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

INTERPOL

При финансовой поддержке Европейского союза

Кибербезопасность и новые технологии

Создание законодательной базы, механизмов обеспечения прозрачности и надзора в отношении сбора данных в Интернете

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

- **Нине Сунде —** суперинтенданту полиции (PhD), Норвежский полицейский университетский колледж

Термины и определения

Административное и уголовное процессуальное право	Административное и уголовное процессуальное право определяет пороговые значения, условия и меры защиты, которые применяются к оперативной деятельности правоохранительных органов. Таким образом, оно служит как для обеспечения деятельности правоохранительных органов, так и снижения возможных рисков для основных прав. Процессуальное право позволяет реализовать различные оперативные возможности.
Административные полномочия	1) Пресечение деятельности по финансированию терроризма посредством сотрудничества с подразделениями финансовой разведки и налоговыми органами. Данная деятельность может быть поставлена под угрозу благодаря новым технологиям, которые позволяют осуществлять переводы, в том числе криптовалюты. 2) Пресечение деятельности, связанной с вербовкой, подстрекательством и коммуникацией. Интернет и социальные сети позволяют охватить широкую аудиторию и служат платформой для коммуникации, подстрекательства и вербовки. Для пресечения такого рода деятельности (и сбора информации об участниках) требуется разработка системы для работы с различными интернет-посредниками. 3) Идентификация, отслеживание, замораживание, арест и конфискация доходов от преступлений.
Верховенство права	Осуществление функций и полномочий основывается на четких положениях закона, в котором содержится исчерпывающее перечисление соответствующих полномочий. Ни при каких обстоятельствах осуществление таких функций и полномочий не может нарушать императивных или не допускающих отступлений норм международного права; осуществление функций и полномочий подлежит независимому утверждению или контролю со стороны судебного или иного уполномоченного органа в соответствии с международными стандартами.
Действия правоохранительных органов	Этот термин, как правило, описывает действия правоохранительных органов, основанные на законе, предпринятые для противодействия угрозе, которые могут включать задержание отдельных лиц, пресечение деятельности злоумышленников (например, удаление контента, арест активов) и т. д.
Дополнительный вид ответственности/ материальная поддержка/соучастие в преступлении	Правонарушения, применимые к субъектам, осуществляющим незаконную деятельность не полностью, а частично. К таким правонарушениям относится «покушение» на осуществление преступной деятельности, а также пособничество или содействие в совершении преступлений. В целом ответственность за дополнительное преступление предполагает необходимость доказывания того, что преступление было совершено главным субъектом, а вспомогательная деятельность — вспомогательным субъектом.
Зеттабайт	Один зеттабайт равен одному миллиарду терабайтов.
Искусственный интеллект (ИИ)	Под этим термином обычно понимают дисциплину, занимающуюся разработкой технологических инструментов, позволяющих имитировать когнитивные функции человеческого мозга, такие как планирование, обучение, рассуждение и анализ.
Использование новых технологий правоохранительными органами	1) Использование на оперативном уровне новых технологий, которые включают мобильные телефоны, нагрудные камеры, устройства дистанционного наблюдения, тактические дроны. 2) Биометрическое распознавание лиц в определенных случаях для улучшения идентификации и предотвращения. 3) Искусственный интеллект (ИИ). 4) Анализ больших объемов данных. 5) Криптография для борьбы с вирусами-вымогателями и для доступа к зашифрованному контенту. 6) Возможности анализа криптовалют.

Киберпреступления	Уголовные преступления, связанные с использованием компьютера, которые препятствуют деятельности, целью которой является обеспечение конфиденциальности, целостности и доступности компьютеров, сетей и хранящихся в них данных.
Новые технологии	Термин «новые технологии» охватывает широкий спектр различных технологий,[1] 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[2].
Общепринятые принципы защиты данных	Глобальные принципы, которые применяются к сбору и обработке персональных данных, такие как принципы конфиденциальности ОЭСР, принципы конфиденциальности АТЭС, Конвенция № 108 Совета Европы, Конвенция Африканского союза о кибербезопасности и защите персональных данных.
Общие полномочия правоохранительных органов	Сбор информации, вызов свидетелей, запрос о представлении информации или вещи, допрос и задержание для допроса.
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 в соответствии с обязательствами государств-членов по международному праву прав человека.
Полномочия правоохранительных органов, связанные с новыми технологиями[3]	1) Оперативное сохранение конкретных компьютерных данных, включая данные о трафике. 2) Ускоренное сохранение и частичное раскрытие данных о трафике. 3) Распоряжение о представлении цифровых доказательств. 4) Поиск и изъятие хранимых компьютерных данных 5) Сбор данных о коммуникационном трафике в режиме реального времени. 6) Перехват данных о содержании коммуникации.
Принципы ООН в области прав человека применительно к контртеррористической деятельности[4]	i) Осуществление функций и полномочий должно основываться на четких положениях закона, в котором содержится исчерпывающее перечисление соответствующих полномочий. ii) Ни при каких обстоятельствах осуществление таких функций и полномочий не может нарушать императивных или не допускающих отступлений норм международного права. iii) В тех случаях, когда осуществление функций и полномочий предполагает ограничение права человека, которое можно ограничивать, любое такое ограничение должно быть как можно менее интрузивным и должно: 1) быть необходимым в демократическом обществе для достижения определенной законной цели в соответствии с международным правом; 2) быть соразмерным пользе, получаемой в случае достижения этой законной цели; 3) Если государство является одной из сторон происходящего вооруженного конфликта, вышеуказанные положения применяются также для обеспечения соблюдения принципов и положений международного гуманитарного права, причем без ущерба для обязательства соблюдать международное право прав человека и международное беженское право. iv) Если наличие веских причин требует установления определенных полномочий для некоторых органов: 1) Такие полномочия должны содержаться в отдельном законодательном акте, который может рассматриваться как уникальное исключение из общепринятого правового ограничения; 2) Положения, в соответствии с которыми устанавливаются такие полномочия, должны применяться с учетом установленных сроков действия и подлежать регулярному пересмотру; и 3) Использование таких полномочий в иных целях, кроме борьбы с терроризмом, должно быть запрещено.

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

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

3 На основании Конвенции Совета Европы о киберпреступности.

4 Согласно Специальному докладчику ООН по борьбе с терроризмом и правам человека относительно ограничений прав и свобод. Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Мартина Шейнина (A/HRC/16/51), Practice XX, URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/178/98/PDF/ G1017898.pdf?OpenElement.

Процессуально-правовые гарантии	1) Четкое определение обстоятельств и оснований, оправдывающих использование полномочий. 2) Ограничение объема и длительности использования таких полномочий. 3) Учет влияния на права, обязанности и законные интересы третьих лиц. 4) Справедливый процесс. 5) Потребность в обеспечении наличия судебного или иного независимого уполномоченного органа в зависимости от риска и условий.
Расширенные полномочия правоохранительных органов, связанные с новыми технологиями	1) Возможность осуществления операций в дарквебе. 2) Удаленный доступ к компьютеру или другому устройству и сбор информации. 3) Удаленный и скрытный доступ к компьютеру или другому устройству и сбор информации. 4) Пресечение злонамеренного использования инфраструктур и веб-сайтов с целью создания риска или ущерба, связанного с компьютером. 5) Пресечение распространения явно злонамеренных речей террористической направленности, например подстрекательств и вербовок, через веб-сайты и платформы с помощью сотрудничества со структурами частного сектора. 6) Возможность ареста криптовалют.
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.
Риск терроризма, связанный с использованием новых технологий[5]	Атаки вирусов-вымогателей/создание вредоносного ПО/DDoS-атаки/BGP-перехват/использование зашифрованных коммуникаций/деятельность в дарквебе в целом/использование криптовалют в преступных целях/угрозы с использованием социальной инженерии — фишинг/смишинг/вишинг/компрометация корпоративной электронной почты/«серая инфраструктура» — абузоустойчивый хостинг/средства анонимизации/отмывание денег с помощью денежных мулов/дезинформация и распространение ложных сведений/использование 3D-печати для изготовления оружия.
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[6].
Террористические преступления с использованием новых технологий	Террористические преступления с использованием новых технологий, включая 1) кибератаки против объектов критически важной инфраструктуры; 2) подстрекательства посредством Интернета и социальных сетей; 3) вербовку через Интернет и социальные сети; 4) распространение террористического контента или радикализации, ведущей к терроризму, в Интернете или социальных сетях; и 5) финансирование терроризма.
Уголовное расследование	Процесс сбора информации (или доказательств) для установления факта совершения преступления, выявления преступника и представления доказательств в поддержку обвинения в судебном процессе.
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.
Уникальная административная поддержка	Правовые полномочия, позволяющие быстро осуществлять закупки, заключать договоры со специалистами в предметной области и заключать договоры в условиях оперативных ограничений.

5 Европол, «Оценка угроз организованной преступности в Интернете (IOCTA). Обновления в стратегии, политике и тактике борьбы с киберпреступностью», URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-report, и Европейское агентство по сетевой и информационной безопасности (ENISA). Отчет ENISA «Ландшафт угроз 2022», URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

6 См. S/RES/1566 (2004), пункт 3.

Уникальные контр-террористические полномочия	1) Включение в список террористических субъектов. 2) Предъявление скрытых доказательств. 3) Защита агентурных источников. 4) Специальные методы расследования, которые включают методы, используемые для сбора информации, такие как электронные или иные формы наблюдения и агентурные операции, без предупреждения тех, в отношении кого применяются данные методы, и в целях выявления и расследования преступлений[7].
Управление расследованиями	Управление расследованиями с использованием общих полномочий правоохранительных органов, цифровых полномочий правоохранительных органов, связанных с новыми технологиями, и расширенных цифровых полномочий правоохранительных органов, связанных с новыми технологиями.
Ценностная цепочка контртеррористической деятельности правоохранительных органов	Ценностная цепочка контртеррористической деятельности правоохранительных органов описывает основные оперативные возможности правоохранительных органов, включающие в себя «общие полномочия правоохранительных органов» и «исключительные контртеррористические полномочия»; полномочия правоохранительных органов, связанные с новыми технологиями; расширенные полномочия правоохранительных органов, связанные с новыми технологиями; и действия правоохранительных органов. Данный термин дополняется определением «использования новых технологий правоохранительными органами»[8].

7 Рекомендация Rec(2005)10 Комитета министров Совета Европы о «специальных методах расследования» в отношении серьезных преступлений, включая акты терроризма, Страсбург, URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805da6f6

8 Как отмечалось, данный термин следует пересматривать, чтобы обеспечить его актуальность по мере развития технологий.

Краткое содержание

Цель Национальной системы оценки возможностей правоохранительных органов в сфере противодействия использованию новых возможностей в террористических целях (далее — «Система оценки возможностей правоохранительных органов») состоит в поддержке наращивания потенциала, оценки зрелости и трансграничного сотрудничества.

В настоящем документе приводится «Национальная эталонная модель возможностей» («модель»), которая описывает ценностную цепочку контртеррористической деятельности правоохранительных органов, а также необходимые политические, правовые и институциональные возможности для ее разработки и внедрения. Модель дополнена моделью оценки зрелости, которая включает более детальные вопросы о каждой из возможностей. Ее целью является поддержка государств-членов в активизации планирования, определения приоритетов и наращивания возможностей.

Модель и элементы модели зрелости основаны на кабинетных исследованиях, опыте и выводах, полученных из параллельных проектов в области кибербезопасности и киберпреступности. Основное внимание в модели уделяется роли правоохранительных органов на стыке контртеррористической деятельности и новых технологий с точки зрения правоохранительных органов. Она охватывает общие политические, правовые и институциональные возможности в рамках этого контекста, учитывая рост значимости цифровой сферы для национальной безопасности, а также для социальной и экономической деятельности. Соображения, связанные с правами человека, включены посредством всех соответствующих политических, правовых и институциональных возможностей в рамках подхода «права человека по умолчанию». Предполагается, что это также смягчит возможные разногласия при развертывании.

Ввиду быстрого темпа технологических изменений модель включает в себя политические и институциональные элементы, которые необходимы для адаптации к новым сценариям угроз, например сканирование горизонта на уровне политики и управление инновационной деятельностью на уровне правоохранительных органов. Этот подход дополнен списком особых примеров использования, который охватывает распространенные конкретные сценарии террористической деятельности с применением новых технологий и использование новых технологий правоохранительными органами. Эти примеры использования отражают текущий сценарий, касающийся угроз и применения технологий, и должны регулярно обновляться. Поскольку модель была разработана на основе кабинетных исследований, консультаций с заинтересованными сторонами и вклада экспертов, положительное влияние на нее окажут полученная обратная связь от государств-членов и опыт, накопленный в ходе ее использования. Эти выводы, полученные после внедрения модели, могут служить в качестве основы для ее обновления по мере необходимости.

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)[9] в июле 2021 года государства-члены выразили глубокую озабоченность по поводу «использования Интернета и других информационно-коммуникационных технологий, включая платформы социальных сетей, в террористических целях, в том числе непрекращающееся распространение 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)[10] и 2396 (2017)[11] Совета Безопасности призывают государства-члены сотрудничать при принятии национальных мер, призванных воспрепятствовать использованию террористами технологий и средств связи для совершения террористических актов. 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[12] 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», указав, что платформы, на которые ссылаются государства-члены, включают, среди прочих, Telegram, Rocket.Chat, Hoop и TamTam. В докладе также говорится о том, что **сторонники ИГИЛ используют платформы в дарквебе** 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[13].

9 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

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

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

12 Тридцатый доклад Группы по аналитической поддержке и наблюдению за санкциями, представленный во исполнение резолюции 2610 (2021) по ИГИЛ: (ДАИШ), «Аль-Каиде» и связанным с ними лицам, группам, предприятиям и организациям S/2022/547 (undocs.org)

13 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 соблюдении прав человека и принципа верховенства права.
 Компонент 1.3	Укрепление потенциала отдельных государств-партнеров в сфере разработки мер реагирования в рамках национальной контртеррористической политики для противодействия использованию террористами новых технологий и применения новых технологий в деле борьбы с терроризмом при полном соблюдении 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 соблюдении 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

Настоящий документ служит всеобъемлющим и в то же время лаконичным источником информации о возможностях правоохранительных органов, необходимых для противодействия использованию новых технологий в террористических целях. Он предназначен для оказания поддержки государствам-членам в разработке и использовании этих возможностей. Документ содержит национальную модель возможностей, состоящую из трех направлений — политического, правового и институционального, а также систему оценки возможностей. Цель этого документа состоит в том, чтобы обеспечить возможность измерения зрелости потенциала и тем самым предоставить государствам-членам поддержку в планировании, управлении и определении приоритетности усилий по наращиванию потенциала и использованию ресурсов.

1.3.1 Сфера охвата

Национальная эталонная модель возможностей и прилагаемая к ней система оценки зрелости предназначены для описания возможностей правоохранительных органов на национальном уровне по противодействию использованию новых технологий в террористических целях. Следовательно, настоящим документом не предусматривается охват всех тех аспектов национальной контртеррористической или правоприменительной политики, которые не имеют отношения к противодействию использованию новых технологий в террористических целях.

1.3.2 Целевая аудитория

Настоящее руководство предназначено в первую очередь для специалистов, отвечающих за разработку политики, а также правоохранительных органов и контртеррористических ведомств.

1.3.3 Преимущества

Цель модели — интегрировать передовой опыт, связанный с возможностями правоохранительных органов в отношении новых технологий. Она может служить опорой для государств-членов в их деятельности, необходимой для разработки и реализации долговременной стратегии.

Эти возможности могут оказать положительное влияние на способность решать проблемы, связанные с киберпреступностью, и обеспечить сбалансированное использование полномочий правоохранительных органов в этой области. Программы наращивания потенциала в сфере борьбы с киберпреступностью повышают гарантии в отношении верховенства права, а также прав человека и гражданина[14]. Программы наращивания потенциала в сфере борьбы с киберпреступностью способствуют развитию человеческого потенциала и совершенствуют управление[15]. Данная модель также может содействовать достижению каждой из следующих целей[16]:

- надзор и подотчетность в отношении необходимых мер по обеспечению правопорядка;
- обеспечение общественной безопасности при соблюдении основных прав;
- выявление пробелов и недостающих элементов в рамках деятельности правоохранительных органов;
- отнесение инвестиций в развитие возможностей правоохранительных органов к числу приоритетных задач;
- информирование о деятельности правоохранительных органов, управление ожиданиями и методами сотрудничества с широкой общественностью и соответствующими представителями в частном секторе;
- обеспечение коммуникации и сотрудничества с международными партнерами;
- содействие в прогнозировании предстоящих проблем.

1.3.4 Ограничения

В модели возможностей основное внимание уделяется национальным контртеррористическим возможностям правоохранительных органов, в частности в сфере противодействия использованию новых технологий в террористических целях, тогда как комплексные контртеррористические стратегии требуют дополнительных мер и возможностей. Несмотря на то, что модель охватывает некоторые из этих дополнительных мер, она не охватывает их все. К таким дополнительным (выходящим за рамки требований) мерам относятся, например, улучшение социальных услуг для создания благоприятной среды, способствующей снижению риска радикализации.

В модели основное внимание уделяется возможностям правоохранительных органов для решения проблем, связанных с новыми технологиями. При этом эти возможности основываются на базовом уровне общих возможностей, имеющихся у правоохранительных органов, таких как установленные правовые основы, правоохранительные процедуры и использование информационных технологий.

---

14 Всемирный банк, «Борьба с киберпреступностью, инструменты и наращивание потенциала для стран с развивающейся экономикой», 2013 г., URL: https://openknowledge.worldbank.org/entities/publication/fde78414-b14c-504b-af5d-78b5b21caaf3, с. 46.

15 Там же, с. 46: ИКТ могут быть «мощными инструментами для развития человеческого потенциала и сокращения масштабов бедности», а программы по наращиванию потенциала в области киберпреступности могут помочь обществам в этом[7]. Вместе с этим усиление доверия, безопасности и надежности ИКТ и ИКТ-систем будет способствовать экономическому развитию, облегчать доступ к образованию и обмену информацией[8]. Эффективные системы уголовного правосудия повышают физическую безопасность и здоровье людей, например, посредством защиты детей от сексуальной эксплуатации и насилия, предотвращения распространения поддельных и некачественных лекарств или защиты людей от преступности в целом. Более строгое соблюдение принципа верховенства права благоприятствует демократическому управлению и уменьшает необоснованное вмешательство в права личности».

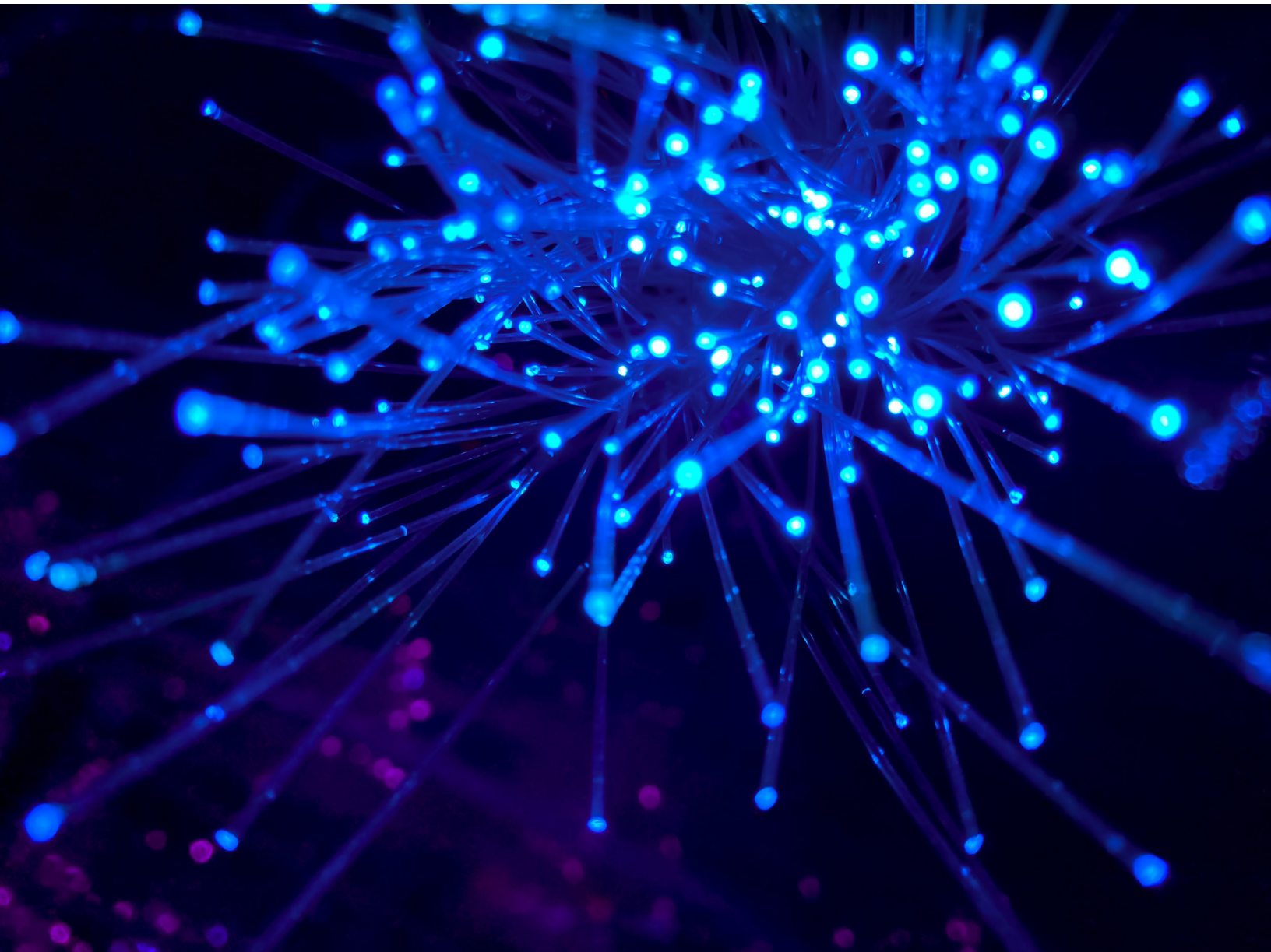
16 См. Европейское агентство по сетевой и информационной безопасности (ENISA), Национальная система оценки возможностей, декабрь 2020 г., URL: https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework, (ENISA), с. 19.

Модель разрабатывалась с перспективой на будущее и возможностью адаптации к новым технологиям по мере их развития. На момент ее разработки в центре внимания новых технологий — Интернет, социальные сети и криптовалюты. В модели заложены основы для сканирования горизонта, чтобы подготовиться к появлению рисков, однако новые скачки в технологическом развитии могут потребовать полного пересмотра модели.

Целью данной модели является описание основных элементов возможностей правоохранительных органов, однако может потребоваться дополнительная адаптация в оценке и применении с учетом уникальных правовых, социальных и экономических условий в государствах-членах.

1.3.5 **Предостережение**

Это первая версия документа, в связи с чем он подлежит подтверждению в процессе деятельности по наращиванию потенциала, что будет служить основой для его будущих обновлений. Изложенная здесь информация предназначена для предоставления государствам-членам руководства и содействия в вопросе наращивания потенциала. Несмотря на все приложенные усилия по обеспечению точности, полноты и актуальности содержания мы не даем никаких заверений или гарантий, явных или подразумеваемых, в отношении точности, надежности, пригодности или доступности информации, содержащейся в настоящем документе.



[II]

Подход

2.1 Обзор

Цель настоящего доклада заключается в том, чтобы предоставить государствам-членам поддержку и возможности для оценки и определения пробелов и областей совершенствования текущего национального контртеррористического потенциала правоохранительных органов в сфере противодействия использованию новых технологий в террористических целях в соответствии с Глобальной контртеррористической стратегией Организации Объединенных Наций и при полном соблюдении 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 принципа 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, политика, 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**

Механизм	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 ею должны осуществляться в соответствии с обязательствами государств-членов по международному 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 реализацией в обоих направлениях — «сверху вниз» и «снизу вверх».

2.3 Методология

РИСУНОК 3

В качестве информационных источников при разработке и составлении настоящего документа был использован широкий спектр материалов, включая документы проекта CT TECH, консультации с заинтересованными сторонами, данные внутреннего анализа, кабинетные исследования, совещания экспертных групп (СЭГ), сотрудничество с различными структурами в рамках Глобального договора по координации контртеррористической деятельности, а также руководящая основа, описанная выше в разделе 2.2. Содержание модели основывается на предыдущих информационных материалах, разработанных для национальных возможностей по борьбе с киберпреступностью, национальных возможностей по обеспечению кибербезопасности и национальных контртеррористических стратегий.

Цель документа состоит в том, чтобы обеспечить общую основу, но с акцентом на контртеррористической деятельности правоохранительных органов в отношении новых технологий, и предоставить практическую и важную информацию. Данный подход подкрепляется терминами и определениями, которые применяются в документе для разъяснения модели возможностей и вопросов для оценки зрелости. Эти термины и определения описывают деятельность правоохранительных органов, а также использование правоохранительными органами новых технологий.

Ввиду быстрого темпа технологических изменений модель включает в себя политические и институциональные элементы, которые необходимы для адаптации к новым сценариям угроз, например сканирование го-

ризонта на уровне политики и управление инновационной деятельностью на уровне правоохранительных органов. Кроме того, чтобы обеспечить актуальность, предлагается периодически обновлять термины и определения, которые более зависят от времени (например, относящиеся к «новым технологиям»).

2.3.1 Совещания экспертных групп и консультации

Данное руководство было разработано при участии экспертов в рамках 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 передового опыта 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 международное право прав человека, международное беженское право и международное гуманитарное право.

2.3.2 Обзор справочных материалов

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

ТАБЛИЦА 3. **Справочные материалы**

1	Интерпол, Руководство по разработке национальной стратегии кибербезопасности, 2021, https://www.interpol.int/content/download/16455/file/Cyber%20Strategy%20Guidebook.pdf
2	Глобальный центр развития потенциала в области кибербезопасности, «Модель зрелости потенциала в области кибербезопасности (CMM) для стран», издание 2021 г., https://gcscc.ox.ac.uk/cmm-2021-edition
3	Европейское агентство по сетевой и информационной безопасности (ENISA), Национальная система оценки возможностей, декабрь 2020 г., https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework
4	Всемирный банк, «Борьба с киберпреступностью, инструменты и наращивание потенциала для стран с развивающейся экономикой», https://openknowledge.worldbank.org/entities/publication/fde78414-b14c-504b-af5d-78b5b21caaf3
5	Совет Европы, Европейский союз, Специализированные подразделения по борьбе с киберпреступностью. «Изучение передового опыта», 2011 г., https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33
6	Совет Европы/Офис программы по борьбе с киберпреступностью [EN], «Глобальное состояние законодательства о киберпреступности в 2013–2023 гг.: беглый обзор», 31 декабря 2022 г., https://rm.coe.int/3148-1-3-4-cyberleg-global-state-dec-2023-v4-public/1680adadf0
7	Европол, «Оценка угроз организованной преступности в Интернете (IOCTA). Обновления в стратегии, политике и тактике борьбы с киберпреступностью», https://www.europol.europa.eu/publications-events/main-reports/iocta-report
8	Управление Организации Объединенных Наций по наркотикам и преступности, «Оперативная информация. Руководство для правоохранительных органов первой линии», ООН, Нью-Йорк, 2010 г., https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Front_Line_Law_Enforcement.pdf
9	Совет Европы, Консультативный комитет по Конвенции о защите физических лиц при автоматизированной обработке персональных данных, «Практическое руководство по использованию персональных данных в сфере деятельности полиции», T-PD (2018), https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5

10 Управление Организации Объединенных Наций по наркотикам и преступности, Совет Безопасности Организации Объединенных Наций, Исполнительный директорат Контртеррористического комитета. «Система раскрытия данных. Общие практики, разработанные международными поставщиками услуг в ответ на запросы зарубежных правительств о предоставлении данных», ООН, 2021, https://sherloc.unodc.org/cld/uploads/res/pdf/data-disclosure-framework_html/Data_Disclosure_Framework.pdf

11 Rick Muir and Stephen Walcott, Unleashing the Value of Digital Forensics («Раскрытие ценности цифровой криминалистики»), The Police Foundation, 2021, https://www.police-foundation.org.uk/publication/unleashing-the-value-of-digital-forensics/

12 Комитет министров Совета Европы, Рекомендация Rec(2005)10 о «специальных методах расследования» в отношении серьезных преступлений, включая акты терроризма, Страсбург, 20 апреля 2005 г., глава 1, https://wcd.coe.int/ViewDoc.jsp?id=849269&Site=COE

13 Tech against Terrorism, «Состояние дел: тенденции использования Интернета террористами и воинствующими экстремистами», 2022 г., https://www.techagainstterrorism.org/2023/01/19/state-of-play-trends-in-terrorist-and-violent-extremist-use-of-the-Internet-2022/

14 ЕВРОПОЛ, «В центре внимания Европола», «Криптовалюты: отслеживание эволюции криминальных финансов», 26.01.22, https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances#downloads

15 ОБСЕ, «Классификация киберинцидентов: доклад о новой практике в регионе ОБСЕ», 2022 г., https://www.osce.org/secretariat/530293

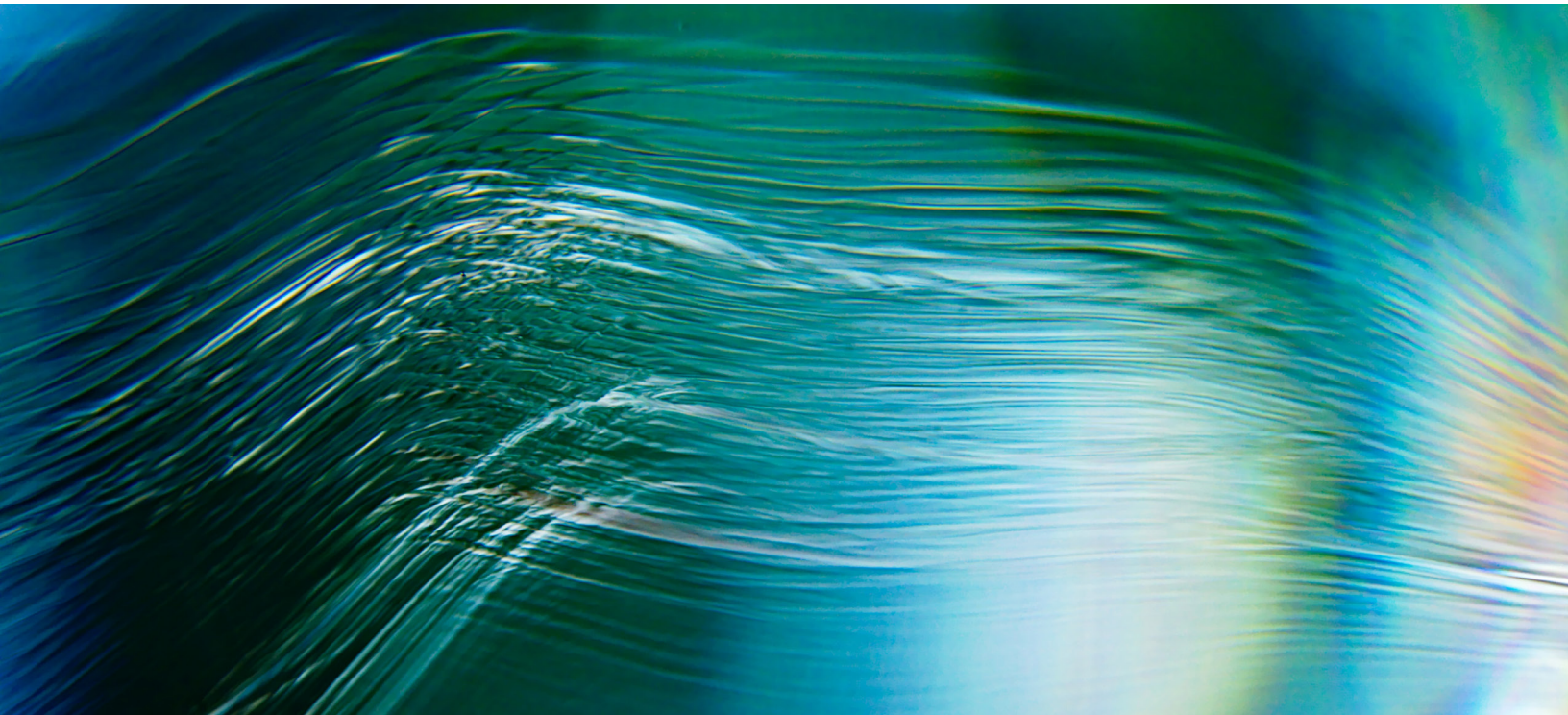
16 «Руководство ОБСЕ по полицейской деятельности на основе оперативных данных и информации», 2017 г., https://www.osce.org/chairmanship/327476

17 Специальный докладчик ООН по борьбе с терроризмом и правам человека относительно ограничений прав и свобод, Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Мартина Шейнина (A/HRC/16/51), Practice XX, https://undocs.org/Home/Mobile?FinalSymbol=a%2Fhrc%2F16%2F51&Language=E&DeviceType=Desktop&LangRequested=False

18 OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

19 ОБСЕ, БДИПЧ, «Права человека в антитеррористических расследованиях. Практическое руководство для сотрудников правоохранительных органов», 2013 г., https://www.osce.org/files/f/documents/5/f/108930.pdf

20 Европейское агентство по сетевой и информационной безопасности (ENISA), отчет ENISA «Ландшафт угроз 2022», https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022



[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. Появление новых технологий принесло правоохранительным органам во всем мире не только возможности, но и создало проблемы, особенно в их борьбе с терроризмом. Для эффективной борьбы с этой постоянно изменяющейся угрозой необходимо, чтобы система модели возможностей правоохранительных органов была ориентирована на новые технологии. Данная система обеспечивает правоохранительные органы системным подходом к пониманию возможностей, которые террористы могут получить благодаря техническим достижениям, а также к противодействию им. Модель возможностей позволит вооружить правоохранительные органы знаниями, необходимыми для разработки упреждающих стратегий, улучшения сбора оперативной информации и подрыва террористических сетей. Такая система позволяет правоохранительным органам оставаться на шаг впереди, адаптироваться к новым тактикам и защищать общество от постоянно меняющихся проблем, возникающих в результате использования террористическими организациями новых технологий.

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[17], из которых более 93 процентов — это пользователи социальных сетей[18]. По оценкам, в 2022 году в мире будет создано более 97 зеттабайт[19] информации[20]. 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, обеспечивающих анонимность и возможность координировать и действовать удаленно.

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

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

19 Один зеттабайт равен одному миллиарду терабайтов.

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

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

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

3.2.1 Вызовы: использование новых технологий в террористических целях

Достижения в области 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 правоохранительной деятельности. 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 имеет разрушительные последствия для реализации права на жизнь, свободу и физическую неприкосновенность потерпевших. Помимо указанных последствий для отдельных лиц, терроризм может дестабилизировать правительства, подрывать функционирование гражданского общества, создавать угрозу миру, безопасности и социально-экономическому развитию. Все эти аспекты оказывают непосредственное влияние на реализацию прав человека. Государства обязаны принимать меры по защите своих граждан и иных лиц от угроз террористических атак и привлекать к ответственности виновных в таких деяниях. Такие меры по борьбе с терроризмом, в том числе деятельность по его предотвращению и преследованию лиц, ответственных за террористические акты, должны сами соответствовать международным стандартам в области прав человека и принципу верховенства права.

Использование новых технологий в контртеррористической деятельности ставит новые задачи в области прав человека. В частности, государства должны обеспечить, чтобы контртеррористические законы, политика и практика гарантировали соблюдение таких прав, как право на неприкосновенность частной жизни, право на свободу выражения мнений, свободу ассоциации, свободу религии, право на свободу и личную неприкосновенность, а также принцип недискриминации и процессуальные права, включая презумпцию невиновности и право на справедливое судебное разбирательство. Кроме того, государства должны строго соблюдать принцип абсолютного запрета пыток.

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[21]. В частности, в четвертом направлении Глобальной контртеррористической стратегии ООН определены меры по обеспечению всеобщего уважения прав человека и принципа верховенства права в качестве фундаментальной основы для борьбы с терроризмом и отмечается, что «действенные меры по борьбе с терроризмом и защита прав человека являются целями, которые не противоречат, а дополняют и взаимно подкрепляют друг друга».

3.2.4 Гендер, технологии и возможности правоохранительных органов

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 и 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, сексуальную ориентацию, возраст и т. д. Мужчины, женщины, девочки и мальчики, а также лица с другими гендерными идентичностями и моделями самовыражения воспринимают безопасность по-разному с учетом своих особых потребностей, уязвимостей и возможностей[22]. Особенно при использовании новых технологий, несмотря на то что из-за отсутствия иерархических структур в Интернете могут быть устранены гендерные ограничения и имеются возможности для расширения прав и возможностей женщин, существует высокая вероятность их вербовки или активного участия в деятельности насильственных экстремистских и

21 A/RES/60/288, резолюция 60/158 Генеральной Ассамблеи, резолюции 1456 (2003), 1624 (2005), 1805 (2008), 2129 (2013), 2178 (2014), 395 (2017) и 2396 (2017) Совета Безопасности.

22 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

террористических групп в Интернете[23]. Имеющиеся данные также свидетельствуют о том, что террористические группы используют гендерные особенности в обмене онлайн-сообщениями; например, ИГИЛ использует в стратегических целях гендерно ориентированные сообщения в вербовке и коммуникациях, меняя свой дискурс в зависимости от целевой группы[24]. Еще один важнейший аспект, касающийся гендера и новых технологий, связан с цифровым гендерным разрывом, при котором во всем мире доступ к Интернету, по оценкам, имеют 85 процентов женщин в сравнении с мужчинами, при этом примерно 1,7 миллиарда женщин в странах глобального Юга не имеют доступа. Такое неравенство порождает проблемы в области прав человека, лежащие в основе всех аспектов кибербезопасности, включая потенциальную подверженность воздействию, отсутствие безопасности или участие в структуре управления[25].

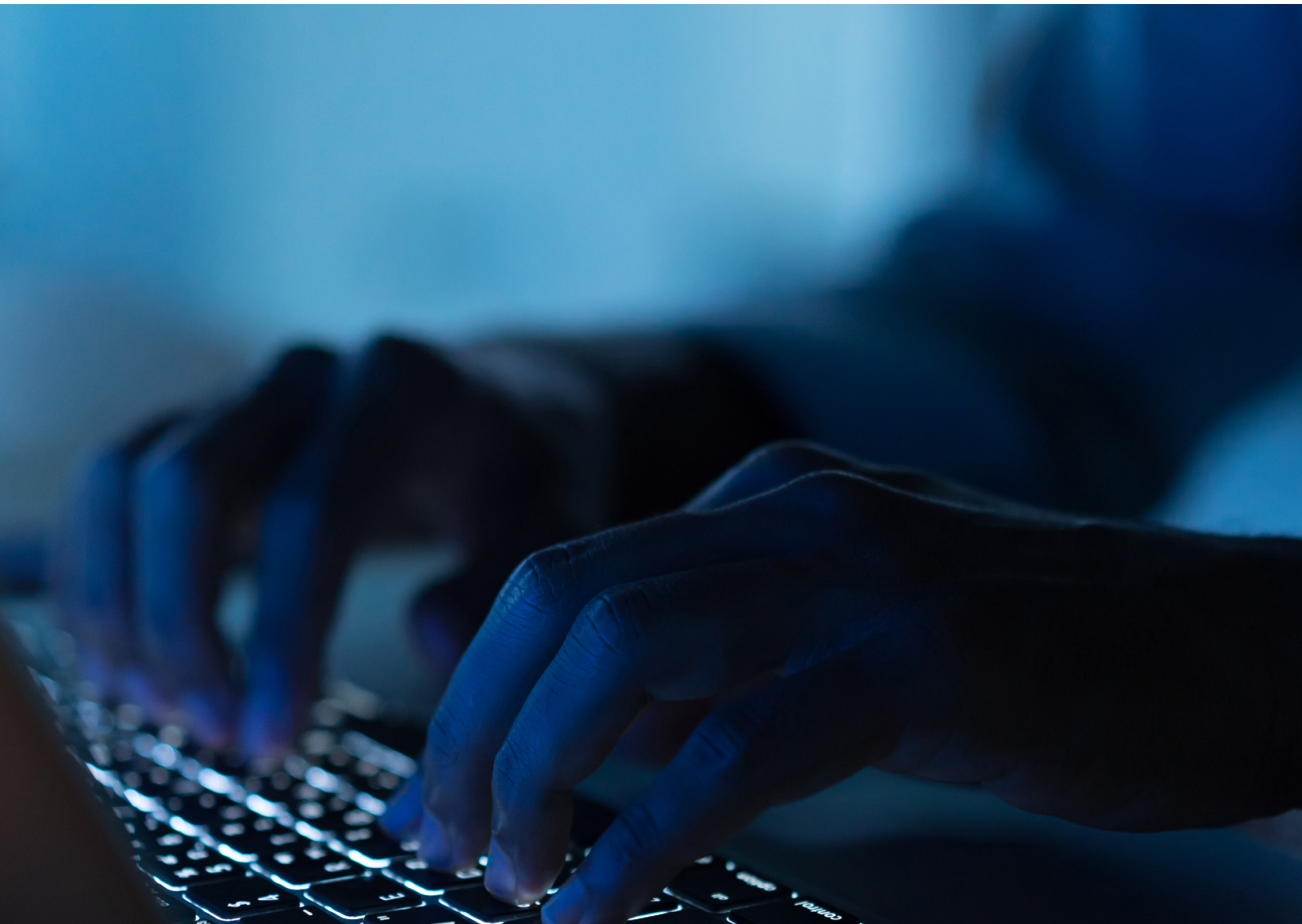
Таким образом, включение гендерных аспектов в потенциал национальных правоохранительных органов и ответные меры является крайне важным для оценки террористических намерений и потенциальных целей, а также для разработки надлежащих ответных мер, ориентированных на удовлетворение особых потребностей и решение проблем уязвимости лиц разной гендерной принадлежности, с учетом интерсекциональных факторов, таких как возраст, инвалидность, этническая принадлежность, язык, национальность, расовая идентичность, религия, сексуальная ориентация или любой другой фактор идентичности и их сочетания.

---

23 ИДКТК, «Вызов со стороны возвращающихся и перемещающихся иностранных боевиков-террористов: перспективы проведения исследований», февраль 2019 г.

24 Nelly Lahoud, 'Empowerment or Subjugation: An Analysis of ISIL's Gendered Messaging' (UN Women, June 2018) («Расширение прав и возможностей или подчинение: анализ гендерно ориентированных сообщений ИГИЛ»).

25 ДКВС, «Гендерное равенство, кибербезопасность и управление сектором безопасности: понимание роли гендера в управлении кибербезопасностью», январь 2023 г., URL: https://www.dcaf.ch/gender-equality-cybersecurity-and-security-sector-governance



[IV] Национальная эталонная модель возможностей

4.1 Обзор

Национальная эталонная модель возможностей служит национальным планом, в котором расписаны необходимые национальные возможности для противодействия использованию новых технологий в террористических целях, а также для применения новых технологий в борьбе с терроризмом. Она позволяет государствам-членам оценить текущие национальные возможности в сравнении с национальной эталонной моделью возможностей, чтобы определить основные пробелы и возможности для дальнейшего совершенствования и развития. Отправной точкой для построения предложенной системы модели являются уникальные элементы пересечения правоохранительной деятельности, террористической деятельности и защиты основных прав. Она базируется на общепринятых правовых и политических принципах в этой области и предназначена для обеспечения эффективной деятельности правоохранительных органов в рамках принятой системы защиты основных прав.

4.1.1 Обзор системы

РИСУНОК 4

L1-Уровень 1; L2-Уровень 2; L3-Уровень 3

Разработка национальной эталонной модели возможностей организована логически в порядке иерархии с функциональным разделением на детализированные группы.

Уровень 1: направления	*Структура национальной эталонной модели возможностей сформирована на основе правового, национально-политического и институционального направлений.*
Уровень 2: возможности	*Каждое из направлений разбивается на блок основных возможностей. Всего была определена **21** основная возможность.*
Уровень 3: субвозможности	*Каждая основная возможность разбивается далее и определяется как субвозможность. Всего было определено **77** субвозможностей.*

4.1.2 Политическое направление

Целью политического направления является анализ элементов политики, необходимых для разработки и реализации комплексного использования новых технологий, руководящих письменных программ для борьбы с терроризмом. Сложность решения вопросов, связанных с использованием новых технологий для террористических целей, требует наличия политики или политик на национальном уровне при поддержке специалистов высшего звена, отвечающих за разработку политики.

Такая политика важна для целей координации внутри государства, а также необходима ее интеграция с соответствующей политикой в области национальной безопасности, кибербезопасности и киберпреступности. Официальное сообщение и публикация политики имеет важное значение для межправительственных отношений, чтобы способствовать укреплению доверия и сотрудничества между соответствующими заинтересованными сторонами внутри государства и за его пределами.

4.1.3 Правовое направление

Правовое направление описывает законы и постановления, которые необходимы для обеспечения и поддержки ценностной цепочки контртеррористической деятельности правоохранительных органов. В связи с социальным и техническим развитием в киберпространстве законодателям необходимо разрабатывать инновационную государственную политику и правовые подходы для решения новых задач, обеспечивая при этом баланс между безопасностью и требованиями в области защиты прав человека. Данные правовые основы должны быть общедоступными для сохранения доверия общественности.

Цель модели — служить руководством к разработке законов и постановлений в соответствии с международным правом и с учетом глобального передового опыта. Она включает в себя общие правовые элементы, которые относятся к деятельности правоохранительных органов, защите прав человека, уголовному праву, процессуальному праву и полномочиям, а также к международному сотрудничеству.

4.1.4 Институциональное направление

Целью данного направления является описание организационных, оперативных и технических возможностей, которые необходимы для выполнения наших основных правоохранительных функций, являющихся частью ценностной цепочки контртеррористической деятельности правоохранительных органов по борьбе с терроризмом, особенно в том, что касается новых технологий. Оно охватывает структуру управления, процесс, процедуры, человеческий капитал и наращивание потенциала, финансовые ресурсы и технологические возможности.

4.2 Правовое направление

Правовое направление описывает законы и постановления, которые необходимы для обеспечения и поддержки ценностной цепочки контртеррористической деятельности правоохранительных органов.

Цель правового направления — служить руководством к разработке законов и постановлений в соответствии с международным правом и с учетом глобального передового опыта. Глобальный передовой опыт,

хотя и необязательно имеющий юридическую силу в рамках ООН, может выступать в качестве поддержки разработки внутренней политики и трансграничного сотрудничества. Глобальный передовой опыт показывает, как превратить абстрактные принципы в конкретные правовые меры. Кроме того, наличие одинаковых правовых норм, основанных на глобальном передовом опыте, в разных юрисдикциях уменьшает трансграничные правовые противоречия[26].

4.2.1 Верховенство права

Это общая основа системы, которая гарантирует ее разработку в рамках общих принципов международного законодательства с соблюдением принципа верховенства права.

Ном.	Субвозможности	Описание
1.1.1	**Верховенство права в соответствии с международными стандартами**	Осуществление функций и полномочий должно быть основано на четких положениях закона, в которых исчерпывающе перечисляются данные полномочия. Ни при каких обстоятельствах осуществление таких функций и полномочий не может нарушать императивных или не допускающих отступлений норм международного права; осуществление функций и полномочий подлежит независимому утверждению или контролю со стороны судебного или иного уполномоченного органа в соответствии с международными стандартами. Данное требование является основополагающим элементом модели возможностей и переносится на субвозможности модели.

4.2.2 Права человека

Любые меры, оказывающие воздействие на права человека или ограничивающие их, должны быть законными, необходимыми и соразмерными. Защита прав человека закреплена в системе посредством трех правовых условий. Первым из основных требований систем, базирующихся на принципе верховенства права, является защита прав человека, служащая минимальной основой для использования полномочий правоохранительных органов. Второе — специальная основа для защиты данных. Третье — материально-правовые и процессуальные элементы, которые входят в состав конкретных норм, например требование судебного одобрения.

Ном.	Субвозможности	Описание
1.2.1	**Приверженность/соответствие руководящим указаниям ООН относительно соблюдения прав человека**	Международные правовые документы о защите прав человека представляют собой общую основу для развития возможностей правоохранительных органов. Таким образом, данные правовые основы служат для дополнения конкретных механизмов защиты прав человека и поощрения прав человека при разработке новых правовых основ. Руководящие указания ООН в этой области используются в качестве исходной базы[27]. В соответствующих случаях эти требования переносятся на модель.
1.2.2	**Правовые полномочия по независимой проверке или возмещению ущерба в случае рисков или нарушений в области прав человека**	Для обеспечения защиты прав человека правовая основа должна включать правовые полномочия по проверке и возмещению ущерба, не связанные с правоохранительными органами.

26 См. Всемирный банк, с. 228.

27 Специальный докладчик ООН по борьбе с терроризмом и правам человека относительно ограничений прав и свобод, Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Мартина Шейнина (A/HRC/16/51), Practice XX, URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/178/98/PDF/G1017898.pdf?OpenElement.

1.2.3	**Применение общепринятых принципов защиты данных к сбору, обработке и использованию персональной информации правоохранительными органами**	Большая часть деятельности правоохранительных органов включает в себя сбор и обработку персональной информации с использованием вычислительных ресурсов, а также средств хранения и обработки. Такая деятельность необходима для эффективной работы правоохранительных органов, однако она создает риски злоупотреблений со стороны внутренних и внешних субъектов и вызывает потерю доверия заинтересованных сторон внутри государства и за его пределами. Любые меры, оказывающие воздействие на права человека или ограничивающие их, должны быть необходимыми и соразмерными. Применение международно признанной правовой основы к данной деятельности может снизить указанные риски и содействовать укреплению доверия общественности[28].
1.2.4	**Управление передовыми технологиями сбора и анализа данных**	Передовые технологии сбора и анализа данных, например системы охранного видеонаблюдения или возможности анализа больших массивов данных, позволяют повысить эффективность деятельности правоохранительных органов. Однако такая деятельность создает риски, связанные со сбором избыточной информации, ее точностью или объективностью, и поэтому должны быть проведены оценки рисков и приняты меры по смягчению рисков, в том числе для снижения риска дискриминации. В частности, сбор, обработка и сохранение должны базироваться на соответствующих критериях и не должны быть избыточными или дискриминационными.

4.2.3 Институциональные мандаты

Согласно принципу верховенства права полномочия исполнительных органов должны основываться на законодательстве, в котором определены цели и сфера действия этих полномочий. Это правовое требование применяется и к учреждениям, участвующим в ценностной цепочке контртеррористической деятельности, и к действиям, которые они могут предпринимать. Его дополняют следующие разделы, в которых описывается правовая основа деятельности правоохранительных органов в рамках ценностной цепочки контртеррористической деятельности.

Решение вопросов, связанных с террористической деятельностью с использованием новых технологий, какой, например, является кибератака террористов, в которую могут быть вовлечены агентство кибербезопасности или группа реагирования на инциденты в сфере компьютерной безопасности (CSIRT), правоохранительные органы и организации по обеспечению национальной безопасности, может представлять собой сложность для институциональных мандатов. В связи с этим подчеркивается важность дополнения правового институционального мандата политическими мандатами и наличия координации между учреждениями.

Ном.	Субвозможности	Описание
1.3.1	**Определение контртеррористических ведущих учреждений**	Задача по борьбе с терроризмом должна четко основываться на законе и включать противодействие использованию новых технологий в террористических целях. Данный элемент системы предназначен для обеспечения ясности относительно соответствующих функций, полномочий и необходимых ресурсов в контртеррористической ценностной цепочке, а также сосредоточен на необходимости уделять надлежащее внимание риску, связанному с использованием новых технологий. Он также служит для четкого определения организаций, которые могут применять контртеррористические меры, и тем самым способствует усилению подотчетности и снижению рисков для прав человека в процессе применения этих мер.

28 К примерам таких правовых основ относятся Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Серия договоров Совета Европы № 108), Директива (ЕС) 2016/680 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования уголовных преступлений, ведения розыскных или судебных действий или исполнения уголовных наказаний, а также Декларация ОЭСР о доступе правительства к персональным данным, хранящимся в частных компаниях, URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487. Преимущество декларации ОЭСР с практической точки зрения состоит в том, что она является документом высокого уровня, но при этом адаптирована для использования правоохранительными органами и была принята юрисдикциями, имеющими различные правовые основы в отношении конфиденциальности и защиты данных, например США, ЕС и странами АТЭС. См. также Kenneth Propp, Gentlemen's Rules for Reading Each Other's Mail: The New OECD Principles on Government Access to Personal Data Held by Private Sector Entities («Правила джентльменов о чтении почты друг друга: новые принципы ОЭСР о доступе правительства к персональным данным, хранящимся в частных компаниях»), Lawfare, 10.01.2023, URL: https://www.lawfareblog.com/gentlemens-rules-reading-each-others-mail-new-oecd-principles-government-access-personal-data-held

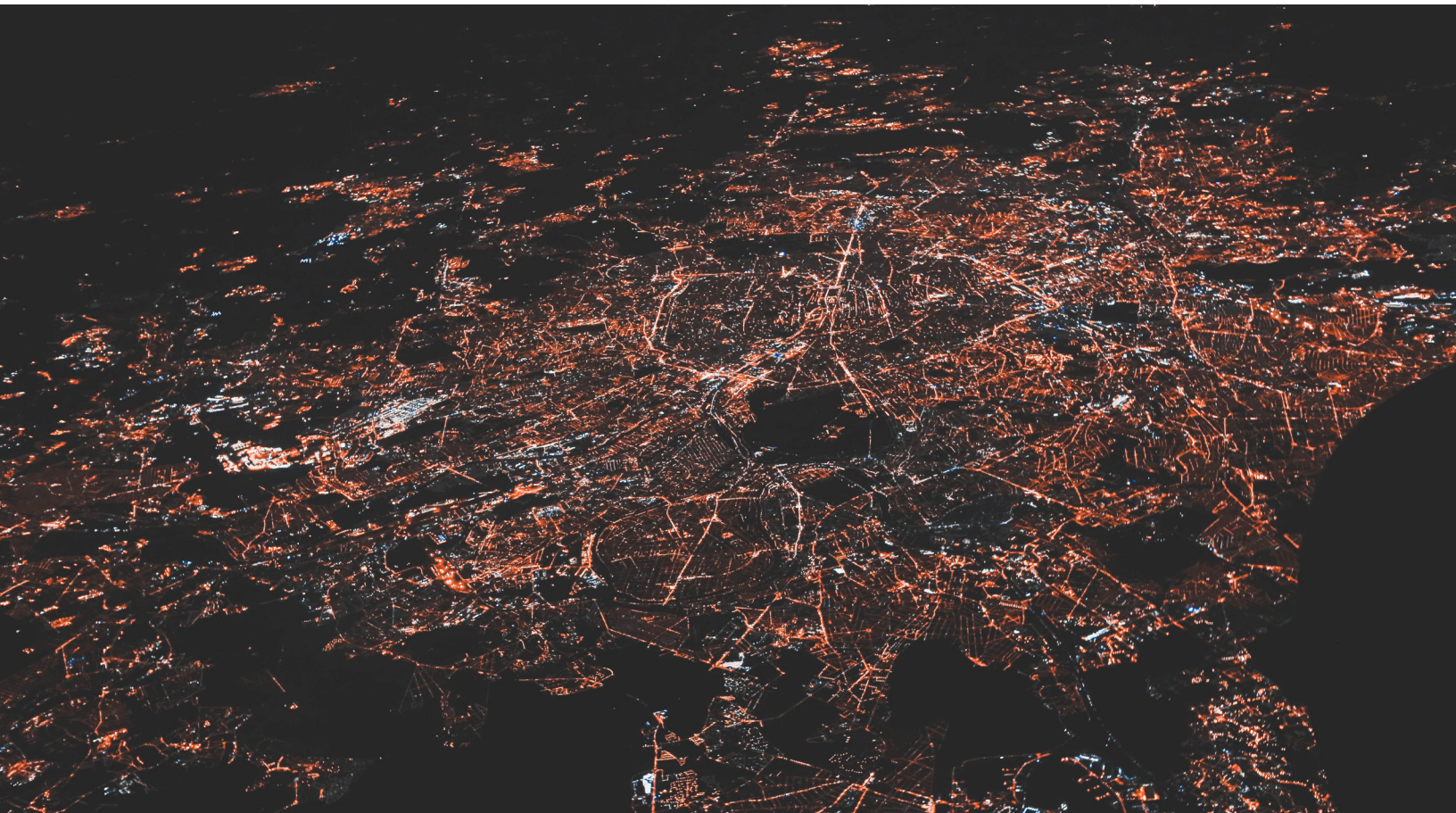
1.3.2	**Определение контртеррористических вспомогательных учреждений**	Закон или основанная на законе политика описывает функции вспомогательных организаций, которым могут не быть поручены контртеррористические операции, но которые служат опорой для ценностной цепочки контртеррористической деятельности.
1.3.3	**Определение механизмов координации (взаимодействий)**	Закон или основанная на законе политика описывает, как контртеррористические организации (когда их несколько) и другие организации согласовывают свою деятельность в рамках ценностной цепочки контртеррористической деятельности. Это особенно важно для сценариев рисков, связанных с новыми технологиями, которые требуют всеобъемлющего контртеррористического реагирования.

4.2.4 Материальное уголовное право

Уголовное право определяет запрещенную деятельность и служит основой для уголовного правосудия. Оно описывает деятельность, которой должны заниматься правоохранительные органы, реализуя свои оперативные полномочия. Следовательно, чтобы обеспечить возможность судебного преследования, материальное уголовное право должно охватывать преступные деяния, связанные с использованием новых технологий в террористических целях.

Определение уголовного преступления должно быть точным и конкретизированным, чтобы предотвратить избыточное судебное преследование или злоупотребление полномочиями правоохранительных органов. Например, в определении, приведенном в резолюции 1566 Совета Безопасности, преступные действия связываются с насилием в отношении людей или угрозами такого насилия, как и в определении, предложенном Специальным докладчиком ООН по борьбе с терроризмом и правам человека.

Следует уточнить, что в целом преступления, которые относятся к террористической деятельности, могут также относиться к такой деятельности в Интернете и не требуют рассмотрения в качестве особых видов или новых преступлений. С точки зрения принципа верховного права рекомендуется иметь четко определенные преступления, которые связаны непосредственно с использованием новых технологий, особенно в условиях конфиденциальности. Наличие особых преступлений может служить руководством для деятельности правоохранительных органов и органов уголовного правосудия благодаря внесению ясности в отношении области охвата запрещенной деятельности. При конструировании составов особых преступлений следует руководствоваться принципом технологической нейтральности, чтобы они были применимы к новым видам технологий.



Поскольку имеющие обязательную силу международные документы в данной области находятся все еще в процессе разработки, общие подходы и международные правовые основы могут служить мощным практическим инструментом. С точки зрения разработки внутренней политики данные основы отражают опыт, полученный благодаря проблемам, связанным с разработкой и реализацией, о которых говорилось выше. С точки зрения международного сотрудничества они могут способствовать трансграничному сотрудничеству по принципу «снизу вверх». Наличие общих подходов снижает потребность государств-членов в оценке правовых основ, использующихся в той или иной стране, и создании уникальных связующих нитей между внутренними правовыми основами.

Ном.	Субвозможности	Описание
1.4.1	**Террористические преступления**	Террористические акты должны быть запрещены уголовным правом. Определение таких актов содержится в резолюции 1566 Совета Безопасности[29]. Данное определение было доработано Специальным докладчиком по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом[30]. Уголовное право должно применяться к преступлениям, связанным с использованием компьютеров, которые умышленно совершены террористической группой в террористических целях. К указанной запрещенной деятельности может относиться кибератака на критически важную инфраструктуру или разработку вируса-вымогателя. Использование Интернета и социальных сетей для подстрекательства к терроризму или распространения незаконного террористического контента также должно быть запрещено[31]. Составы преступлений должны иметь узкий охват, чтобы они не ограничивали разрешенные законом высказывания, включая политические выступления. Хотя данные действия могут быть незаконными с точки зрения контртеррористических санкций или киберпреступности, конкретизация преступлений позволяет адаптировать их к данному контексту и способствует исключению двусмысленного толкования как на национальном, так и международном уровнях. Таким образом, террористические преступления должны включать все террористические преступления с использованием новых технологий.

29 Резолюция 1566 (2004), принятая Советом Безопасности ООН на его 5053-м заседании 8 октября 2004 года, S/RES/1566 (2004), URL: https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1566(2004)&Language=E&DeviceType=Desktop&LangRequested=False

30 Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом, 2010, A/HRC/16/51, URL: https://undocs.org/Home/Mobile?FinalSymbol=a%2Fhrc%2F16%2F51&Language=E&DeviceType=Desktop&LangRequested=False

31 В резолюции 1624 Совета Безопасности ООН содержится призыв к государствам ввести законы, запрещающие подстрекательство к терроризму, однако не приводится определение подстрекательства. Специальный докладчик ООН по борьбе с терроризмом и правам человека предложил следующее определение: это преступление заключается в умышленном и противозаконном распространении или направлении иным образом обращения к общественности с целью подстрекательства к совершению террористического преступления, если такое поведение, являющееся или не являющееся прямой пропагандой террористических преступлений, создает угрозу того, что такое преступление или преступления могут быть совершены. Регламент ЕС 2021/784 определяет террористический контент следующим образом: «1) побуждает кого-либо к совершению террористических преступлений или содействию им или к участию в деятельности террористической группировки; (2) подстрекает к осуществлению террористических преступлений или пропагандирует их; и (3) дает инструкцию по проведению атак». Регламент 2021/784 Европейского парламента и Совета о борьбе с распространением террористического контента в Интернете, статья 2 (7): Террористический контент…: «(a) подстрекает к совершению какого-либо из преступлений, о которых говорится в пунктах (a)–(i) статьи 3 (1) Директивы ЕС 2017/541, при этом такой материал прямо или косвенно, например путем прославления террористических актов, пропагандирует совершение террористических преступлений, тем самым создавая опасность совершения одного или нескольких таких преступлений; (b) побуждает лицо или группу лиц к совершению одного из преступлений, о которых говорится в пунктах (a)–(i) статьи 3 (1) Директивы ЕС 2017/541, или содействию ему; (c) побуждает лицо или группу лиц к участию в деятельности террористической группировки в значении пункта (b) статьи 4 Директивы ЕС 2017/541; (d) дает инструкции о создании или использовании взрывчатых веществ, огнестрельного или иного оружия, а также вредных или опасных веществ, или о иных конкретных методах или способах для целей совершения или содействия совершению одного из террористических преступлений, о которых говорится в пунктах (a)–(i) статьи 3 (1) Директивы ЕС 2017/541», URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32021R0784

1.4.2	**Киберпреступность: компьютеры**	Уголовные преступления, связанные с использованием компьютера, препятствуют деятельности, целью которой является обеспечение конфиденциальности, целостности и доступности компьютеров, сетей и хранимых в них данных[32]. Указанные преступления служат основой для деятельности правоохранительных органов, направленной против злоумышленной киберактивности. Они обеспечивают нормативную основу для противодействия злоумышленной террористической кибердеятельности. Одобренные (хотя и не общепринятые) международные правовые основы в сфере киберпреступности служат надежным справочным материалом для разработки проектов законов, а также содержат практические сведения об их применении. Они также служат основой для трансграничного сотрудничества и их применения всеми сторонами. Общая правовая основа по киберпреступности также предусматривает предотвращение террористической кибердеятельности. Это связано с тем, что преступная и террористическая деятельность часто пересекаются. Отличить преступную деятельность, связанную с компьютерами, от террористической деятельности может быть сложно.
1.4.3	**Дополнительные виды ответственности/ соучастие в преступлении**	Материальное уголовное право также включает принципы, которые применяются к субъектам, осуществляющим незаконную деятельность не полностью, а частично. К таким дополнительным преступлениям относится «покушение» на осуществление преступной деятельности, а также пособничество или содействие в совершении преступлений[33]. В целом ответственность за дополнительное преступление предполагает необходимость доказывания того, что преступление было совершено главным субъектом, а вспомогательная деятельность — вспомогательным субъектом.

4.2.5 Административное и уголовное процессуальное право

Административное и уголовное процессуальное право определяет пороговые значения, условия и меры защиты, которые применяются к оперативной деятельности правоохранительных органов. Таким образом, оно служит как для обеспечения деятельности правоохранительных органов, так и снижения возможных рисков для основных прав. Процессуальное право позволяет реализовать различные оперативные возможности. Оно также служит основой для трансграничного сотрудничества правоохранительных органов благодаря обеспечению возможности сотрудничества за пределами границ государств в ценностной цепочке контртеррористической деятельности. Оно служит основой для уголовного расследования правонарушений, указанных в разделе 2.1, иных уголовных преступлений, совершенных с помощью новых технологий, а также сбора в электронной форме доказательств совершения уголовного преступления.

Ном.	Субвозможности	Описание
1.5.1	**Общие полномочия правоохранительных органов**	Это основные полномочия, которые позволяют правоохранительным органам осуществлять деятельность в рамках ценностной цепочки правоохранительной деятельности. К ним относятся сбор информации, вызов свидетелей, обыск и арест имущества, запрос о представлении информации или вещи, допрос и задержание для допроса.

32 Согласно определению в Конвенции № 185 Совета Европы компьютерное преступление включает следующие категории: 1) Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем: неправомерный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы и противозаконное использование устройств; 2) Преступления, связанные с использованием компьютерных средств: подлог с использованием компьютерных технологий, мошенничество с использованием компьютерных технологий; 3) Преступления, связанные с контентом: детская порнография; 4) Преступления, связанные с нарушением авторского права и смежных прав; и 5) Дополнительные виды ответственности и санкции: покушение, пособничество или подстрекательство к совершению преступления, корпоративная ответственность.

33 См. Конвенцию № 185, подраздел 5, и пояснительное примечание, раздел 118.

1.5.2	**Полномочия правоохранительных органов, связанные с новыми технологиями**	Это основные полномочия, касающиеся сбора цифровых доказательств, которые являются особыми из-за их источников, переменчивого характера и риска манипуляций. К данным полномочиям относятся: оперативное сохранение конкретных компьютерных данных, включая данные о трафике, ускоренное сохранение и частичное раскрытие данных о трафике, распоряжения о представлении цифровых доказательств, поиск цифровых доказательств, сбор данных о трафике и контенте в режиме реального времени.
1.5.3	**Расширенные полномочия правоохранительных органов, связанные с новыми технологиями**	Эти полномочия предназначены для разработки сценариев угроз, в которых новые технологии используются злоумышленно. Они могут применяться в качестве толкования существующих процессуальных полномочий. При наличии возможности рекомендуется отдельно определить конкретные правовые полномочия в целях укрепления принципа верховенства права, обеспечения ясности и законодательного надзора[34].
1.5.4	**Уникальные контртеррористические полномочия**	Уникальная угроза терроризма привела к возникновению уникальных возможностей, целью которых является усиление традиционной деятельности правоохранительных органов по борьбе с преступностью. К ним относится следующее: 1. Включение в список террористических субъектов. 2. Предъявление скрытых доказательств с защитой конфиденциальности. 3. Защита агентурных источников. 4. Оперативные возможности по применению особых методов расследования.
1.5.5	**Уникальная административная поддержка**	Чтобы справиться со сценариями рисков, связанных с новыми технологиями, которые быстро развиваются, правоохранительным органам может потребоваться оперативно дополнить свои возможности путем закупки новых услуг и продуктов. На правоохранительные органы распространяется действие административных правил закупок и заключения договоров, которые могут быть непригодны для таких сценариев. Следовательно, необходимо обеспечить наличие системы уникальной административной поддержки, которая учитывала бы юридические и финансовые обязательства правоохранительных органов как государственных организаций, но при этом позволяла бы заключать договоры в оперативном порядке.

4.2.6 Юрисдикция и сотрудничество

Юрисдикция — это правовое понятие, описывающее связь между юридической властью государства и географической территорией[35]. Учитывая трансграничный характер использования новых технологий в террористических целях, важно понять и определить то, каким образом правоохранительные органы могут выполнять свою работу в случае осуществления злоумышленной деятельности за пределами государства. Следовательно, действие юрисдикции распространяется на преступника, затрагиваемый целевой объект или на необходимые доказательства. В случае распространения юрисдикции за пределы физических границ она должна соответствовать признанным международным стандартам[36]. Когда деятельность государства невозможна за пределами физических границ, ему необходима надлежащая правовая база, позволяющая сотрудничать с соответствующими государствами.

34 Такие полномочия могут включать: возможность осуществления операций в дарквебе; удаленный доступ к компьютеру или другому устройству и сбор информации; удаленный и скрытный доступ к компьютеру или другому устройству и сбор информации; пресечение злонамеренного использования инфраструктур и веб-сайтов с целью создания риска или ущерба, связанного с компьютером; пресечение распространения явно злонамеренных выступлений террористической направленности, например, подстрекательств и вербовок, через веб-сайты и платформы с помощью сотрудничества с субъектами частного сектора; и возможность ареста криптовалют.

35 Всемирный банк, с. 121—122: по сути, считается, что юрисдикция государства состоит из трех различных видов полномочий: законодательные полномочия, то есть власть, относящаяся к полномочиям устанавливать законы; судебные полномочия, то есть власть, относящаяся к полномочиям расследовать и разрешать споры; и исполнительные полномочия, то есть власть, относящаяся к полномочиям принуждать или наказывать в соответствии с законодательными полномочиями и после применения судебных полномочий.

36 Например, см. статью 32 Конвенции о киберпреступности Совета Европы: Статья 32. Трансграничный доступ к хранимым компьютерным данным с соответствующего согласия или к общедоступным данным: Сторона может без согласия другой Стороны: *a*) получать доступ к публичным (из открытых источников) компьютерным данным независимо от их географического местоположения; или *b*) получать через компьютерную систему на своей территории доступ к хранимым на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему.

Ном.	Субвозможности	Описание
1.6.1	**Четкая юрисдикционная правовая политика**	Политика в отношении юрисдикционной сферы онлайн-деятельности в рамках международной передовой практики является важным руководством для деятельности правоохранительных органов. Она служит основой для деятельности, которая входит в состав контртеррористической ценностной цепочки. Она также определяет роль трансграничных соглашений об оказании помощи. Учитывая постоянное развитие данной сферы, не все из указанных элементов должны базироваться на законодательстве, их можно изложить в обязательной политике.
1.6.2	**Официальные юридические соглашения для осуществления трансграничного сотрудничества**	Двусторонние и многосторонние юридические соглашения служат прочной правовой основой для трансграничного сотрудничества правоохранительных органов. Такие соглашения, например Конвенция Совета Европы о киберпреступности, обеспечивают возможность трансграничной помощи, в том числе взаимной правовой помощи, сотрудничества правоохранительных органов и совместных расследований.
1.6.3	**Правовая экосистема, обеспечивающая неофициальное сотрудничество**	Некоторая деятельность, касающаяся трансграничного сотрудничества между правоохранительными органами, зависит от добровольных не имеющих обязательной силы соглашений. Такие соглашения, хотя и неофициальные, могут быть полезны в качестве дополнения других мер в трансграничном контексте. Для обеспечения возможности такого сотрудничества необходимо создать условия для правового сотрудничества, а правовая экосистема не должна ему препятствовать. Так, поддержкой такого сотрудничества может стать наличие четкой правовой основы в области защиты данных, поскольку в ней рассматриваются вопросы прав человека.

4.3 Политическое направление национальной контртеррористической деятельности

Политическое направление включает в себя элементы, необходимые для разработки и реализации комплексной руководящей письменной программы для борьбы с терроризмом[37]. Национальная политика важна для создания общепринятого общегосударственного подхода к террористическим угрозам с четким мандатом на высоком уровне. Комплексная политика важна для целей координации внутри государства, а также необходима ее интеграция с соответствующей политикой в области национальной безопасности, кибербезопасности и киберпреступности[38]. 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 укрепления элементов системы возможностей.

Национальная политика также необходима для сотрудничества с неправительственными заинтересованными сторонами и организациями в рамках контртеррористической ценностной цепочки. Следовательно,

37 Поскольку способы формулирования и реализации политики в этой области правительствами могут различаться, темы, включенные в политическое направление, могут содержаться в нескольких внутренних документах (которые являются «письменными имеющими обязательную силу директивами») при условии, что эти документы имеют соответствующую связь и необходимую координацию.

38 Всемирный банк, с. 46: «Как и любая другая программа по наращиванию потенциала, требующая технического сотрудничества, программы по наращиванию потенциала в сфере киберпреступности внедряются с целью поддержки процессов изменений. Для того чтобы эти процессы, а также их цели и ожидаемые результаты начали действовать, они должны быть не только определены, но и „принадлежать" учреждению, получающему поддержку. Результатом этого является создание общеорганизационной „культуры", примером для которой служит руководство сверху и которая реализуется на всех уровнях. Без приверженности высшего руководства четко определенному процессу изменений будет трудно внедрить более серьезные институциональные вопросы, связанные с культурой». Всемирный банк, с. 228: «Во всех странах существует потребность в том, чтобы политики и законодатели понимали проблемы киберпреступности и их многонациональную направленность. В исследовании ЮНКТАД с участием представителей правительств 48 развивающихся стран подчеркивается необходимость повышения осведомленности и знаний среди представителей законодательных и судебных органов в отношении законодательства о киберпреступности и правоприменительной политики. Более половины представителей сообщили о сложностях в понимании правовых вопросов, связанных с киберпреступностью. Около 40 процентов также отметили, что из-за отсутствия понимания у парламентариев может затягиваться принятие соответствующих законов. Без осведомленности и знаний сложно разработать грамотную политику и законы, а также обеспечить их соблюдение».

политика должна поддерживать координацию, коммуникацию и сотрудничество с частным сектором, общественностью и международными партнерами. Официальное сообщение и публикация основных принципов политики может способствовать укреплению доверия и сотрудничества между соответствующими заинтересованными сторонами внутри государства и за его пределами[39].

Как указано выше, политическое направление сосредоточено на контртеррористическом потенциале использования новых технологий и не ставит своей целью охватить всю национальную контртеррористическую стратегию.

4.3.1 Разработка политики и ее реализация

В решении проблем, связанных с терроризмом, разработка национальной политики и ее реализация является чрезвычайно важной возможностью для правительств. Она включает в себя создание политики, в которой определяются оперативные возможности и результаты обеспечения безопасности, ее внедрение, а также ее реализацию. Разработка национальной политики и ее реализация требуют сотрудничества и взаимодействия с заинтересованными правительственными структурами, организациями гражданского общества и частным сектором, чтобы обеспечить отражение в ней различных потребностей и взглядов населения. Для разработки эффективной национальной политики и ее реализации требуются прочная институциональная основа, квалифицированные кадры, а также надежные процессы и процедуры, которые обеспечивали бы ее доказательность, эффективность и подотчетность.

Национальная контртеррористическая стратегия государства-члена должна быть приведена в соответствие с контртеррористической стратегией ООН. Стратегия ООН является общей основой для поощрения принятия мер по борьбе с терроризмом при соблюдении прав человека. Она служит руководством по развитию возможностей и наращиванию потенциала. В трансграничном контексте она способствует обеспечению совместимости и позволяет улучшить сотрудничество. Национальная контртеррористическая стратегия государства-члена должна быть согласована с соответствующими региональными стратегиями. Благодаря совместимости с региональными стратегиями уменьшаются институциональные и политические различия и обеспечиваются условия для возможностей быстрого реагирования и более эффективного трансграничного сотрудничества.

Ном.	Субвозможности	Описание
2.1.1	**Управление**	Для разработки национальной контртеррористической стратегии и надзора за ее развертыванием в политике должен быть определен орган высокого уровня, подотчетный высшему руководству. Для обеспечения поддержки органу, которому поручены разработка и надзор, в выполнении целей и задач, в политике должны содержаться требования к соответствующим государственным учреждениям об участии в данном процессе, а также о предоставлении запрашиваемой информации и отчетов о деятельности. Политикой должны устанавливаться команды по управлению политикой и ее реализации, а также должен быть разработан документ «Политика в отношении политики», который будет служить руководством по разработке и применению потенциала управления политикой со стандартными формами и процессами.
2.1.2	**Научная деятельность и исследования**	Предоставление разработчикам политики основанного на доказательствах понимания, контекста, вызовов и возможностей использования новых технологий террористами в качестве основы для выбора курса политики.
2.1.3	**Выбор курса политики и координация**	Выработкой направлений политики с использованием единого подхода, национальных ресурсов и средств должно заниматься государство.
2.1.4	**Стратегическая согласованность**	Политика, касающаяся использования новых технологий в террористических целях, пересекается с национальной политикой в области уголовного правосудия, национальной безопасности и кибербезопасности. Каждый из этих документов может иметь общие цели и меры и может охватывать разные сценарии рисков. Следовательно, для разработки политики необходимо использовать единый подход. Приведение данных документов в соответствие с требованиями может помочь унифицировать меры, повысить эффективность и снизить возможные конфликты, связанные с оперативной деятельностью.

39 К международным заинтересованным сторонам относятся другие государства, международные организации и международные участники отрасли ИКТ. Они также включают более эффективное согласование донорских взносов и партнерского сотрудничества. (Всемирный банк, с. 48–49).

4.3.2 Управление реализацией политики

Реализация национальной контртеррористической политики подразумевает эффективное управление процессом реализации политики и стратегий, направленных на предотвращение и выявление угроз, а также на их реагирование. Эффективная реализация национальной контртеррористической политики также предусматривает координацию и сотрудничество между различными государственными структурами и с международными партнерами. Для обеспечения эффективной реализации национальной контртеррористической политики правительства должны ставить четкие цели, выделять достаточные ресурсы, а также регулярно оценивать и корректировать свою политику и стратегии в зависимости от изменения условий в отношении угроз.

Ном.	Субвозможности	Описание
2.2.1	**Развитие возможностей**	Эффективное определение приоритетности и развитие необходимых возможностей на национальном уровне по противодействию использованию новых технологий в террористических целях.
2.2.2	**Вмешательства в отношении угроз**	Эффективное определение приоритетности вмешательств (предотвращение, пресечение, недопущение, защита и судебное преследование) в рамках противодействия использованию новых технологий в террористических целях соответствует национальной контртеррористической политике, стратегии и национальному плану действий.
2.2.3	**Распределение институциональных функций и сфер ответственности**	В политике должны быть четко определены институциональные мандаты и механизмы межведомственного сотрудничества с четким распределением функций и сфер ответственности в отношении контртеррористических усилий по противодействию использованию новых технологий в террористических целях.
2.2.4	**Управление ресурсами**	Определение приоритетности и выделение необходимых ресурсов для обеспечения выполнения целей и задач политики.
2.2.5	**Управление сотрудничеством**	Контртеррористические организации (когда их несколько) и другие организации согласовывают свою деятельность в рамках ценностной цепочки контртеррористической деятельности. Это важно для обеспечения всеобъемлющего контртеррористического реагирования. С его помощью можно установить неохваченные участки, которые могут быть причиной пробелов в ценностной цепочке контртеррористической деятельности.

4.3.3 Управление эффективностью политики

Управление эффективностью политики предполагает применение системного и структурированного подхода к контролю и оценке реализации политики, чтобы определять ее эффективность и принимать обоснованные решения о будущих направлениях политики. Для управления эффективностью национальной политики необходимы установление четких показателей и параметров эффективности, сбор и анализ данных, а также механизмы отчетности для информирования ключевых заинтересованных сторон об эффективности политики.

Ном.	Субвозможности	Описание
2.3.1	**Критерии эффективности политики**	Заданные показатели эффективности политики определяют желаемые цели и результаты, которые необходимо достигнуть.
2.3.2	**Оценка влияния политики**	Процесс регулярной оценки эффективности и влияния национальной политики, реализуемой для противодействия применению новых технологий в террористических целях.
2.3.3	**Управление пересмотром политики**	Процесс регулярного пересмотра выбранного курса политики и ее эффективности, а также обновления курса политики для достижения желаемых результатов.

4.3.4 Управление информационным обеспечением политики

Управление информационным обеспечением политики включает разработку передачи четких и кратких сообщений, коммуникационных каналов и стратегий взаимодействия, чтобы способствовать повышению понимания и прозрачности государственной политики, а также доверия к ней. Благодаря наращиванию потенциала в управлении информационным обеспечением национальной политики правительства могут повысить влияние своей политики, способствовать укреплению поддержки общества и выстроить более эффективные и доверительные отношения с гражданами и заинтересованными лицами.

Ном.	Субвозможности	Описание
2.4.1	**Стратегическая коммуникация**	Информирование о целях и мерах политики имеет важное значение для укрепления доверия и сотрудничества с организациями частного сектора, гражданами и международными партнерами. Обеспечение прозрачности и возможности проведения общественных обсуждений позволяет снизить опасения по поводу использования полномочий, касающихся борьбы с терроризмом.

4.3.5 Сотрудничество государственного и частного секторов

Решение вопросов, связанных с новыми технологиями, требует сотрудничества с компаниями частного сектора. Уникальные характеристики новых технологий и их использование требуют сотрудничества и партнерских отношений для достижения эффективной деятельности правоохранительных органов.

Ном.	Субвозможности	Описание
2.5.1	**Партнерство государственного и частного секторов**	Партнерство государственного и частного секторов предусматривает сотрудничество с поставщиками в области ИКТ для лучшего понимания технических особенностей, а также с поставщиками услуг, которые могут помочь обнаружить или пресечь злоумышленную деятельность. В некоторых случаях устойчивость частного сектора к злоупотреблению новыми технологиями является наиболее эффективным методом предотвращения конкретной угрозы. Особенно важным является сотрудничество с международными компаниями, к которым формальные правовые основы могут применяться по-разному. Оно должно быть важной частью управления политикой на высоком уровне.
2.5.2	**Консультации заинтересованных сторон**	Консультации с заинтересованными сторонами способствуют достижению некоторых важных целей политики. Они позволяют доводить до сведения разработчиков политики информацию и опыт частного сектора и гражданского общества. Это особенно важно в контексте новых технологий, где частный сектор занимает главенствующую роль в характеристиках цифровой экосистемы. Консультации с заинтересованными сторонами также позволяют совместно обсуждать проблемы, касающиеся политики, и различные меры по их решению. Благодаря им неправительственные заинтересованные стороны могут понять точку зрения правительства. Участие заинтересованных сторон может повысить легитимность процесса реализации политики и усилить доверие общественности.

4.3.6 Национальные контртеррористические элементы

Чтобы должным образом уменьшить террористические угрозы, в национальной политике должно быть уделено внимание национальной классификации инцидентов и развитию международного сотрудничества. С соответствующими организациями необходимо разработать комплексный план по снижению рисков. Классификация инцидентов важна для управления национальными инцидентами, спровоцированными новыми технологиями (например, киберинцидентами), на национальном уровне и для международного взаимодействия. Стандартный подход к категоризации и приоритизации инцидентов важен для сортировки, определения приоритетности и координации мер реагирования.

Национальная классификация инцидентов имеет важное значение для подготовки к террористическому акту, который может перерасти в событие национального масштаба, а также устранения его последствий. Учитывая новые сценарии угроз использования новых технологий в террористических целях, такие как вирусы-вымогатели, которые затрагивают инфраструктуру, предоставляющую основные услуги, для смягчения и ликвидации последствий может потребоваться деятельность правоохранительных и других органов. Составление перечня и классификация данных событий служит основой для подготовки, разработки мер по смягчению последствий и координации действий на межведомственном уровне[40].

40 В контексте киберинцидентов см. ОБСЕ, «Классификация киберинцидентов: доклад о новой практике в регионе ОБСЕ, 2022 г., URL: https://www.osce.org/secretariat/530293. Выводы, полученные из отчета ОБСЕ, актуальны не только для событий, связанных с киберсферой.

Международное сотрудничество необходимо для поддержки трансграничной контртеррористической деятельности правоохранительных органов. С террористической угрозой необходимо бороться в принципе, однако в сценариях угроз, связанных с использованием новых технологий, это еще важнее, учитывая глобальный характер технологий. Контртеррористическая деятельность правоохранительных органов требует прочных механизмов для обеспечения трансграничного сотрудничества, поскольку террористическая деятельность осуществляется во всем мире. Контртеррористическая деятельность в области новых технологий опирается на такие возможности, что обусловлено трансграничным характером инфраструктуры ИКТ.

Ном.	Субвозможности	Описание
2.6.1	**Национальная классификация инцидентов**	Для обеспечения поддержки национальной политики необходимо поручить общегосударственному органу разработать матрицу классификации инцидентов на национальном уровне. Создание всеобъемлющей национальной матрицы инцидентов подразумевает сбор информации у соответствующих организаций, а также проведение дискуссий.
2.6.2	**Международное сотрудничество**	Общегосударственный орган, которому поручена разработка национальной политики, должен следить за развитием и продвижением необходимых механизмов сотрудничества. В его обязанности входит определение целей международного сотрудничества, внутриправительственной координации, правовых и методических основ, механизмов оперативного сотрудничества и контактных лиц.

4.4 Институциональное направление

Целью данного направления является описание организационных, оперативных и технических возможностей, которые необходимы для выполнения наших основных правоохранительных функций, описанных в разделе 2.1. Оно охватывает управление, процесс, процедуры, человеческий капитал, наращивание потенциала, финансовые ресурсы и технологические возможности.

4.4.1 Стратегическое планирование и эффективность

Общая цель стратегического планирования состоит в обеспечении возможности для организации эффективно ориентироваться в быстро меняющихся условиях, а также реагировать на новые вызовы и возможности и адаптироваться к ним. При наличии четкого понимания своей миссии и целей и благодаря разработке эффективных стратегий по достижению этих целей организация может обеспечить себе долгосрочный успех и устойчивость. Стратегическое планирование направлено на согласование целей, приоритетов, ресурсов и действий правоохранительных органов, чтобы они могли выполнять поставленные перед ними задачи в соответствии с указаниями руководства, а также национальной политикой и стратегиями.

Управление эффективностью позволяет с помощью предоставляемых средств оценить успехи и достижения в отношении приоритетов, целей, задач и результатов, определенных в процессе стратегического планирования.

Ном.	Субвозможности	Описание
3.1.1	**Национальный план действий**	Национальный план действий должен переносить фокус внимания национальной политики на роли и сферы ответственности правоохранительных органов при реализации контртеррористического жизненного цикла. Он также поддерживает общегосударственный подход посредством разъяснения взаимодействий правоохранительных органов в рамках политики по борьбе с киберпреступностью и обеспечению кибербезопасности, а также с другими правительственными организациями, участвующими в жизненном цикле контртеррористической деятельности.
3.1.2	**Оперативный план и бюджет**	Оперативный план и бюджет служат для определения подробных организационных задач по операциям и возможностям. Специальный бюджет, выделенный на финансирование этих задач, помогает выполнить план и обеспечивает возможность управления эффективностью.
3.1.3	**Управление эффективностью**	Процесс мониторинга и оценки успехов в институциональном плане по достижению стратегических целей. Он включает разработку системы измерения и анализа ключевых показателей эффективности (КПЭ), согласованных со стратегическими целями организации.

4.4.2 Управление

Управление — это механизм подотчетности с эффективными процессами принятия решений, структурами и системами, направленный на достижение целей и выполнение правовых обязательств. Оно включает в себя разработку и реализацию политики, процедур, средств контроля и гарантий для обеспечения прозрачности, подотчетности и этичного поведения во всех операциях организации. Управленческий потенциал крайне необходим правоохранительным органам для управления рисками, выстраивания доверительных отношений с общественностью, обеспечения соблюдения нормативных требований и достижения устойчивых результатов.

Ном.	Субвозможности	Описание
3.2.1	**Структура управления**	Официально установленная иерархия подотчетности и ключевых полномочий по принятию решений для управления стратегическими решениями, в том числе сверху вниз и между структурными подразделениями. Специальные возможности использования новых технологий руководящим звеном («цифровая грамотность») для обеспечения поддержки надзорной деятельности.
3.2.2	**Управление рисками**	Процесс управления рисками предусматривает выявление, определение приоритетности, смягчение и управление институциональными стратегическими и операционными рисками.
3.2.3	**Соблюдение требований**	Означает комплекс мер политики, процедур и руководящих принципов, которые учреждение устанавливает для соблюдения действующих законов, постановлений и отраслевых стандартов.
3.2.4	**Оценка воздействия на права человека**	Выявление, оценка и смягчение потенциального воздействия на права человека институциональных операций, мероприятий, политики и действий, касающихся новых технологий и борьбы с терроризмом.
3.2.5	**Защита данных**	Правоохранительные органы осуществляют сбор и обработку информации, позволяющей установить личность, с учетом конкретных правовых принципов для предотвращения рисков для конфиденциальности. Эти принципы должны быть введены в действие с помощью специальной независимой внутренней системы, включающей профильных специалистов, политику и процедуры. (Обеспечение защиты персональной информации от несанкционированного доступа, использования, раскрытия или уничтожения. Это крайне важно для защиты неприкосновенности частной жизни, сохранения доверия и соблюдения нормативно-правовых требований.)

4.4.3 Управление выполнением задач и координация деятельности

Управление выполнением задач и координация деятельности, основанные на соответствующей информации, позволяют более эффективно осуществлять деятельность и сотрудничество правоохранительных органов с другими ведомствами.

Ном.	Субвозможности	Описание
3.3.1	**Сканирование горизонта**	Систематический процесс сбора и анализа информации из широкого круга источников для выявления новейших тенденций, рисков и возможностей новейших технологий и ее влияния на терроризм и возможности государств. Это прогностическая деятельность, которая позволяет предвидеть будущие проблемы и возможности и подготовиться к ним.
3.3.2	**Управление угрозами**	Системный процесс сбора и анализа информации из широкого круга источников для выявления возникающих угроз, классификации их по степени серьезности и определения приоритетности контртеррористических мер.
3.3.3	**Обмен информацией**	Для содействия сотрудничеству и координации правоохранительные органы должны иметь в своем распоряжении организационные, правовые и технические инструменты для обмена информацией, которые могут быть использованы для смягчения последствий использования новых технологий в террористических целях. Сюда входят соглашения и протоколы по обмену информацией, а также система классификации информации.

4.4.4 Партнерство и сотрудничество

Уникальные характеристики новых технологий и их использование требуют сотрудничества и партнерских отношений для достижения эффективной деятельности правоохранительных органов. К их числу относится сотрудничество с поставщиками в области ИКТ для лучшего понимания технических особенностей, а также с поставщиками услуг, которые могут помочь обнаружить или пресечь злоумышленную деятельность. В некоторых случаях содействие повышению устойчивости частного сектора к злонамеренному использованию новых технологий является наиболее эффективным методом предотвращения конкретной угрозы. Особенно важным является сотрудничество с международными компаниями, к которым формальные правовые основы могут применяться по-разному. Привлечение частного сектора с начального этапа разработки правовой основы может оказаться взаимовыгодным.

Ном.	Субвозможности	Описание
3.4.1	**Управление отношениями с государственными органами**	Правоохранительным органам необходимо координировать внутриправительственную деятельность на протяжении всего жизненного цикла контртеррористической деятельности. Для этого полезно создать один центральный внешний орган, поддерживающий внутриправительственное сотрудничество.
3.4.2	**Управление контртеррористической партнерской деятельностью**	Решение вопросов, связанных с новыми технологиями, требует сотрудничества с компаниями частного сектора. Для этого требуются знания и понимание действующих правовых основ и других аспектов, которые формируют такие отношения, включая общественное мнение и потенциальные бизнес-риски. Управление этой функцией должно осуществляться централизованно, чтобы способствовать управлению знаниями и распространению опыта политики, процедур и ожиданий частного сектора.
3.4.3	**Взаимодействие с общественностью/ сообществом**	Официальная политика и формализованный процесс согласования и разрешения обмена соответствующей информацией с общественностью, которая, помимо прочего, может включать информацию об угрозах, операциях, а также просветительскую информацию и т. д., с целью повышения доверия и репутации правоохранительных органов.
3.4.4	**Международное сотрудничество**	Официальная политика и формализованный процесс, а также специально назначенный персонал для обеспечения трансграничного сотрудничества. (Контртеррористическая деятельность правоохранительных органов требует прочных механизмов для обеспечения трансграничного сотрудничества, поскольку террористическая деятельность осуществляется во всем мире. Контртеррористическая деятельность в области новых технологий опирается на такие возможности, что обусловлено трансграничным характером инфраструктуры ИКТ.)

4.4.5 Управление оперативной деятельностью

Управление оперативной деятельностью касается политики и процедур, обеспечивающих реализацию ценностной цепочки контртеррористической деятельности. В рамках управления оперативной деятельностью должна быть предусмотрена возможность координировать стратегические контртеррористические усилия, а также циклы быстрого принятия решений, чтобы принимать ответные меры, ставить задачи и координировать деятельность правоохранительных органов в меняющихся обстоятельствах.

Ном.	Субвозможности	Описание
3.5.1	**Управление надзорной деятельностью**	Эффективный механизм управления и надзора за деятельностью правоохранительных органов, обеспечивающий соблюдение соответствующих законов и правил, а также эффективное выполнение возложенных на них задач. Он включает внутренние нормативные документы, процедуры и специальные вспомогательные службы, отвечающие за предоставление информации, распределение задач и координацию. Меры политики, процедуры и возможности должны быть направлены на обеспечение осведомленности руководства о текущей ситуации и операциях в долгосрочной, среднесрочной и краткосрочной перспективе.

3.5.2	**Управление сбором оперативной информации**	Разведка является неотъемлемой частью борьбы с террористическими угрозами и включает сбор информации, ее анализ и оценку, создание материалов с оперативной информацией и предоставление их соответствующим операторам, а также лицам, ответственным за планирование и принятие решений. Внедрение новых технологий требует новых видов сбора информации о новых инструментах и методах, но также позволяет использовать новые методы сбора, обработки и предоставления информации в жизненном цикле разведки. Разведывательный цикл можно описать как включающий «постановку задачи», «сбор», «оценку», «упорядочение», «анализ», «определение выводов» и «распространение». Учитывая глобальный характер инфраструктуры ИКТ и тот факт, что большая ее часть представляет собой рыночную экосистему в рамках частного сектора, разведывательная деятельность в значительной степени зависит от умения понимать технологические тенденции и сотрудничать с другими представителями государственного сектора, частным сектором и международными партнерами. При сборе оперативных данных и информации о злоумышленной кибердеятельности важно принимать во внимание новые режимы работы, новые компьютерные системы и инструменты и новые платежные сервисы.
3.5.3	**Управление расследованиями**	Формализованный процесс проведения всесторонних и эффективных расследований путем сбора информации и доказательств для оценки мер, которые необходимо предпринять. Для эффективной деятельности правоохранительных органов по проведению расследований требуется сочетание специальных навыков, профессиональной подготовки и технологий. Следователи должны обладать знаниями соответствующих законов и процедур, а также опытом в таких областях, как криминалистическая экспертиза, наблюдение и методы допроса. Они также должны иметь доступ к инструментам, например к оборудованию для анализа мест преступлений, базам данных уголовных дел и другой информации, а также к системам коммуникации, которые позволяют им работать с другими ведомствами и обмениваться информацией.
3.5.4	**Действия правоохранительных органов**	Соображения по поводу оперативной деятельности или сбора оперативной информации могут инициировать выбор действий по предупреждению или пресечению. Организация должна иметь в своем распоряжении возможности управления надзором, включающие внутренние документы, процедуры и специальные вспомогательные отделы, отвечающие за отчетность, постановку задач и координацию деятельности с другими отделами правоохранительных органов и другими гражданскими организациями. Меры политики, процедуры и возможности должны быть направлены на обеспечение осведомленности руководства о текущей ситуации и операциях в долгосрочной, среднесрочной и краткосрочной перспективе.
3.5.5	**Управление взаимодействием с органами уголовного правосудия**	Функционирование «уголовного правосудия» четко определено, и сотрудничество с прокуратурой, судами и другими соответствующими ведомствами является эффективным. Руководство регулярно осуществляет анализ данных взаимодействий и обеспечивает функционирование процесса в соответствии с ожиданиями.
3.5.6	**Реагирование на инциденты**	Решение вопросов, связанных с инцидентами, требует ключевых процессов и действий со стороны правоохранительных органов и других соответствующих инстанций. Планирование, подготовка, определение четких сфер ответственности и механизмов сотрудничества имеют важное значение при работе с инцидентами. Тестирование и урегулирование инцидентов повышают осведомленность и подготовленность. Эти аспекты особенно важны для событий, которые имеют национальное значение или требуют межведомственного сотрудничества для смягчения последствий инцидента.

4.4.6 Оперативная поддержка

Правоохранительным органам требуются надежная организационная инфраструктура и технические решения для поддержки различных операций, которые входят в состав жизненного цикла контртеррористической деятельности. Такая инфраструктура включает политику, кадры и технологии, которые необходимо интегрировать в управление операциями.

Ном.	Субвозможности	Описание
3.6.1	**Управление данными и информацией**	Возможность получать, сохранять данные и иметь к ним доступ с учетом производственной необходимости и в соответствии с правилами и требованиями в отношении конфиденциальности и хранения данных. Сюда относятся все данные, полученные, например из систем правоохранительных органов, от других организаций, из видео, датчиков или устройств, Интернета и социальных сетей, а также возможность соединить все источники данных в систему единого окна, чтобы предоставить доступ правоохранительным органам.
3.6.2	**Техническая поддержка**	Средства предоставления технических решений (включая технологии) для практической реализации и обеспечения правоохранительной деятельности в рамках разведки, расследований, операций и судебного преследования. Правоохранительным органам требуется надежная ИКТ-инфраструктура для поддержки оперативных или вспомогательных возможностей. Правоохранительные органы должны применять технологии для проведения операций, в том числе адаптировать гражданские технологии для целей правоохранительной деятельности. К ним относятся технологии обработки информации и коммуникаций. Они представляют собой особую важность в контексте использования новых технологий. Также сюда может входить поддержка лаборатории криминалистики, анализ цифровых данных и сбор информации из открытых источников.

4.4.7 Управление инновационной деятельностью

Чтоб эффективно осуществлять деятельность в условиях ограниченных ресурсов, правоохранительным органам необходимо внедрять новые технологии и методы работы, а также они должны быть готовы к злоумышленному использованию новых технологий. Для достижения указанной цели правоохранительным органам необходимо инвестировать в технологическое сканирование, а также развитие и обеспечение инноваций.

Ном.	Субвозможности	Описание
3.7.1	**Технологическое сканирование**	Проведение мониторинга и анализа новых технологий с целью выявления возможностей для осуществления инновационной деятельности. Оно включает в себя сбор и анализ данных о технических достижениях, новых продуктах, патентах, научных исследованиях, рыночных тенденциях и поставщиках технологий, чтобы выявлять, какие технологии могут нарушать деятельность или создавать новые возможности. В рамках инновационной деятельности сканирование технологий позволяет организациям опережать террористические угрозы благодаря выявлению новых технологий, которые могут улучшать возможности, повышать эффективность или снижать затраты. Оно также может помогать им выявлять потенциальные риски или проблемы, которые могут возникать в результате появления новых технологий, и подготовиться к ним заранее.
3.7.2	**Инновационное развитие и обеспечение**	Формализованный процесс, который способствуют формированию культуры инноваций и обслуживания, позволяющей определять приоритетные возможности и задачи, изучать потенциальные решения, определять осуществимость посредством пилотирования, разработки прототипа и запуска минимально жизнеспособного продукта, а также масштабировать успешные решения в процессе своей деятельности.
3.7.3	**Модель партнерства**	Определение подходящего внешнего партнерства, которое может позволить усилить инновационные возможности и средства для реализации инновационных проектов, позволяя учреждениям осуществлять оценку специализированных навыков, опыта и технологий быстро и в требуемом масштабе.
3.7.4	**Поддержка инновационной деятельности**	Предоставление необходимых ресурсов для поддержки и реализации инновационной деятельности, включающей стратегическое партнерство, механизм закупок, маркетинг и коммуникации, механизм финансирования, корпоративную культуру и инновационную инфраструктуру.

4.4.8 Обучение и развитие трудовых ресурсов

Человеческий капитал является неотъемлемой частью возможностей правоохранительных органов и требует внимания со стороны политики и руководства, чтобы принимать надлежащие меры в отношении новых технологий. Новые технологии создают дополнительные проблемы ввиду конкуренции с работодателями частного сектора в плане найма квалифицированных специалистов.

Кроме того, использование технологий для борьбы с терроризмом и противодействие использованию новых технологий в террористических целях требуют адаптации гражданских технологических знаний к контексту деятельности правоохранительных органов, например к работе в рамках правовых полномочий и цифровой криминалистики. Изменения технологического ландшафта также требуют в ходе процесса обучения адаптации существующих возможностей к новым сценариям.

Ном.	Субвозможности	Описание
3.8.1	**Расширение знаний**	Расширение базы знаний правоохранительных органов и ее обновление по мере необходимости позволяют обеспечить ясность относительно областей знаний, которые составляют основу и влияют на деятельность правоохранительных органов и особенно на развитие человеческого капитала и управление им. База знаний состоит из научных и отраслевых знаний, касающихся новых технологий, а также уникальных областей обеспечения правопорядка, таких как отправление правосудия или цифровая криминалистика. База знаний должна включать области, актуальные для всех сотрудников, а также более узкие области. Подготовка базы знаний позволяет обратить внимание на те области, в которых знания и обучение уже имеются, и на те, которые необходимо целенаправленно развивать. Она также позволяет оценить, какие функции должны выполняться государственными служащими, подрядчиками и сторонними поставщиками услугам.
3.8.2	**Требования к квалификации сотрудников**	Определение и установление требований к навыкам, знаниям и компетенциям в зависимости от должностных функций и обязанностей.
3.8.3	**Оценка потребностей в обучении**	Оценка сотрудников на предмет соответствия требованиям к квалификации, чтобы определить существующие пробелы или области совершенствования в требуемых навыках, знаниях и компетенциях. Оценка потребностей в обучении ляжет в основу требований к учебной подготовке и профессиональному развитию.
3.8.4	**Модель обеспечения профессиональной подготовки**	Модель обеспечения профессиональной подготовки должна предусматривать эффективное обучение в каждой из областей, включенных в базу знаний правоохранительных органов. Основу данной модели могут составлять существующие учебные заведения (например, полицейская академия или университет), специализированные уникальные тренинги, которые проводятся своими силами или с привлечением сторонних организаций, а также партнерские программы обмена.
3.8.5	**Развитие карьеры**	У правоохранительных органов есть четкая политика в отношении путей продвижения по службе, позволяющая удерживать и продвигать высококлассных специалистов, а также механизмы, обеспечивающие надлежащее укомплектование кадрами и их соответствие требованиям, связанные с возложенными задачами. Политика должна быть направлена на получение максимальной выгоды от обучения и опыта, полученного предоставленного приглашенными специалистами, а также давать возможность заменять экспертов, которые не показали хороших результатов или не обладают навыками работы в новых условиях.

4.4.9 Обеспечение возможностей: вспомогательные бизнес-функции

Эффективная деятельность правоохранительных органов требует надлежащей организационной поддержки, которая также способствует использованию контртеррористических возможностей[41].

Ном.	Субвозможности	Описание
3.9.1	**Закупки**	Организации необходимы процедуры и специалисты, чтобы иметь возможность заключать договоры и закупать товары и услуги в рамках правовой и финансовой основы, применимой к государственным учреждениям. Для содействия оперативной и уникальной с технологической точки зрения деятельности организация должна иметь возможности для быстрой закупки в рамках действующей правовой основы.
3.9.2	**Финансы**	Правоохранительные органы должны осуществлять свою деятельность в рамках четкого бюджета, определенного на краткосрочный, среднесрочный и долгосрочный периоды, который обеспечивает возможность проведения операций, а также наращивания новых возможностей. Управление бюджетом должно допускать гибкость в работе, чтобы реагировать на новые угрозы и при этом соответствовать согласованной правовой основе.
3.9.3	**ИКТ**	ИКТ-инфраструктура и возможности имеют существенно важное значение для надлежащего и эффективного функционирования правоохранительных органов, а также обеспечения поддержки специализированного использования новых технологий для борьбы с терроризмом.
3.9.4	**Безопасность**	Применение мер, методов и ресурсов для защиты активов, операций и информации организации от потенциальных угроз, рисков и несанкционированного доступа. Она охватывает различные аспекты, в том числе физическую безопасность, информационную безопасность и управление рисками.
3.9.5	**Кибербезопасность**	Внутренняя безопасность и кибербезопасность необходимы для защиты собираемой или получаемой конфиденциальной информации, а также для обеспечения оперативной устойчивости. Организация применяет стандарты высокого уровня по кибербезопасности к своим системам, процессам и кадрам, чтобы гарантировать оперативную устойчивость и конфиденциальность информации. Внутренние процессы обеспечения безопасности позволяют осуществлять межведомственный обмен секретной информацией.
3.9.6	**Правовое обеспечение**	Правоохранительные органы должны иметь надлежащую правовую поддержку в их оперативной и вспомогательной деятельности. Сотрудники отдела правового обеспечения участвуют в программах обучения для правоохранительных органов с целью совершенствования подхода, ориентированного на выполнение задач, и повышения эффективности работы.

41 Поскольку речь идет об общих возможностях, они изложены кратко. О случаях, когда такие возможности требуют особого внимания в контексте борьбы с терроризмом, говорится выше.

[V] Модель зрелости

5.1 Обзор

Модель зрелости — система, используемая для оценки текущего уровня возможностей в конкретной области и обеспечения дорожной карты для их совершенствования. В контексте контртеррористической деятельности правоохранительных органов данная модель зрелости может быть использована для оценки возможностей правоохранительных органов на национальном уровне в отношении противодействия использованию новых технологий в террористических целях, а также в качестве дорожной карты для наращивания и совершенствования данных возможностей.

Модель зрелости, содержащаяся в настоящем документе, основана на комплексном исследовании, проведенном Европейским агентством по сетевой и информационной безопасности (ENISA) для создания Национальной системы оценки возможностей, и адаптирована в контексте противодействия использованию новых технологий для террористических целей.

Цель модели оценки зрелости возможностей — помочь государствам определить сильные и слабые стороны их текущих возможностей и обеспечить структурированный подход к совершенствованию этих возможностей с течением времени. Это инструмент для непрерывного улучшения, который предусматривает регулярную оценку с целью определения приоритетных направлений согласно национальной контртеррористической политике и стратегии государства. Кроме того, она может быть использована для сравнения с другими государствами и определения передовых методов и областей для сотрудничества.

В целом модель оценки зрелости возможностей правоохранительных органов является ценным инструментом для правоохранительных органов, которые стремятся расширить свои возможности в сфере противодействия использованию новых технологий в террористических целях и опережать новые угрозы, постоянно возникающие во все более сложном цифровом мире.

5.2 Структура модели зрелости

РИСУНОК 5

В основе модели зрелости лежит национальная эталонная модель возможностей. Модель зрелости подробно описывает возможности и субвозможности с помощью ряда показателей, которые оформлены в виде вопросов и распределены по пяти уровням зрелости. Каждая субвозможность подробно описывается посредством вопросов согласно уровню зрелости. Каждый уровень зрелости базируется на выполненных требованиях предыдущего уровня зрелости.

5.3 Уровни зрелости

Модель зрелости состоит из пяти уровней зрелости. Каждый уровень зрелости основывается на предыдущем уровне, а целью является достижение высшего уровня.

Определения уровней зрелости
Нулевой
Наглядные доказательства наличия или практического использования возможности отсутствуют.
Базовый
Наглядные доказательства наличия возможности в базовой форме, может быть разовой, бессистемной, слабо определенной и ограниченной.
Сформированный
Наглядные доказательства наличия постоянной возможности, которая однако не оптимизирована.
Продвинутый
Наглядные доказательства наличия эффективной возможности, которая считается «зрелой» и четко определенной.
Высший
Наглядные доказательства наличия эффективной возможности, которая изменяется в зависимости от ситуации или условий, чтобы соответствовать требованиям.

5.4 Показатели: структура оценки

Модель нацелена на упрощение оценки благодаря вопросам, на которые можно ответить «да» или «нет» и которые требуют менее качественной оценки. Эти вопросы таким образом уточняют, как возможности и субвозможности могут преобразовываться. Предполагается, что они будут допускать неограниченное число ответов и позволять государствам-членам применять их по своему усмотрению, но при этом будут содержать указания на важные необходимые элементы. Разработанные показатели будут сверяться с реальными примерами, которые могут лечь в основу обновления модели.

Для каждого уровня зрелости есть список показателей, которые оформлены в виде вопросов для оценки на уровне субвозможностей. Показатели используются для описания и оценки возможности. Показатели распределены на две следующие категории:

- **Общие:** общие показатели — это стандартные показатели для оценки кадров, структуры, процессов и требований в отношении инфраструктуры;
- **Специальные:** в соответствующих случаях к специальным относятся технические показатели, связанные с технологиями, правами человека и гендерными аспектами.

5.5 Уровни зрелости: направление, возможность, субвозможность

Оценка зрелости предусматривает три уровня измерений — на уровне направления, возможности и субвозможности.

Общий балл — среднее значение баллов трех субвозможностей. Его целью является предоставление общего показателя уровня зрелости государства-члена; однако, учитывая различия и взаимосвязь между законодательством в области политики и институциональными возможностями, его следует рассматривать вместе с индивидуальными баллами возможностей и субвозможностей. Общий балл подразумевает очень обобщенное представление об уровне зрелости. Баллы возможностей и субвозможностей позволяют сосредоточиться на тех областях, которые требуют большего внимания и приоритета.

Балл возможностей — это наименьший общий знаменатель среди баллов субвозможностей. Балл субвозможностей представляет собой результат среднего значения подробных вопросов. Использование «наименьшего общего знаменателя» основано на взаимозависимости между элементами субвозможностей.

5.6 Модель зрелости возможностей: правовое направление

1	L1	Правовое направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
1.1	**L2**	**Верховенство права**					
1.1.1	L3	**Верховенство права в соответствии с международными стандартами**	**Верховенство права в соответствии с международными стандартами отсутствует**	**ОБЩИЕ:** Имеются ли официальные юридически обязывающие внешнеполитические заявления правительства в отношении применимости принципа верховенства права? Существуют ли процедуры по укреплению принципов верховенства права в правовой системе при подготовке законодательства и правового руководства? Проводила ли ООН анализ деятельности государства-члена на наличие нарушений принципа верховенства права? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Закреплены ли в конституционно-правовой основе принципы верховенства права? Имеется ли всеобъемлющая внутренняя правовая политика для обеспечения применения принципов верховенства права? **СПЕЦИАЛЬНЫЕ:** Имеются ли официальные юридически обязывающие заявления правительства в отношении применимости принципов верховенства права к использованию новых технологий в борьбе с терроризмом? Имеется ли официальная юридически обязывающая политика, требующая проверки законности разработки и применения новых технологий?	**ОБЩИЕ:** Имеется ли обязательная правовая политика по независимой проверке применения принципа верховенства права в соответствии с руководящими указаниями ООН? Принимается ли активное участие в дискуссиях ООН по вопросам разработки и применения руководства? **СПЕЦИАЛЬНЫЕ:** Имеется ли обязательная правовая политика, требующая от правовых учреждений смягчения рисков, связанных с использованием правоохранительными органами новых технологий, для принципов верховенства права? Принимается ли активное участие в дискуссиях ООН по вопросам разработки и применения руководства в отношении новых технологий? Имеется ли специальное практическое руководство по реализации принципов верховенства права в отношении использования новых технологий для борьбы с терроризмом? Имеется ли официальная юридически обязывающая политика, требующая независимой проверки законности разработки и применения новых технологий?	**ОБЩИЕ:** Возглавляют ли представители правоохранительных органов рабочие группы по разработке стандартов в ООН или на других международных площадках? Имеется ли юридически обязывающая политика прозрачности в отношении оценки принципов верховенства права в контртеррористической деятельности правоохранительных органов? **СПЕЦИАЛЬНЫЕ:** Имеется ли правовая основа для привлечения гражданского общества на стыке принципов верховенства права и деятельности правоохранительных органов? Имеется юридически обязывающая политика в отношении публикации оценки принципов верховенства права и контртеррористической деятельности правоохранительных органов, связанной с новыми технологиями?
1.2	**L2**	**Права человека**					
1.2.1	L3	**Приверженность/соответствие руководящим указаниям ООН**	**Приверженность/соответствие руководящим указаниям ООН отсутствует**	**ОБЩИЕ:** Имеются ли процедуры в отношении применения руководящих указаний ООН в рамках подготовки законодательства и правового руководства? Проводила ли ООН анализ деятельности государства-члена на наличие нарушений прав человека? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеются ли официальные юридически обязывающие внешнеполитические заявления правительства в отношении применимости правовой основы? Имеется ли всеобъемлющая внутренняя правовая политика для внедрения руководящих указаний ООН в процесс выработки мер политики? **СПЕЦИАЛЬНЫЕ:** Имеются ли официальные юридически обязывающие заявления правительства в отношении применимости правовой основы к использованию новых технологий в борьбе с терроризмом? Имеется ли специальное практическое руководство по реализации принципов прав человека в отношении использования новых технологий для борьбы с терроризмом? Соблюдаются ли международные требования в отношении контроля над экспортом?	**ОБЩИЕ:** Имеется ли обязательная правовая политика, требующая оценки воздействия на права человека новых видов деятельности правоохранительных органов в соответствии с руководящими указаниями ООН? Принимается ли активное участие в дискуссиях ООН по вопросам разработки и применения руководства? **СПЕЦИАЛЬНЫЕ:** Имеется ли обязательная правовая политика, требующая оценки воздействия на права человека новых видов использования новых технологий? Имеется ли официальная обязательная правовая политика, требующая оценки воздействия на права человека при разработке или закупке новых технологий? Принимается ли активное участие в дискуссиях ООН по вопросам разработки и применения руководства в отношении новых технологий?	**ОБЩИЕ:** Возглавляют ли представители правоохранительных органов рабочие группы по разработке стандартов в ООН или на других международных площадках? Имеется ли юридически обязывающая политика прозрачности в отношении воздействия на права человека и его смягчения контртеррористической деятельности правоохранительных органов? **СПЕЦИАЛЬНЫЕ:** Имеется ли официальная обязательная правовая политика, требующая независимой оценки воздействия на права человека при разработке или закупке новых технологий? Имеется ли правовая основа для привлечения гражданского общества с целью поддержки сканирования горизонта на наличие потенциальных проблем в области прав человека в результате использования новых технологий? Имеется ли юридически обязывающая политика прозрачности в отношении воздействия на права человека и его смягчения контртеррористической деятельности правоохранительных органов, которая включает использование новых технологий?

1	L1	Правовое направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
1.2.2	L3	**Правовые полномочия для независимой проверки**	**Правовые полномочия для независимой проверки отсутствуют**	**ОБЩИЕ:** Имеются ли правовые полномочия для независимой проверки ценностной цепочки контртеррористической деятельности правоохранительных органов? Закреплено ли в законе назначение, независимость и свобода действий учреждения, являющегося объектом проверки? Являются ли решения, связанные с проверкой общедоступными? **СПЕЦИАЛЬНЫЕ:** Имеются ли правовые полномочия, адаптированные специально для ценностной цепочки контртеррористической деятельности правоохранительных органов в отношении новых технологий?	**ОБЩИЕ:** Имеются ли широкие правовые полномочия для независимой проверки всей ценностной цепочки контртеррористической деятельности правоохранительных органов? **СПЕЦИАЛЬНЫЕ:** Имеет ли проверяющее учреждение доступ к независимым техническим рекомендациям?	**ОБЩИЕ:** Позволяет ли процесс проверки осуществлять проверку политики и процедур правоохранительных органов и проверку в целом (а не только проверку конкретного случая)? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Может ли процесс проверки быть инициирован третьей стороной (например, неправительственной организацией)? Существуют ли требования к прозрачности деятельности проверяющего учреждения? **СПЕЦИАЛЬНЫЕ:** Имеется ли в правовой основе требование о наличии технической квалификации у проверяющего учреждения?
1.2.3	L3	**Применение общепринятых принципов защиты данных**	**Применение общепринятых принципов защиты данных отсутствует**	**ОБЩИЕ:** Имеют ли какие-либо из общепринятых принципов защиты данных обязательную юридическую силу для правоохранительных органов? **СПЕЦИАЛЬНЫЕ** Неприменимо	**ОБЩИЕ:** Входят ли общепринятые принципы защиты данных в состав всеобъемлющей правовой основы, имеющей обязательную силу для правоохранительных органов? Имеют ли правоохранительные органы четкий мандат в отношении службы защиты данных? Имеют ли правоохранительные органы обязательные внутренние документы и процедуры для внедрения правовой основы о защите данных? Проводят ли правоохранительные органы обучение по защите данных для соответствующих руководителей и сотрудников? **СПЕЦИАЛЬНЫЕ:** Обязан ли ИКТ-персонал правоохранительных органов сотрудничать со службой защиты данных в соответствии с внутренней политикой?	**ОБЩИЕ:** Имеет ли служба защиты данных четко определенный мандат, основанный на законе, который включает полномочия по развитию и надзору относительно использования ИКТ в правоохранительных органах с целью соблюдения общепринятых принципов защиты данных? Имеет ли служба защиты данных четкие правила о независимости и конфликте интересов, основанные на законе? Имеет ли служба защиты данных независимые аудиторские полномочия? Имеет ли служба защиты данных требования по обязательной отчетности? Имеется ли правовая основа для независимого возмещения ущерба субъектам данных? **СПЕЦИАЛЬНЫЕ:** Имеется ли обязательная правовая политика, требующая оценки воздействия на защиту данных при разработке или закупке новых технологий? Имеется ли обязательное правовое руководство службы защиты данных по проведению оценок воздействия на неприкосновенность частной жизни?	**ОБЩИЕ:** Имеется ли обязательное требование о публикации службой защиты данных отчетов о своей деятельности? Имеются ли обязательные требования к службе защиты данных в отношении предоставления отчетности в парламент? Являются ли правоохранительные органы или служба защиты данных стороной официальных соглашений о сотрудничестве с другими службами защиты данных? **СПЕЦИАЛЬНЫЕ:** Имеется ли подробное руководство по защите данных, касающееся использования новых технологий? Проводит ли служба защиты данных обучение персонала использованию новых технологий и защите данных?

1	L1	Правовое направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
1.2.4	L2	**Управление передовыми технологиями сбора и анализа данных**	**Управление передовыми технологиями сбора и анализа данных отсутствует**	**ОБЩИЕ:** Имеют ли правоохранительные органы уровень зрелости 3 в части защиты данных? **СПЕЦИАЛЬНЫЕ:** Располагают ли правоохранительные органы специальной политикой по использованию новых технологий сбора? Располагают ли правоохранительные органы специальной политикой по использованию передовых технологий анализа данных?	**ОБЩИЕ:** Имеют ли правоохранительные органы уровень зрелости 4 в части защиты данных? Имеют ли правоохранительные органы классификацию воздействия на неприкосновенность частной жизни, в которой определены сильное, среднее и слабое воздействия? **СПЕЦИАЛЬНЫЕ:** Предусматривает ли внедрение новых методов сбора данных или передовых технологий анализа данных необходимость проведения оценки воздействия на защиту данных, в которой рассматриваются риски, касающиеся чрезмерного сбора, справедливости и объективности?	**ОБЩИЕ:** Имеется ли обязательная политика по независимому аудиту для решения вопросов, касающихся справедливости, объективности и рисков автоматизированных решений, которые оказывают значительное влияние на неприкосновенность частной жизни? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Опубликовано ли правоохранительными органами руководство по оценке рисков, связанных с передовыми технологиями анализа данных? Участвуют ли правоохранительные органы в глобальных дискуссиях, посвященных новым методам сбора и передовым технологиям анализа данных? **СПЕЦИАЛЬНЫЕ:** Неприменимо
1.3	**L2**	**Институциональные мандаты**					
1.3.1	L3	**Определение ведущих контртеррористических учреждений**	**Определение ведущих контртеррористических учреждений отсутствует**	**ОБЩИЕ:** Имеется ли общее письменное юридически обязательное предписание, которое в соответствии с законом возлагает на правоохранительные органы и другие учреждения полномочия по борьбе с терроризмом? **СПЕЦИАЛЬНЫЕ:** Рассматриваются ли в правовой политике, имеющей обязательную силу, вопросы противодействия использованию новых технологий в террористических целях?	**ОБЩИЕ:** Имеется ли конкретный и подробный правовой мандат, основанный на законе, для каждого контртеррористического ведомства? **СПЕЦИАЛЬНЫЕ:** Рассматриваются ли всесторонне в конкретной политике вопросы противодействия использованию новых технологий в террористических целях?	**ОБЩИЕ:** Имеется ли обязательная правовая политика, определяющая полномочия и порядок подчиненности в отношении операций? **СПЕЦИАЛЬНЫЕ:** Определен ли в конкретном законодательстве правовой мандат правоохранительных органов для противодействия использованию новых технологий в террористических целях?	**ОБЩИЕ:** Осуществляется ли периодический пересмотр сферы действия мандата, чтобы учесть изменения в террористической деятельности? Допускает ли законодательство возможность обновления или изменения сферы действия мандата при условии парламентского надзора? **СПЕЦИАЛЬНЫЕ:** Осуществляется ли периодический пересмотр сферы действия мандата, чтобы учесть изменения в области использования новых технологий в террористических целях?
1.3.2	L3	**Определение вспомогательных контртеррористических учреждений**	**Определение вспомогательных контртеррористических учреждений отсутствует**	**ОБЩИЕ:** Имеется ли общее письменное юридически обязательное предписание, которое в соответствии с законом поручает правоохранительным органам и другим учреждениям обеспечение контртеррористической поддержки? **СПЕЦИАЛЬНЫЕ:** Применяется ли общая имеющая юридическую силу вспомогательная политика к новым технологиям?	**ОБЩИЕ:** Имеется ли всеобъемлющая юридически обязательная директива для контртеррористических вспомогательных учреждений? **СПЕЦИАЛЬНЫЕ:** Применяется ли политика к новым технологиям?	**ОБЩИЕ:** Имеют ли механизмы координации и коммуникации обязательную юридическую силу для контртеррористических вспомогательных учреждений? Имеются ли обязательные требования в отношении сообщения вспомогательным учреждениям и правоохранительным органам о подозрениях в террористической деятельности? **СПЕЦИАЛЬНЫЕ:** Рассматриваются ли в обязательной политике координации и сообщений непосредственно новые технологии?	**ОБЩИЕ:** Имеется ли обязательная правовая политика по координации функций, охватывающая все государственные ведомства? **СПЕЦИАЛЬНЫЕ:** Осуществляется ли периодический пересмотр сферы действия мандата, чтобы учесть изменения в области использования новых технологий в террористических целях?

1	L1	Правовое направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
1.3.3	L3	**Определение механизмов координации**	**Определение механизмов координации отсутствует**	**ОБЩИЕ:** Имеется ли общая политика, в которой определены обмен информацией и сотрудничество внутри государства? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли всеобъемлющая юридически обязывающая политика в отношении обмена информацией в контртеррористических целях? Имеется ли всеобъемлющая политика по координации деятельности в рамках контртеррористической ценностной цепочки во всех контртеррористических организациях? Имеется ли всеобъемлющий перечень неконтртеррористических организаций, которые имеют значение для поддержки ценностной цепочки контртеррористической деятельности? **СПЕЦИАЛЬНЫЕ:** Существует ли механизм координации действий правоохранительных органов с национальной группой реагирования на инциденты в сфере компьютерной безопасности (CSIRT)?	**ОБЩИЕ:** Имеется ли специальный координационный орган высокого уровня с достаточными ресурсами? Четко ли определен порядок подчиненности во время национального инцидента? Имеют ли механизмы координации возможности для ситуационной осведомленности в режиме реального времени? **СПЕЦИАЛЬНЫЕ:** Имеется ли специальная координационная политика по новым технологиям? Имеется ли специальный координационный орган высокого уровня с достаточными ресурсами для новых технологий? Имеют ли механизмы координации возможности для ситуационной осведомленности в режиме реального времени в отношении ИКТ?	**ОБЩИЕ:** Осуществляется ли ежегодный пересмотр координационной политики? **СПЕЦИАЛЬНЫЕ:** Неприменимо
1.4	**L2**	**Материальное уголовное право**					
1.4.1	L3	**Террористические преступления**	**Уголовное право по террористическим преступлениям отсутствует**	**ОБЩИЕ:** Содержатся ли в уголовном кодексе какие-либо из террористических преступлений? Является ли законодательство четким и узконаправленным? **СПЕЦИАЛЬНЫЕ:** Содержатся ли в уголовном кодексе какие-либо из террористических преступлений с использованием новых технологий?	**ОБЩИЕ:** Был ли представлен законопроект о преступлениях, не подпадающих под действие закона, на рассмотрение в законодательный орган? Является ли законодательство четким и узконаправленным? **СПЕЦИАЛЬНЫЕ:** Был ли представлен законопроект о террористических преступлениях, совершенных с использованием новых технологий, не подпадающих под действие закона, на рассмотрение в законодательный орган? Относятся ли высказывания, квалифицированные как преступления, к подстрекательству и вербовке, а не к разрешенным законом политическим заявлениям?	**ОБЩИЕ:** Охватывают ли законы, подзаконные акты и другие нормы все террористические преступления? Являются ли правовые нормы четкими и узконаправленными? Опубликованы ли главным органом преследования руководящие указания по судебному преследованию? **СПЕЦИАЛЬНЫЕ:** Охватывают ли законы, подзаконные акты и другие нормы все террористические преступления с использованием новых технологий?	**ОБЩИЕ:** Являются ли руководящие указания по судебному преследованию общедоступными? Приведены ли террористические преступления в соответствие с ведущими мировыми стандартами? **СПЕЦИАЛЬНЫЕ:** Участвуют ли правоохранительные органы в международных правовых дискуссиях, посвященных борьбе с терроризмом?
1.4.2	L3	**Киберпреступность: компьютеры**	**Уголовное право по киберпреступлениям (компьютерам) отсутствует**	**ОБЩИЕ:** Содержатся ли в уголовном кодексе какие-либо из киберпреступлений? Является ли законодательство четким и узконаправленным? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Был ли представлен законопроект о киберпреступлениях, не подпадающих под действие закона, на рассмотрение в законодательный орган? Является ли законодательство четким и узконаправленным? **СПЕЦИАЛЬНЫЕ:** Относятся ли высказывания, квалифицированные как преступления, к подстрекательству и вербовке, а не к разрешенным законом политическим заявлениям?	**ОБЩИЕ:** Охватывают ли законы, подзаконные акты и другие нормы все киберпреступления? Являются ли правовые нормы четкими и узконаправленными? Опубликованы ли главным органом преследования руководящие указания по судебному преследованию? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Являются ли руководящие указания по судебному преследованию общедоступными? Приведены ли киберпреступления в соответствие с ведущими мировыми стандартами? **СПЕЦИАЛЬНЫЕ:** Участвуют ли правоохранительные органы в международных дискуссиях по вопросу разработки модели, касающейся киберпреступлений?

1	L1	Правовое направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
1.4.3	L3	**Дополнительные преступления/ преступления, связанные с предоставлением материальной поддержки**	**Уголовное право, касающееся дополнительных преступлений/ преступлений, связанных с предоставлением материальной поддержки, отсутствует**	**ОБЩИЕ:** Включает ли уголовное право дополнительные преступления? Является ли законодательство четким и узконаправленным? **СПЕЦИАЛЬНЫЕ:** Включены ли в законодательство дополнительные преступления, которые относятся к киберпреступлениям? Включены ли в законодательство дополнительные преступления террористического характера с использованием новых технологий?	**ОБЩИЕ:** Был ли представлен законопроект о преступлениях, не подпадающих под действие закона, на рассмотрение в законодательный орган? Является ли законодательство четким и узконаправленным? **СПЕЦИАЛЬНЫЕ:** Был ли представлен законопроект о не подпадающих под действие закона дополнительных преступлениях, которые относятся к дополнительным киберпреступлениям, на рассмотрение в законодательный орган?	**ОБЩИЕ:** Охватывают ли законы, подзаконные акты и другие нормы все соответствующие дополнительные преступления террористического характера? Являются ли правовые нормы четкими и узконаправленными? Опубликованы ли главным органом преследования руководящие указания по судебному преследованию? **СПЕЦИАЛЬНЫЕ:** Охватывают ли законы, подзаконные акты и другие нормы все соответствующие дополнительные киберпреступления террористического характера? Охватывают ли законы, подзаконные акты и другие нормы все соответствующие дополнительные преступления террористического характера с использованием новых технологий?	**ОБЩИЕ:** Являются ли руководящие указания по судебному преследованию общедоступными? Приведены ли террористические преступления в соответствие с ведущими мировыми стандартами? **СПЕЦИАЛЬНЫЕ:** Участвуют ли правоохранительные органы в международных правовых дискуссиях, посвященных борьбе с терроризмом?
1.5	**L2**	**Административное и процессуальное право**					
1.5.1	L3	**Общие полномочия правоохранительных органов**	**Административное и процессуальное право для общих полномочий правоохранительных органов отсутствует**	**ОБЩИЕ:** Позволяет ли уголовно-процессуальное право осуществлять некоторые из общих полномочий правоохранительных органов? Имеются ли процессуальные гарантии для данных полномочий? Осуществляется ли законопроектная деятельность для укрепления всеобъемлющей законодательной базы? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Был ли внесен законопроект с целью дополнения законодательных полномочий? Включает ли законопроект действующие процессуальные гарантии? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Охватывают ли законы и подзаконные акты общие полномочия правоохранительных органов всесторонне? Включает ли закон действующие процессуальные гарантии? Подготовлен ли органом преследования проект руководящих принципов по внедрению? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Осуществляется ли регулярная проверка полномочий правоохранительных органов на основании опыта внедрения и с учетом развития судебной практики? **СПЕЦИАЛЬНЫЕ:** Неприменимо
1.5.2	L3	**Полномочия по работе с цифровой информацией и доказательствами**	**Административное и процессуальное право для полномочий по работе с цифровой информацией и доказательствами отсутствует**	**ОБЩИЕ:** Включены ли в правовую основу полномочия правоохранительных органов, связанные с использованием новых технологий? Имеются ли процессуальные гарантии для данных полномочий? Осуществляется ли законотворческая деятельность для укрепления всеобъемлющей законодательной базы? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Был ли внесен законопроект с целью дополнения законодательных полномочий? Включает ли законопроект действующие процессуальные гарантии? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Обеспечивают ли законы и подзаконные акты правовые полномочия, связанные с использованием новых технологий? Включает ли закон действующие процессуальные гарантии? Подготовлен ли органом преследования проект руководящих принципов по внедрению? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Осуществляется ли регулярная проверка полномочий правоохранительных органов в отношении законодательства о цифровых доказательствах на основании глобальной передовой практики, опыта внедрения и с учетом развития судебной практики? **СПЕЦИАЛЬНЫЕ:** Неприменимо

1	L1	Правовое направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
1.5.3	L3	**Расширенные полномочия правоохранительных органов, связанные с новыми технологиями**	**Административное и процессуальное право для уникальных полномочий, связанных с технологиями, отсутствует**	ОБЩИЕ: Обеспечивает ли правовая основа возможность использования некоторых из передовых новых технологий в рамках полномочий правоохранительных органов? Имеются ли процессуальные гарантии для данных полномочий? Осуществляется ли законотворческая деятельность для укрепления всеобъемлющей законодательной базы? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Был ли внесен законопроект с целью дополнения законодательных полномочий? Включает ли законопроект действующие процессуальные гарантии? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Включает ли правовая основа передовые новые технологии в рамках полномочий правоохранительных органов? Включает ли закон действующие процессуальные гарантии? Подготовлен ли органом преследования проект руководящих принципов по внедрению? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Регулярно ли пересматривается законодательная база в отношении новых технологий на основании глобальной передовой практики, опыта внедрения и с учетом развития судебной практики? СПЕЦИАЛЬНЫЕ: Неприменимо
1.5.4	L3	**Уникальные контртеррористические полномочия**	**Административное и процессуальное право для уникальных контртеррористических полномочий отсутствует**	ОБЩИЕ: Позволяет ли правовая основа использовать какие-либо уникальные контртеррористические полномочия? Имеются ли процессуальные гарантии для данных полномочий? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Был ли внесен законопроект с целью дополнения законодательных полномочий? Включает ли законопроект действующие процессуальные гарантии? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Позволяет ли правовая основа использовать все уникальные контртеррористические полномочия? Включает ли закон действующие процессуальные гарантии? Подготовлен ли органом преследования проект руководящих принципов по внедрению? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Осуществляется ли регулярная проверка уникальных контртеррористических полномочий правоохранительных органов на основании опыта внедрения глобальной передовой практики и с учетом развития судебной практики? СПЕЦИАЛЬНЫЕ: Неприменимо
1.5.5	L3	**Уникальная административная поддержка**	**Административное и процессуальное право для уникальной административной поддержки отсутствует**	ОБЩИЕ: Позволяет ли правовая основа, применимая к деятельности правоохранительных органов, использовать какие-либо элементы уникальной административной поддержки? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется ли в свободном доступе практическое руководство по средствам уникальной административной поддержки? Имеется ли законотворческая или нормотворческая деятельность в отношении всех элементов уникальной административной поддержки? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется ли всеобъемлющая правовая основа для обеспечения уникальной административной поддержки? Имеется ли в свободном доступе практическое руководство по средствам уникальной административной поддержки? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Осуществляется ли регулярный пересмотр средств уникальной административной поддержки в зависимости от оперативных потребностей? СПЕЦИАЛЬНЫЕ: Неприменимо
1.6	**L2**	**Юрисдикция и сотрудничество**					
1.6.1	L3	**Четкая юрисдикционная правовая политика**	**Четкая юрисдикционная правовая политика отсутствует**	ОБЩИЕ: Издавал ли главный орган преследования указания по проведению операций правоохранительными органами и юрисдикционной политике? Доступна ли политика соответствующим заинтересованным сторонам организации? СПЕЦИАЛЬНЫЕ: Издавал ли главный орган преследования указания по проведению операций правоохранительными органами, уникальным контртеррористическим полномочиям и юрисдикционной политике, связанной с новыми технологиями?	ОБЩИЕ: Издавал ли главный орган преследования всеобъемлющие указания по проведению операций правоохранительными органами [«контртеррористическая ценностная цепочка»] и юрисдикционной политике? СПЕЦИАЛЬНЫЕ: Издавал ли главный орган преследования всеобъемлющие указания по юрисдикционной политике? Имеется ли процесс для разработки решений проблем юрисдикционного характера, связанных с использованием новых технологий?	ОБЩИЕ: Включены ли какие-либо элементы юрисдикционной политики в законодательство? Были ли одобрены элементы юрисдикционной политики судами? СПЕЦИАЛЬНЫЕ: Включена ли юрисдикционная политика в отношении использования новых технологий правоохранительными органами в законодательство? Были ли одобрены элементы юрисдикционной политики судами?	ОБЩИЕ: Участвуют ли правоохранительные органы в международных мероприятиях по разработке норм в этой области? СПЕЦИАЛЬНЫЕ: Неприменимо

1	L1	Правовое направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
1.6.2	L3	**Официальные юридические соглашения по трансграничному сотрудничеству**	**Официальные юридические соглашения по трансграничному сотрудничеству отсутствуют**	**ОБЩИЕ:** Имеет ли государство-член правовую основу, которая позволяет обеспечить трансграничное сотрудничество правоохранительных органов? Подписали ли правоохранительные органы соглашения о сотрудничестве, позволяющие оказывать трансграничную помощь в ценностной цепочке контртеррористической деятельности? **СПЕЦИАЛЬНЫЕ:** Предусмотрен ли сбор и обмен цифровыми доказательствами в соглашениях о сотрудничестве с правоохранительными органами?	**ОБЩИЕ:** Отвечает ли государство-член требованиям, предъявляемым к членству, в соответствующих многосторонних договорах о сотрудничестве с правоохранительными органами? Имеет ли государство-член официальные соглашения с государствами-членами, которые имеют важное значение для его деятельности по борьбе с терроризмом? **СПЕЦИАЛЬНЫЕ:** Соблюдены ли требования государством-членом, чтобы стать участником многостороннего договора в области киберпреступности? Имеет ли государство-член официальные соглашения с государствами-членами, которые имеют важное значение для его деятельности по борьбе с терроризмом и противодействию использованию новых технологий?	**ОБЩИЕ:** Является ли государство-член участником соответствующих многосторонних договоров о сотрудничестве с правоохранительными органами? **СПЕЦИАЛЬНЫЕ:** Является ли государство-член участником соответствующих многосторонних договоров о сотрудничестве с правоохранительными органами по вопросу киберпреступности?	**ОБЩИЕ:** Принимает ли государство-член активное участие в разработке новых двусторонних или многосторонних документов по контртеррористической деятельности правоохранительных органов? **СПЕЦИАЛЬНЫЕ:** Принимает ли государство-член активное участие в разработке новых двусторонних или многосторонних документов по контртеррористической деятельности правоохранительных органов, касающейся новых технологий?
1.6.3	L3	**Правовая экосистема, обеспечивающая неофициальное сотрудничество**	**Правовая экосистема, обеспечивающая неофициальное сотрудничество, отсутствует**	**ОБЩИЕ:** Являются ли элементы принципов защиты данных частью правовой экосистемы? Имеются ли правовые гарантии, ограничивающие возможности правительства по изъятию интеллектуальной собственности у частного сектора? Одинаковый ли в целом режим у иностранных компаний в национальном законодательстве? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеет ли государство-член правовую основу защиты данных в соответствии с общепринятыми принципами? Является ли судебное возмещение ущерба в целом доступным для иностранных компаний? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Отражена ли деятельность, касающаяся доступа правительства, в обязательном прозрачном отчете? Проводится ли форум с участием заинтересованных сторон, включая компании частного сектора, для содействия сотрудничеству государственного и частного секторов в деле борьбы с терроризмом? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Активно ли участвует государство-член в международных дискуссиях, посвященных вопросам управления, с участием заинтересованных сторон? Проводится ли национальный форум с участием заинтересованных сторон? **СПЕЦИАЛЬНЫЕ:** Проводится ли национальный форум по вопросам новых технологий с участием заинтересованных сторон?

5.7 Модель зрелости возможностей: политическое направление

2	L1	Политическое направление национальной контртеррористической деятельности	Нулевой	Базовый	Сформированный	Продвинутый	Высший
2.1	**L2**	**Разработка политики и управление ею**					
2.1.1	L3	**Управление**	**Управление отсутствует**	**ОБЩИЕ:** Имеется ли компетентный орган высокого уровня, который подотчетен высшему органу управления в вопросах развития и реализации национальной контртеррористической политики? Охватывает ли национальная контртеррористическая политика вопросы условий окружающей среды, способствующих возникновению террористической угрозы? Являются ли процедуры управления разовыми или неофициальными? **СПЕЦИАЛЬНЫЕ:** Включены ли новые технологии по борьбе с терроризмом в разработку и развертывание национальной контртеррористической политики?	**ОБЩИЕ:** Должны ли государственные учреждения принимать участие в разработке национальной контртеррористической политики, в том числе предоставлять информацию? Оказывает ли компетентный орган высокого уровня влияние на развитие и надзор в отношении национальных контртеррористических мероприятий? Имеет ли высший орган управления всеобъемлющий перечень национальных контртеррористических мероприятий? Определены ли правительством контртеррористическая политика и цели эффективности? **СПЕЦИАЛЬНЫЕ:** Имеет ли компетентный орган высокого уровня ресурсы и полномочия для сбора информации о новых технологиях? Имеет ли высший орган управления всеобъемлющий перечень национальных контртеррористических мероприятий, включающих новые технологии? Определены ли правительством политика использования новых технологий в контртеррористических целях и цели эффективности? Рассматривается ли в политике использование новых технологий для поощрения культуры толерантности, уважения и ответственного использования новых технологий?	**ОБЩИЕ:** Утверждена ли на высшем уровне управления обязательная письменная политика в отношении политики, которая будет служить руководством при разработке политики и осуществлении надзора? Предусматривает ли национальная контртеррористическая политика координацию усилий для устранения условий, способствующих возникновению террористических угроз? Назначены ли высшим органом управления команды по руководству и управлению политикой для разработки национальной контртеррористической политики и надзора за ее реализацией? Дает ли политика возможность осуществления надзора за национальными контртеррористическими мероприятиями? Осуществляется ли регулярная оценка целей политики и целей эффективности в отношении борьбы с терроризмом? Оценивались ли затраты и риски изменений политики по отношению к потенциальным значениям? **СПЕЦИАЛЬНЫЕ:** Включает ли мандат, касающийся разработки политики, новые технологии для борьбы с терроризмом? Входят ли в состав команды по разработке политики технические специалисты? Осуществляется ли регулярная оценка целей политики и целей эффективности в отношении противодействия использованию новых технологий в террористических целях? Включает ли политика усилия по обеспечению цифровой грамотности, которые могут способствовать формированию культуры толерантности в Интернете?	**ОБЩИЕ:** Полностью ли действует национальная политика в отношении политики и переносится ли она на процессы организационного планирования и составления бюджета? Осуществляется ли пересмотр национальной политики в отношении политики с целью адаптации к изменениям, основанным на эффективности в достижении целей политики и предотвращении террористического риска и воздействия? Осуществляется ли координация контртеррористической политики с социальной и экономической политикой для содействия социальной включенности? **СПЕЦИАЛЬНЫЕ:** Охватывает ли политика в отношении политики вопросы, связанные с новыми технологиями, согласно современной глобальной политике? Осуществляется ли координация контртеррористической политики с социальной и экономической политикой для содействия социальной включенности в Интернете?

2	L1	Политическое направление национальной контртеррористической деятельности	Нулевой	Базовый	Сформированный	Продвинутый	Высший
2.1.2	L3	Научная деятельность и исследования	Научная деятельность и исследования отсутствуют	ОБЩИЕ: Осуществляется ли общесистемная функция по составлению основанных на доказательствах отчетов по террористической деятельности для разработчиков политики высокого уровня? Является ли практика подготовки отчетов о террористической деятельности разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Осуществляется ли общесистемная функция по составлению основанных на доказательствах отчетов по использованию технологий в террористических целях для разработчиков политики высокого уровня? Осуществляется ли координация функций по подготовке отчетов о террористической деятельности с функциями по подготовке отчетов об использовании новых технологий в террористических целях?	ОБЩИЕ: Имеется ли комплексный подход к подготовке отчетов о террористической деятельности? Имеются ли специалисты по подготовке таких отчетов? Является ли ведение отчетности структурированным, документированным и постоянным? СПЕЦИАЛЬНЫЕ: Охватывает ли комплексный подход использование новых технологий в террористических целях? Участвуют ли специалисты по новым технологиям в подготовке отчетов?	ОБЩИЕ: Приведены ли в соответствие стратегия и план передачи террористической оперативной информации с общими приоритетами политики? Есть ли специальный отдел по составлению отчетов? Обязывает ли политика другие государственные организации участвовать в подготовке отчетов о террористической деятельности и предоставлять информацию? Имеется ли возможность проведения полноценных исследований? Проводятся ли консультации с представителями научных кругов при сборе и обобщении информации и знаний? Имеется ли независимая проверка отчетности для повышения конкретности и качества отчетов? СПЕЦИАЛЬНЫЕ: Приведено ли представление отчетности в области технологий в соответствие с общими приоритетами политики? Обязывает ли политика государственные структуры, отвечающие за отдельные части технологической экосистемы (например, Министерство связи), предоставлять информацию и опыт в отношении этой деятельности? Участвуют ли неправительственные организации в процессе подготовки отчета? Имеется ли возможность проведения полноценных исследований в отношении новых технологий? Проводятся ли консультации с представителями научных кругов и отрасли в технологической области при сборе информации и знаний?	ОБЩИЕ: Поддерживает ли отдел информирования о террористических угрозах отношения с отделами в других государствах-членах по обмену информацией и сотрудничеству? СПЕЦИАЛЬНЫЕ: Поддерживает ли отдел информирования о террористических угрозах отношения с отделами по противодействию использованию новых технологий и технологическими компаниями в других государствах-членах по обмену информацией и сотрудничеству?

2	L1	Политическое направление национальной контртеррористической деятельности	Нулевой	Базовый	Сформированный	Продвинутый	Высший
2.1.3	L3	**Выбор курса политики и координация**	**Выбор курса политики и координация отсутствуют**	ОБЩИЕ: Осуществляется ли общесистемная функция по сведению информации о национальных ресурсах и инструментах по борьбе с терроризмом для разработчиков политики высокого уровня? Является ли практика подготовки таких отчетов о террористической деятельности разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Осуществляется ли общесистемная функция по сведению информации о национальных ресурсах и инструментах по борьбе с терроризмом в контексте новых технологий для разработчиков политики высокого уровня? Осуществляется ли координация функций по подготовке отчетов о контртеррористической деятельности с функциями по подготовке отчетов об использовании новых технологий для борьбы с терроризмом?	ОБЩИЕ: Имеется ли комплексный подход к разработке политики и подготовке отчетов о ресурсах и инструментах для борьбы с террористической деятельностью? Имеются ли специалисты по подготовке таких отчетов? Является ли ведение отчетности структурированным, документированным и постоянным? СПЕЦИАЛЬНЫЕ: Охватывает ли комплексный подход использование новых технологий в террористических целях? Участвуют ли специалисты по новым технологиям в подготовке отчетов?	ОБЩИЕ: Есть ли специальный отдел по составлению отчетов по выбору курса политики? Обязывает ли политика другие государственные организации участвовать в такой деятельности и предоставлять информацию? Имеется ли возможность проведения полноценных исследований? Проводятся ли консультации с представителями научных кругов при сборе и обобщении информации, знаний, а также при разработке вариантов политики? Имеется ли независимая проверка политики для повышения конкретности и качества рекомендаций? СПЕЦИАЛЬНЫЕ: Обязывает ли политика государственные структуры, отвечающие за отдельные части технологической экосистемы (например, Министерство связи), предоставлять информацию и опыт в отношении этой деятельности? Участвуют ли неправительственные организации в выработке курса политики? Имеется ли возможность проведения полноценных исследований в отношении новых технологий? Проводятся ли консультации с представителями научных кругов и отрасли в технологической области при сборе информации, знаний и разработке вариантов?	ОБЩИЕ: Поддерживает ли специальный отдел отношения с отделами в других государствах-членах по обмену информацией и сотрудничеству? Работает ли специальный отдел в соответствии с признанной передовой практикой? СПЕЦИАЛЬНЫЕ: Поддерживает ли специальный отдел отношения с отделами по противодействию использованию новых технологий и технологическими компаниями в других государствах-членах по обмену информацией и сотрудничеству?

2	L1	Политическое направление национальной контртеррористической деятельности	Нулевой	Базовый	Сформированный	Продвинутый	Высший
2.1.4	L3	Стратегическая увязка	Стратегическая увязка отсутствует	**ОБЩИЕ:** Осуществляется ли общесистемная функция по сведению информации о национальной политике и мероприятиях по борьбе с терроризмом для разработчиков политики высокого уровня? Является ли практика подготовки таких отчетов о террористической деятельности разовой или неофициальной? Учитывается ли такая информация при принятии новой политики или адаптации политики в этой области? **СПЕЦИАЛЬНЫЕ:** Осуществляется ли общесистемная функция по сведению информации о национальной политике и мероприятиях по противодействию возникновению риска, связанного с использованием новых технологий, для разработчиков политики высокого уровня? Учитывается ли такая информация при принятии новой политики или адаптации политики в этой области? Регулярно ли осуществляется обмен информацией о политике в рамках осуществления функций по подготовке отчетов о политике и мероприятий?	**ОБЩИЕ:** Имеется ли комплексный подход к координации политики по разработке и развертыванию национальной политики и мероприятий по борьбе с терроризмом? Осуществляется ли сбор информации о национальной политике и усилиях в центральном подразделении? Используются ли в подходе одинаковые классификации целей и мер для возможности сравнения? Является ли подход структурированным, документированным и постоянным? Учитывается ли в ходе стратегической увязки действующая региональная политика? **СПЕЦИАЛЬНЫЕ:** Охватывает ли комплексный подход злонамеренное использование новых технологий? Участвуют ли специалисты по новым технологиям в координации политики? Учитывается в ходе стратегической увязки действующая региональная политика в отношении новых технологий (при наличии таковой)?	**ОБЩИЕ:** Есть ли специальный отдел, занимающийся сбором информации о действующей политике и возможных мерах реагирования? Обязывает ли политика другие государственные организации участвовать в такой деятельности и предоставлять информацию? Осуществляется ли координация мер на протяжении жизненного цикла контртеррористической деятельности на уровне политики? Является ли политика обязательной для всех соответствующих государственных органов? Рассматривается ли в политике управление национальным кризисом? **СПЕЦИАЛЬНЫЕ:** Обязывает ли политика государственные структуры, отвечающие за отдельные части технологической экосистемы (например, Министерство связи), предоставлять информацию и опыт в отношении этой деятельности? Участвуют ли неправительственные организации в выработке курса политики? Имеется ли возможность проведения полноценных исследований в отношении новых технологий? Проводятся ли консультации с представителями научных кругов и отраслей в технологической области при сборе информации, знаний и разработке вариантов?	**ОБЩИЕ:** Осуществляется ли регулярный пересмотр целей и мер политики для оценки необходимости иного распределения сфер ответственности между государственными организациями в рамках контртеррористической деятельности? Имеется ли независимая проверка политики для повышения конкретности и качества рекомендаций? Соответствует ли стратегическая увязка глобальной передовой практике? **СПЕЦИАЛЬНЫЕ:** Осуществляется ли специальный пересмотр целей и мер на основании новых технологий?

2	L1	Политическое направление национальной контртеррористической деятельности	Нулевой	Базовый	Сформированный	Продвинутый	Высший
2.2	**L2**	**Управление реализацией политики**					
2.2.1	L3	**Развитие потенциала**	**Развитие потенциала отсутствует**	ОБЩИЕ: Имеется ли компетентный орган высокого уровня, который подотчетен высшему органу управления в вопросах развития и реализации национального контртеррористического потенциала? Является ли практика развития потенциала разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Включены ли новые технологии по борьбе с терроризмом в развитие и оценку национального контртеррористического потенциала на уровне политики?	ОБЩИЕ: Имеется ли комплексный подход к координации оценки и развития национального контртеррористического потенциала? Осуществляется ли сбор информации о потенциале в центральном подразделении? Используются ли в подходе одинаковые классификации для описания контртеррористического потенциала? Является ли подход структурированным, документированным и постоянным? Используются ли в качестве основы подхода оценки угроз? Используется ли развитие потенциала в качестве основы политики в области человеческого капитала и обучения? Определяет ли развитие потенциала приоритеты по закупкам? Охватывает ли развитие потенциала контртеррористическую ценностную цепочку? СПЕЦИАЛЬНЫЕ: Распространяется ли комплексный подход на потенциал по противодействию злонамеренному использованию новых технологий? Охватывает ли комплексный подход потенциальные области применения новых технологий правоохранительными органами и необходимую поддержку для ценностной цепочки контртеррористической деятельности правоохранительных органов? Участвуют ли специалисты по новым технологиям в координации политики?	ОБЩИЕ: Осуществляется ли развитие потенциала посредством среднесрочного и долгосрочного плана развития? Используются ли в качестве основы развития потенциала отраслевые и научные знания о необходимых наборах навыков? Проводится ли анализ усилий по развитию потенциала ежегодно? СПЕЦИАЛЬНЫЕ: Соответствует ли развитие потенциала наборам навыков, характерным для частного сектора?	ОБЩИЕ: Проводится ли анализ усилий по развитию потенциала сторонним экспертом? Обеспечивается ли развитие кадрового потенциала по борьбе с терроризмом через центральный учебный центр? Имеются ли механизмы, позволяющие немедленно обеспечить развитие потенциала в короткий срок? Соответствуют ли требования к развитию потенциала правоохранительных органов программам обучения? СПЕЦИАЛЬНЫЕ: Соответствуют ли требования к развитию потенциала правоохранительных органов программам обучения новым технологиям?

2	L1	Политическое направление национальной контртеррористической деятельности	Нулевой	Базовый	Сформированный	Продвинутый	Высший
2.2.2	L3	**Вмешательства в отношении угроз**	**Вмешательства в отношении угроз отсутствуют**	ОБЩИЕ: Имеется ли компетентный орган высокого уровня, который разрабатывает руководящие принципы по вмешательствам в отношении угроз? СПЕЦИАЛЬНЫЕ: Включены ли новые технологии, используемые для борьбы с терроризмом, в руководящие указания по контртеррористическим вмешательствам в отношении угроз?	ОБЩИЕ: Имеется ли комплексный подход к надзорной деятельности за вмешательствами в отношении угроз? Имеется ли у правоохранительных органов функция сортировки, чтобы принимать решения о вмешательствах в отношении угроз? Используются ли в подходе одинаковые классификации для описания контртеррористических угроз и вмешательств? Имеются ли оперативные возможности ситуационной осведомленности для составления перечня растущих угроз? Является ли подход структурированным, документированным и постоянным? Используются ли в качестве основы подхода оценки угроз? Служит ли подход руководством для деятельности в контртеррористической ценностной цепочке? Согласована ли политика вмешательства в отношении угроз с национальной классификацией инцидентов? Согласуется ли вмешательство в отношении угроз с соображениями по поводу судебного преследования? СПЕЦИАЛЬНЫЕ: Охватывает ли комплексный подход вмешательства с целью противодействия злонамеренному использованию новых технологий? Охватывает ли комплексный подход вмешательства с применением новых технологий правоохранительными органами и необходимую поддержку для ценностной цепочки контртеррористической деятельности правоохранительных органов? Являются ли специальные новые технологии частью разработки политики?	ОБЩИЕ: Имеются ли совместные оперативные возможности ситуационной осведомленности для всех контртеррористических организаций? Имеются ли возможности трансграничного сотрудничества для вмешательства в отношении угроз? Используются ли в качестве основы политики вмешательства в отношении угроз событие национального масштаба или национальное мероприятие? Существует ли общая национальная классификация в качестве ориентира по вмешательствам в отношении угроз для контртеррористических организаций и деятельности? СПЕЦИАЛЬНЫЕ: Имеются ли возможности трансграничного сотрудничества для решения проблем, связанных с новыми технологиями?	ОБЩИЕ: Осуществляется ли ежегодный пересмотр политики вмешательств в отношении угроз? СПЕЦИАЛЬНЫЕ: Включает ли политика вмешательств в отношении угроз оперативное взаимодействие с ИКТ-компаниями?

2	L1	Политическое направление национальной контртеррористической деятельности	Нулевой	Базовый	Сформированный	Продвинутый	Высший
2.2.3	L3	**Распределение институциональных функций и обязанностей**	**Распределение институциональных функций и обязанностей отсутствует**	ОБЩИЕ: Существует ли общая политика, возлагающая на правоохранительные органы и другие организации мандат по борьбе с терроризмом? СПЕЦИАЛЬНЫЕ: Рассматривается ли в политике использование технологий для борьбы с терроризмом?	ОБЩИЕ: Имеется ли подробный политический мандат для каждой контртеррористической организации? Охватывает ли политический мандат механизмы координации между правоохранительными органами и другими контртеррористическими организациями? Определяет ли политический мандат взаимодействие с неконтртеррористическими организациями в рамках ценностной цепочки контртеррористической деятельности? Подкреплен ли политический мандат достаточным бюджетом, охватывающим краткосрочный, среднесрочный и долгосрочный периоды? СПЕЦИАЛЬНЫЕ: Рассматриваются ли всесторонне в политике вопросы о деятельности по противодействию использованию новых технологий?	ОБЩИЕ: Имеется ли комплексный подход к определению институциональных функций и обязанностей в ценностной цепочке контртеррористической деятельности? Существуют ли четко определенные линии коммуникации и обязанности по обмену информацией между контртеррористическими организациями? Охватывает ли политика вопросы, связанные с координацией национального кризиса? Охватывает ли политика взаимодействия с контртеррористическими вспомогательными учреждениями? Осуществляется ли регулярный пересмотр политики, чтобы определить неохваченные участки в контртеррористических операциях? СПЕЦИАЛЬНЫЕ: Имеется ли четкий порядок действий между правоохранительными органами, учреждениями национальной безопасности и кибербезопасности при работе с киберинцидентами? Затрагивает ли координация политики вопросы совместного использования возможностей ИКТ или новых технологий, чтобы обеспечить объединение ресурсов для развития возможностей?	ОБЩИЕ: Легли ли в основу национальной политики национальное мероприятие или оперативное событие национального масштаба в части, касающейся институциональных обязанностей и координации? СПЕЦИАЛЬНЫЕ: Неприменимо
2.2.4	L3	**Управление ресурсами**	**Управление ресурсами отсутствует**	ОБЩИЕ: Имеется ли компетентный орган высокого уровня, который подотчетен высшему органу управления в вопросах управления ресурсами в рамках контртеррористической политики? Являются ли процедуры управления ресурсами разовыми или неофициальными? Имеются ли цели и задачи политики, которые служили бы руководством по управлению ресурсами? СПЕЦИАЛЬНЫЕ: Включена ли деятельность, связанная с новыми технологиями, в рамках контртеррористической ценностной цепочки в распределение национальных ресурсов для целей борьбы с терроризмом?	ОБЩИЕ: Должны ли контртеррористические учреждения принимать участие в разработке мер управления национальными контртеррористическими ресурсами, в том числе предоставлять информацию? Оказывает ли компетентный орган высокого уровня влияние на развитие и надзор в отношении управления национальными контртеррористическими ресурсами? Имеет ли высший государственный орган всеобъемлющий перечень для управления национальными ресурсами в целях борьбы с терроризмом? Определены ли правительством комплексная контртеррористическая политика и цели эффективности? СПЕЦИАЛЬНЫЕ: Имеет ли компетентный орган высокого уровня ресурсы и полномочия для сбора информации о ресурсах для новых технологий? Имеет ли высший орган управления всеобъемлющий перечень национальных контртеррористических потребностей, включающих новые технологии? Определены ли правительством политика использования новых технологий в контртеррористических целях и цели эффективности?	ОБЩИЕ: Утверждена ли высшим органом управления юридически обязательная письменная политика по управлению ресурсами? Имеются ли в контртеррористических организациях сотрудники по ресурсам, которые отчитываются перед органом высокого уровня по управлению ресурсами? Позволяет ли политика проведение независимой проверки использования ресурсов для контртеррористических мероприятий? Осуществляется ли регулярная оценка целей политики и целей эффективности в отношении использования контртеррористических ресурсов? Предусматривает ли управление ресурсами адаптацию с учетом производственной необходимости? СПЕЦИАЛЬНЫЕ: Включает ли политика управления ресурсами новые технологии борьбы с терроризмом? Входят ли в состав команды по управлению ресурсами технические специалисты? Осуществляется ли регулярная оценка используемых ресурсов на предмет контртеррористического использования новых технологий?	ОБЩИЕ: Действует ли управление ресурсами в течение краткосрочного, среднесрочного и долгосрочного периодов? Осуществляется ли независимый анализ управления национальными ресурсами? СПЕЦИАЛЬНЫЕ: Охватывает ли управление ресурсами вопросы, связанные с новыми технологиями, согласно современной глобальной политике?

2	L1	Политическое направление национальной контртеррористической деятельности	Нулевой	Базовый	Сформированный	Продвинутый	Высший
2.2.5	L3	**Управление сотрудничеством**	**Управление сотрудничеством отсутствует**	ОБЩИЕ: Является ли практика управления сотрудничеством разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Существует ли управление сотрудничеством с использованием новых технологий для борьбы с терроризмом?	ОБЩИЕ: Имеется ли комплексный подход к управлению сотрудничеством? Имеются ли специалисты по управлению сотрудничеством? Являются ли методы управления сотрудничеством структурированными, документированными и постоянными? Имеется ли регулярное взаимодействие правоохранительных органов с другими контртеррористическими организациями по обсуждению сотрудничества и координации? Охватывает ли политический мандат механизмы координации между правоохранительными органами и другими контртеррористическими организациями? Определяет ли политический мандат взаимодействие с неконтртеррористическими организациями в рамках ценностной цепочки контртеррористической деятельности? Имеется ли общая классификация для описания угроз и вмешательств, касающихся борьбы с терроризмом? Имеются ли оперативные возможности ситуационной осведомленности для управления оперативным сотрудничеством? Является ли подход структурированным, документированным и постоянным? Используются ли в качестве основы подхода оценки угроз? Служит ли подход руководством для деятельности в контртеррористической ценностной цепочке? СПЕЦИАЛЬНЫЕ: Рассматриваются ли всесторонне в политике вопросы о деятельности по противодействию использованию новых технологий?	ОБЩИЕ: Существуют ли четко определенные линии коммуникации и обязанности по обмену информацией между контртеррористическими организациями? Охватывает ли политика вопросы координации национального кризиса? Охватывает ли политика взаимодействия с контртеррористическими вспомогательными учреждениями? Осуществляется ли регулярный пересмотр политики, чтобы определить неохваченные участки в контртеррористических операциях? СПЕЦИАЛЬНЫЕ: Имеется ли четкий порядок действий между правоохранительными органами, учреждениями национальной безопасности и кибербезопасности при работе с киберинцидентами? Затрагивает ли координация политики вопросы совместного использования возможностей ИКТ или новых технологий, чтобы обеспечить объединение ресурсов для развития возможностей?	ОБЩИЕ: Легли ли в основу национальной политики национальное мероприятие или оперативное событие национального масштаба в части, касающейся управления сотрудничеством? Осуществляется ли независимая оценка эффективности управления сотрудничеством? СПЕЦИАЛЬНЫЕ: Неприменимо

2	L1	Политическое направление национальной контртеррористической деятельности	Нулевой	Базовый	Сформированный	Продвинутый	Высший
2.3	**L2**	**Управление эффективностью политики**					
2.3.1	L3	**Критерии эффективности политики**	**Критерии эффективности политики отсутствуют**	**ОБЩИЕ:** Имеется ли процедура или практика оценки эффективности? Является ли практика управления эффективностью разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к управлению эффективностью? Имеются ли специалисты по управлению эффективностью? Являются ли методы управления эффективности структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеются ли управление эффективностью или план, которые приведены в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел или координатор по вопросам управления эффективностью? Являются ли показатели эффективности четко определенными, измеримыми и контролируемыми? Осуществляется ли регулярный анализ и аудит деятельности по управлению эффективностью? Имеются ли стандарты и требования, касающиеся управления эффективностью? **СПЕЦИАЛЬНЫЕ:** Имеются ли конкретные целевые показатели эффективности оперативных средств контроля в отношении обмена информацией, данных, технологий, прав человека и гендерных аспектов?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов управления эффективностью на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты отчетов по эффективности в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит методов управления эффективностью независимым органом? Отражает ли практика управления эффективностью международные стандарты, руководящие указания и практический опыт? **СПЕЦИАЛЬНЫЕ:** Включает ли управление эффективностью целевые показатели и контроль показателей эффективности, связанных с обменом информацией и данными, технологиями, правами человека и гендерными аспектами?
2.3.2	L3	**Оценка влияния политики**	**Оценка влияния политики отсутствует**	**ОБЩИЕ:** Является ли оценка влияния разовой или неофициальной? Четко ли определены цели контртеррористической политики? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к оценке влияния? Являются ли методы оценки влияния структурированными, документированными и постоянными? Четко ли сформулированы цели контртеррористической политики, чтобы имелась возможность оценки влияния? Осуществляется ли оценка и контроль эффективности политики в сравнении с конкретными показателями эффективности? Обеспечена ли деятельность по оценке влияния надлежащими ресурсами? Имеется ли матрица влияния для обеспечения поддержки оценки влияния? **СПЕЦИАЛЬНЫЕ:** Охватывает ли деятельность по оценке влияния мероприятия правоохранительных органов по противодействию использованию новых технологий в террористических целях? Охватывает ли деятельность по оценке влияния использование новых технологий правоохранительными органами?	**ОБЩИЕ:** Используются ли в качестве основы для оценки влияния исследования, оперативные данные и анализ? Используются ли в качестве основы для оценки влияния всесторонние консультации с государственными контртеррористическими организациями? Есть ли специальный отдел по оценке влияния политики с достаточными ресурсами и полномочиями? **СПЕЦИАЛЬНЫЕ:** Предоставляется ли поддержка технического специалиста в вопросах, связанных с новыми технологиями, в рамках оценки влияния политики?	**ОБЩИЕ:** Осуществляется ли анализ и обновление процесса измерения оценки влияния на регулярной основе в целях постоянного совершенствования? Имеется ли консультативный орган по вопросам управления оценкой влияния, в состав которого входят сторонние эксперты, например, из отрасли, других государственных органов и т. д.? **СПЕЦИАЛЬНЫЕ:** Предоставляется ли поддержка независимого технического специалиста в вопросах, связанных с новыми технологиями, в рамках оценки влияния политики?

2	L1	Политическое направление национальной контртеррористической деятельности	Нулевой	Базовый	Сформированный	Продвинутый	Высший
2.3.3	L3	**Управление пересмотром политики**	**Управление пересмотром политики отсутствует**	**ОБЩИЕ:** Является ли пересмотр политики разовым или неофициальным? Четко ли определены цели контртеррористической политики? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к пересмотру целей и мер контртеррористической политики? Являются ли методы управления пересмотром политики структурированными, документированными и постоянными? Четко ли сформулированы цели контртеррористической политики, чтобы имелась возможность пересмотра политики? Обеспечена ли деятельность по пересмотру политики надлежащими ресурсами? Обеспечивается ли процесс пересмотра политики поддержкой требований к отчетности? **СПЕЦИАЛЬНЫЕ:** Охватывает ли деятельность по пересмотру политики мероприятия по противодействию использованию новых технологий в террористических целях? Охватывает ли деятельность по пересмотру политики использование новых технологий правоохранительными органами?	**ОБЩИЕ:** Используются ли в качестве основы для пересмотра политики исследования, оперативные данные и анализ? Используются ли в качестве основы для пересмотра политики всесторонние консультации с государственными контртеррористическими организациями? Есть ли специальный отдел по оценке политики с надлежащим обеспечением ресурсами? **СПЕЦИАЛЬНЫЕ:** Основывается ли пересмотр политики на новых технологических тенденциях? Осуществляется ли пересмотр политики при поддержке компетентного технического специалиста?	**ОБЩИЕ:** Осуществляется ли анализ и обновление процесса пересмотра политики на регулярной основе в целях постоянного совершенствования? Имеется ли консультативный орган по вопросам пересмотра политики, в состав которого входят сторонние эксперты, например, из отрасли, других государственных органов и т. д.? **СПЕЦИАЛЬНЫЕ:** Неприменимо
2.4	**L2**	**Управление информационным обеспечением политики**					
2.4.1	L3	**Стратегическая коммуникация**	**Стратегическая коммуникация отсутствует**	**ОБЩИЕ:** Является ли практика коммуникации разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к стратегической коммуникации? Имеются ли специалисты по коммуникациям с общественностью/сообществом? Являются ли методы коммуникации структурированными, документированными и постоянными? Определены ли четкие цели информационной политики? Разъясняются ли в информационной политике сложности правоохранительных органов в борьбе с терроризмом и необходимые контртеррористические действия? **СПЕЦИАЛЬНЫЕ:** Повышает ли информационная политика осведомленность об использовании новых технологий в террористических целях? Имеется ли специальное общедоступное контактное лицо для сообщений со стороны общественности о рисках или угрозах, связанных с использованием новых технологий для борьбы с терроризмом? Используют ли правоохранительные органы социальные сети для информационного обеспечения и взаимодействия с общественностью? Разъясняются ли в информационной политике сложности правоохранительных органов в противодействии использованию новых технологий в террористических целях и необходимые контртеррористические действия? Рассматривает ли информационная политика вопросы сотрудничества государственного и частного секторов?	**ОБЩИЕ:** Приведена ли информационная политика в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел по связям с общественностью? Осуществляется ли оценка и контроль эффективности целей политики в области коммуникаций с общественностью в сравнении с конкретными показателями эффективности? Осуществляется ли регулярный анализ и аудит коммуникаций с общественностью? Имеются ли стандарты и требования, касающиеся коммуникаций с общественностью? Рассматриваются ли в информационной политике оценки воздействия на гендерные аспекты и права человека? **СПЕЦИАЛЬНЫЕ:** Было ли проведено исследование об использовании населением новых технологий? Приведена ли политика взаимодействия правоохранительных органов с общественностью в соответствие с политикой взаимодействия в области кибербезопасности? Приведена ли информационная политика в соответствие с обязательствами по обеспечению прозрачности и передовым опытом относительно использования новых технологий?	**ОБЩИЕ:** Осуществляется ли анализ и обновление информационной политики на регулярной основе в целях постоянного совершенствования? Поддерживается ли политикой раскрытие информации о правоохранительных органах в тех случаях, когда это необходимо в интересах общества? Включает ли политика информирование о внутренних анализах и аудитах контртеррористической деятельности и операций правоохранительных органов в тех случаях, когда это необходимо в интересах общества? Было ли проведено исследование уровня общественного доверия правоохранительным органам? Были ли доведены результаты исследования уровня общественного доверия до сведения руководства правоохранительных органов? **СПЕЦИАЛЬНЫЕ:** Поддерживает ли политика публикацию внутренних анализов и аудитов, касающихся использования технологий, прав человека и гендерных аспектов, в тех случаях, когда это необходимо в интересах общества?

2	L1	Политическое направление национальной контртеррористической деятельности	Нулевой	Базовый	Сформированный	Продвинутый	Высший
2.5	**L2**	**Сотрудничество государственного и частного секторов**					
2.5.1	L3	**Сотрудничество государственного и частного секторов**	**Сотрудничество государственного и частного секторов отсутствует**	**ОБЩИЕ:** Рассматривает ли политика вопросы сотрудничества государственного и частного секторов? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Рассматриваются ли в политике вопросы сотрудничества государственного и частного секторов всесторонне? Должны ли правоохранительные органы сообщать об инициативах по сотрудничеству между государственным и частным секторами? Являются ли методы международного сотрудничества государственного и частного секторов структурированными, документированными и постоянными? Имеется ли внутренняя политика для прав и ограничений в отношении функций, касающихся отношений государственного и частного секторов? **СПЕЦИАЛЬНЫЕ:** Существуют ли партнерские отношения и сотрудничество с частными ИКТ-компаниями? Имеются ли стандартные процедуры и формы сотрудничества в отношении новых технологий?	**ОБЩИЕ:** Регулярно ли проводятся встречи с заинтересованными сторонами в рамках общей стратегии и приоритетов организации? Осуществляется ли оценка и контроль эффективности взаимодействия с заинтересованными сторонами в сравнении с конкретными показателями? Сообщаются ли правоохранительными органами руководящие принципы взаимодействия с заинтересованными сторонами частному сектору? **СПЕЦИАЛЬНЫЕ:** Охватывает ли политика консультации с глобальными ИКТ-компаниями? Имеется ли стратегия развития партнерства с частными ИКТ-компаниями? Могут ли ИКТ-компании заблаговременно стараться устранять новые угрозы и проблемы, связанные с использованием технологий?	**ОБЩИЕ:** Имеется ли план сотрудничества государственного и частного секторов? Обсуждаются ли важные меры политики на совещаниях по сотрудничеству государственного и частного секторов? **СПЕЦИАЛЬНЫЕ:** Проводятся ли регулярно консультации с технологическими компаниями в процессе разработки политики? Поощряет ли политика стратегическое сотрудничество и партнерство с частными ИКТ-компаниями?
2.5.2	L3	**Консультации заинтересованных сторон**	**Консультации заинтересованных сторон отсутствуют**	**ОБЩИЕ:** Являются ли консультации с заинтересованными сторонами разовыми или неофициальными? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход в отношении консультаций с заинтересованными сторонами? Имеются ли специалисты по проведению консультаций с заинтересованными сторонами? Являются ли консультации с заинтересованными сторонами структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Включены ли ИКТ-компании в политику консультаций с заинтересованными сторонами? Имеют ли правоохранительные органы перечень основных заинтересованных лиц в области ИКТ, которые имеют значение для контртеррористической деятельности правоохранительных органов в отношении новых технологий? Имеют ли ИКТ-компании четко определенное контактное лицо для обмена сведениями, касающимися политики?	**ОБЩИЕ:** Регулярно ли проводятся встречи с заинтересованными сторонами в рамках общей стратегии и приоритетов организации? Осуществляется ли оценка и контроль эффективности взаимодействия с заинтересованными сторонами в сравнении с конкретными показателями? Сообщаются ли правоохранительными органами руководящие принципы взаимодействия с заинтересованными сторонами частному сектору? **СПЕЦИАЛЬНЫЕ:** Охватывает ли политика консультации с глобальными ИКТ-компаниями? Имеется ли стратегия развития партнерства с частными ИКТ-компаниями? Могут ли ИКТ-компании заблаговременно стараться устранять новые угрозы и проблемы, связанные с использованием технологий?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующей практики консультаций с заинтересованными сторонами на регулярной основе в целях постоянного совершенствования? **СПЕЦИАЛЬНЫЕ:** Принимают ли участие крупнейшие в мире технические заинтересованные стороны в регулярных дискуссиях?

2	L1	Политическое направление национальной контртеррористической деятельности	Нулевой	Базовый	Сформированный	Продвинутый	Высший
2.6	**L2**	**Национальные контртеррористические элементы**					
2.6.1	L3	**Национальная классификация инцидентов**	**Национальная классификация инцидентов отсутствует**	**ОБЩИЕ:** Есть ли государственное учреждение, имеющее полномочия классифицировать инцидент как национальный? Являются ли методы классификации национальных инцидентов разовыми или неофициальными? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к классификации инцидентов? Имеются ли всеобъемлющие механизмы предоставления отчетности, позволяющие классифицировать инциденты? Имеется ли организация национального уровня, которой поручена разработка национальной системы классификации инцидентов? Существует ли общая национальная классификация инцидентов для контртеррористических организаций и деятельности? Доводится ли национальная система классификации до сведения всех государственных организаций? Четко ли в политике определено лицо, которое может объявить о национальном инциденте? Позволяет ли национальная классификация инцидентов определить орган, ответственный за событие? **СПЕЦИАЛЬНЫЕ:** Включает ли национальная система классификации инциденты, которые произошли в результате злонамеренного использования новых технологий?	**ОБЩИЕ:** Основана ли национальная система классификации инцидентов на текущих национальных обзорах для определения критически важных функций? Предоставляется ли информация органами государственного регулирования, отвечающими за важные сервисы, в качестве ориентира для системы классификации? Приведена ли национальная система классификации в соответствие с общей стратегией и приоритетами? Осуществляется ли регулярный пересмотр пороговых значений национальной системы классификации инцидентов? Является ли национальная система классификации обязательной для всех государственных организаций? **СПЕЦИАЛЬНЫЕ:** Составляет ли основу национальной системы классификации оперативная информация о возможном злоупотреблении новыми технологиями?	**ОБЩИЕ:** Осуществляется ли анализ и обновление национальной системы классификации на регулярной основе в целях постоянного совершенствования? Используются ли в качестве основы национальной системы классификации мероприятие или устранение инцидента национального уровня? **СПЕЦИАЛЬНЫЕ:** Неприменимо
2.6.2	L3	**Международная координация**	**Международная координация отсутствует**	**ОБЩИЕ:** Является ли практика международной координации разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к международному сотрудничеству среди всех контртеррористических организаций? Имеются ли специалисты по международной координации? Являются ли методы международной координации структурированными, документированными и постоянными? Осуществляется ли обмен информацией о международном сотрудничестве между контртеррористическими организациями? **СПЕЦИАЛЬНЫЕ:** Охватывает ли политика надежные связи с другими правоохранительными органами? Включает ли политика программу присоединения к соглашениям, которые применяются к трансграничному сотрудничеству в рамках ценностной цепочки контртеррористической деятельности с использованием новых технологий? Включает ли политика участие правоохранительных органов в надежной круглосуточной сети в области киберпреступности (например, Интерпол)? Поощряет ли политика обмен информацией контртеррористическими организациями на тактическом уровне?	**ОБЩИЕ:** Имеются ли план по международному сотрудничеству и методы, которые приведены в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел международного сотрудничества? Осуществляется ли оценка и контроль эффективности международного сотрудничества в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит деятельности по международному сотрудничеству? Имеются ли стандарты и требования, касающиеся международного сотрудничества? **СПЕЦИАЛЬНЫЕ:** Определяет ли политика средства контроля международного сотрудничества в отношении обмена информацией и использования технологий, касающихся вопросов прав человека и гендерных аспектов, а также принципов верховенства права? Поощряет ли политика регулярное участие правоохранительных органов в международных дискуссиях, посвященных борьбе с терроризмом и новым технологиям?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов международного сотрудничества на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты международного сотрудничества в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит методов международного сотрудничества независимым органом? Разрабатывается ли политика посредством регулярного взаимодействия с неправительственными заинтересованными сторонами в других странах, которые имеют важное значение для контртеррористических операций? **СПЕЦИАЛЬНЫЕ:** Поощряет ли политика участие государства-члена в международных дискуссиях, посвященных борьбе с терроризмом и новым технологиям (например, руководство международной целевой группой, выполнение функций председателя комитета в международной организации, проведение международной/региональной конференции)? Взаимодействует ли государство-член на регулярной основе с неправительственными заинтересованными сторонами в других странах, использующими новые технологии, которые имеют важное значение для контртеррористических операций?

5.8 Модель зрелости возможностей: институциональное направление

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.1	**L2**	**Стратегическое планирование и управление эффективностью**					
3.1.1	L3	**Национальный план действий**	**Национальный план действий отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы национального плана действий (НПД) в обязательной политике? Является ли разработка НПД разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли Национальный план действий (НПД)? Являются ли методы разработки НПД структурированными, документированными и постоянными? Имеются ли специалисты по разработке НПД? Четко ли в НПД установлены и распределены функции и обязанности в отношении ключевых приоритетов и действий? Осуществляется ли рассмотрение, принятие и утверждение НПД министерским органом в официальном порядке? **СПЕЦИАЛЬНЫЕ:** Рассматриваются ли в НПД какие-либо аспекты новых технологий, прав человека и гендера? Рассматриваются ли в НПД уникальные технологические характеристики и особенности обеспечения безопасности государства-члена?	**ОБЩИЕ:** Приведен ли НПД в полное соответствие с Глобальной контртеррористической стратегией Организации Объединенных Наций? Координируется ли разработка НПД централизованно с участием координатора? Осуществляется ли оценка и контроль эффективности НПД в сравнении с конкретными показателями эффективности? Распространяется ли НПД на все контртеррористические организации? Распространяется ли НПД на все вспомогательные организации? Публикуется ли общедоступная отредактированная версия НПД? **СПЕЦИАЛЬНЫЕ:** Включает ли НПД специальное управление для обучения новым технологиям? Рассматриваются ли в НПД новые технологии, права человека и гендер комплексно?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов разработки НПД на регулярной основе в целях постоянного совершенствования? **СПЕЦИАЛЬНЫЕ:** Отражены ли в НПД не имеющие обязательной силы передовой опыт и международные стандарты, руководства и методы, связанные с правами человека, гендерными аспектами, защитой данных, управлением, управлением эффективностью деятельности и принципами верховенства права?
3.1.2	L3	**Оперативный план и бюджет**	**Оперативный план и бюджет отсутствуют**	**ОБЩИЕ:** Имеются ли какие-либо элементы оперативного плана в обязательном плане? Является ли разработка оперативного плана и бюджета разовой или неофициальной? Включены элементы оперативного плана в ежегодный бюджет? Были ли какие-либо аспекты оперативного плана согласованы с соответствующими государственными учреждениями? **СПЕЦИАЛЬНЫЕ:** Отражены ли в оперативных планах приоритеты по наращиванию потенциала, связанного с новыми технологиями?	**ОБЩИЕ:** Имеется ли годовой оперативный план? Имеются ли специалисты по оперативному планированию? Являются ли методы разработки оперативного плана структурированными, документированными и постоянными? Имеется ли запланированный годовой бюджет, выделенный на реализацию оперативного плана? Был ли оперативный план частично согласован с другими государственными учреждениями? **СПЕЦИАЛЬНЫЕ:** Используется ли в качестве основы для оперативных планов в части, касающейся наращивания потенциала, связанного с новыми технологиями, опыт правоохранительных органов в сфере противодействия терроризму? Принимает ли участие в разработке оперативного плана и бюджета технический специалист?	**ОБЩИЕ:** Приведены ли оперативный план и бюджет в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел или координатор по вопросам оперативного планирования? Осуществляется ли оценка и контроль эффективности оперативного плана в сравнении с конкретными показателями? Осуществляется ли пересмотр годового бюджета в течение финансового года и корректируется ли он в соответствии с оперативными потребностями? Был ли оперативный план согласован с другими государственными учреждениями? **СПЕЦИАЛЬНЫЕ:** Используются ли в качестве основы для оперативных планов в части, касающейся наращивания потенциала, связанного с новыми технологиями, исследования, оперативные данные и анализ?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов оперативного планирования на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты оперативных планов и отчетов в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит оперативных планов и бюджетов независимым органом? **СПЕЦИАЛЬНЫЕ:** Отражены ли в оперативных планах приоритеты, связанные с правами человека, гендерными аспектами и принципами верховенства права? Имеется ли штатный технический специалист, оказывающий экспертную поддержку в отношении новых технологий при планировании и составлении бюджета?

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.1.3	L3	**Управление эффективностью**	**Управление эффективностью отсутствует**	ОБЩИЕ: Имеются ли какие-либо элементы определения управления эффективностью? Имеется ли процедура или практика оценки эффективности? Является ли практика управления эффективностью разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется ли комплексный подход к управлению эффективностью? Имеются ли специалисты по управлению эффективностью? Являются ли методы управления эффективности структурированными, документированными и постоянными? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеются ли управление эффективностью или план, которые приведены в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел или координатор по вопросам управления эффективностью? Являются ли показатели эффективности четко определенными, измеримыми и контролируемыми? Осуществляется ли регулярный анализ и аудит деятельности по управлению эффективностью? Имеются ли стандарты и требования, касающиеся управления эффективностью? СПЕЦИАЛЬНЫЕ: Имеются ли конкретные целевые показатели эффективности оперативных гарантий в отношении обмена информацией, данных, технологий, прав человека и гендерных аспектов?	ОБЩИЕ: Осуществляется ли анализ и обновление соответствующих методов управления эффективностью на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты отчетов по управлению эффективностью в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит методов управления эффективностью независимым органом? Отражает ли практика управления эффективностью международные стандарты, руководящие указания и практический опыт? СПЕЦИАЛЬНЫЕ: Включает ли управление эффективностью целевые показатели и контроль показателей эффективности, связанных с обменом информацией и данными, технологиями, правами человека и гендерными аспектами?
3.2	**L2**	**Управление**					
3.2.1	L3	**Модель управления**	**Модель управления и структура отсутствуют**	ОБЩИЕ: Имеются ли какие-либо элементы управления и структуры? Является ли практика управления разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется ли комплексный подход к управлению? Являются ли методы управления структурированными, документированными и постоянными? Четко ли определены в управлении внутренние взаимодействия, линии коммуникации и порядок подчиненности между структурными подразделениями организации? СПЕЦИАЛЬНЫЕ: Предусматривает ли практика управления какие-либо элементы надзора за использованием новых технологий, правами человека, гендерными аспектами, принципами верховенства права и соблюдением требований?	ОБЩИЕ: Имеется ли модель управления, которая приведена в соответствие с общей стратегией и приоритетами организации? Имеется ли официальная модель и структура управления, включающая в себя управление рисками и соблюдение нормативных требований? Осуществляется ли оценка и контроль эффективности методов управления в сравнении с конкретными показателями эффективности? Имеется ли четкое делегирование полномочий и распределение функций и обязанностей для принятия решений? СПЕЦИАЛЬНЫЕ: Обеспечивает ли практика управления всесторонний надзор за оперативным использованием новых технологий? Обеспечивает ли практика управления всесторонний надзор в отношении вопросов, связанных с новыми технологиями, правами человека, гендерными аспектами, принципами верховенства права и соблюдением требований? Имеется ли независимый орган, который анализирует практику использования новых технологий и ее возможные последствия для прав человека, принципов верховенства права и соблюдения нормативных требований?	ОБЩИЕ: Осуществляется ли анализ и обновление соответствующих методов управления на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты решений и отчетов в области управления в тех случаях, когда это необходимо в интересах общества? Имеется ли консультативный орган по вопросам управления, в состав которого входят сторонние эксперты, например, из отрасли, других государственных органов и т. д.? Отражает ли практика управления международные стандарты, руководящие указания и практический опыт? СПЕЦИАЛЬНЫЕ: Включают ли гарантии управления и принятие решений обмен информацией, использование данных и новых технологий, права человека, соображения по поводу гендерного равенства, а также принципы верховенства права, которые отражают международные руководящие указания и опыт?

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.2.2	L3	**Управление рисками**	**Потенциал для управления рисками отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы процессов управления рисками? Является ли практика управления рисками разовой или неофициальной или применяется к организации лишь частично? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к управлению рисками? Имеются ли специалисты по управлению рисками? Являются ли методы управления рисками структурированными, документированными и постоянными? Имеется ли всеобъемлющая политика в отношении рисков, действие которой распространяется на всю организацию? Включает ли политика пересмотр справочника рисков? **СПЕЦИАЛЬНЫЕ:** Охватывает ли управление рисками какие-либо элементы риска, связанные с правами человека, гендерными аспектами и использованием новых технологий?	**ОБЩИЕ:** Имеются ли стратегия или план управления рисками, которые приведены в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел по рискам? Осуществляется ли оценка и контроль эффективности управления рисками в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит деятельности по управлению рисками? Имеются ли стандарты и требования, касающиеся управления рисками? Доходят ли национальные риски по ступенчатой схеме до уровня оперативных рисков и назначается ли ведущий орган, ответственный за риск? **СПЕЦИАЛЬНЫЕ:** Используется ли практический опыт управления рисками в качестве основы для специальных мер по устранению рисков в отношении обмена информацией, использования данных и новых технологий, прав человека и гендерных аспектов, а также правовых требований?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов управления рисками на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты отчетов по оценке рисков? Осуществляется ли регулярный анализ и аудит методов управления рисками независимым органом? Отражает ли практика управления рисками международные стандарты, руководящие указания и практический опыт (например, ISO 31000)? **СПЕЦИАЛЬНЫЕ:** Включает ли управление рисками соответствующие аспекты обмена информацией, использования данных и новых технологий, прав человека и гендерной проблематики, а также правовых требований?
3.2.3	L3	**Соблюдение требований**	**Соблюдение требований отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы механизма и процесса обеспечения соблюдения требований? Является ли практика обеспечения соблюдения требований разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к обеспечению соблюдения требований? Имеются ли специалисты по обеспечению соблюдения требований? Являются ли методы обеспечения соблюдения требований структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Охватывает ли практика по обеспечению соблюдения требований какие-либо элементы использования новых технологий, прав человека и гендерных аспектов в соответствии с национальными требованиями?	**ОБЩИЕ:** Имеется ли план по обеспечению соблюдения требований, который приведен в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел по обеспечению соблюдения требований? Осуществляется ли оценка и контроль эффективности соблюдения требований в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит деятельности по обеспечению соблюдения требований? Имеются ли стандарты и требования, касающиеся обеспечения соблюдения требований? **СПЕЦИАЛЬНЫЕ:** Имеются ли гарантии соблюдения требований в рамках контртеррористической деятельности правоохранительных органов в отношении обмена информацией и использования технологий, связанных с правами человека и гендерными аспектами, а также принципами верховенства права?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов обеспечения соблюдения требований на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты отчетов по соблюдению требований? Осуществляется ли регулярный анализ и аудит методов обеспечения соблюдения требований независимым органом? Отражены ли в практике по обеспечению соблюдения требований международные руководящие указания и опыт? **СПЕЦИАЛЬНЫЕ:** Включают ли гарантии управления и принятие решений обмен информацией, использование данных и новых технологий, права человека и гендерные аспекты, а также принципы верховенства права, которые отражают международные руководящие указания и опыт?

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.2.4	L3	**Оценка воздействия на гендерные аспекты и права человека**	**Возможность оценки воздействия на гендерные аспекты и права человека отсутствует**	ОБЩИЕ: Имеются ли какие-либо элементы практики проведения оценки воздействия на гендерные аспекты и права человека? Является ли практика оценки воздействия на гендерные аспекты и права человека разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется комплексный подход к оценке воздействия на гендерные аспекты и права человека? Имеются специалисты по оценке воздействия на гендерные аспекты и права человека? Являются ли методы оценки воздействия на гендерные аспекты и права человека структурированными, документированными и постоянными? Имеется ли политика оценки воздействия на гендерные аспекты и права человека, включающая четкие пороговые значения, методы оценки и меры по смягчению последствий? СПЕЦИАЛЬНЫЕ: Включают ли оценки воздействия на гендерные аспекты и права человека использование технологий?	ОБЩИЕ: Имеется ли план по правам человека и гендерным аспектам, который приведен в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел по правам человека и гендерным аспектам, который подотчетен высшему руководству? Осуществляется ли оценка и контроль эффективности воздействия на гендерные аспекты и права человека в сравнении с конкретными показателями? Оказывают ли оценки воздействия на гендерные аспекты и права человека влияние на оперативную деятельность и принятие решений? Осуществляется ли регулярная проверка и аудит деятельности, связанной с воздействием на гендерные аспекты и права человека? Имеются ли стандарты и требования, касающиеся прав человека и гендерных аспектов? Согласованы ли права человека и гендерные аспекты со службой защиты данных? СПЕЦИАЛЬНЫЕ: Используются ли в качестве основы оперативной работы анализы воздействия на права человека и гендерные аспекты? Имеются ли гарантии учета прав человека и гендерных аспектов в рамках контртеррористической деятельности правоохранительных органов в отношении обмена информацией и использования технологий, а также принципа верховенства права? Внедрены ли оценки воздействия в процессы закупки новых технологий и служат ли они основой для закупок и развития использования новых технологий?	ОБЩИЕ: Отражают ли меры в области прав человека и гендерной проблематики международные стандарты, руководящие указания и практический опыт? Используются ли соответствующие права человека и гендерная практика в качестве основы для деятельности и влияния на принятие решений? Осуществляется ли анализ и обновление практического опыта в области прав человека и гендерных аспектов на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты отчетов, касающихся прав человека и гендерных аспектов? Осуществляется ли регулярный анализ и аудит практического опыта в области прав человека и гендерных аспектов независимым органом? Имеется ли консультативный комитет по правам человека для поддержки бюро по правам человека, состоящего из соответствующих правительственных и неправительственных заинтересованных сторон? Достаточно ли выделено кадровых и финансовых ресурсов для проведения оценок воздействия на гендерные аспекты и права человека? СПЕЦИАЛЬНЫЕ: Предоставляют ли отделы по правам человека и гендерным вопросам данные для процессов в рамках политики, касающихся использования технологий и их воздействия на права человека и гендерные аспекты?

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.2.5	L3	**Защита данных**	**Возможность защиты данных отсутствует**	ОБЩИЕ: Имеются ли какие-либо элементы практики защиты данных? Является ли практика обеспечения защиты данных разовой или неофициальной? Учитывают ли правоохранительные органы принципы защиты данных при осуществлении деятельности? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется ли комплексный подход к защите данных? Имеются ли специалисты по защите данных? Являются ли методы защиты данных структурированными, документированными и постоянными? Назначен ли сотрудник по защите данных с четкими организационными полномочиями? СПЕЦИАЛЬНЫЕ: Используется ли политика защиты данных в качестве основы для деятельности и использования новых технологий и данных, прав человека и гендерных аспектов в соответствии с национальными требованиями? Имеются ли специальные методы защиты данных и конфиденциальности для контртеррористической разведки и расследований?	ОБЩИЕ: Имеются ли стратегия или план по защите данных, которые приведены в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел по защите данных, который подотчетен высшему руководству? Осуществляется ли оценка и контроль эффективности защиты данных в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит деятельности по защите данных? Имеются ли стандарты и требования по защите данных внутри организации? Пройдено ли руководителями обучение по защите данных? СПЕЦИАЛЬНЫЕ: Имеются ли гарантии защиты данных в рамках контртеррористической деятельности правоохранительных органов в отношении обмена информацией и использования технологий, прав человека и гендерных аспектов, а также принципов верховенства права? Имеется ли общая политика, требующая оценки воздействия на неприкосновенность частной жизни при внедрении новых технологий? Внедрены ли оценки воздействия на неприкосновенность частной жизни в процессы закупки новых технологий и служат ли они основой для закупок и развития использования новых технологий?	ОБЩИЕ: Осуществляется ли анализ и обновление соответствующих методов защиты данных на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты отчетов по защите данных? Осуществляется ли регулярный анализ и аудит методов защиты данных независимым органом? Отражены ли в мерах защиты данных международные руководящие указания и опыт? Проводит ли служба защиты данных консультации по вопросам государственной политики в отношении возможностей правоохранительных органов, влияющих на неприкосновенность частной жизни? Внедрили ли организации обучение по защите данных? СПЕЦИАЛЬНЫЕ: Осуществляется ли регулярный анализ и аудит методов защиты данных независимым органом особенно по вопросам использования технологий, данных, прав человека и гендера? Публикует ли служба защиты данных отредактированную информацию о проведенных оценках воздействия на неприкосновенность частной жизни?

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.3	**L2**	**Управление выполнением задач и координация деятельности**					
3.3.1	L3	**Сканирование горизонта**	**Возможность сканирования горизонта отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы возможности сканирования горизонта и считаются ли они действующими? Является ли практика сканирования горизонта разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к сканированию горизонта? Являются ли методы сканирования горизонта структурированными, документированными и постоянными? Имеются ли специалисты по сканированию горизонта? Планируется ли и осуществляется ли деятельность по сканированию горизонта через регулярные промежутки времени (например, ежегодно, каждые 4 года и т. д.)? **СПЕЦИАЛЬНЫЕ:** Способна ли группа по сканированию горизонта составлять прогнозы относительно использования новых технологий террористами?	**ОБЩИЕ** Имеется ли план по сканированию горизонта, который приведен в соответствие с общей стратегией и приоритетами организации? Включена ли эта тема в национальный план действий? Имеется ли специальный отдел по сканированию горизонта? Осуществляется ли оценка и контроль эффективности сканирования горизонта в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит деятельности по сканированию горизонта? Имеются ли стандарты и требования, касающиеся управления угрозами? Используются ли выводы и результаты сканирования горизонта в качестве основы для стратегической и долгосрочной национальной политики и развития возможностей? Проводятся ли в рамках практики сканирования горизонта консультации и привлечение широкого круга заинтересованных сторон из отрасли, правительства, гражданского общества, научных кругов и т. д.? **СПЕЦИАЛЬНЫЕ:** Имеются ли гарантии учета прав человека, гендерных аспектов и принципа верховенства права в рамках сканирования горизонта в отношении обмена информацией и использования технологий?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов сканирования горизонта на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты сканирования горизонта в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит методов сканирования горизонта независимым органом? Осуществляется ли координация деятельности по сканированию горизонта с союзниками? **СПЕЦИАЛЬНЫЕ:** Осуществляется ли регулярный анализ и аудит методов сканирования горизонта независимым органом особенно по вопросам использования технологий, прав человека и гендерных аспектов?

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.3.2	L3	**Управление угрозами**	**Возможность управления угрозами отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы процесса управления угрозами? Является ли практика управления угрозами разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к управлению угрозами? Имеются ли специалисты по управлению угрозами? Являются ли методы управления угрозами структурированными, документированными и постоянными? Согласовываются ли мероприятия по управлению рисками с другими национальными организациями в сфере безопасности? **СПЕЦИАЛЬНЫЕ:** Охватывают ли методы управления угрозами риск, связанный с новыми технологиями, для критически важных социальных и правительственных мероприятий? Охватывает ли деятельность по управлению угрозами использование новых технологий в контртеррористических целях?	**ОБЩИЕ:** Имеются ли план по управлению угрозами и методы, которые приведены в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел управления угрозами? Осуществляется ли оценка и контроль эффективности управления угрозами в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит деятельности по управлению угрозами? Имеются ли стандарты и требования, касающиеся управления угрозами? Имеются ли договоры и соглашения об управлении угрозами, позволяющие обмениваться информацией с международными партнерами? **СПЕЦИАЛЬНЫЕ:** Включает ли управление угрозами соответствующие соображения по поводу прав человека, гендерных аспектов и принципов верховенства права? Имеются ли в штате отдела управления угрозами технические специалисты? Имеет ли отдел управления угрозами рабочие взаимоотношения с поставщиками новых технологий? Имеет ли отдел управления угрозами рабочие взаимоотношения с гражданскими органами власти для оценки критических процессов и уязвимостей гражданского сектора?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов управления угрозами на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты управления угрозами в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит методов управления угрозами независимым органом? Осуществляется ли координация деятельности по управлению угрозами с союзниками? **СПЕЦИАЛЬНЫЕ:** Осуществляется ли регулярный анализ и аудит методов управления угрозами независимым органом особенно по вопросам использования технологий, прав человека и гендера?

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.3.3	L3	**Обмен информацией**	**Возможность обмена информацией отсутствует**	ОБЩИЕ: Имеются ли какие-либо элементы процесса обмена информацией? Является ли деятельность по обмену информацией разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется ли комплексный подход к обмену информацией? Являются ли методы обмена информацией структурированными, документированными и постоянными? Имеется ли надежная техническая инфраструктура для обмена информацией? Имеется ли система классификации информации и определения приоритетности для упрощения обмена информацией? СПЕЦИАЛЬНЫЕ: Имеется ли безопасная техническая инфраструктура для обмена техническими показателями и информацией, которые касаются рисков, связанными с новыми технологиями, и мер по их уменьшению? Имеются ли соглашения об обмене информации с поставщиками новых технологий?	ОБЩИЕ: Имеются ли план по обмену информацией и методы, которые приведены в соответствие с общей стратегией и приоритетами организации? Имеются ли договоры и соглашения об обмене информации, позволяющие обмениваться информацией с международными партнерами? Есть ли специальный отдел по обмену информацией? Осуществляется ли оценка и контроль эффективности обмена информации в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит деятельности по обмену информацией? Имеются ли стандарты и требования, касающиеся обмена информацией? Согласованы ли договоренности об обмене информацией с другими мероприятиями по обмену информацией (например, обмен информацией с национальной группой реагирования на инциденты в сфере компьютерной безопасности (CSIRT))? СПЕЦИАЛЬНЫЕ: Имеются ли гарантии учета прав человека, гендерных аспектов и принципа верховенства права в рамках обмена информации в отношении обмена информацией и использования технологий, связанного с правами человека, гендерными аспектами и принципами верховенства права?	ОБЩИЕ: Осуществляется ли анализ и обновление соответствующих методов обмена информацией на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты обмена информацией в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит методов обмена информацией независимым органом? СПЕЦИАЛЬНЫЕ: Осуществляется ли регулярный анализ и аудит методов обмена информацией независимым органом особенно по вопросам использования технологий, прав человека и гендера?
3.4	**L2**	**Партнерство и сотрудничество**					
3.4.1	L3	**Управление отношениями с государственными органами**	**Потенциал управления отношениями с государственными органами отсутствует**	ОБЩИЕ: Имеется ли неофициальная политика или какие-либо элементы управления отношениями с государственными органами? Является ли практика управления отношениями с государственными органами разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется ли комплексный подход к управлению отношениями с государственными органами? Имеются ли специалисты по управлению отношениями с государственными органами? Являются ли методы управления отношениями с государственными органами структурированными, документированными и постоянными? Имеется ли главный координатор по управлению отношениями с государственными органами? Имеется ли регулярное взаимодействие правоохранительных органов с соответствующими заинтересованными правительственными структурами по обсуждению сотрудничества и координации? СПЕЦИАЛЬНЫЕ: Имеется ли специальная процедура управления отношениями с государственными органами, чтобы справиться со сценариями рисков, связанных с новыми технологиями? Включает ли специальная процедура соответствующие контакты для быстрого реагирования?	ОБЩИЕ: Имеется ли план по управлению отношениями с государственными органами, который приведен в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел или координатор по вопросам управления отношениями с государственными органами? Осуществляется ли оценка и контроль эффективности управления отношениями с государственными органами в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит деятельности по международному сотрудничеству? Имеются ли стандарты и требования, касающиеся управления отношениями с государственными органами? СПЕЦИАЛЬНЫЕ: Имеются ли гарантии учета прав человека, гендерных аспектов и принципа верховенства права в рамках управления отношениями с государственными органами в том, что касается обмена информацией и использования технологий?	ОБЩИЕ: Осуществляется ли анализ и обновление соответствующих методов управления отношениями с государственными органами на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты управления отношениями с государственными органами в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит методов управления отношениями с государственными органами независимым органом? СПЕЦИАЛЬНЫЕ: Осуществляется ли регулярный анализ и аудит методов отношениями с государственными органами независимым органом особенно по вопросам использования технологий, прав человека и гендера? Включена ли деятельность правоохранительных органов в процессы неправоохранительной политики, связанные с новыми технологиями?

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.4.2	L3	**Управление контртеррористической партнерской деятельностью**	**Возможность управления контртеррористической партнерской деятельностью отсутствует**	ОБЩИЕ: Имеется ли неофициальная политика или какие-либо элементы управления контртеррористической партнерской деятельностью? Является ли практика управления контртеррористической партнерской деятельностью разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется ли комплексный подход к управлению контртеррористической партнерской деятельностью? Имеются ли специалисты по управлению контртеррористической партнерской деятельностью? Являются ли методы управления контртеррористической партнерской деятельностью структурированными, документированными и постоянными? СПЕЦИАЛЬНЫЕ: Имеется ли специальная процедура управления контртеррористической партнерской деятельностью, чтобы справиться со сценариями рисков, связанных с новыми технологиями? Включает ли специальная процедура соответствующие контакты для быстрого реагирования? Являются ли контртеррористические структуры, не входящие в состав правоохранительных органов, частью оценки технических рисков?	ОБЩИЕ: Имеется ли план управления контртеррористической партнерской деятельностью, который приведен в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел или координатор по вопросам управления контртеррористической партнерской деятельностью? Осуществляется ли оценка и контроль эффективности управления контртеррористической партнерской деятельностью в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит деятельности по управлению контртеррористической партнерской деятельностью? Имеются ли стандарты и требования, касающиеся управления контртеррористической партнерской деятельностью? СПЕЦИАЛЬНЫЕ: Имеются ли гарантии учета прав человека, гендерных аспектов и принципа верховенства права в рамках управления контртеррористической партнерской деятельностью в отношении обмена информацией и использования технологий? Имеется ли четкая процедура координации с национальной группой реагирования на инциденты в сфере компьютерной безопасности (CSIRT)/учреждениями по кибербезопасности?	ОБЩИЕ: Осуществляется ли анализ и обновление соответствующих методов управления контртеррористической партнерской деятельностью на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты управления контртеррористической партнерской деятельностью в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит методов управления контртеррористической партнерской деятельностью независимым органом? СПЕЦИАЛЬНЫЕ: Осуществляется ли регулярный анализ и аудит методов управления контртеррористической партнерской деятельностью независимым органом особенно по вопросам использования технологий, прав человека и гендера? Включены ли правоохранительные органы в процессы в рамках политики в области новых технологий для борьбы с терроризмом, не связанные с правоохранительными органами?

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.4.3	L3	**Взаимодействие с общественностью/сообществом**	**Возможность взаимодействия с общественностью/сообществом отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы взаимодействия с общественностью/сообществом? Является ли практика взаимодействия с общественностью/сообществом разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к взаимодействию с общественностью/сообществом? Имеются ли специалисты по взаимодействию с общественностью/сообществом? Являются ли методы взаимодействия с общественностью/сообществом структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Повышает ли практика взаимодействия с общественностью/сообществом осведомленность об использовании новых технологий в террористических целях? Имеется ли специальное общедоступное контактное лицо для сообщений со стороны общественности о рисках или угрозах, связанных с использованием новых технологий для борьбы с терроризмом? Используют ли правоохранительные органы социальные сети для информационного обеспечения и взаимодействия с общественностью? Существуют ли четкие рекомендации и действия по поддержке пострадавших от злоупотребления новыми технологиями (например, от вирусов-вымогателей)? Была ли опубликована вами информация о роли правоохранительных органов и их поддержке, оказанной пострадавшим от злоупотребления новыми технологиями (например, от вирусов-вымогателей)?	**ОБЩИЕ:** Имеются ли стратегия или план по взаимодействию с общественностью/сообществом, которые приведены в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел по связям с общественностью? Осуществляется ли оценка и контроль эффективности взаимодействия с общественностью/сообществом в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит взаимодействия с общественностью/сообществом? Имеются ли стандарты и требования, касающиеся взаимодействия с общественностью/сообществом? **СПЕЦИАЛЬНЫЕ:** Было ли проведено исследование об использовании населением новых технологий? Проводились ли консультации с лидерами сообществ по поводу размещения важнейших цифровых социальных функций? Приведена ли политика взаимодействия правоохранительных органов с общественностью в соответствие с политикой взаимодействия в области кибербезопасности?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов взаимодействия с общественностью/сообществом на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты контртеррористической деятельности и операций правоохранительных органов в тех случаях, когда это необходимо в интересах общества? Раскрываются ли публично аспекты внутренних анализов и аудитов контртеррористической деятельности и операций правоохранительных органов в тех случаях, когда это необходимо в интересах общества? Было ли проведено исследование, касающееся доверия общественности и взаимодействия с нею? **СПЕЦИАЛЬНЫЕ:** Раскрываются ли публично внутренние анализы и аудиты, касающиеся использования технологий, прав человека, гендерных аспектов и принципов верховенства права, в тех случаях, когда это необходимо в интересах общества?

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.4.4	L3	Международное сотрудничество	Возможность международного сотрудничества отсутствует	ОБЩИЕ: Имеются ли какие-либо элементы международного сотрудничества? Является ли практика международного сотрудничества разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется ли комплексный подход к международному сотрудничеству? Имеются ли специалисты по международному сотрудничеству? Являются ли методы международного сотрудничества структурированными, документированными и постоянными? СПЕЦИАЛЬНЫЕ: Имеют ли отделы, входящие в ценностную цепочку контртеррористической деятельности с использованием новых технологий, четкие указания относительно юрисдикции и трансграничного международного сотрудничества? Имеют ли правоохранительные органы надежные связи с другими правоохранительными органами? Участвуют ли правоохранительные органы в соглашениях, которые применяются к трансграничному сотрудничеству в рамках ценностной цепочки контртеррористической деятельности с использованием новых технологий? Участвуют ли правоохранительные органы в надежной круглосуточной сети в области киберпреступности (например, Интерпол)? Обмениваются ли правоохранительные органы информацией на тактическом уровне?	ОБЩИЕ: Имеются ли план по международному сотрудничеству и методы, которые приведены в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел международного сотрудничества? Осуществляется ли оценка и контроль эффективности международного сотрудничества в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит деятельности по международному сотрудничеству? Имеются ли стандарты и требования, касающиеся международного сотрудничества? СПЕЦИАЛЬНЫЕ: Имеются ли гарантии учета прав человека, гендерных аспектов и принципа верховенства права в рамках международного сотрудничества в отношении обмена информацией и использования технологий? Регулярно ли правоохранительные органы участвуют в актуальных международных дискуссиях, посвященных борьбе с терроризмом и новым технологиям? Участвовали ли правоохранительные органы в международной операции или мероприятии, в которых используются новые технологии?	ОБЩИЕ: Осуществляется ли анализ и обновление соответствующих методов международного сотрудничества на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты международного сотрудничества в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит методов международного сотрудничества независимым органом? Взаимодействуют ли правоохранительные органы на регулярной основе с неправительственными заинтересованными сторонами в других странах, которые имеют важное значение для контртеррористических операций? СПЕЦИАЛЬНЫЕ: Осуществляется ли регулярный анализ и аудит методов международного сотрудничества независимым органом особенно по вопросам использования технологий, прав человека и гендера? Принимают ли правоохранительные органы активное участие в международных дискуссиях, посвященных борьбе с терроризмом и новым технологиям (например, руководство международной целевой группой, выполнение функций председателя комитета в международной организации, проведение международной/региональной конференции)? Взаимодействуют ли правоохранительные органы на регулярной основе с неправительственными заинтересованными сторонами в других странах, использующими новые технологии, которые имеют важное значение для контртеррористических операций?
3.5	L2	Управление оперативной деятельностью					
3.5.1	L3	Управление надзорной деятельностью	Возможность управления надзорной деятельностью отсутствует	ОБЩИЕ: Имеются ли какие-либо элементы управления надзором? Является ли практика управления надзорной деятельностью разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется ли комплексный подход к управлению надзорной деятельностью? Имеются ли специалисты по управлению надзорной деятельностью? Являются ли методы управления надзорной деятельностью структурированными, документированными и постоянными? Существуют ли механизмы отчетности для поддержки управления надзорной деятельностью? СПЕЦИАЛЬНЫЕ: Имеются ли возможности в отношении ситуационной осведомленности в режиме реального времени для поддержки контртеррористического использования технологий? Имеется ли поддержка возможностей использования новых технологий в борьбе с терроризмом во всех отделах организации?	ОБЩИЕ: Имеются ли план по управлению надзорной деятельностью и методы, которые приведены в соответствие с общей стратегией и приоритетами организации? Имеется ли специальный отдел по управлению надзорной деятельностью? Осуществляется ли оценка и контроль эффективности управления надзорной деятельностью в сравнении с конкретными показателями? Имеются ли стандарты и требования, касающиеся управления надзорной деятельностью? СПЕЦИАЛЬНЫЕ: Имеются ли национальные технические возможности в отношении ситуационной осведомленности? Управляются ли технические контртеррористические возможности в соответствии с центральной политикой, определяющей приоритеты и ресурсы для поддержки контртеррористических операций?	ОБЩИЕ: Осуществляется ли анализ и обновление соответствующих методов управления надзорной деятельностью на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты отчетов по управлению надзорной деятельностью в тех случаях, когда это необходимо в интересах общества? Имеется ли независимый надзорный механизм, который осуществляет аудит и анализ операций? СПЕЦИАЛЬНЫЕ: Включает ли мандат управления надзором оперативный надзор, касающийся использования технологий, прав человека и гендерных аспектов?

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.5.2	L3	**Управление сбором оперативной информации**	**Возможность управления сбором оперативной информации отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы практики управления сбором оперативной информации? Является ли практика управления сбором оперативной информации разовой или неофициальной? Доступны ли материалы с оперативной информацией для соответствующей оперативной контртеррористической деятельности? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к управлению сбором оперативной информации? Имеются ли специалисты по управлению сбором оперативной информации? Являются ли методы управления разведкой структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Является ли организация участником соглашений об обмене информацией с частным сектором или получает ли она информацию в результате таких соглашений? Имеется ли базовая возможность получения оперативных данных об использовании таких базовых технологий, как Интернет, социальные сети и т. д., в террористических целях? Имеются ли в штате организации технические специалисты, обеспечивающие поддержку возможностей управления сбором оперативной информации?	**ОБЩИЕ:** Имеются ли план по управлению сбором оперативной информации и методы, которые приведены в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел по сбору оперативной информации? Осуществляется ли оценка и контроль эффективности управления сбором оперативной информации в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит деятельности по сбору оперативной информации? Имеются ли стандарты и требования, касающиеся сбора оперативной информации? Разрабатываются ли материалы с оперативной информацией для стратегического, оперативного и тактического использования в соответствии с требованиями специалистов-практиков? **СПЕЦИАЛЬНЫЕ:** Имеется ли повышенная возможность получения оперативных данных об использовании таких основных технологий, как даркнет, социальные сети и т. д., в террористических целях? Имеются ли гарантии учета прав человека, гендерных аспектов и принципа верховенства права для использования технологий в рамках практики сбора оперативной информации? Учитывает ли практика сбора оперативной информации права человека и гендерную специфику?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов управления сбором оперативной информации на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты сбора оперативной информации и дел в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит методов сбора оперативной информации независимым органом? Предоставляются ли материалы с оперативной информацией в рамках обмена информацией на основе классификации информационной безопасности? Объединяются ли материалы с оперативной информацией с другими продуктами и источниками? **СПЕЦИАЛЬНЫЕ:** Осуществляется ли регулярный анализ и аудит методов сбора оперативной информации независимым органом особенно по вопросам использования технологий, прав человека и гендера? Полностью ли учитывает практика сбора оперативной информации права человека и гендерную специфику?
3.5.3	L3	**Управление расследованиями**	**Возможность управления расследованиями отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы практики управления расследованиями? Является ли практика управления расследованиями разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к управлению расследованиями? Имеются ли специалисты по расследованиям? Являются ли методы управления расследованиями структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Имеют ли следователи расширенные возможности для расследования, анализа и получения доказательств использования базовых технологий (например, Интернета, социальных сетей и т. д.)? Могут ли следователи проводить базовую цифровую криминалистическую экспертизу?	**ОБЩИЕ:** Имеется ли план по управлению расследованиями, который приведен в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел по проведению расследований? Осуществляется ли оценка и контроль эффективности управления расследованиями в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит расследований? Имеются ли стандарты и требования, касающиеся расследований? **СПЕЦИАЛЬНЫЕ:** Имеют ли следователи расширенные возможности для расследования, анализа и получения доказательств использования новых технологий (например, даркнета, криптовалют и т. д.)? Могут ли следователи проводить цифровую расширенную криминалистическую экспертизу? Имеются ли гарантии учета прав человека, гендерных аспектов и принципа верховенства права в рамках использования оперативной информации и технологий?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих контртеррористических действий правоохранительных органов на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты контртеррористических действий правоохранительных органов в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит контртеррористических действий правоохранительных органов независимым органом? **СПЕЦИАЛЬНЫЕ:** Осуществляется ли регулярный анализ и аудит контртеррористических действий правоохранительных органов независимым органом особенно по вопросам использования технологий, прав человека и гендера?

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.5.4	L3	**Действия правоохранительных органов**	**Потенциал для контртеррористической деятельности у правоохранительных органов отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы контртеррористических действий правоохранительных органов? Являются ли действия правоохранительных органов структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к деятельности правоохранительных органов? Имеются ли специалисты по контртеррористической деятельности правоохранительных органов? Являются ли действия правоохранительных органов структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Способны ли правоохранительные органы пресечь или предотвратить использование базовых технологий (т. е. Интернета, социальных сетей и т. д.) в террористических целях? Имеются ли специалисты по цифровой деятельности?	**ОБЩИЕ:** Имеется ли оперативный контртеррористический план правоохранительных органов по использованию набора инструментов действий правоохранительных органов, который приведен в соответствие с общей стратегией и приоритетами организации? Осуществляется ли оценка и контроль эффективности действий правоохранительных органов в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит контртеррористических действий правоохранительных органов? Имеются ли стандарты и требования, касающиеся контртеррористических действий правоохранительных органов? **СПЕЦИАЛЬНЫЕ:** Способны ли правоохранительные органы с помощью контртеррористических административных действий пресечь или предотвратить использование новых технологий (т. е. дарквеба, криптовалют и т. д.) в террористических целях? Имеются ли средства контроля за соблюдением прав человека, гендерных аспектов и принципов верховенства права при использовании технологий?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих контртеррористических действий правоохранительных органов на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты контртеррористических действий правоохранительных органов в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит контртеррористических действий правоохранительных органов независимым органом? **СПЕЦИАЛЬНЫЕ:** Осуществляется ли регулярный анализ и аудит контртеррористических действий правоохранительных органов независимым органом особенно по вопросам использования технологий, прав человека и гендера?
3.5.5	L3	**Управление взаимодействием с органами уголовного правосудия**	**Потенциал для управления взаимодействием с органами уголовного правосудия отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы взаимодействия с органами уголовного правосудия? Является ли практика взаимодействия с органами уголовного правосудия разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к управлению взаимодействием с органами уголовного правосудия? Имеются ли специалисты по взаимодействию с органами уголовного правосудия? Являются ли методы управления взаимодействием с органами уголовного правосудия структурированными, документированными и постоянными? Упорядочены ли процессы уголовного правосудия между правоохранительными органами, органами, осуществляющими преследование, судами и органами содержания под стражей? **СПЕЦИАЛЬНЫЕ:** Имеются ли стандарты или минимальные требования, касающиеся цифровых доказательств и цепочки обеспечения сохранности? Прошли ли специалисты-практики в области уголовного правосудия специальную подготовку по использованию новых технологий для борьбы с терроризмом?	**ОБЩИЕ:** Приведен ли план по взаимодействию с органами уголовного правосудия в соответствие с общей стратегией и приоритетами организации? Осуществляется ли оценка и контроль эффективности управления взаимодействием с органами уголовного правосудия в сравнении с конкретными показателями? Осуществляется ли независимый анализ результативности и эффективности уголовного правосудия? Имеются ли стандарты и требования, касающиеся управления взаимодействием с органами уголовного правосудия? **СПЕЦИАЛЬНЫЕ:** Вовлечены ли специалисты-практики в области уголовного правосудия в обучение по использованию новых технологий для борьбы с терроризмом?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов взаимодействия с органами уголовного правосудия на регулярной основе в целях постоянного совершенствования? Используется ли для разработки политики опрос, в котором оценивались бы эффективность и удовлетворенность заинтересованных сторон в контексте уголовного правосудия? Является ли эффективной система уголовного правосудия в соответствии с международными контрольными показателями? **СПЕЦИАЛЬНЫЕ:** Неприменимо

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.5.6	L3	**Управление мерами реагирования на инциденты**	**Возможность управления мерами реагирования на инциденты отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы практики и планов реагирования на инциденты? Является ли практика реагирования на инциденты разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к управлению мерами реагирования на инциденты? Являются ли методы реагирования на инциденты структурированными, документированными и постоянными? Имеются ли планы реагирования на инциденты? Четко ли определены и понятны функции и обязанности во время реагирования на инциденты и проходит ли обучение персонал? **СПЕЦИАЛЬНЫЕ:** Имеются ли конкретные планы реагирования на инциденты для решения проблем, связанных с цифровыми и новыми технологиями?	**ОБЩИЕ:** Приведен ли план по управлению мерами реагирования на инциденты в соответствие с общей стратегией и приоритетами организации? Осуществляется ли оценка и контроль эффективности управления мерами реагирования на инциденты в сравнении с конкретными показателями? Разрабатываются ли планы реагирования на инциденты в соответствии с оценкой рисков и вероятных сценариев? Имеются ли механизм передачи вопросов, касающихся реагирования на инциденты, на рассмотрение вышестоящему руководству и структура командования? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов управления мерами реагирования на инциденты на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты отчетов по анализу инцидентов в тех случаях, когда это необходимо в интересах общества? Являются ли планы реагирования на инциденты изменчивыми, чтобы иметь возможность управлять сложными сценариями? **СПЕЦИАЛЬНЫЕ:** Являются ли планы реагирования на инциденты изменчивыми, чтобы иметь возможность управлять сложными сценариями, включающими как физические, так и цифровые меры реагирования на инциденты?
3.6	**L2**	**Оперативная поддержка**					
3.6.1	L3	**Управление данными и информацией**	**Потенциал для управления данными и информацией отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы практики управления данными и информацией? Является практика управления данными и информацией разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к управлению данными и информацией? Имеются ли специалисты по управлению данными и информацией с помощью ИКТ? Являются ли методы управления данными и информацией структурированными, документированными и постоянными? Разработаны ли решения по управлению данными и информацией для конечных пользователей в правоохранительных органах, которые осуществляют контртеррористическую деятельность? Имеются ли функциональные ограничения доступа к данным и информации, обусловленные требованиями безопасности? Осуществляется ли сбор и организация данных комплексно? **СПЕЦИАЛЬНЫЕ:** Осуществляется ли сбор оперативной информации по технической угрозе и управление ею?	**ОБЩИЕ:** Имеются ли стратегия или план по управлению данными и информацией, которые приведены в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел по управлению данными и информацией? Осуществляется ли оценка и контроль эффективности управления данными и информацией в сравнении с конкретными показателями? Доступны ли данные всем клиентам правоохранительных органов на основе принципа служебной необходимости? Используют ли правоохранительные органы передовые аналитические возможности? **СПЕЦИАЛЬНЫЕ:** Осуществляется ли сбор технических данных и управление ими в соответствии с принятыми стандартами кибербезопасности? Участвует ли организация в соглашениях об обмене информацией между государственным и частным секторами? Обмениваются ли правоохранительные органы информацией с национальной группой реагирования на инциденты в сфере компьютерной безопасности (CSIRT)?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов управления данными и информацией на регулярной основе в целях постоянного совершенствования? Проводят ли правоохранительные органы аналитику своих данных? **СПЕЦИАЛЬНЫЕ:** Неприменимо

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.6.2	L3	**Техническая поддержка**	**Потенциал для технической поддержки отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы технической поддержки? Является ли практика технической поддержки разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеются ли комплексный подход и средства контроля в отношении технической поддержки? Имеются ли специалисты по оказанию технической поддержки? Являются ли методы обеспечения технической поддержки структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Может ли техническая поддержка предоставлять базовые технические решения для разведывательной и следственной деятельности? Имеют ли правоохранительные органы доступ к ИКТ-услугам в области криминалистики?	**ОБЩИЕ:** Имеются ли стратегия или план использования технологий, которые приведены в соответствие с общей стратегией и приоритетами организации? Осуществляется ли оценка и контроль эффективности технической поддержки в сравнении с конкретными показателями? Способна ли техническая поддержка в полной мере предоставлять технические решения для требований правоохранительных органов по борьбе с терроризмом? Есть ли специальный отдел по разработке и закупке технических решений для разведки и расследований? **СПЕЦИАЛЬНЫЕ:** Может ли техническая поддержка предоставлять передовые технические решения для разведывательной и следственной деятельности? Имеется ли в правоохранительных органах ИКТ-центр судебной экспертизы с надлежащим обеспечением техническим персоналом? Включены ли требования в области прав человека и воздействие на гендерные аспекты в процесс предоставления технических решений?	**ОБЩИЕ:** Осуществляется ли пересмотр и обновление методов технической поддержки на регулярной основе в целях постоянного совершенствования? **СПЕЦИАЛЬНЫЕ:** Имеются ли возможности для проведения исследований и разработок для поддержки будущих технических решений? Имеется ли модель партнерства в области исследований и разработок с отраслью, научными кругами и другими организациями для стимулирования инноваций?
3.7	**L2**	**Управление инновационной деятельностью**					
3.7.1	L3	**Технологическое сканирование**	**Потенциал для технологического сканирования отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы технологического сканирования? Является ли практика технологического сканирования разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеется ли комплексный подход к проведению сканирования технологий/отрасли? Являются ли методы технологического сканирования структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Основаны ли технологическое сканирование и приоритеты в области технологий на общей стратегии и приоритетах организации и согласованы с ними? Осуществляется ли оценка и контроль методов технологического сканирования в сравнении с конкретными показателями эффективности? Имеются ли стандарты и требования, касающиеся проведения технологического сканирования? Определены ли текущие требования к возможностям и проблемы при проведении технологического сканирования? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Осуществляется ли пересмотр и обновление соответствующих методов технологического сканирования на регулярной основе в целях постоянного совершенствования? **СПЕЦИАЛЬНЫЕ:** Неприменимо

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.7.2	L3	**Инновационное развитие и обеспечение**	**Потенциал для инновационного развития и обеспечения отсутствует**	ОБЩИЕ: Имеются ли какие-либо элементы инновационного развития и обеспечения? Является ли практика развития и обеспечения инноваций разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется ли комплексный подход к развитию и обеспечению инноваций? Являются ли методы развития и обеспечения инноваций структурированными, документированными и постоянными? Приветствуются и поощряются ли инновации? СПЕЦИАЛЬНЫЕ: Применяется ли данный подход к деятельности правоохранительных органов по борьбе с использованием новых технологий в террористических целях?	ОБЩИЕ: Имеются ли стратегия или план по инновациям, которые приведены в соответствие с общей стратегией и приоритетами организации? Осуществляется ли оценка и контроль эффективности инноваций в сравнении с конкретными показателями? Имеются ли специалисты по управлению изменениями для предоставления инновационных решений? Имеется ли культура поощрения инноваций? СПЕЦИАЛЬНЫЕ: Имеются ли узкие специалисты по ИКТ-инновациям?	ОБЩИЕ: Осуществляется ли пересмотр и обновление соответствующей инновационной деятельности на регулярной основе в целях постоянного совершенствования? Есть ли специальный отдел по управлению изменениями для внедрения инноваций? Осуществляется ли определение приоритетности, утверждение и поощрение инновационной деятельности сверху вниз? СПЕЦИАЛЬНЫЕ: Неприменимо
3.7.3	L3	**Модель инновационного партнерства**	**Потенциал для обеспечения модели партнерства отсутствует**	ОБЩИЕ: Имеются ли какие-либо элементы инновационного партнерства? Является ли практика в отношении модели партнерства разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется ли комплексный подход к инновационному партнерству? Являются ли методы в отношении модели партнерства структурированными, документированными и постоянными? СПЕЦИАЛЬНЫЕ: Применяется ли данный подход к деятельности правоохранительных органов по борьбе с использованием новых технологий в террористических целях?	ОБЩИЕ: Имеются ли стратегия или план по инновационному партнерству, которые приведены в соответствие с общей стратегией и приоритетами организации? Осуществляется ли оценка и контроль эффективности модели инновационного партнерства в сравнении с конкретными показателями? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Осуществляется ли пересмотр и обновление соответствующих методов инновационного партнерства на регулярной основе в целях постоянного совершенствования? Существуют ли средства инкубации и инвестирования в стартапы в области перспективных технологий, относящихся к ценностной цепочке контртеррористической деятельности правоохранительных органов?
3.7.4	L3	**Поддержка инновационной деятельности**	**Потенциал для поддержки инновационной деятельности отсутствует**	ОБЩИЕ: Имеются ли какие-либо элементы поддержки инновационной деятельности? Является ли практика поддержки инновационной деятельности разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Применяются ли возможности обеспечения поддержки инновационной деятельности к ИТК?	ОБЩИЕ: Имеется ли комплексный подход к поддержке инновационной деятельности? Имеются ли выделенные ресурсы (финансовые и людские ресурсы, инфраструктура и т. д.) на поддержку инновационной деятельности? Являются ли методы поддержки инновационной деятельности структурированными, документированными и постоянными? СПЕЦИАЛЬНЫЕ: Применяется ли данный подход к деятельности правоохранительных органов по борьбе с использованием новых технологий в террористических целях?	ОБЩИЕ: Приведена ли поддержка инновационной деятельности в соответствие со стратегией и планом в области инноваций и общей стратегией и приоритетами организации? Осуществляется ли оценка и контроль эффективности поддержки инновационной деятельности в сравнении с конкретными показателями? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Осуществляется ли пересмотр и обновление методов поддержки инновационной деятельности на регулярной основе в целях постоянного совершенствования? СПЕЦИАЛЬНЫЕ: Неприменимо

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.8	**L2**	**Человеческий капитал, обучение и развитие трудовых ресурсов**					
3.8.1	L3	**Требования к квалификации сотрудников**	**Потенциал в отношении требований к квалификации сотрудников отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы определения требований к квалификации сотрудников? Являются ли требования к квалификации сотрудников разовыми или неофициальными? **СПЕЦИАЛЬНЫЕ:** Включают ли требования к квалификации сотрудников использование правоохранительными органами новых технологий?	**ОБЩИЕ:** Имеется ли комплексный подход к определению требований к квалификации сотрудников? Имеются ли специалисты для определения требований к квалификации сотрудников? Является ли деятельность, связанная с требованиями к квалификации сотрудников, структурированной, документированной и постоянной? **СПЕЦИАЛЬНЫЕ:** Определены ли в требованиях к квалификации сотрудников технические навыки, необходимые для работы с новыми технологиями? Применяются ли оценка и требования к квалификации сотрудников, включающей использование новых технологий, ко всем функциям в контртеррористической ценностной цепочке и в процессе уголовного правосудия? Включают ли требования к квалификации сотрудников периодическое обучение новым технологиям?	**ОБЩИЕ:** Приведены ли требования к квалификации сотрудников в соответствие с общей кадровой стратегией и приоритетами организации? Определяются ли требования к квалификации сотрудников текущими возможностями и задачами? Имеются ли стандарты и требования по определению требований к квалификации сотрудников? Осуществляется ли регулярная оценка уровня квалификации имеющегося штата сотрудников? **СПЕЦИАЛЬНЫЕ:** Включают ли требования к квалификации сотрудников соображения по поводу гендерных аспектов применительно к новым технологиям?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующей деятельности, связанной с требованиями к квалификации сотрудников, на регулярной основе в целях постоянного совершенствования? **СПЕЦИАЛЬНЫЕ:** Определяются ли в требованиях к квалификации сотрудников новые технические навыки, необходимые для будущего технологического потенциала?
3.8.2	L3	**Оценка потребностей в обучении**	**Потенциал для оценки потребностей в обучении отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы проведения оценки потребностей в обучении? Является ли практика оценки потребности в обучении разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Приведена ли оценка потребностей в обучении в соответствие с общей кадровой стратегией и приоритетами организации? Имеется ли комплексный подход к проведению оценки потребностей в обучении? Имеются ли кадры, обученные проведению оценки потребностей в обучении? Являются ли методы оценки потребностей в обучении структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Определяют ли оценки потребностей в обучении необходимую техническую подготовку в отношении возможностей использования новых технологий?	**ОБЩИЕ:** Проводятся ли оценки потребностей в обучении на индивидуальной основе? Имеются ли стандарты и требования по проведению оценок потребностей в обучении? **СПЕЦИАЛЬНЫЕ:** Включают ли оценки потребностей в обучении возможности учета гендерных требований?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов оценки потребностей в обучении на регулярной основе в целях постоянного совершенствования? **СПЕЦИАЛЬНЫЕ:** Определяет ли оценка потребностей в обучении будущие потребности в обучении для новых возможностей? Изучаются ли в рамках оценки потребностей в обучении гендерные аспекты (знания и навыки)?

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.8.3	L3	**Модель обеспечения профессиональной подготовки**	**Потенциал в отношении модели обеспечения профессиональной подготовки отсутствует**	ОБЩИЕ: Имеются ли какие-либо элементы обеспечения профессиональной подготовки? Является ли практика использования модели партнерства разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Соответствует ли профессиональная подготовка общей кадровой стратегии и стратегии организации? Имеется ли комплексный подход к профессиональной подготовке? Имеется ли специализированное обучение для руководящих кадров? Подходит ли модель обеспечения профессиональной подготовки для разных профессий и функций? Являются ли методы модели обеспечения профессиональной подготовки структурированными, документированными и постоянными? СПЕЦИАЛЬНЫЕ: Применима ли модель обеспечения профессиональной подготовки ко всем функциям, для выполнения которых требуются навыки в использовании новых технологий в контртеррористической ценностной цепочке и в процессе уголовного правосудия? Включает ли профессиональная подготовка взаимодействие с представителями отрасли и научных кругов?	ОБЩИЕ: Соответствует ли профессиональная подготовка индивидуальным требованиям и должности? Есть ли специальный отдел управления профессиональной подготовкой? Осуществляется ли оценка и контроль обучения в сравнении с конкретными показателями? Соответствует ли обучение требованиям к квалификации сотрудников, оценке потребностей в обучении и развитию карьеры? СПЕЦИАЛЬНЫЕ: Включает ли профессиональная подготовка курсы отраслевого и научного уровня? Учитывает ли профессиональная подготовка использование новых технологий, правовые аспекты, права человека и гендерные аспекты?	ОБЩИЕ: Осуществляется ли анализ и обновление соответствующих методов обеспечения профессиональной подготовки на регулярной основе в целях постоянного совершенствования? Рассматривается ли программой профессиональной подготовки возможность обмена с партнерами по борьбе с терроризмом? СПЕЦИАЛЬНЫЕ: Интегрирована ли модель обеспечения профессиональной подготовки с академической подготовкой в области новых технологий?
3.8.4	L3	**Развитие карьеры**	**Потенциал для развития карьеры отсутствует**	ОБЩИЕ: Имеются ли какие-либо элементы развития карьеры и продвижения по службе? Является ли практика развития карьеры разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеются ли специалисты отдела кадров по вопросам развития карьеры? Являются ли методы развития карьеры структурированными, документированными и постоянными? СПЕЦИАЛЬНЫЕ: Имеются ли пути развития специальных профессиональных навыков, связанных с технологиями?	ОБЩИЕ: Соответствует ли развитие карьеры общей кадровой стратегии и стратегии организации? Есть ли специальный отдел кадров для управления развитием карьеры? СПЕЦИАЛЬНЫЕ: Учитывают ли стратегии и методы развития карьеры и продвижения по службе гендерное равенство и поощряют ли занятие женщинами руководящих должностей? Существуют ли механизмы, которые позволяют специалистам из частного сектора участвовать в работе правоохранительных органов в течение определенного периода времени?	ОБЩИЕ: Осуществляется ли анализ и обновление деятельности, связанной с развитием карьеры и продвижением по службе, на регулярной основе в целях постоянного совершенствования и в соответствии с принципами равенства и недискриминации? СПЕЦИАЛЬНЫЕ: Существуют ли механизмы предоставления специалистам правоохранительных органов профессиональных отпусков для работы в частных технологических компаниях?
3.9	**L2**	**Обеспечение возможностей: бизнес-функции**					
3.9.1	L3	**Закупки**	**Потенциал в отношении закупок отсутствует**	ОБЩИЕ: Имеются ли какие-либо элементы практики закупок? Является ли практика закупок разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеются ли комплексный подход к закупкам и средства контроля? Имеются ли специалисты по закупкам? Являются ли методы закупок структурированными, документированными и постоянными? СПЕЦИАЛЬНЫЕ: Имеется ли практика закупок оперативных технологических решений для контртеррористической деятельности правоохранительных органов?	ОБЩИЕ: Имеются ли стратегия или план закупок, которые приведены в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел по закупкам? Осуществляется ли оценка и контроль эффективности закупок в сравнении с конкретными показателями? СПЕЦИАЛЬНЫЕ: Имеются ли специальная практика или правила закупок оперативных технологических решений, которые являются конфиденциальными для контртеррористической деятельности правоохранительных органов?	ОБЩИЕ: Осуществляется ли анализ и обновление соответствующих методов закупок на регулярной основе в целях постоянного совершенствования? Осуществляется ли независимый анализ и аудит закупочной деятельности на регулярной основе? Раскрываются ли публично аспекты методов отчетов и договоров в области управления в тех случаях, когда это необходимо в интересах общества? СПЕЦИАЛЬНЫЕ: Неприменимо

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.9.2	L3	**Финансы**	**Потенциал в отношении финансов отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы практики управления финансами? Являются ли финансовые методы разовыми или неофициальными? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеются ли комплексный подход к финансам и средства контроля? Имеются ли специалисты по финансам? Являются ли методы финансовой деятельности структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Имеется ли специально выделенный бюджет для требуемого технологического потенциала?	**ОБЩИЕ:** Имеются ли стратегия или план управления финансами, которые приведены в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел по финансам? Осуществляется ли оценка и контроль эффективности финансового управления в сравнении с конкретными показателями? Осуществляется ли регулярный анализ и аудит финансов? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих методов управления финансовой деятельностью на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты эффективности финансовой деятельности или отчетов в тех случаях, когда это необходимо в интересах общества? Осуществляется ли регулярный анализ и аудит финансов независимым органом? **СПЕЦИАЛЬНЫЕ:** Неприменимо
3.9.3	L3	**ИКТ**	**Потенциал в отношении ИКТ отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы практики использования и поддержки ИКТ? Являются ли ИКТ-методы разовыми или неофициальными? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеются ли комплексный подход к управлению ИКТ и средства контроля? Имеются ли специалисты по ИКТ? Являются ли ИКТ-методы структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеются ли стратегия или план по ИКТ, которые приведены в соответствие с общей стратегией и приоритетами организации? Есть ли специальный отдел по ИКТ? Учитываются ли требования к ИКТ в бизнес-процессах и требованиях организации и приведены ли они в соответствие с ними? Осуществляется ли оценка и контроль эффективности ИКТ в сравнении с конкретными показателями? Приведена ли политика по ИКТ в соответствие с управлением инновационной деятельностью? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих мер ИКТ и инцидентов в сфере ИКТ на регулярной основе в целях постоянного совершенствования? **СПЕЦИАЛЬНЫЕ:** Неприменимо
3.9.4	L3	**Безопасность**	**Потенциал в отношении безопасности отсутствует**	**ОБЩИЕ:** Имеются ли какие-либо элементы практики обеспечения безопасности? Является ли практика обеспечения безопасности разовой или неофициальной? **СПЕЦИАЛЬНЫЕ:** Неприменимо	**ОБЩИЕ:** Имеются ли комплексный подход к обеспечению безопасности и средства контроля физической защиты и защиты персонала, основанные на оценке угроз? Имеются ли специалисты по безопасности? Являются ли методы обеспечения безопасности структурированными, документированными и постоянными? **СПЕЦИАЛЬНЫЕ:** Имеются ли меры по обеспечению безопасности персонала и физической безопасности для защиты технологий, технологических возможностей и конфиденциальной информации?	**ОБЩИЕ:** Имеются ли стратегия или план по безопасности, которые приведены в соответствие с общей стратегией и приоритетами организации и общей оценкой угроз? Согласована ли стратегия безопасности с другими организациями в сфере безопасности? Есть ли специальный отдел по безопасности? Служит ли процесс оценки рисков/угроз для безопасности основой для политики и методов обеспечения безопасности? Осуществляется ли оценка и контроль эффективности безопасности в сравнении с конкретными показателями? **СПЕЦИАЛЬНЫЕ:** Имеются ли меры по обеспечению безопасности персонала и физической безопасности для защиты технологий, технологических возможностей и конфиденциальной информации с учетом оценки рисков безопасности, а также индивидуальных допусков к закрытой информации, должностных обязанностей и технологий? Проводится ли оценка рисков в плане безопасности для технологий?	**ОБЩИЕ:** Осуществляется ли анализ и обновление соответствующих мер безопасности и инцидентов в сфере безопасности на регулярной основе в целях постоянного совершенствования? Раскрываются ли публично аспекты инцидентов в сфере безопасности в тех случаях, когда это необходимо в интересах общества? Существует ли механизм передачи сведений об инцидентах, связанных с безопасностью, вышестоящему руководству? **СПЕЦИАЛЬНЫЕ:** Неприменимо

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.9.5	L3	**Кибербезопасность**	**Потенциал в отношении кибербезопасности отсутствует**	ОБЩИЕ: Имеются ли какие-либо элементы практики обеспечения кибербезопасности? Является ли практика обеспечения кибербезопасности разовой или неофициальной? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеются ли комплексный подход к обеспечению безопасности и средства контроля в отношении кибербезопасности, основанные на оценке рисков и угроз? Имеются ли специалисты по кибербезопасности? Являются ли методы обеспечения кибербезопасности структурированными, документированными и постоянными? Осведомлено ли руководство ИКТ о соображениях по поводу кибербезопасности и принимает ли их во внимание? Имеют ли правоохранительные органы обязательное руководство по кибербезопасности для сотрудников? СПЕЦИАЛЬНЫЕ: Имеются ли специальные меры кибербезопасности для оперативных технологий, используемых правоохранительными органами для борьбы с терроризмом?	ОБЩИЕ: Имеется ли стратегия по кибербезопасности, которая приведена в соответствие с общей национальной стратегией и приоритетами организации в области кибербезопасности? Есть ли специальный внутренний отдел по кибербезопасности? Интегрирован ли отдел обеспечения кибербезопасности в организационные процессы? Служит ли процесс оценки рисков/угроз для кибербезопасности основой для политики и методов обеспечения кибербезопасности? Осуществляется ли оценка и контроль эффективности безопасности в сравнении с конкретными показателями? Соответствует ли политика обеспечения кибербезопасности международному передовому опыту и стандартам по кибербезопасности организации? Проводились ли обучение и повышение уровня осведомленности сотрудников? Проводился ли независимый аудит кибербезопасности? Имеют ли правоохранительные органы возможности ситуационной осведомленности в режиме реального времени о своих ИКТ? Существует ли координация и сотрудничество с национальной группой реагирования на инциденты в сфере компьютерной безопасности (CSIRT)? СПЕЦИАЛЬНЫЕ: Объединены ли отделом обеспечения кибербезопасности закупки и развитие новых возможностей в области ИКТ?	ОБЩИЕ: Осуществляется ли анализ и обновление соответствующих мер кибербезопасности и инцидентов в сфере кибербезопасности на регулярной основе в целях постоянного совершенствования? Находится ли сфера кибербезопасности в ведении высшего руководства? Раскрываются ли публично аспекты инцидентов в сфере кибербезопасности в тех случаях, когда это необходимо в интересах общества? Существует ли механизм передачи сведений об инцидентах, связанных с кибербезопасностью, вышестоящему руководству? СПЕЦИАЛЬНЫЕ: Неприменимо

3	L1	Институциональное направление	Нулевой	Базовый	Сформированный	Продвинутый	Высший
3.9.6	L3	Правовое обеспечение	Потенциал в отношении правового обеспечения отсутствует	ОБЩИЕ: Имеются ли в правоохранительных органах особые специалисты по правовой поддержке? СПЕЦИАЛЬНЫЕ: Неприменимо	ОБЩИЕ: Имеется ли в правоохранительных органах собственный отдел правового обеспечения для поддержки всей их деятельности? Входит ли руководитель отдела правового обеспечения в состав высшего руководства? Имеют ли документальное оформление функции и основные услуги отдела правового обеспечения? Существует ли механизм передачи правовых вопросов вышестоящему руководству? Имеются ли в штате отдела правового обеспечения юристы в областях деятельности правоохранительных органов (см. правовое направление)? СПЕЦИАЛЬНЫЕ: Привлекается ли отдел правового обеспечения к проверке деятельности правоохранительных органов, которая касается использования технологий, прав человека и гендерных аспектов? Имеются ли конкретные указания относительно того, когда требуется юридическая консультация по вопросам использования технологий, прав человека и гендерных аспектов? Есть ли в отделе правового обеспечения специалист по правовым вопросам электронных доказательств? Предоставляет ли отдел правового обеспечения заблаговременно рекомендации и консультации по вопросам использования технологий, прав человека и гендерных аспектов?	ОБЩИЕ: Приведен ли план работы по правовым вопросам в соответствие с общей стратегией и приоритетами организации? Осуществляется ли оценка и контроль эффективности правового обеспечения в сравнении с конкретными показателями? Имеются ли в штате отдела правового обеспечения специалисты по правовым вопросам для всех основных направлений деятельности правоохранительных органов и вспомогательной деятельности? Осуществляет ли отдел правового обеспечения деятельность по обучению и непрерывному юридическому образованию? СПЕЦИАЛЬНЫЕ: Есть ли в отделе правового обеспечения специалист по правовым вопросам защиты данных? Есть ли в отделе правового обеспечения специалист по интернет-посредникам? Есть ли в отделе правового обеспечения юрист по правилам удаления контента?	ОБЩИЕ: Осуществляется ли анализ и обновление соответствующих методов правового обеспечения на регулярной основе в целях постоянного совершенствования? Привлекается ли отдел правового обеспечения к участию в международных правовых дискуссиях, посвященных вопросам борьбы с терроризмом? Раскрываются ли публично аспекты отчетов по правовым вопросам в тех случаях, когда это необходимо в интересах общества? СПЕЦИАЛЬНЫЕ: Привлекается ли отдел правового обеспечения к участию в международных правовых дискуссиях, посвященных вопросам борьбы с терроризмом и использования новых технологий?

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)