер, как, например, сотрудничество с другими секторами и (или) государствами-членами. Поскольку технологии становятся все более сложными, важно, чтобы государства-члены поддерживали и повышали уровень своего национального потенциала, чтобы оставаться достаточно подготовленными как к решению новых задач, так и к использованию новых технологий для реализации новых возможностей в борьбе с терроризмом. Как будет показано ниже, некоторые из средств, с помощью которых можно повысить национальный потенциал государства-члена, — это обучение и подготовка соответствующих практикующих специалистов и заинтересованных сторон, а также такие средства, как обмен информацией и инновации.

5.2.4 Сотрудничество

Сотрудничество играет важную роль в создании общего, целостного государственного подхода к террористическим угрозам с четким мандатом на высоком уровне. Оно важно также для целей внутригосударственной координации и интеграции с другими заинтересованными сторонами. Необходимо определить механизм сотрудничества между организациями в рамках соответствующей политики. Наличие национальной контртеррористической политики также необходимо для сотрудничества с неправительственными заинтересованными сторонами и организациями. Политика должна поддерживать координацию, коммуникацию и сотрудничество с частным сектором, общественностью и международными партнерами.

Поскольку благодаря технологиям террористические угрозы все чаще становятся вопросами, пересекающими границы государств и различные сферы деятельности (цифровые действия, которые приводят к физическому ущербу), в контртеррористической политике необходимо делать акцент на сотрудничестве между заинтересованными сторонами. Сюда входит межведомственная координация внутри государства-члена и между государствами-членами, партнерство между НПО и гражданским обществом, а также разработка методов обмена информацией. В данном контексте сотрудничество должно также включать межсекторальное сотрудничество между государственным сектором и представителями частного сектора, такими как технологические компании, а также консультации с экспертами из профессионального мира и научных кругов.

Угроза использования новых технологий в террористических целях требует комплексных и скоординированных усилий соответствующих заинтересованных сторон. Государства-члены также должны взаимодействовать с широкой общественностью для содействия повышению цифровой грамотности и осведомленности. Взаимодействие с сообществами также важно для укрепления доверия. Примеры передовой практики также указывают на необходимость сотрудничества государственных органов с различными заинтересованными сторонами (включая компании, общественных лидеров, школы, религиозные организации и т. д.) для выявления и устранения потенциальных уязвимостей. Использование общего языка может способствовать минимизации страха и предвзятости, а также информировать общественность о том, как лучше использовать предоставляемые услуги, чтобы укрепить отношения, основанные на прозрачности и рациональном использовании ресурсов.

5.3 Ключевые сквозные компоненты контртеррористической политики в отношении использования новых технологий

Для решения проблем, связанных с новыми технологиями, необходимо включить ключевые междисциплинарные компоненты в рамки контртеррористической политики. Эти компоненты охватывают обмен информацией, инновации, управление данными, использование правовой основы и наращивание потенциала. «Сквозной» характер этих компонентов означает, что каждый из них повышает способность политики достигать целей, поставленных в четырех основных направлениях. Признавая и интегрируя эти ключевые компоненты, контртеррористическая политика может эффективно противостоять уникальным угрозам и рискам, связанным с использованием новых технологий в террористических целях.

5.3.1 **Обмен информацией**

В области сотрудничества одной из ключевых практик, на которой необходимо сосредоточиться в рамках контртеррористической политики, является обмен информацией, который подразумевает сбор, анализ и распространение информации из оперативных и открытых источников с соответствующими заинтересованными сторонами, включая правоохранительные органы и другие государственные ведомства. В рамках межсекторального сотрудничества это может включать в себя обмен информацией и консультации с научными кругами, частным сектором и НПО.

При разработке контртеррористической политики выделяется несколько ключевых проблем, которые возникают при обсуждении обмена информацией. Первая из этих проблем — простота и эффективность обмена информацией. Чтобы обеспечить эффективный обмен информацией между заинтересованными сторонами, необходимо, чтобы у них была единая терминология как для оценки террористических угроз, так и для реагирования на них. Общий язык реагирования должен также включать виды ответственности, распределенные между различными заинтересованными сторонами.

Еще одним ключевым компонентом в разработке практики обмена информацией является определение средств, с помощью которых этот обмен осуществляется. Обмен информацией между заинтересованными сторонами, расположенными в разных местах, должен осуществляться с помощью защищенных средств, чтобы заинтересованные стороны могли поддерживать оперативную безопасность при оценке угроз и реагировании на них. Помимо обмена информацией между заинтересованными сторонами и практикующими специалистами, важно, чтобы существовал легкодоступный способ, с помощью которого общественность могла бы делиться информацией с соответствующими правоохранительными органами. Одним из примеров является платформа, позволяющая общественности отмечать свою оценку серьезности информации об угрозе, а также делиться ею с соответствующими органами власти[51].

5.3.2 **Инновации**

Террористы постоянно ищут новые способы использования технологий для достижения своих целей. В результате этого политика, меры и стратегии борьбы с терроризмом также должны меняться, чтобы соответствовать этим угрозам. Это требует инноваций как в технологиях, так и в политике. Существует несколько видов инноваций, имеющих отношение к контртеррористической политике, включая оперативные и технологические инновации, цель которых заключается в расширении возможностей сбора информации и правоохранительной деятельности для обеспечения быстрого и эффективного реагирования на террористическую деятельность[52].

Технологические инновации формируют как потенциальные угрозы, так и новые способы борьбы с ними. В рамках оценки эффективности контртеррористической политики (о чем говорится в разделе 5.1.2) необходимо оценить, насколько эта политика соответствует (или не соответствует) технологическим инновациям. Эффективная контртеррористическая политика должна признавать технологические инновации, существующие на момент ее публикации, а также пытаться предсказать потенциальные будущие инновации, которые могут потребовать мер реагирования в рамках национальной контртеррористической политики[53]. Операционные инновации описывают способ, с помощью которого заинтересованные стороны корректируют свой подход к оценке угроз и тактике реагирования, используя технологические инновации и, в более общем смысле, стратегические/тактические/методологические инновации[54]. Инновации зачастую требуют сотрудничества между государственными учреждениями, частными компаниями и академическими институтами. Политические меры государств-членов должны быть направлены на стимулирование и поощрение инноваций, что требует инвестиций, ресурсов и поддержки для разработки и внедрения инновационных технологий. Правительства и частные организации должны быть готовы инвестировать в исследования и разработки, а также оказывать поддержку

51 «Как можно помочь: форма публичного вклада», Служба безопасности и разведки Новой Зеландии, URL: https://providinginformation.nzsis.govt.nz/#0gkxcyt3gyevyf7lm9l8xiz65 (дата обращения: 1 июля 2024 г.).

52 Robert G. Spulak, Science Technology and Innovation in Combating Terrorism («Наука, технологии и инновации в борьбе с терроризмом»), февраль 2015 г., URL: https://www.osti.gov/biblio/1513954

53 См., например, Соединенное Королевство, «CONTEST: Контртеррористическая стратегия Соединенного Королевства» (Соединенное Королевство: Британская корона, 2018 г.), 24, URL: https://www.gov.uk/government/publications/counter-terrorism-strategy-contest-2023

54 Spulak, Science Technology and Innovation in Combating Terrorism («Наука, технологии и инновации в борьбе с терроризмом»).

в реализации новых мер. Кроме того, в связи с быстрыми темпами изменений необходимо создавать политическую основу, способную адаптироваться к меняющимся угрозам. Это включает в себя межправительственное «сканирование горизонта»[55] на уровне политики и управление инновациями на институциональном уровне.

5.3.3 Управление данными

Управление данными в контексте борьбы с терроризмом и новых технологий относится к процессам и системам, используемым для сбора, анализа, хранения и обмена информацией, связанной с террористическими угрозами. С ростом использования новых технологий, таких как искусственный интеллект, машинное обучение и анализ больших данных, управление данными становится важнейшим компонентом усилий по борьбе с терроризмом.

Эффективное управление данными имеет важнейшее значение для борьбы с терроризмом и требует использования новых технологий и инструментов для своевременного и безопасного сбора, анализа и обмена информацией. Оно позволяет правоохранительным и разведывательным органам выявлять и отслеживать потенциальные угрозы, следить за деятельностью известных террористов и их сообщников, а также предотвращать или срывать террористические атаки. Это предполагает сбор и анализ широкого спектра данных. Обеспечение сотрудничества между секторами и заинтересованными сторонами из нескольких регионов и (или) государств-членов требует надлежащего обращения с данными, которые относятся к соответствующим угрозам. Это включает в себя такие вопросы, как надлежащая организация и способы документирования данных, чтобы к ним можно было легко и безопасно обращаться и обмениваться ими между заинтересованными сторонами из разных секторов и государств-членов. Кроме того, политика борьбы с терроризмом должна предусматривать такие способы защиты данных, которые не нарушают неприкосновенность частной жизни и (или) сохраняют определенные ограничения на сбор данных в целях защиты прав человека.

В рамках управления данными политика борьбы с терроризмом должна определять как процесс, так и политику использования аналитических данных и баз данных в качестве средства для сбора информации и анализа террористических угроз. Контртеррористическая политика должна учитывать возможности использования новых технологий, таких как искусственный интеллект, для сортировки, обработки и анализа данных об угрозах, собранных заинтересованными сторонами[56]. Необходимо следить за тем, чтобы собранные и сохраненные данные не нарушали права на неприкосновенность частной жизни и не допускали дискриминации людей о признаку пола, расы, цвета кожи, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного, сословного или иного положения. В рамках практики обмена информацией между заинтересованными сторонами, особенно заинтересованными сторонами, расположенными в разных государствах, необходимо разработать политику, обеспечивающую безопасный обмен

55 В обзоре Джона Дэя (Jon Day review) сканирование горизонта определяется следующим образом: «систематическое изучение информации для выявления потенциальных угроз, рисков, возникающих проблем и возможностей за пределами парламентского срока, что позволяет повысить готовность и включить меры по смягчению последствий и эксплуатации в процесс разработки политики».

56 Соединенное Королевство, «CONTEST: Контртеррористическая стратегия Соединенного Королевства», 24.

данными, не ставящий под угрозу оперативную безопасность специалистов, занимающихся устранением угрозы. Кроме того, это должно быть сделано таким образом, чтобы защитить частную жизнь людей, чьи данные были собраны, и чтобы доступ к этим данным имели только специалисты, занимающиеся конкретным делом, за счет применения шифрования и других мер безопасности для защиты данных от несанкционированного доступа или взлома, а также соблюдения соответствующих законов и нормативно-правовых документов в области защиты информации.

5.3.4 Правовая основа

Правовая основа в контексте борьбы с терроризмом и новых технологий — это совокупность законов, нормативно-правовых актов и политики, регулирующих деятельность правоохранительных органов, сбор, использование, хранение и обмен информацией, связанной с террористическими угрозами, а также использование новых технологий для борьбы с терроризмом. Правовая основа необходима для того, чтобы усилия по борьбе с терроризмом соответствовали правовым и этическим нормам, защищали права личности и неприкосновенность частной жизни, а также не допускали злоупотребления властью со стороны правоохранительных и разведывательных органов. Это предполагает установление строго пропорционального баланса между необходимостью принятия эффективных контртеррористических мер и защитой индивидуальных прав и свобод. Она играет важнейшую роль в обеспечении эффективности, законности и соблюдения прав и свобод человека в контексте борьбы с терроризмом и использовании новых технологий для противодействия растущей угрозе терроризма.

Важно иметь определение терроризма на рабочем уровне, которое можно было бы использовать в качестве основы для юридических действий, включая анализ способов, с помощью которых террористы могут использовать новые технологии[57]. Глобальный характер цифровой эпохи создает уникальные трудности для стран в разработке и осуществлении контртеррористической политики, поскольку терроризм в эпоху новых технологий может с легкостью пересекать государственные границы. Даже если террорист действует в пределах одного государства, он может побудить других к подстрекательству к терроризму и дальнейшим террористическим действиям на территории другого государства. При рассмотрении правовых рамок политики борьбы с терроризмом особое внимание следует уделять защите прав человека. Правовая основа, в рамках которой проводится контртеррористическая политика, должна также предусматривать презумпцию недопустимости использования незаконно полученных доказательств в суде в рамках усилий по защите прав человека и неприкосновенности частной жизни в процессе реагирования на террористическую деятельность.

5.3.5 Наращивание потенциала

При разработке контртеррористической политики важно заложить в нее основу, касающуюся таких вопросов, как обучение и подготовка. В данном случае под обучением понимается подготовка соответствующих заинтересованных сторон и практикующих специалистов, а также информирование представителей общественности. Цель обучения лиц, принимающих решения, и других заинтересованных сторон — помочь им в передаче знаний и возможностей для эффективного реагирования на террористические угрозы. Это могут быть образовательные семинары, моделирование, курсы повышения квалификации и другие средства, позволяющие им понять свою роль в борьбе с террористическими угрозами, исходящими от новых технологий, и обеспечить, чтобы характер их мер реагирования оставался актуальным с учетом постоянного развития технологий. Кроме того, обучение практикующих специалистов и представителей общественности в рамках контртеррористической политики повышает осведомленность этих групп и позволяет расширить национальный потенциал реагирования на террористические угрозы и на террористическую деятельность[58]. Например, создание и реализация программ, направленных на обучение специалистов по дерадикализации и (или) отстранению известных террористов, может обеспечить необходимое вмешательство в отношении угроз для предотвращения дальнейших террористических действий со стороны этих субъектов[59].

57 Freese, "Evidence-Based Counter-terrorism or Flying Blind? How to Understand and Achieve What Works («Борьба с терроризмом, основанная на фактических данных, или полет вслепую? Как понять и достичь того, что работает»), 43.

58 Содружество Австралии, «Белая книга внешней политики за 2017 год», в ред. Morris Walker Pty Ltd (Австралия, 2017 г.), 38, URL: https://www.dfat.gov.au/publications/minisite/2017-foreign-policy-white-paper

59 Vidino and Bennett, A Review of Transatlantic Best Practices for Countering Radicalization in Prisons and Terrorist Recidivism («Обзор трансатлантического передового опыта по противодействию радикализации в тюрьмах и террористическому рецидивизму»), 7–8.

[VI] Примеры передовой практики в области мер реагирования в рамках контртеррористической политики

6.1 Обзор

При разработке модели контртеррористической политики, способной эффективно учитывать потенциальные возможности и проблемы, возникающие при использовании новых технологий, использовались источники из числа международных организаций, государств-членов, научных кругов и представителей частного сектора. Ниже приводятся некоторые выводы, касающиеся практики, которая может быть интегрирована в контртеррористическую политику. Подборка выводов направлена на рассмотрение как элементов построения успешной контртеррористической политики в ответ на использование новых технологий в террористических целях, так и способов, с помощью которых разработчики политики и другие практикующие специалисты могут повысить свою способность противостоять этим угрозам. Эти выводы представлены в следующих разделах через призму четырех интегральных соображений контртеррористической политики (раздел 5.2), взятых из модели, представленной в разделе 5.1. Исходя из этих соображений, представленные здесь ресурсы охватывают некоторые примеры передовой практики в рамках ключевых компонентов контртеррористической политики в отношении новых технологий (раздел 5.3).

6.2 Осведомленность

Осведомленность, как обсуждалось в разделе 5.2.1, находится в контексте предоставления инструментов, знаний и участия практикующих специалистов и представителей общественности для выявления угроз, сообщения о них или реагирования на них. ОБСЕ предлагает подходы к программам обучения и подготовки. Первая из этих программ представляет собой серию семинаров, специально направленных на повышение осведомленности общественности о мерах по борьбе с терроризмом[60]. ОБСЕ рекомендует специалистам по борьбе с терроризмом проводить «штабные учения», которые служат как в качестве рабочих групп для экспертов из правительства, частного сектора и академических кругов (среди прочих), так и в качестве форума, на котором можно обсуждать сценарии, тем самым предоставляя средства для дальнейшего развития национального потенциала по реагированию на террористические угрозы[61]. В дополнение к тренингам и «штабным учениям» Институт Брукингса рекомендует проводить моделирование в формате «военных игр» с участием практикующих специалистов из разных ведомств и секторов[62]. Цель таких учений — отработать ответные действия на атаки (включая альтернативные планы действий)[63]. Здесь цель аналогична цели учений «красной команды», которые, помимо отработки процедур реагирования, также помогают тем, кто разрабатывает меры реагирования, понять пробелы, в которых необходимо улучшить политику реагирования[64].

60 OSCE Transnational Threats Department, "OSCE Anti-Terrorism Reference" (Organization for Security and Co-Operation in Europe, July 2020), 25 («Справочник ОБСЕ по борьбе с терроризмом»).

61 Ibid, 25–26.

62 Bruce Schneier and Tarah Wheeler, Hacked Drones and Busted Logistics Are the Cyber Future of Warfare («Взломанные дроны и разрушенная логистика — кибербудущее войны»), Brookings, Tech Stream (блог), June 4, 2021, URL: https://www.brookings.edu/techstream/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare

63 Ibid.

64 David Romyn and Mark Kebbell, Terrorists' Planning of Attacks: A Simulated 'Red-Team' Investigation into Decision-Making («Планирование террористами нападений: моделирование процесса принятия решений с помощью «красной команды»), *Psychology, Crime & Law 20*, no. 5 (May 28, 2014): 483, URL: https://doi.org/10.1080/1068316X.2013.793767

В ходе дискуссий в рамках «кабинетных учений», проводимых ОБСЕ, а также в контртеррористической стратегии США особое внимание уделяется включению вопросов защиты критической инфраструктуры от террористических атак в более широкую контртеррористическую повестку дня, особенно с учетом ее уязвимости к кибератакам[65].

Желаемые результаты политики должны учитывать следующее:

- глубокое понимание процесса обнаружения угроз и реагирования на них заинтересованными сторонами;
- широкую осведомленность общественности об угрозах и мерах реагирования на них;
- повышение осведомленности с помощью программ обучения и подготовки, таких как:
  - тренинги для практикующих специалистов и представителей общественности;
  - симуляции и учения «красной команды»;
  - кабинетные учения;
  - симуляции в формате «военных игр».

6.3 Вмешательства в отношении угроз

Как уже говорилось ранее, одним из средств, с помощью которых государство-член может реализовать меры по противодействию угрозам, является использование упреждающего подхода к обеспечению безопасности. Такой подход предполагает вмешательства в отношении угроз на достаточно ранней стадии и как можно ближе к источнику, чтобы предотвратить реализацию террористических атак[66].

Одним из методов противодействия угрозам является внедрение принципов проектной безопасности и безопасности по умолчанию. Концепция проектной безопасности подразумевает, что одной из целей при создании или разработке продукта или политики является включение мер безопасности, позволяющих эффективно противостоять угрозам[67]. Подход, основанный на концепции проектной безопасности, рекомендуется Европейской комиссией для защиты общественных мест от террористических атак[68].

Кроме того, в недавней публикации Агентства по кибербезопасности и защите инфраструктуры США (CISA), Федерального управления по информационной безопасности Германии (BSI) и восьми других органов по безопасности и кибербезопасности государств-членов ЕС подчеркивается важность применения концепции проектной безопасности в контексте конкретных технологий[69]. Помимо концепции проектной безопасности в публикации также подчеркивается важность безопасности по умолчанию. Это означает, что конечный «продукт» (технология или, в данном случае, политика) должен быть безопасным и обеспечивать средства защиты, как часть содержания самого продукта/политики, когда он будет выпущен[70]. Обе эти концепции могут быть применены в процессе разработки контртеррористической политики с помощью таких средств, как разработка СОПов по реагированию на конкретные виды технологий, которые можно легко адаптировать под различные сценарии. Реализация этих концепций также может быть осуществлена путем уделения особого внимания использованию технологий практикующими специалистами в качестве средства обеспечения безопасности таких систем, как системы критической инфраструктуры государства-члена.

65 Департамент ОБСЕ по транснациональным угрозам, «Справочник ОБСЕ по борьбе с терроризмом», 26; Соединенные штаты Америки, «Национальная контртеррористическая стратегия Соединенных Штатов Америки», 19–20.

66 Национальный центр кибербезопасности, «Концепция проектируемой безопасности», Национальный центр кибербезопасности, 7 марта 2018 г., https://www.ncsc.gov.uk/information/secure-default

67 Европейская комиссия, «Проектируемая безопасность: защита общественных мест от террористических атак», 23; Агентство по кибербезопасности и защите инфраструктуры США и соавт., «Изменение баланса рисков кибербезопасности: принципы и подходы к проектируемой безопасности и безопасности по умолчанию», 3–4.

68 Европейская комиссия, «Проектируемая безопасность: Защита общественных мест от террористических атак».

69 Агентство по кибербезопасности и защите инфраструктуры США и соавт., «Изменение баланса рисков кибербезопасности: принципы и подходы к проектируемой безопасности и безопасности по умолчанию».

70 Там же, 5–6.

В работе, представленной на конференции Европола, авторы предлагают несколько шагов, с помощью которых, изменив политику, можно выработать упреждающий подход к борьбе с радикализацией, ведущей к терроризму, особенно в местах лишения свобод[71]. В числе рекомендаций предлагается обмен информацией между пенитенциарными учреждениями и другими государственными органами как средство выявления признаков радикализации среди заключенных, определяемых практикующими специалистами, прошедшими обучение по выявлению и коррекции подобного поведения[72]. Предлагается, что в случае обнаружения подобного поведения такие люди должны пройти процедуру дерадикализации или отстранения[73].

Еще одним средством, с помощью которого государства-члены могут осуществлять вмешательства в отношении угроз, является создание правовой основы, на которой зиждется соответствующая политика. В рамках обсуждения вопросов о применении концепций проектной безопасности и безопасности по умолчанию организации — авторы доклада «Изменение баланса рисков кибербезопасности: принципы и подходы к проектной безопасности и безопасности по умолчанию» отметили усилия Европейского Союза по обеспечению правовой основы, посредством которой вопросы кибербезопасности включены в Закон о киберустойчивости[74]. Этот закон, внесенный на рассмотрение в конце 2022 года, направлен на обеспечение мер регулирования, которые призваны гарантировать, что новые технологии будут реализованы с применением концепции проектной безопасности, за счет чего продукты, попадающие на рынок будут по умолчанию менее уязвимыми к нарушениям безопасности[75]. Это послужит превентивной мерой в контексте вмешательств в отношении угроз, делая продукты, доступные потребителям, менее уязвимыми для потенциальных угроз.

Еще одним примером использования правовой основы в качестве вмешательства в отношении угроз является система, включающая международную правовую базу для деятельности по борьбе с терроризмом, за которую выступает Организация Объединенных Наций. Целью такой системы является обеспечение ответственности за террористические действия независимо от местонахождения совершающего их лица[76]. В рамках этой международной правовой базы Организация Объединенных Наций разработала 19 международно-правовых документов по предупреждению террористических атак[77]. Чтобы международная правовая база могла работать так, как задумано, в государствах-членах должна быть установлена или санкционирована законом контртеррористическая политика, которая должна подвергаться независимому надзору.

71 Vidino and Bennett, A Review of Transatlantic Best Practices for Countering Radicalization in Prisons and Terrorist Recidivism («Обзор трансатлантического передового опыта противодействия радикализации в тюрьмах и террористическому рецидивизму»).

72 Vidino and Bennett, 5–6.

73 Vidino and Bennett, 8.

74 Агентство по кибербезопасности и защите инфраструктуры США и соавт., «Изменение баланса рисков кибербезопасности: принципы и подходы к проектной безопасности и безопасности по умолчанию», 3.

75 Европейская комиссия, «Закон о киберустойчивости», 15 сентября 2022 г., URL: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

76 «Международная правовая основа», Организация Объединенных Наций: по наркотикам и преступности, URL: https://www.unodc.org/unodc/en/firearms-protocol/international-legal-framework.html (дата обращения: 1 июля 2024 г.); Counter Terrorism Legal Framework: Lessons Learned from IDLO Policy Dialogues in Collaboration with UNODC («Правовая основа борьбы с терроризмом: уроки, извлеченные из политических диалогов МОПР в сотрудничестве с УНП ООН»), Development Law Update, no. 2 (2007 г.), URL: https://www.files.ethz.ch/isn/138640/14.pdf

77 Контртеррористическое управление Организации Объединенных Наций, «Международные правовые документы», URL: https://www.unodc.org/unodc/en/ (дата обращения: 1 июля 2024 г.); Департамент по противодействию транснациональным угрозам, «Статус универсальных контртеррористических конвенций и протоколов, а также других международных и региональных правовых инструментов, касающихся терроризма и сотрудничества по уголовным делам в регионе ОБСЕ» (Организация по безопасности и сотрудничеству в Европе (ОБСЕ), июль 2018 г.), URL: https://www.osce.org/files/f/documents/5/8/17138_0.pdf

Желаемые результаты политики должны учитывать следующее:

- расширение сотрудничества между секторами, агентствами, государствами-членами и т. д. в целях противодействия угрозе использования новых технологий в террористических целях;
- достижение национальных целей в области борьбы с терроризмом по предотвращению, срыву, отрицанию, защите, восстановлению и судебному преследованию;
- разработку превентивных мер реагирования на угрозы, которые могут включать:
  - концепции проектируемой безопасности и безопасности по умолчанию;
  - идентификацию угроз и определение приоритетов;
  - дерадикализацию и отстранение.

6.4 Национальный потенциал

С целью наращивания национального потенциала государства-члена по реагированию на террористические угрозы государства-члены внедряют передовые практики, из которых можно извлечь полезный опыт. Например, в контртеррористической стратегии Финляндии отмечается необходимость технологических инноваций и обсуждается необходимость продолжения наращивания киберпотенциала страны, особенно в отношении средств сбора оперативной информации[78]. Еще один пример пересечения инноваций и национального потенциала можно найти в контртеррористической стратегии Соединенного Королевства. Одной из обсуждаемых форм сотрудничества является сотрудничество между представителями правительства и частного сектора с упором на построение отношений между правительством и технологическим сектором в рамках инновационных усилий по дальнейшему наращиванию технологического потенциала страны для реагирования на террористическую деятельность[79]. Кроме того, в контртеррористической стратегии подчеркивается важность собственного «наращивания потенциала», а также необходимость оказания помощи другим государствам-членам в повышении их способности реагировать на террористические угрозы.

Наращивание национального потенциала также может быть достигнуто за счет реализации программ обучения и подготовки. В дополнение к практике обучения и подготовки, обсуждаемой в разделе 6.1 (которая, помимо повышения осведомленности, также способствует наращиванию национального потенциала по выявлению угроз и реагирования на них), тренинги, подробно описанные в документе Европола относительно усилий по дерадикализации (см. также раздел 6.2), проводимые в пенитенциарных учреждениях, также могут способствовать укреплению национального потенциала по сокращению радикализации и реагированию на нее.

Ключевым компонентом усиления инноваций в рамках национального потенциала по борьбе с терроризмом могут стать инновации в программах исследований и разработок. Исследования ЕС в области безопасности[80] сосредоточены на разработке инициатив, направленных на повышение потенциала правоохранительных органов в таких областях, как разработка решений для анализа больших данных. Кроме того, в рамках будущей исследовательской программы Horizon Europe исследования дополнительно интегрируются в жизненный цикл

78 Министерство внутренних дел Финляндии, «Национальная контртеррористическая стратегия на 2022–2025 гг.», Публикации Министерства внутренних дел, 2022:38 (Хельсинки, Финляндия: Министерство внутренних дел Финляндии, 2022 г.), 24, URL: https://julkaisut.valtioneuvosto.fi/handle/10024/164447

79 Соединенное Королевство, «CONTEST: Контртеррористическая стратегия Соединенного Королевства», 28.

80 Европейская комиссия, «Контртеррористическая повестка ЕС: предвидеть, предупреждать, защищать, реагировать». Сообщение Комиссии Европейскому парламенту, Совету, Европейскому экономическому и социальному комитету и Комитету по делам регионов (Брюссель, Бельгия: Европейская комиссия, 2020 г.), URL: https://home-affairs.ec.europa.eu/system/files/2020-12/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf

политики безопасности, чтобы обеспечить ориентированный на воздействие результат, отвечающий выявленным потребностям правоохранительных органов[81].

Желаемые результаты политики должны учитывать следующее:

- расстановку приоритетов в отношении ресурсов с четким распределением ролей и сфер ответственности;
- повышение национального потенциала за счет следующего:
  - обмена информацией;
  - инноваций, исследований и разработок;
  - сотрудничества и партнерства;
  - наращивания потенциала.

6.5 Сотрудничество

Сотрудничество как основа разработки и реализации контртеррористической политики, связанной с новыми технологиями, может принимать разные формы и осуществляться на многих уровнях (межгосударственном, межведомственном, межсекторальном и т. д.). В частности, литература, исследованная при составлении настоящего доклада, позволила выявить множество форм передовой практики, которые помогают разрабатывать и реализовывать меры реагирования в рамках контртеррористической политики.

В резюме материалов конференции, посвященных национальным и региональным стратегиям борьбы с терроризмом, КТЦ ООН рекомендует, например, государствам-членам сотрудничать и консультировать друг друга при разработке стратегий борьбы с терроризмом[82]. В данном контексте концепция обмена информацией, представленная в разделе 5.3.1, выходит за рамки простого обмена информацией, поскольку она связана с конкретными угрозами и подчеркивает важность обмена информацией в форме примеров передовой практики. Такая рекомендация имеет особое значение при обсуждении разработки контртеррористической политики, связанной с новыми технологиями. Государства-члены могут делиться друг с другом разработками в области борьбы с использованием новых технологий в террористических целях и использования новых технологий в качестве средства реагирования на террористическую деятельность. Еще одним ценным примером передовой практики в данном документе является практика создания региональных стратегий для случаев, когда террористическая деятельность и подстрекательство к терроризму принимают трансграничный характер, что становится все более распространенным в эпоху цифровых технологий[83]. Аналогичным образом, Европейский Союз обозначил трансграничное сотрудничество в качестве «международного ответа» на глобальные угрозы[84].

Что касается управления данными, то контртеррористическая стратегия Испании затрагивает два основных аспекта, которые необходимо учитывать в политике борьбы с терроризмом: возможность использования данных и возможность доступа к данным для тех, кому они необходимы, и их защита от тех, кто не должен иметь к ним доступа[85]. В документе подчеркивается необходимость шифрования для безопасного обмена данными

81 См., например, проекты DANTE и TENSOR («Обнаружение и анализ онлайн-контента и финансовой деятельности, связанных с терроризмом»), Европейская комиссия: (CORDIS), URL: https://cordis.europa.eu/project/id/700367 (дата обращения: 1 июля 2024 г.); Европейская комиссия: Информационная служба общественных исследований и разработок (CORDIS), «Поиск и анализ гетерогенного онлайн-контента для распознавания террористической деятельности», URL: https://cordis.europa.eu/project/id/700024 (дата обращения: 1 июля 2024 г.).

82 Контртеррористический центр Организации Объединенных Наций (КТЦ ООН), «Итог обсуждений: международная конференция по национальным и региональным стратегиям борьбы с терроризмом — 31 января — 1 февраля 2013 г.», краткое содержание конференции (Богота, Колумбия, 2013 г.), 5, URL: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/bogota_jan-feb2013.pdf

83 Там же, 7.

84 «Директива (ЕС) 2017/541 Европейского парламента и Совета от 15 марта 2017 г. о борьбе с терроризмом и замене рамочного решения Совета 2002/475/JHA и внесении изменений в Решение Совета 2005/671/JHA, 88/7.

85 Министерство внутренних дел Испании, «Национальная контртеррористическая стратегия», 2019 г., 53–54, URL: https://www.dsn.gob.es/sites/dsn/files/Estrategia%20contra%20%20Terrorismo_EN_0.pdf

между заинтересованными сторонами из разных секторов. В нем также подчеркивается необходимость организации данных таким образом, чтобы заинтересованные стороны имели возможность легко и эффективно сортировать и использовать их[86].

Одним из методов обмена информацией посредством управления данными является создание реестра рисков, который будет служить базой данных о существующих угрозах и имеющихся данных, собранных об этих угрозах среди заинтересованных сторон. Модель реестра рисков, разработанная Транспортным агентством Новой Зеландии, представляет собой хороший пример типов информации, которая должна быть включена в реестр рисков страны, например, справочный номер угрозы, раздел, в котором указана дата и описание последнего раза, когда действия были предприняты против угрозы, план действий на случай реализации угрозы, а также распределение ролей, которые каждая заинтересованная сторона должна исполнять в случае материализации угрозы[87].

Одним из способов безопасного обмена таким реестром и сопровождающей его информацией является принятие модели, аналогичной «кластерной» модели, практикуемой в Соединенном Королевстве. Кластерная модель является средством межотраслевого регионального сотрудничества между государственными органами, представителями частного сектора и научными кругами. В рамках данной модели каждый регион представлен в виде отдельного кластера, который работает в полунезависимом режиме и расставляет приоритеты в отношении угроз таким образом, который в наибольшей степени соответствует его конкретной зоне ответственности (ЗО). Заинтересованные стороны в каждом кластере обмениваются информацией и передовым опытом. При этом кластеры объединяются в единую централизованную структуру, в рамках которой они в конечном итоге сообщают о выявленных угрозах и делятся соответствующей информацией с заинтересованными сторонами на национальном уровне[88]. Локализованный характер модели обеспечивает более детальный подход к оценке угроз и установлению приоритетов в отношении ЗО, а также позволяет заинтересованным сторонам на национальном уровне получить более глубокое понимание каждого из регионов, входящих в сферу их ответственности.

Желаемые результаты политики должны учитывать следующее:

- укрепление сотрудничества между национальными CSIRT, правоохранительными органами и органами уголовного правосудия для расследования и преследования террористов;
- укрепление сотрудничества между правоохранительными органами и частными ИКТ-компаниями;
- расширение сотрудничества на региональном и международном уровне;
- улучшение обмена информацией посредством:
  - обмена примерами передовой практики;
  - заключения соглашений об обмене информацией;
  - совершенствования подхода и практики управления данными.

86 Там же.

87 Транспортное агентство Новой Зеландии, «Реестр рисков» (Правительство Новой Зеландии, Транспортное агентство Новой Зеландии), URL: https://www.nzta.govt.nz/roads-and-rail/rail/operating-a-railway/risk-management/risk-register (дата обращения: 1 июля 2024 г.).

88 Объединение киберкластеров Великобритании (UKC3), «Операционная основа киберкластеров», *UK Cyber Cluster Collaboration* (блог), URL: https://ukc3.co.uk/cyber-cluster-operating-framework (дата обращения: 1 июля 2024 г.).

Контртеррористическое управление Организации Объединенных Наций
Центральные учреждения Организации Объединенных Наций
New York, NY 10017

www.un.org/counterterrorism

КОНТРТЕРРОРИСТИЧЕСКОЕ УПРАВЛЕНИЕ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ
Контртеррористический центр ООН (КТЦ ООН)

24-09828