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

INTERPOL

При финансовой поддержке
Европейского союза

Кибербезопасность и новые технологии

Проведение оценки террористической угрозы: анализ использования новых технологий в террористических целях

Выражение признательности

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

Контртеррористическое управление Организации Объединенных Наций

Центральные учреждения Организации Объединенных Наций

New York, NY 10017

www.un.org/counterterrorism

200, Quai Charles de Gaulle
69006 Lyon, France

www.interpol.int/en

Содержание

Совместное предисловие 4
Выражение признательности 5
Термины и определения 5
Краткое содержание 8

[I]
БАЗОВАЯ ИНФОРМАЦИЯ 9
1.1 Обзор 9
1.2 Инициатива CT TECH 10
1.3 Цель и назначение документа 11

[II]
ПОДХОД 13
2.1 Обзор 13
2.2 Руководящая основа 13
2.3 Методология 15

[III]
ВВЕДЕНИЕ 19
3.1 Обзор 19
3.2 Новые технологии и борьба с терроризмом 19

[IV]
ОЦЕНКА УГРОЗ И РИСКОВ 23
4.1 Обзор 23
4.2 Цикл управления угрозами и рисками 24

[IV]
ПЕРЕДОВОЙ ОПЫТ В СФЕРЕ ОЦЕНКИ УГРОЗ 33
5.1 Обзор 33
5.2 Межучрежденческий подход и информационно-аналитические центры 33
5.3 Подход, основанный на оценке рисков 35
5.4 Определение уровня угрозы 35
5.5 Сбор и анализ информации об угрозах 37
5.6 Непрерывная оценка 38
5.7 Расширение обмена оперативной информацией 39
5.8 Исследования и инновации 40

[ПРИЛОЖЕНИЕ A]
ПРИМЕР МОДЕЛИ ОЦЕНКИ ДЛЯ АТРИБУЦИИ УГРОЗ 42
A.1 Обзор 42

[ПРИЛОЖЕНИЕ B]
ПРИМЕР НЕПРАВОМЕРНОГО ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ТЕРРОРИСТАМИ 43
B.1 Обзор 43

[ПРИЛОЖЕНИЕ C]
РУКОВОДЯЩИЕ ВОПРОСЫ ДЛЯ ПРОВЕДЕНИЯ ОЦЕНКИ УГРОЗ 47
C.1 Обзор 47
C.2 Руководящие вопросы 47

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 принципа верховенства права.

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

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

Стивен Кавана
Исполнительный директор,
Полицейская служба Интерпола

Выражение признательности

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

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

Термины и определения

Вектор угрозы	Конкретный метод или средство, с помощью которого субъект угрозы осуществляет атаку[1].
Действия правоохранительных органов	Этот термин, как правило, описывает действия правоохранительных органов, предпринимаемые для противодействия угрозе, которые могут включать задержание отдельных лиц, пресечение деятельности злоумышленников (например, удаление контента, арест активов) и т. д.
Доказательства	Официальный термин для обозначения информации, являющейся частью судебного процесса, которая используется для подтверждения или опровержения совершения предполагаемого преступления. Все доказательства являются информацией, но не вся информация является доказательством. Таким образом, информация – это первоначальная, исходная форма доказательств[2].
Зеттабайт	Один зеттабайт равен одному миллиарду терабайтов.
Искусственный интеллект	Под этим термином обычно понимают дисциплину, занимающуюся разработкой технологических инструментов, позволяющих имитировать когнитивные функции человеческого мозга, такие как планирование, обучение, рассуждение и анализ.
Ландшафт угроз	Под ландшафтом угроз понимается общая картина потенциальных террористических угроз, с которыми может столкнуться страна, регион или организация. Он включает в себя спектр террористических групп, их возможности, намерения и тактики, а также уязвимость потенциальных целей и возможные последствия атаки.

1 Mary E. Shacklett, "What Is Attack Vector" («Что такое вектор атаки?»), Tech Target, April 2021, URL: https://www.techtarget.com/searchsecurity/definition/attack-vector

2 Руководство ИДКТК по содействию использованию и признанию приемлемости в качестве доказательств в национальных уголовных судах информации, собранной, обработанной, сохраняемой и передаваемой военными для целей судебного преследования за террористические преступления (2021 г.), URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_military_evidence_guidelines.pdf

Новые технологии	Термин «новые технологии» охватывает широкий спектр различных технологий[3], 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[4].
Объект угрозы	Конкретный объект, местоположение или группа, которым угрожает потенциальная террористическая атака.
Оперативная информация	Результат сбора, разработки, распространения, анализа и интерпретации данных, полученных из широкого круга источников, для информирования лиц, ответственных за принятие решений, 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.
Оперативная информация из открытых источников (OSINT)	Оперативная информация, полученная из общедоступных источников[5].
Оперативная информация из социальных сетей (SOCMINT)	Оперативная информация, собранная с помощью социальных сетей.
Оценка угроз	Инструмент, основанный на согласованной методологии, который обеспечивает анализ данных и руководство к действию по решению выявленных проблем, которые могут нанести вред государству и обществу в будущем[6].
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.
Субъект угрозы	Физическое или юридическое лицо, использующее новые технологии в террористических целях, например, для радикализации, вербовки и подстрекательства к совершению террористических актов, для финансирования и планирования своей деятельности, а также для совершения террористического акта. В контексте борьбы с терроризмом и новых технологий речь идет об использовании новых технологий либо для совершения злонамеренных действий, либо для побуждения других лиц к совершению террористических актов[7].
Судебное преследование/ разрешение дел	Юридический процесс, который предусматривает предъявление обвинений в терроризме физическому или юридическому лицу, проведение судебных слушаний, вынесение решения или приговора по делу и назначение наказания осужденному.

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

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

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

6 Управление Организации Объединенных Наций по наркотикам и преступности, «Руководство по подготовке и использованию оценки угроз, связанных с серьезными преступлениями и организованной преступностью: руководство SOCTA» (Нью-Йорк, штат Нью-Йорк: Организация Объединенных Наций, 2010 г.), URL: https://www.unodc.org/documents/organized-crime/SOCTA_Handbook.pdf

7 Канадский центр кибербезопасности, «Знакомство со средой киберугроз», 2023—2024 гг. (Центр безопасности коммуникаций Канады, 2022 г.), 2, URL: https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

Терроризм	Преступные деяния, в том числе против гражданского населения, совершаемые с намерением причинить смерть или тяжкие 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[8].
Уголовное правосудие	Юридический процесс, который предусматривает предъявление обвинений в терроризме физическому или юридическому лицу, проведение судебных слушаний, разрешение дела, назначение наказания, а также исправление и реабилитацию осужденных.
Уголовное расследование	Процесс сбора информации (или доказательств) для установления факта совершения преступления, выявления преступника и представления доказательств в поддержку обвинения в судебном процессе.

8 См. S/RES/1566 (2004), пункт 3.

Краткое содержание

Цель этого документа состоит в том, чтобы предоставить государствам-членам руководство по эффективной оценке и снижению террористических угроз, в особенности тех, которые связаны с использованием новых технологий, а также реагированию на такие угрозы. Проводя структурированную оценку угроз и рисков, государства-члены могут повысить уровень своей ситуационной осведомленности и общественной безопасности, а также усилить потенциал реагирования для более эффективной борьбы с терроризмом. Этот документ был составлен на основе результатов кабинетных исследований, консультаций с заинтересованными сторонами, совещаний экспертных групп и изучения передового опыта применения существующих методик оценки угроз и рисков. Противодействие использованию новых технологий в террористических целях требует понимания их применения, разработки нормативно-правовой базы и политики, а также наращивания оперативного потенциала с соблюдением прав человека и международно-правовых обязательств.

Оценка угроз и рисков является важнейшим компонентом контртеррористической деятельности, благодаря которому специалисты, отвечающие за разработку политики, могут лучше понять существующие и потенциальные угрозы, а также ресурсы, необходимые для их устранения. В настоящем документе описана методологическая структура процесса оценки угроз и рисков. Кроме того, он призван стать руководством по передовой практике в области проведения оценки угроз и рисков использования новых технологий в террористических целях. В нем также представлен уникальный цикл управления угрозами и рисками — структурированный процесс, направленный на оценку потенциальных угроз от использования новых технологий, которые существуют для страны на национальном уровне, и управление такими угрозами. Этот процесс включает в себя выявление субъектов угроз и последующий анализ их намерений и технологических возможностей для совершения террористического акта. Следующий шаг — разработка сценариев угроз, которая включает в себя анализ возможностей субъектов угроз и их доступа к новым технологиям, а также определение типов потенциальных атак и уровня их сложности. Полученный сценарий угрозы охватывает все варианты типов атак на различные уязвимые цели. Последующий этап состоит в оценке и определении приоритетности угроз в контексте мер реагирования на использование новых технологий в террористических целях. Этот этап может включать среди прочего разработку стандартных операционных процедур (СОП) для реагирования на конкретные виды технологий с учетом различных сценариев. Разработка мер реагирования на угрозы — это непрерывный процесс, который включает в себя регулярный анализ существующих сценариев угроз, выявление новых потенциальных угроз, а также актуализацию оценки угроз и стратегий реагирования.

Настоящий документ предназначен в первую очередь для специалистов-практиков, отвечающих за проведение национальной оценки террористических угроз и рисков в сотрудничестве с заинтересованными сторонами. Он призван обеспечить лучшее понимание террористических угроз и использования новых технологий для эффективного информирования разработчиков национальной политики и лиц, ответственных за принятие решений. В этом руководстве также содержатся примеры передовой практики и другая полезная информация для повышения уровня ситуационной осведомленности и усиления потенциала реагирования. Добившись глубокого понимания использования новых технологий в террористических целях с помощью структурированного процесса оценки угроз и рисков, государства-члены могут повысить эффективность своих контртеррористических мероприятий, в том числе получить ценную информацию о ландшафте угроз. Кроме того, практика проведения эффективных оценок угроз и рисков может способствовать повышению уровня общественной безопасности и разработке упреждающих мер по предотвращению или минимизации последствий террористической деятельности.

[I] Базовая информация

1.1 Обзор

Государства – члены Организации Объединенных Наций придают большое значение вопросу влияния новых технологий в борьбе с терроризмом. В ходе седьмого обзора Глобальной контртеррористической стратегии Организации Объединенных Наций (A/RES/75/291)[9] в июле 2021 года государства-члены выразили глубокую озабоченность «использованием Интернета и других информационно-коммуникационных технологий, включая платформы социальных сетей, в террористических целях, в том числе непрекращающимся распространением террористического контента», и попросили Контртеррористическое управление и другие соответствующие структуры в рамках Глобального договора по координации контртеррористической деятельности «совместно поддерживать инновационные меры и подходы в том, что касается наращивания у государств-членов (по их запросу) способности учитывать в деле предупреждения терроризма и борьбы с ним те вызовы и возможности, которые порождаются новыми технологиями, включая аспекты, относящиеся к правам человека». Резолюции 2178 (2014)[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». Платформы, на которые ссылаются государства-члены, включают Telegram, Rocket.Chat, Hoop и TamTam, среди прочих. В докладе также говорится о том, что **сторонники ИГИЛ используют платформы в 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, URL: http://undocs.org/S/RES/2178(2014)

11 Резолюция 2396 (2017) Совета Безопасности, 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 контртеррористической политики в ответ на вызовы и возможности новых технологий в деле борьбы с терроризмом при полном соблюдении 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 национальных контртеррористических мер реагирования 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 соблюдении прав человека и принципа верховенства права.
 Компонент 2.3	Расширение международного сотрудничества и обмена информацией между органами полиции государств-партнеров по вопросам противодействия использованию террористами новых технологий и применения новых технологий в борьбе с терроризмом.

1.3 Цель и назначение документа

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

1.3.1 Сфера охвата

Настоящий документ посвящен процессу оценки угроз и рисков на национальном уровне. Он призван повысить осведомленность и стать руководством по передовой практике в области разработки и реализации процедуры оценки угроз и рисков. Цель этого документа заключается в том, чтобы предоставить государствам-членам необходимые инструменты для проведения национальной оценки угроз и рисков, связанных с использованием новых технологий в террористических целях, в рамках как текущих, так и будущих ландшафтов угроз. Документ согласован с Глобальной контртеррористической стратегией Организации Объединенных Наций и

в нем подчеркивается важность соблюдения прав человека и принципа верховенства права в деле противодействия терроризму. В его основу легли результаты кабинетных исследований существующих методологий оценки угроз, консультации с заинтересованными сторонами и совещания экспертных групп. Источниками данных для кабинетных исследований послужили национальные оценки угроз и рисков государств-членов.

1.3.2 Целевая аудитория

Настоящий документ предназначен в первую очередь для специалистов-практиков, отвечающих за проведение национальной оценки террористических угроз и рисков в сотрудничестве с заинтересованными сторонами. Он призван обеспечить лучшее понимание террористических угроз и использования новых технологий для эффективного информирования разработчиков национальной политики и лиц, ответственных за принятие решений. В нем также представлена важная и полезная информация для повышения уровня их ситуационной осведомленности и усиления потенциала реагирования.

1.3.3 Преимущества

Добившись глубокого понимания использования новых технологий в террористических целях с помощью структурированного процесса оценки угроз и рисков, государства-члены могут повысить эффективность своих контртеррористических мероприятий, включив практическую информацию в анализ ландшафта угроз. Это позволит улучшить их ситуационную осведомленность, способствуя принятию более эффективных и комплексных мер по реагированию на потенциальные угрозы, распределению ресурсов и осуществлению стратегического планирования. Кроме того, проведение оценки угроз и рисков может содействовать повышению уровня общественной безопасности и разработке упреждающих мер по предотвращению или минимизации последствий террористической деятельности.

1.3.4 Ограничения

Несмотря на многочисленные преимущества документа «Проведение оценки террористической угрозы: использование новых технологий в террористических целях», существует ряд ограничивающих и сдерживающих факторов, которые следует учитывать при его использовании. К ним относятся:

- быстро меняющийся ландшафт угроз: ландшафт угроз постоянно меняется, а это значит, что любая оценка угроз является лишь «моментальным снимком», полученным по состоянию на период ее проведения. Таким образом, данные оценки угроз могут быстро устареть, если их не актуализировать для обеспечения их релевантности и точности в условиях меняющегося ландшафта угроз и непрерывного технологического прогресса;
- ограниченный доступ к информации: доступ к информации о потенциальных террористических угрозах может быть ограничен, особенно если речь идет о секретных разведывательных данных или конфиденциальной информации, которыми владеют правительства иностранных государств или представители частного сектора. Это фактор может затруднить проведение комплексной оценки угроз и рисков;
- сложность технологического ландшафта: технологический ландшафт характеризуется сложной структурой и подвержен быстрым изменениям, что создает определенные трудности в попытке отследить появление новейших технологий и их применение для совершения потенциальных террористический действий;
- ограниченность ресурсов: ресурсы (такие как деньги, рабочая сила, технологические возможности) для проведения оценки угроз могут быть ограничены;
- размеры и многообразие страны, равно как и уровень ее контртеррористического потенциала, также могут влиять на ее подход к проведению оценки и понимание собственных угроз и рисков.

[II]

Подход

2.1 Обзор

Цель настоящего доклада заключается в том, чтобы предоставить государствам-членам необходимые инструменты для проведения эффективной оценки угроз в рамках противодействия использованию новых технологий в террористических целях, которая согласована с Глобальной контртеррористической стратегией Организации Объединенных Наций и реализуется 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 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 лиц, 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 терроризме 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, ответственных за принятие решений, 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.
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, сотрудничество с различными структурами в рамках Глобального договора по координации контртеррористической деятельности, а также руководящую основу, описанную выше в разделе 2.2. Исследования и консультации с заинтересованными сторонами и экспертами были направлены на определение эффективной методологии оценки угроз и реагирования на них, а также возможностей ее применения для устранения типов угроз, возникающих вследствие использования новых технологий, в том числе наряду с применением новых технологий специалистами для реагирования на угрозы.

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

2.3.1 Совещания экспертных групп и консультации

Данное руководство было разработано при участии экспертов в рамках совещаний экспертных групп (СЭГ), а также по результатам индивидуальных консультаций и обзоров. СЭГ объединили экспертов и практиков из контртеррористических служб и правоохранительных органов, правозащитных организаций, частного сектора, научных кругов и гражданского общества для обсуждения вопросов, связанных с противодействием использованию новых технологий в террористических целях, применением новых технологий в рамках проводимой работы, определением 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 право прав человека, беженское и гуманитарное право.

2.3.2 Обзор справочных материалов

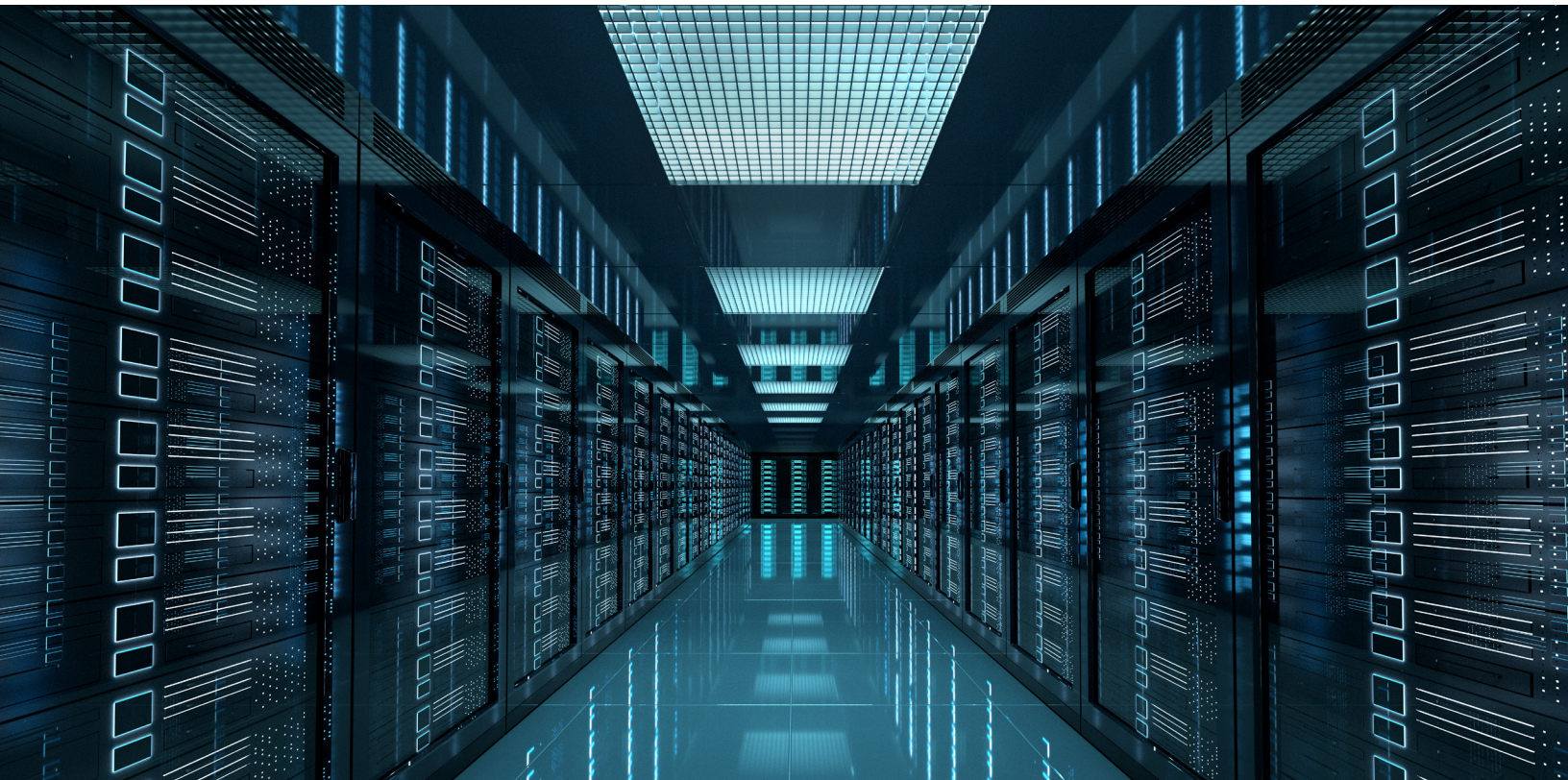
При разработке настоящего руководства были задействованы, приняты во внимание, дополнены и использованы в качестве основы данные имеющихся исследований, руководств и публикаций, среди которых:

ТАБЛИЦА 3. **Справочные материалы**

1	Amritt, Carl, Eliot Bradshaw, and Alyssa Schulenberg. "Threat Assessment and Management: Practices Across the World" («Оценка угроз и управление ими: обзор примеров из мировой практики»). Domestic Preparedness, February 1, 2023, https://www.domesticpreparedness.com/preparedness/threat-assessment-and-management-practices-across-the-world/
2	Bloom, Mia, Hicham Tiflati, and John Horgan. "Navigating ISIS's Preferred Platform: Telegram" («Обзор предпочтительной платформы ИГИЛ: Telegram»). *Terrorism and Political Violence 31, no. 6* (November 2, 2019): 1242–54, https://doi.org/10.1080/09546553.2017.1339695
3	Канада, Министерство общественной безопасности. «Национальная концепция уровней террористической угрозы Канады», консультации, 25 августа 2016 г., https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html
4	Канадский центр кибербезопасности. «Знакомство со средой киберугроз», 2023—2024 гг. Центр безопасности коммуникаций Канады, 2022 г., https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment
5	Центр анализа терроризма (CTA). «Оценка террористической угрозы для Дании». Дания: Центр анализа терроризма (CTA), март 2022 г., https://www.readkong.com/page/assessment-of-the-terrorist-threa-t-to-denmark-march-2021-4207448
6	CIVI.POL Conseil и Королевский объединенный институт оборонных исследований, «Оперативное руководство по подготовке и реализации мер, направленных на противодействие терроризму и насильственному экстремизму в третьих странах, при финансовой поддержке ЕС». Европейская комиссия, 2018 г., https://ct-morse.eu/wp-content/uploads/2017/11/EU-CT-CVE-guidelines.pdf
7	Cole, Mara. "Towards Proactive Airport Security Management: Supporting Decision Making through Systematic Threat Scenario Assessment" («Упреждающий подход к управлению системой безопасности в аэропортах: поддержка принятия решений с помощью систематической оценки сценариев угроз»). *Journal of Air Transport Management 35* (March 1, 2014): 12–18, https://doi.org/10.1016/j.jairtraman.2013.11.002
8	Координационная группа по анализу угроз (CUTA). «Общая база данных (CDB)», https://cuta.belgium.be/the-common-database-cdb/ (дата обращения: 5 июня 2024 г.).
9	Coordination Unit for Threat Analysis (CUTA). "The Strategic Note Extremism and Terrorism (Strategy T.E.R.)." https://cuta.belgium.be/the-strategic-note-extremism-and-terrorism-strategy-t-e-r/ (дата обращения: 5 июня 2024 г.).
10	Erez Magen, and R. "Enabling Advancements in Security-Danger and Opportunities." Maarachot (Systems) (blog), March 29, 2022. («Новые достижения в области безопасности: опасности и возможности»). Maarachot (Systems) (blog), March 29.
11	Европейская комиссия. «Проектируемая безопасность: защита общественных мест от террористических атак». Люксембург: Европейский союз, 2022 г. https://home-affairs.ec.europa.eu/news/security-design-protection-public-spaces-terrorist-attacks-2022-12-14_en
12	Европейская комиссия. «Контртеррористическая повестка ЕС: предвидеть, предупреждать, защищать, реагировать». Сообщение Комиссии Европейскому парламенту, Совету, Европейскому экономическому и социальному комитету и Комитету по делам регионов. Брюссель, Бельгия: Европейская комиссия, 2020 г., https://ec.europa.eu/newsroom/pps/items/696784/en
13	Европейская комиссия: Информационная служба общественных исследований и разработок (CORDIS). «Обнаружение и анализ онлайн-контента и финансовой деятельности, связанных с терроризмом». https://cordis.europa.eu/project/id/700367, (дата обращения: 5 июня 2024 г.).
14	Европейская комиссия: Информационная служба общественных исследований и разработок (CORDIS). «Поиск и анализ гетерогенного онлайн-контента для распознавания террористической деятельности», https://cordis.europa.eu/project/id/700024 (дата обращения: 5 июня 2024 г.).

15	Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ). «Национальная оценка рисков отмывания денег и финансирования терроризма», февраль 2013 г., https://www.fatf-gafi.org/en/publications/Methodsandtrends/Nationalmoneylaunderingandterroristfinancingriskassessment.html
16	Flanders, Rob, Lucy Johnson, Matthew Trevelyan, Anna Whitmore, Lisa Lesowiec, and Rajinder Tumber. "Cyber Threat Intelligence in Government: A Guide for Decision Makers and Analysts" («Сбор и анализ оперативной информации о киберугрозах на государственном уровне: руководство для лиц, ответственных за принятие решений, и аналитиков»). 2nd ed. United Kingdom, 2019.
17	Hemmingsen, Ann-Sophie. "An Introduction to the Danish Approach to Countering and Preventing Extremism and Radicalization." Copenhagen, Denmark: Danish Institute for International Studies, 2015 («Введение в датский подход к предотвращению экстремизма и радикализации и противодействию им»), https://www.ft.dk/samling/20151/almdel/reu/bilag/248/1617692.pdf
18	Министерство внутренних дел Испании. Национальная контртеррористическая стратегия, 2019 г., https://www.dsn.gob.es/eu/file/4271/download?token=-K6uOf-C
19	Международная организация по стандартизации. ISO 31000 «Менеджмент риска. Принципы и руководство», второе издание. Швейцария, 2018 г., https://www.iso.org/standard/65694.html
20	Lotz, Volkmar. "Threat Scenarios as a Means to Formally Develop Secure Systems" («Сценарии угроз как средство формальной разработки безопасных систем»). In Computer Security — ESORICS 96, edited by Elisa Bertino, Helmut Kurth, Giancarlo Martella, and Emilio Montolivo, 242–65. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996.
21	Министерство юстиции Швеции. «Предотвратить, упредить, защитить: шведская контртеррористическая стратегия». Швеция: Органы государственной власти Швеции, 2014 г., https://www.government.se/legal-documents/2015/09/skr.-201415146/
22	Национальный координационный центр по безопасности и борьбе с терроризмом. «Оценка террористической угрозы NCTV: угроза в Нидерландах и для Нидерландов стала более сложной и глобальной — Раздел «Новости» — Национальный координационный центр по безопасности и борьбе с терроризмом». Министерство юстиции и безопасности: Национальный координационный центр по безопасности и борьбе с терроризмом. Министерство юстиции и безопасности, 7 ноября 2022 г., https://english.nctv.nl/latest/news/2022/11/07/nctvs-terrorist-threat
23	Национальный координационный центр по безопасности и борьбе с терроризмом. «Оценка террористической угрозы в Нидерландах», Министерство юстиции и безопасности,14 мая 2020 г., https://english.nctv.nl/topics/terrorist-threat-assessment-netherlands
24	Neil J. Smelser. "Motivation, Social Origins, Recruitment, Groups, Audiences, and the Media in the Terrorism Process" («Мотивация, социальные истоки, вербовка, группы, аудитории и СМИ в террористической деятельности»). In The Faces of Terrorism: Social and Psychological Dimensions, 92–119. Science Essentials. Princeton, N.J.: Princeton University Press, 2007, https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,sso&db=e000xww&AN=286616&authtype=sso&custid=s5903540&lang=he&site=eds-live&scope=site&authtype=ip,sso&custid=s5903540
25	Служба безопасности и разведки Новой Зеландии. «Объединенная группа по оценке угроз». Служба безопасности и разведки Новой Зеландии, https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/combined-threat-assessment-group/ (дата обращения: 5 июня 2024 г.).
26	Служба безопасности и разведки Новой Зеландии. «Как можно помочь: форма участия общественности», https://providinginformation.nzsis.govt.nz/ (дата обращения: 5 июня 2024 г.).
27	Служба безопасности и разведки Новой Зеландии. «Национальный уровень террористической угрозы», https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/national-terrorism-threat-level/ (дата обращения: 5 июня 2024 г.).
28	Транспортное агентство Новой Зеландии. «Реестр рисков». Правительство. Транспортное агентство Новой Зеландии, https://www.nzta.govt.nz/roads-and-rail/rail/operating-a-railway/risk-management/risk-register/ (дата обращения: 5 июня 2024.).
29	ProtectUK. «Уровни угрозы», 12 марта, 2022 г., https://www.protectuk.police.uk/threat-levels
30	Romyn, David, and Mark Kebbell. "Terrorists' Planning of Attacks: A Simulated 'Red-Team' Investigation into Decision-Making" («Планирование террористами нападений: моделирование процесса принятия решений силами «красной команды»). *Psychology, Crime & Law 20*, no. 5 (May 28, 2014): 480–96, https://www.doi.org/
31	Служба безопасности MI5. «Объединенный аналитический центр по терроризму». https://www.mi5.gov.uk/joint-terrorism-analysis-centre (дата обращения: 5 июня 2024.).
32	Shacklett, Mary E. "What Is Attack Vector?" («Что такое вектор атаки?»), Tech Target, April 2021, https://www.techtarget.com/searchsecurity/definition/attack-vector

33	Strachan-Morris, David. "Threat and Risk: What Is the Difference and Why Does It Matter?" («Угроза и риск: в чем отличия и почему они важны?»). *Intelligence and National Security 27*, no. 2 (April 1, 2012): 172–86, https://doi.org/10.1080/02684527.2012.661641
34	Thorne, David. "National Level Threat Assessment-Canadian Model." («Оценка угроз на национальном уровне: канадская модель», доклад для 2-го семинара по упреждающему подходу к борьбе с терроризмом. Исламабад, Пакистан: Управление Организации Объединенных Наций по наркотикам и преступности, 12 апреля 2018 г.), https://www.unodc.org/documents/pakistan//Report-2nd-Workshop-Proactive-Approach-to-CT-web.pdf
35	Объединение киберкластеров Великобритании (UKC3). «Операционная основа киберкластеров». UK Cyber Cluster Collaboration (блог), https://ukc3.co.uk/cyber-cluster-operating-framework/ (дата обращения: 5 июня 2024 г.).
36	Контртеррористический центр Организации Объединенных Наций и Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия. «Алгоритмы и терроризм: злонамеренное использование искусственного интеллекта в террористических целях». Совместный доклад. Организация Объединенных Наций, 2021 г., https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes
37	Контртеррористический центр Организации Объединенных Наций и Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия. «Борьба с терроризмом в Интернете с помощью искусственного интеллекта: обзор для правоохранительных и антитеррористических агентств в Южной Азии и Юго-Восточной Азии». Совместный доклад. Организация Объединенных Наций, 2021 г., https://unicri.it/News/-Countering-Terrorism-Online-with-Artificial-Intelligence
38	Управление Организации Объединенных Наций по наркотикам и преступности. «Руководство по подготовке и использованию оценки угроз, связанных с серьезными преступлениями и организованной преступностью: руководство SOCTA». Нью-Йорк, штат Нью-Йорк: Организация Объединенных Наций, 2010 г., https://www.unodc.org/documents/organized-crime/SOCTA_Handbook.pdf
39	Исполнительный директорат Контртеррористического комитета Совета Безопасности Организация Объединенных Наций (ИДКТК). «Аналитическая записка ИДКТК: противодействие террористической пропаганде онлайн и офлайн». Организация Объединенных Наций, 2020 г., https://www.un.org/securitycouncil/ctc/content/cted-analytical-brief-%E2%80%93-countering-terrorist-narratives-online-and-offline
40	Соединенный Штаты Америки. «Национальная стратегия борьбы с терроризмом Соединенных Штатов Америки». Вашингтон, округ Колумбия: Белый дом, 2018 г., https://purl.fdlp.gov/GPO/gpo109871
41	Государственный департамент Соединенный Штатов Америки. «О нас: Центр глобального взаимодействия», https://www.state.gov/about-us-global-engagement-center-2/ (дата обращения: 5 июня 2024 г).
42	Waitzman, Eren. "National Risk Register: Preparing for National Emergencies." («Национальный реестр рисков: обеспечение готовности к национальным чрезвычайным ситуациям». Парламент Соединенного Королевства: Библиотека Палаты лордов, 14 декабря 2022 г.), https://lordslibrary.parliament.uk/national-risk-register-preparing-for-national-emergencies/



[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. Для эффективного противодействия этой угрозе крайне важно проводить комплексные оценки угроз, предусматривающих проведение многостороннего анализа потенциальных рисков, уязвимостей и последствий, связанных с освоением террористами новых технологий. Понимая все тонкости сложной взаимосвязи этих элементов, правоохранительные органы смогут разработать упреждающие стратегии и принять соответствующие меры для смягчения угроз, возникающих в результате использования террористами новейших 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[14], из которых более 93 процентов — это пользователи социальных сетей[15]. По оценкам, в 2022 году в мире будет создано более 97 зеттабайт[16] информации[17]. В то время как подобные технологические достижения способствуют преобразованию общества во имя всеобщего блага, террористы используют эти технологии в 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.

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

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

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

16 Один зеттабайт равен одному миллиарду терабайтов.

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

3.2.1 Вызовы: использование новых технологий в террористических целях

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

3.2.2 Возможности: контртеррористическая деятельность правоохранительных органов

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

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

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

ООН, Интерпол и ЕС неоднократно подчеркивали взаимосвязь между новыми технологиями, борьбой с терроризмом и правами человека, включая гендерное равенство. В Глобальной контртеррористической стратегии ООН и различных резолюциях Генеральной Ассамблеи и Совета Безопасности подчеркиваются обязательства государств-членов по соблюдению международного права прав человека, международного беженского права и международного гуманитарного права в деле противодействия терроризму. В частности, согласно Глобальной контртеррористической стратегии ООН «действенные меры по борьбе с терроризмом и защита прав человека являются целями, которые не противоречат, а дополняют и взаимно подкрепляют друг друга», в связи с чем необходимо принять меры по обеспечению всеобщего уважения прав человека и принципа верховенства права в качестве фундаментальной основы борьбы с терроризмом. В связи с этим в Стратегии государствам-членам предлагается бороться с использованием Интернета и других информационно-коммуникационных технологий, включая платформы социальных сетей, в террористических целях, в том числе с непрекращающимся распространением террористического контента, при соблюдении международного права, включая международное право прав человека, а также право на свободу выражения мнений.

3.2.4 Гендер, технологии и оценка угроз

Понятие «гендер» охватывает роли, поведение, занятия и качества, которые в конкретном обществе в определенный период времени считаются подходящими для мужчин и женщин, девочек и мальчиков. Помимо социальных атрибутов и возможностей, ассоциируемых с принадлежностью к мужскому или женскому полу, гендер связан с отношениями между женщинами и мужчинами, девочками и мальчиками. Гендер является частью более широкого социокультурного контекста и пересекается с другими факторами идентичности, включая пол, социальный класс, расовую принадлежность, уровень бедности, этническую принадлежность, сексуальную ориентацию, возраст и т. д. Мужчины, женщины, девочки и мальчики, а также лица с другими гендерными идентичностями и моделями самовыражения чувствуют себя в безопасности по-разному и в соответствии со своими особыми потребностями, уязвимостями и возможностями[18]. В частности, несмотря на отсутствие иерархических структур в Интернете, которое позволяет устранить гендерные ограничения и создает возможности для расширения прав и возможностей женщин, использование новых технологий также повышает вероятность их вербовки или активного участия в деятельности насильственных экстремистских и террористических групп в Интернете[19]. По имеющимся данным, террористические группы умело используют гендерные аспекты в своих онлайн-коммуникациях; например, ИГИЛ построило свою страте-

18 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

19 ИДКТК, «Гендерные аспекты мер реагирования, принимаемых в связи с возвращением иностранных боевиков-террористов: перспективы исследований», февраль 2019 г., URL: https://www.un.org/securitycouncil/ctc/content/gender-dimensions-response-returning-foreign-terrorist-fighters-research-perspectives

гию вербовки и общения в Интернете на противоречивых гендерно ориентированных сообщениях, меняя свой дискурс в зависимости от целевой группы[20]. Еще один важный аспект, касающийся гендера и новых технологий, связан с цифровым гендерным разрывом, согласно которому во всем мире доступ женщин к Интернету оценивается в 85 процентов по сравнению с мужчинами, при этом около 1,7 млрд женщин из стран глобального Юга вообще не имеют доступа к нему. Такое неравенство создает проблемы в области прав человека, лежащие в основе всех аспектов кибербезопасности, включая потенциальную подверженность риску, отсутствие безопасности или участие в структуре управления[21].

Следовательно, учет гендерных аспектов при оценке террористических угроз и реагировании на них имеет решающее значение для анализа намерений и потенциальных целей террористов, а также для разработки соответствующих мер реагирования с учетом особых потребностей и уязвимостей представителей различных гендеров и таких взаимопересекающихся факторов, как возраст, инвалидность, этническая принадлежность, язык, национальность, расовая принадлежность, религия, сексуальная ориентация или любой другой фактор идентичности и их сочетания.

20 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»).

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

[IV] Оценка угроз и рисков

4.1 Обзор

При осуществлении контртеррористических мероприятий важно проводить различие между оценкой угроз и оценкой рисков. Сочетание этих двух инструментов лежит в основе эффективного реагирования специалистов на местах и заинтересованных сторон на потенциальные угрозы в их ЗО. Угроза описывает в основном, «кто» и «что» является субъектами угрозы, и их предполагаемые действия. Риск описывает вероятность осуществления угрозы и степень потенциального ущерба от таких действий[22]. Таким образом, оценка рисков может быть построена и проведена на основе данных, полученных в ходе оценки угроз[23].

Оценка угроз — первый элемент этого цикла. Угроза — это продукт возможностей и намерений[24]. Потенциал включает в себя известные способности террористической группы, ее материально-технические ресурсы, возможности командования и управления, процент успешно реализованных атак, сложность предыдущих атак, уровень подготовки и все, что известно о возможностях, которые она пытается получить[25]. В контексте контртеррористических мероприятий, направленных на противодействие использованию террористами новых технологий, к потенциалу также относятся виды новых технологий, имеющихся у субъекта угрозы, и то, насколько хорошо он может управлять этими технологиями или использовать их. Намерения в данном случае выступают в качестве мерила желания и возможности субъекта угрозы совершить террористическую атаку[26].

При определении риска осуществления различных угроз необходимо оценивать вероятность (а также повторность) совершения атаки и ущерб, который она может нанести[27]. В контексте новых технологий под ущербом можно понимать как физический ущерб (будь то прямой результат атаки или остаточный эффект от повреждения системы), так и ущерб системе (например, различные кибератаки могут привести к потере или утечке данных, сбоям в работе системы, функциональному отказу критически важных объектов инфраструктуры и т. д.)[28].

Кроме того, при планировании, сборе, анализе и распространении результатов оценки угроз и оперативной информации крайне важно учитывать гендерные аспекты, поскольку это может способствовать выявлению незамеченных признаков нестабильности, преодолению потенциальных гендерных предубеждений и всестороннему пониманию социального контекста и динамики[29]. Учет гендерных аспектов на всех этапах разведывательного цикла также позволяет предвосхитить и минимизировать любые негативные последствия сбора и распространения оперативной информации для прав человека тех, кого они затрагивают. Таким

22 David Strachan-Morris, "Threat and Risk: What Is the Difference and Why Does It Matter?" («Угроза и риск: в чем отличия и почему они важны?»), *Intelligence and National Security* 27, no. 2 (April 1, 2012): 172–86, URL: https://doi.org/10.1080/02684527.2012.661641

23 Strachan-Morris, 180.

24 Strachan-Morris, 174.

25 Strachan-Morris, 174.

26 Strachan-Morris, 173.

27 Strachan-Morris, 173 and 180.

28 Strachan-Morris, 180.

29 Lauren Hutton et al., "Intelligence and Gender", (OSCE, 2019). («Разведывательные службы и гендер»), URL: https://www.dcaf.ch/tool-14-intelligence-and-gender

образом, гендерные аспекты важны не только для получения точной и ценной оперативной информации, но и для обеспечения соответствия разведывательных операций международным стандартам в области прав человека и гендерного равенства.

Ниже проиллюстрированы процессы оценки угроз и рисков, их различия и взаимосвязь:

РИСУНОК 4

Оценка угроз и рисков — это процесс выявления потенциальных угроз и оценки вероятности их осуществления и их потенциальных последствий с целью разработки стратегий и политики по минимизации связанных с ними рисков или управлению такими рисками. Процесс оценки угроз и рисков предусматривает выявление угроз, а также анализ намерений и потенциала субъектов угроз совершить террористический акт. Результаты оценки угроз являются основой для реализации остальных этапов цикла, поскольку они дают первоначальное представление о потенциальной террористической угрозе.

Оценка угроз используется для понимания потенциальных угроз, стоящих перед отдельными лицами, организациями и (или) государствами-членами с учетом таких факторов, как субъект угрозы (его идеология, потенциал и намерения) и потенциальные объекты угрозы. Она способствует выработке направлений контртеррористической политики и мер реагирования и является неотъемлемым компонентом контртеррористической деятельности, поскольку дает разработчикам политики и другим заинтересованным сторонам более глубокое понимание как существующих угроз, так и ресурсов, которые могут потребоваться для борьбы с этими угрозами. Например, оценки угроз позволяют выявить применение террористами новых технологий, а также определить, каким образом можно использовать новые технологии в качестве ресурса для реагирования на новые угрозы. В контексте понимания использования новых технологий в террористических целях оценки угроз позволяют государствам-членам понять потенциальные угрозы, а также противодействовать существующим, которые требуют разного уровня внимания, путем определения их приоритетности.

Оценка угроз и рисков — это процесс формирования целостного представления об угрозах, мерах безопасности и потенциальных планах по борьбе с этими угрозами для лиц, ответственных за принятие решений. В каждом из следующих разделов описаны ключевые компоненты процесса оценки угроз и рисков, а также подробно представлены такие понятия, как оценка угроз, сценарии угроз, оценка субъектов и сценариев угроз, приоритизация рисков, меры реагирования на угрозы и оценка воздействия плана реагирования на предыдущие компоненты.

Наряду с методологией оценки угроз и рисков и реагирования на них также приведены примеры передовой практики государств-членов и международных организаций в контексте оценки угроз и рисков.

4.2 Цикл управления угрозами и рисками

РИСУНОК 5

Представленный выше цикл управления угрозами и рисками — это структурированный процесс, направленный на оценку потенциальных угроз для страны на национальном уровне. Он включает в себя ряд этапов, которые необходимы для оценки и ослабления потенциальных угроз и связанных с ними рисков. «Горизонт» цикла управления угрозами и рисками — это период оценки потенциальных угроз и управления рисками. В тех случаях, когда эволюция новых технологий рассматривается как часть оценки угроз и рисков, «горизонт» цикла может быть более длительным и составлять от двух до пяти лет.

Рамочная модель оценки угроз и рисков использования новых технологий в террористических целях состоит из нескольких этапов, которые вместе образуют цикл управления угрозами и рисками. Она включает в себя оценку угроз, разработку сценариев угроз, оценку субъектов и сценариев угроз, а также определение приоритетности рисков, выработку мер реагирования на угрозы и оценку воздействия.

4.2.1 Оценка субъекта угрозы

РИСУНОК 6

Для проведения анализа субъекта угрозы необходимо изучить множество ситуационных факторов. Среди них — намерения и потенциал. Под намерениями понимается желание субъекта угрозы в сочетании с его уверенностью. Потенциал субъекта угрозы включает имеющиеся в его распоряжении ресурсы (например, финансовые, технологические, людские и т. д.), а также навыки или знания, которыми он обладает для использования этих ресурсов.

Для понимания концепции намерений применительно к анализу субъекта угрозы также важно понимать, что намерения (или мотивация) не являются монолитным элементом, а состоят из множества факторов, которые побуждают субъекта угрозы совершить нападение[30]. Преступные акты, которые совершает субъект угрозы, нацелены на то, чтобы «вызвать состояние ужаса у широкой общественности, или группы лиц, или отдельных лиц, запугать население или заставить правительство или международную организацию совершить какое-либо действие или воздержаться от его совершения, и представляют собой преступления по смыслу международных конвенций и протоколов, касающихся терроризма, и в соответствии с содержащимися в них определениями»[31]. За этими актами могут стоять недовольства религиозного, политического, социального,

30 Neil J. Smelser, "Motivation, Social Origins, Recruitment, Groups, Audiences, and the Media in the Terrorism Process" («Мотивация, социальные истоки, вербовка, группы, аудитории и СМИ в террористической деятельности»), in *The Faces of Terrorism: Social and Psychological Dimensions*, Science Essentials (Princeton, N.J.: Princeton University Press, 2007), 92–119, URL: https://press.princeton.edu/books/paperback/9780691149356/the-faces-of-terrorism

31 См. резолюцию 1566 Совета Безопасности.

экономического характера или их сочетание. Мотивы, которыми руководствуются разные субъекты угрозы, также могут отличаться[32]. Следовательно, важно понять причины, по которым субъект угрозы может быть вовлечен в террористическую деятельность, либо мотивацию или цели субъекта угрозы, которые его побуждают к совершению террористической атаки. Факторы намерения могут быть идеологическими, а также связанными с политическими убеждениями, желаниями или состоянием психического здоровья, и все они могут повлиять на намерение субъекта угрозы совершить теракт. Например, идейные подходы, используемые для оправдания нападений, совершаемых группами на почве ксенофобии, расизма и иных форм нетерпимости, а также во имя религий или убеждений, часто характеризуются женоненавистничеством; такие группы также склонны проявлять нетерпимость в отношении сексуальной ориентации и гендерной идентичности[33]. Оценив намерения субъекта угрозы, аналитики могут определить потенциальные объекты угрозы и типы атак, которые он может планировать. Одним из других ключевых компонентов в понимании намерений, лежащих в основе угрозы, является понимание предполагаемого объекта угрозы, поскольку осознание своей целевой аудитории и последствий нападения на эту аудиторию может оказать значительное влияние на субъекта угрозы и способы осуществления им атаки[34].

Под потенциалом понимаются ресурсы и навыки/знания (или опыт), которыми располагает субъект угрозы для совершения террористического акта. К ним относятся доступ к людским ресурсам или организации, инструментам и оборудованию (например, доступ к оружию и (или) технологиям), обучение, а также уровень финансовой или иной поддержки. Оценив потенциал субъекта угрозы, специалисты-практики могут определить степень вероятности совершения им успешной террористической атаки.

Как намерения, так и потенциал являются важными факторами при анализе субъектов угроз, поскольку субъект угрозы с сильными намерениями, но ограниченным потенциалом может быть не в состоянии осуществить террористическую атаку, а субъект угрозы с сильным потенциалом, но слабыми намерениями может быть недостаточно мотивирован для совершения нападения. Учет обоих факторов при проведении оценки угроз позволяет получить более полное представление об угрозе, исходящей от конкретного субъекта угрозы или террористической организации, и принять соответствующие меры для предотвращения или ослабления угрозы совершения террористического акта.

4.2.2 Разработка сценариев угроз

РИСУНОК 7

32 Канадский центр кибербезопасности, «Знакомство со средой киберугроз», 2023–2024 гг., 2, URL: https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

33 A/77/266.

34 Neil J. Smelser, "Motivation, Social Origins, Recruitment, Groups, Audiences, and the Media in the Terrorism Process" («Мотивация, социальные истоки, вербовка, группы, аудитории и СМИ в террористической деятельности»), 106.

Вторым этапом цикла управления угрозами и рисками является разработка сценариев угроз, в ходе которой информацию об угрозах, полученную в результате анализа субъектов угроз, подвергают дальнейшему анализу, чтобы получить представление о субъекте(ах), векторах, объектах угроз и технологиях, используемых для их осуществления. Анализ субъектов угроз и разработка сценариев угроз — это два взаимосвязанных инструмента, которые используются как при управлении угрозами и рисками, так и при планировании мер в области безопасности. Если оценка угроз состоит в выявлении и анализе потенциальных угроз, то сценарии угроз — это конкретные примеры таких угроз, которые используются на этапе планирования и подготовки к ним. Результатом разработки сценариев угроз станет более глубокое понимание механики совершения потенциальной атаки, технологий, используемых для ее реализации и стоящего за ней террориста.

Разработка сценариев угроз предполагает выявление потенциальных субъектов угроз, которые могут использовать новые технологии в террористических целях. К ним могут относиться известные террористические группы, лица с экстремистскими убеждениями или другие субъекты, которые могут пытаться использовать технологии в злонамеренных целях. Затем необходимо проанализировать потенциал субъектов угрозы, а также учесть их доступ к новым технологиям и уровень их технических знаний. Этот анализ позволит определить типы потенциальных атак и уровень их сложности. Далее следует проанализировать потенциальные уязвимости или типы атак, которые могут повлиять на полученные данные, включая предполагаемые субъекты угроз[35].

Часть процесса разработки тестовых сценариев для оценки угроз, рисков и мер реагирования на них заключается в том, чтобы создать базу для упреждающего подхода к управлению угрозами, которым смогут пользоваться заинтересованные стороны. В рамках такого подхода еще одной мерой, которую могут принять заинтересованные стороны, является внедрение принципов «проектной безопасности». Концепция проектной безопасности подразумевает установку средств обеспечения безопасности на этапе возведения объекта для его надлежащей защиты от угроз в рамках существующей структуры/конфигурации/конструкции[36]. Примером применения такой концепции в контексте мер реагирования на угрозу использования новых технологий в террористических целях может служить разработка СОПов по реагированию на конкретные виды технологий, которые можно легко адаптировать под различные сценарии.

Полученный сценарий угрозы охватывает все итерации типов атак, объектами которых являются различные уязвимости[37]. В рамках этого анализа одной из ключевых составляющих при разработке сценариев угроз является понимание контекста и «сочетание определенных ключевых элементов»[38]. Иными словами, серьезность угрозы будет зависеть от того, сколько ключевых элементов существует в рамках конкретного сценария. При подготовке к обеспечению защиты от угроз разработка и анализ сценариев угроз становятся ключевыми элементами в предотвращении нанесения ущерба в будущем. Сценарий угрозы описывает гипотетический пример развития различных событий, которые могут произойти, и, как правило, разрабатывается после выявления и оценки угроз (см. раздел 4.2.1). Цель создания сценариев угроз заключается в том, чтобы заблаговременно подготовиться к будущим атакам и защититься от них до того, как они станут серьезной угрозой. На рисунке 8 ниже представлены составляющие каждого из компонентов сценария угрозы[39].

35 Volkmar Lotz, "Threat Scenarios as a Means to Formally Develop Secure Systems" («Сценарии угроз как средство формальной разработки безопасных систем») in *Computer Security — ESORICS 96*, ed. Elisa Bertino et al. (Berlin, Heidelberg: Springer Berlin Heidelberg, 1996), 250; Mara Cole, "Towards Proactive Airport Security Management: Supporting Decision Making through Systematic Threat Scenario Assessment" («Упреждающий подход к управлению системой безопасности в аэропортах: поддержка принятия решений с помощью систематической оценки сценариев угроз»), *Journal of Air Transport Management 35* (March 1, 2014): 15, URL: https://doi.org/10.1016/j.jairtraman.2013.11.002

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

37 Там же.

38 Cole, "Towards Proactive Airport Security Management: Supporting Decision Making through Systematic Threat Scenario Assessment" («Упреждающий подход к управлению системой безопасности в аэропортах: поддержка принятия решений с помощью систематической оценки сценариев угроз»), 12.

39 О субъектах угроз см. также Канадский центр кибербезопасности, «Знакомство со средой киберугроз», 2023–2024 гг., 2.

4.2.3 Оценка сценариев и приоритизация угроз

РИСУНОК 8

Третий этап цикла управления угрозами и рисками заключается в оценке субъектов и сценариев угроз и в приоритизации рисков, в ходе чего угрозы и связанные с ними риски рассматриваются с учетом факторов осуществимости, вероятности, последствий и критичности. Цель этой части цикла — обеспечить понимание серьезности угрозы и рисков, которые она представляет, чтобы специалисты-практики могли принимать обоснованные решения о том, какие угрозы требуют выделения большего количества ресурсов для реагирования на них. По результатам оценки и приоритизации можно будет определить уровень серьезности угрозы с помощью модели светофора (которая будет рассмотрена ниже), что позволит выбрать подходящие варианты политики для принятия мер реагирования (см. раздел 4.2.4). Оценка угроз и приоритизация рисков необходимы для проверки реалистичности потенциальной угрозы и определения приоритетности наиболее опасных угроз для государства-члена. Решение этих задач позволит правильно распределить государственные ресурсы для реагирования на угрозы или их ослабления. При этом следует учитывать, что государства-члены не располагают всеми ресурсами для борьбы с каждой выявленной угрозой. Следовательно, угрозы необходимо приоритизировать, чтобы добиться максимального эффекта от применяемых мер реагирования.

Прежде чем приступать к приоритизации риска, он должен пройти оценку, в ходе которой специалисты-практики, являющиеся экспертами в этой области, определяют такие факторы, как осуществимость представленной угрозы, а также вероятность того, что такая угроза или атака могут быть реализованы. Оценка осуществимости потенциальной атаки предполагает понимание намерений и потенциала субъекта угрозы, а также его подготовительных мероприятий. Если намерения, потенциал и предварительные действия, предшествующие атаке, не совпадают, угроза может быть признана мало осуществимой. При обсуждении вероятности или допустимости совершения террористического акта следует проанализировать потенциальный риск его реализации. Также необходимо оценить уязвимости объекта угрозы в государстве и принятых государством мер противодействия. Если угроза осуществима, но объект угрозы не является высокоуязвимым либо меры противодействия, принятые для реагирования на потенциальные угрозы, эффективны, оцениваемая угроза будет иметь более низкий приоритет, чем та, которая признана осуществимой, но объект угрозы либо не имеет надлежащих механизмов защиты, либо имеет уязвимость, которая еще не устранена.

По завершении оценки угроз необходимо определить приоритетность рисков, которые они представляют, для обеспечения разработки плана реагирования и эффективного распределения ресурсов. В процессе приоритизации угроз и сопутствующих рисков следует учитывать такие факторы, как понимание последствий

угрозы в случае ее реализации и критичность связанного с ней риска. В контексте понимания риска, связанного с угрозой, специалистам необходимо оценить потенциальное воздействие новых технологий, являющихся частью угрозы, на объекты инфраструктуры, службы и людей.

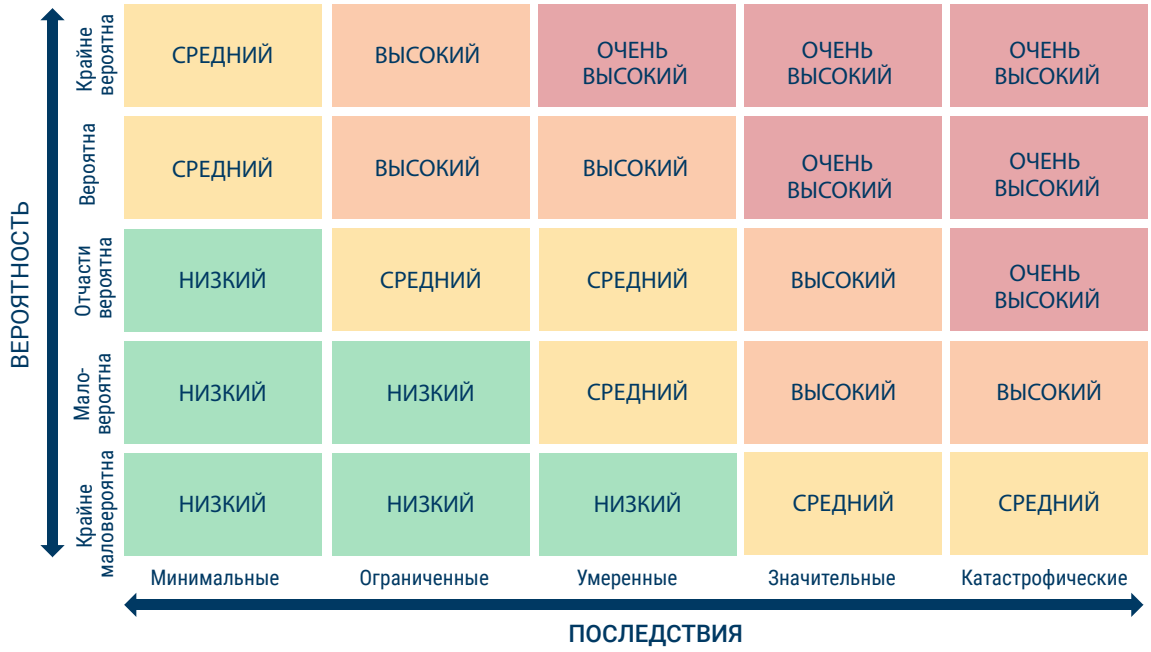
Частью эффективной оценки угрозы является понимание оптимального варианта ее классификации для принятия действенных мер реагирования на нее. Чтобы классифицировать угрозу, необходимо оценить ее вероятность, воздействие и меры по управлению угрозами. «Вероятность» означает вероятность возникновения угрозы, а «воздействие» — степень и масштаб воздействия. Под «мерами по управлению угрозами» понимается действующая политика или технологии, обеспечивающие защиту от угроз. На рисунке ниже представлена модель, которую можно использовать для оценки и классификации угроз.

РИСУНОК 9

Дополнительным компонентом процесса оценки угроз и приоритизации рисков является оценка уровня угрозы и связанных с ней рисков. При определении уровня угрозы и связанных с ней рисков рекомендуется использовать модель светофора для обеспечения четкой приоритизации угроз.

Ниже приведена наглядная модель распределения различных уровней угроз, которая показывает, как следует их оценивать при определении уровня угрозы в рамках проведения оценки угроз и рисков.

РИСУНОК 10

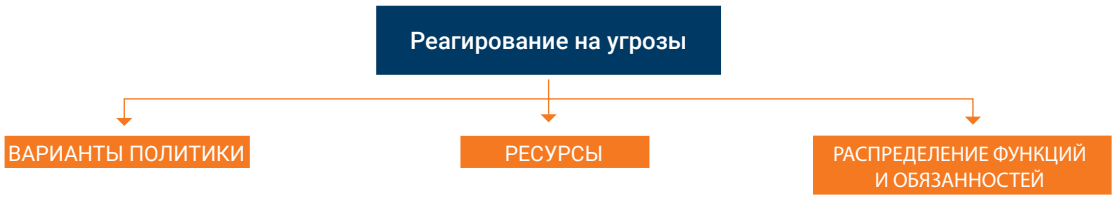


Определение того, какой уровень угрозы считать низким, средним, высоким или очень высоким, может варьироваться, но именно на него ориентируются лица, ответственные за принятие решений, при установлении порогового значения, иначе говоря, «приемлемого уровня риска».

Еще одним компонентом, обеспечивающим достаточную подготовку разработчиков контртеррористической политики к потенциальным угрозам, является метод «красной команды». Этот процесс включает в себя моделирование потенциальных угроз, с помощью которого команда реагирования сможет отработать правильные ответные действия и выявить потенциальные недостатки в текущих мерах реагирования. Для этого создается «красная команда», задача которой — смоделировать атаку[40]. Применение подобных методик позволит командам реагирования отработать надлежащий протокол действий в отношении активных угроз и выявить элементы протокола, которые необходимо усовершенствовать, чтобы перевести меры реагирования из теоретической плоскости в практическую, где они будут применены, в случае если угроза будет обнаружена и потребует немедленного реагирования.

4.2.4 Реагирование на угрозы

РИСУНОК 11



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

Четвертый этап цикла управления угрозами и рисками — это выработка мер реагирования, в ходе которого специалисты-практики разрабатывают план действий, обсуждают ресурсы, необходимые для реагирования на угрозу, и распределяют функции и обязанности между конкретными специалистами. Цель этой части цикла состоит в том, чтобы заложить основу для будущих действий, которые необходимо предпринять для предотвращения или снижения последствий террористической атаки. Результатом этапа выработки мер реагирования станет подробный план действий, список ресурсов, необходимых для его выполнения, а также документ, определяющий функции и обязанности каждого специалиста-практика, участвующего в реализации плана действий.

Разработка плана действий включает в себя подробное описание ресурсов, которые будут выделены для реагирования на угрозу. Любые меры реагирования на угрозы должны соответствовать основным принципам прав человека, включая принципы законности, пропорциональности и недискриминации. При выработке мер реагировании также необходимо учитывать гендерные аспекты угрозы, что будет гарантировать соответствие принимаемых мер особым потребностям и уязвимостям представителей разных гендеров. Кроме того, для обеспечения эффективного реагирования на угрозы важно определить функции и обязанности каждой из заинтересованных сторон, чтобы все они работали на достижение единой цели, а действия одной заинтересованной стороны не противоречили действиям другой.

4.2.5 Оценка воздействия

РИСУНОК 12

Оценка воздействия включает в себя всесторонний анализ различных факторов, таких как характер и уровень террористической угрозы, эффективность предлагаемых контртеррористических мер по снижению потенциала угрозы, последствия угрозы и снижение уязвимости объектов угрозы. Оценка воздействия — это процесс оценки и анализа потенциальных эффектов или последствий предлагаемой политики и оперативного плана по ослаблению угрозы. Это инструмент для выявления потенциальных угроз и определения подходящих мер реагирования на уровне принятия решений или действий, а также для управления ими.

На данном этапе воздействие определяют и оценивают для учета потенциальных последствий предлагаемых действий в процессе принятия решений; такая оценка может способствовать минимизации любых негативных последствий и расширению любого позитивного влияния. В целом оценка воздействия призвана обеспечить понимание потенциальных последствий оценки угрозы для разработчиков политики и лиц, ответственных за принятие решений, что позволит им принимать обоснованные решения о том, какие меры являются более оптимальными.

[IV] Передовой опыт в сфере оценки угроз

5.1 Обзор

Внедрение передового опыта специалистами-практиками по оценке угроз и рисков на национальном уровне может способствовать повышению качества и точности их оценок, более эффективному выявлению потенциальных угроз и принятию обоснованных решений о введении соответствующих мер. При подготовке модели цикла управления угрозами и рисками были изучены многочисленные материалы различных государств-членов в области оценки угроз и рисков и управления ими. Результаты проведенного исследования представлены в следующих разделах в виде примеров передовой практики. В целом процесс оценки угроз и рисков может состоять из различных видов оценок, проводимых на разных уровнях (местном, региональном), для формирования общенационального понимания террористических угроз, при этом каждая такая оценка вносит свой вклад в общую картину. Кроме того, специалисты-практики должны быть готовы к угрозам со стороны новых и новейших технологий, которые используются или могут быть использованы для совершения террористического акта. Несмотря на то что любой подход, принятый государством-членом, может зависеть от его правовой базы в сфере противодействия терроризму, контртеррористической стратегии, механизмов координации и операционных процессов, ниже приведены некоторые рекомендации по надлежащей практике в области оценки угроз и рисков, реализация которых поможет специалистам по оценке контртеррористических угроз и рисков расширить свой потенциал для включения компонента «использование новых технологий в террористических целях» в цикл управления угрозами и рисками (см. раздел 4).

5.2 Межучрежденческий подход и информационно-аналитические центры

Эффективный процесс оценки субъектов и сценариев угроз предполагает сотрудничество различных государственных ведомств (включая правоохранительные органы, службу разведки, пограничную службу и т. д.). Его реализация в рамках межучрежденческого подхода позволяет получить более полное и целостное понимание потенциальных угроз. Одним из примеров передовой практики, описанный в совместной публикации Европейской комиссии, CIVI.POL Conseil и Королевского объединенного института оборонных исследований (RUSI), является выявление заинтересованных сторон[41], в рамках которого они определяются как «партнеры, целевые группы и бенефициары»[42].

41 CIVI.POL Conseil и Королевский объединенный институт оборонных исследований, «Оперативное руководство по подготовке и реализации мер, направленных на противодействие терроризму и насильственному экстремизму в третьих странах, при финансовой поддержке ЕС» (Европейская комиссия, 2018 г.), 32, URL: https://ct-morse.eu/wp-content/uploads/2017/11/EU-CT-CVE-guidelines.pdf

42 Там же.

Программа CONTEST правительства Соединенного Королевства — это стратегия, позволяющая снизить террористические риски для СК при участии нескольких государственных органов[43]. В рамках этой программы Объединенный аналитический центр по терроризму (JTAC) самостоятельно устанавливает уровни угроз[44]. JTAC объединяет самых разных специалистов по борьбе с терроризмом из органов полиции, государственных департаментов и служб для совместного анализа и обработки информации. JTAC — автономная организация, состоящая из представителей 16 государственных департаментов и служб. Она устанавливает уровни угроз и выпускает предупреждения об угрозах и других связанных с терроризмом вопросах для многочисленных государственных органов и ведомств, а также готовит более подробные отчеты о тенденциях, террористических сетях и потенциале[45].

Подход Дании к предупреждению насильственного экстремизма и радикализации и противодействию им основан на широком сотрудничестве различных социальных служб, органов системы образования, здравоохранения, полиции, разведки и служб безопасности[46]. Центр анализа терроризма (CTA) ежегодно публикует «Оценку террористической угрозы для Дании», в котором определяет общий уровень террористической угрозы в стране и оценивает угрозу интересам Дании за рубежом. CTA был создан в качестве датского центра обмена информацией для анализа и оценки потенциальной или вероятной террористической угрозы для Дании и интересов страны за рубежом. В его состав входят сотрудники четырех датских ведомств (Датской службы безопасности и разведки, Датской службы оборонной разведки, Министерства иностранных дел и Агентства по чрезвычайным ситуациям). Уровень террористической угрозы, приведенный в «Оценке террористической угрозы для Дании» отражает соответствующие случаи и тенденции в Дании и за рубежом, которые в совокупности влияют на результат оценки[47].

В Новой Зеландии Объединенная группа по оценке угроз (CTAG) — это межведомственная организация, созданная и возглавляемая Службой безопасности и разведки Новой Зеландии (NZSIS)[48]. По запросу государственных учреждений группа проводит независимые оценки угроз, существующих для страны, ее жителей и интересов за рубежом. В состав CTAG входят аналитики из NZSIS и других государственных органов, включая полицию Новой Зеландии, Вооруженные силы Новой Зеландии, Бюро безопасности правительственной связи (GCSB), Управление гражданской авиации и Службу авиационной безопасности, а также Департамент исправительных учреждений. В работе CTAG также принимают участие другие органы государственного управления, среди которых — Министерство иностранных дел и торговли, Министерство транспорта и Таможенная служба Новой Зеландии.

В Канаде за определение национального уровня угрозы отвечает Центр комплексной оценки терроризма (ITAC). Штатные сотрудники центра активно сотрудничают с государственными учреждениями Канады. Кроме того, ITAC работает в партнерстве с компетентными органами по оценке угроз Австралии (NTAC), Новой Зеландии (CTAG), Соединенного Королевства (JTAC) и США (НКЦ)[49]. Принятая модель предполагает не только работу с внутренней межучрежденческой командой, но и более тесное сотрудничество страны с зарубежными организациями, что может способствовать расширению таких элементов оценки, как объем

43 Соединенное Королевство, «CONTEST: контртеррористическая стратегия Соединенного Королевства» (Соединенное Королевство: Британская корона, 2018), URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf

44 «Объединенный аналитический центр по терроризму», Служба безопасности MI5, URL: https://www.mi5.gov.uk/joint-terrorism-analysis-centre (дата обращения: 5 июня 2024 г.).

45 Там же.

46 Ann-Sophie Hemmingsen, "An Introduction to the Danish Approach to Countering and Preventing Extremism and Radicalisation" (Copenhagen, Denmark: Danish Institute for International Studies, 2015) («Введение в датский подход к предотвращению экстремизма и радикализации и противодействию им»), URL: https://www.ft.dk/samling/20151/almdel/reu/bilag/248/1617692.pdf

47 Центр анализа терроризма (CTA), «Оценка террористической угрозы для Дании» (Дания: Центр анализа терроризма (CTA), март 2022 г., URL: https://politi.dk/en/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-terrortruslen-mod-danmark/vtd_2022_uk.pdf

48 Служба безопасности и разведки Новой Зеландии, «Объединенная группа по оценке угроз», Служба безопасности и разведки Новой Зеландии, URL: https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/combined-threat-assessment-group/ (дата обращения: 5 июня 2024 г.).

49 David Thorne, "National Level Threat Assessment-Canadian Model" («Оценка угроз на национальном уровне: канадская модель», доклад для 2-го семинара по упреждающему подходу к борьбе с терроризмом (Исламабад, Пакистан: Управление Организации Объединенных Наций по наркотикам и преступности, 12 апреля 2018 г.)), 87, URL: https://www.unodc.org/documents/pakistan//Report-2nd-Workshop-Proactive-Approach-to-CT-web.pdf

собранной оперативной информации об угрозах в отношении конкретных субъектов угроз. В Швеции Национальный центр по оценке террористической угрозы опирается в своей работе на сотрудничество между вооруженными силами, Радиоуправлением национальной обороны и Шведской службой безопасности. В рамках этой модели различные государственные органы осуществляют совместный сбор и анализ оперативной информации и проводят оценку уровня угрозы в стране[50].

5.3 Подход, основанный на оценке рисков

При проведении оценки субъектов и сценариев террористических угроз некоторые страны и международные организации используют подход, основанный на оценке рисков. Он позволяет организациям принимать обоснованные решения, эффективно распределять ресурсы и управлять рисками на упреждение, снижая вероятность возникновения террористических событий и их последствия. При применении подхода, основанного на оценке рисков, оценивают вероятность совершения и потенциальные последствия террористической атаки с целью приоритизации выделяемых ресурсов и разработки планов реагирования.

Национальный реестр рисков (NRR) Соединенного Королевства (СК) — это публичная версия закрытой оценки рисков национальной безопасности (NSRA), проводимой правительством в отношении СК или его интересов за рубежом. Он предоставляет широкой общественности информацию о «наиболее значительных рисках», которые, по данным правительства, могут произойти и иметь для страны самые разные последствия, — например, о террористических актах или природных явлениях, таких как наводнения. В нем также подробно описано, каким образом правительство выявляет, оценивает, реагирует на потенциальные чрезвычайные ситуации и готовится к ним. В качестве еще одного примера можно привести модель реестра рисков, разработанную Транспортным агентством Новой Зеландии. В ней представлена информация, которую следует включить в реестр рисков страны, например, номер угрозы, раздел с указанием даты последнего принятия мер реагирования в отношении угрозы и их описанием, план реагирования и распределение функций между заинтересованными сторонами в случае возникновения угрозы нападения.

Группа разработки финансовых мер по борьбе с отмыванием денег (ФАТФ) — это независимый межправительственный орган, который разрабатывает и продвигает политику защиты глобальной финансовой системы от отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения. Так, в деле противодействия отмыванию денег и (или) финансированию терроризма ФАТФ рекомендует использовать подход, основанный на оценке рисков, который является важным условием эффективного распределения ресурсов. Кроме того, по ее утверждению, оценки рисков, проводимые странами, следует использовать для определения более высоких и более низких рисков с целью их последующего устранения путем применения усиленных или упрощенных мер соответственно. По рекомендации ФАТФ, важно заранее определить источники данных, тип информации, инструменты и аналитические методики для их последующего применения при проведении оценки рисков. Для того чтобы национальная оценка рисков дала наиболее точные результаты, желательно, чтобы аналитические данные и выводы, представленные в рамках оценки, были в максимально возможной степени основаны на объективной информации. Сведения, используемые для проведения оценки рисков, могут быть получены из различных источников (как качественных, так и количественных).

5.4 Определение уровня угрозы

Определение уровня угрозы — важный аспект оценки субъектов и сценариев угрозы, а также инструмент управления угрозами. Он позволяет организациям и отдельным лицам оценить уровень угрозы, связанной с террористической ситуацией или событием, и предпринять соответствующие действия для управления угрозой или ее ослабления.

50 Министерство юстиции Швеции, «Предотвратить, упредить, защитить: шведская контртеррористическая стратегия» (Швеция: Органы государственной власти Швеции, 2014 г.), URL: https://www.government.se/contentassets/b56cad17b4434118b16cf449dbdc973d/en_strategi-slutlig-eng.pdf

Британский JTAC[51] оценивает уровень угрозы в любых заданных обстоятельствах с учетом нескольких факторов:

- **Имеющаяся оперативная информация.** Зачастую анализ основан на широком спектре информации, часть которой нередко имеет фрагментарный характер, включая данные об уровне и характере текущей террористической активности, результаты сравнения с событиями в других странах и предыдущими атаками.
- **Потенциал террористов.** Анализ имеющейся информации о потенциале террористов и методах, которые они могут использовать, проводимый на основе данных о предыдущих атаках или оперативной информации, а также анализ потенциального масштаба террористического акта.
- **Намерения террористов.** Использование оперативной и общедоступной информации для изучения общих целей террористов и потенциальных способов их достижения, включая объекты, которые они могут атаковать.
- **Временные рамки.** Установленный уровень угрозы и вероятность совершения террористического акта в ближайшем будущем.

Оценки, проводимые новозеландской CTAG, предусматривают анализ намерений и потенциала субъекта угрозы совершить атаку. Оценка — это качественное и аналитическое исследование. CTAG использует структурированные аналитические методы и инструменты при проведении оценок. Она учитывает контекст внутреннего терроризма и значимые международные факторы угрозы[52]. Оценивая уровень угрозы, CTAG рассматривает текущие намерения и потенциал отдельных лиц или групп лиц совершить террористический акт. ITAC Канады проводит оценки угроз, в рамках которых рассматривает и определяет национальный уровень угрозы, а также анализирует возможность изменения уровня угрозы в связи со «специальным мероприятием» (например, саммитом)[53]. Проведение дополнительных оценок с учетом «специального мероприятия» означает, что уровень угрозы (национальный или региональный) может повыситься в случае наступления широко освещаемого события, но такое изменение обусловлено исключительно таким событием и является временным относительно последовательности и сферы применения результатов основной части национальной оценки угроз. В рамках шкалы уровней угрозы канадская модель также показывает, как угроза в целом может повлиять на общественность и ее способность придерживаться обычного режима жизнедеятельности[54].

Одним из примеров передовой практики по определению уровня угрозы является создание шкалы, по которой можно определить уровень угрозы в стране. Новозеландская служба безопасности и разведки представляет пятиступенчатую модель оценки уровня угрозы — от очень низкого до экстремального[55]. Канада и Нидерланды предлагают свои модели оценки уровней угрозы, которые могут пригодиться в качестве практической основы, с подробным указанием мер, принимаемых на каждом из уровней. В рамках канадской модели выделяют пять уровней угроз: очень низкий, низкий, средний, высокий и критический, а диапазон вероятности реализации угрозы варьируется от крайне маловероятной до весьма вероятной (и, возможно, неминуемой)[56]. При этом канадская модель предусматривает принятие мер по обеспечению безопасности и защиты населения от потенциальной террористической атаки на самых ранних этапах. Когда уровень угрозы считается «средним», принимаются дополнительные меры безопасности. На «высоком» и «критическом» уровнях меры безопасности продолжают усиливаться, а также добавляется элемент информирования населения о возможных действиях, которые ему необходимо предпринять для обеспечения своей безопасности[57]. Как и в предыдущих примерах, в модели Нидерландов используется пятиступенчатая шкала: от

51 «Уровни угрозы», ProtectUK, 12 марта, 2022 г., URL: https://www.protectuk.police.uk/threat-levels

52 Служба безопасности и разведки Новой Зеландии, «Национальный уровень террористической угрозы», URL: https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/national-terrorism-threat-level/ (дата обращения: 5 июня 2024 г.).

53 Thorne, "National Level Threat Assessment-Canadian Model" («Оценка угроз на национальном уровне: канадская модель»), 87–89.

54 См. таблицу там же, 88.

55 Служба безопасности и разведки Новой Зеландии, «Национальный уровень террористической угрозы».

56 Министерство общественной безопасности Канады, «Национальная концепция уровней террористической угрозы Канады», консультации, 25 августа 2016 г., URL: https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html

57 Там же.

уровня 1 (минимального) до уровня 5 (критического)[58]. Помимо самой модели, Национальный координационный центр по безопасности и борьбе с терроризмом публикует инфографику в течение года с указанием уровня угрозы и сопутствующими пояснениями[59].

ВСТАВКА 1

***Модель и формулировки взяты из следующих источников:**
Канада, Министерство общественной безопасности, «Национальная концепция уровней террористической угрозы Канады», консультации, 25, августа 2016 г., https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html
Национальный координационный центр по безопасности и борьбе с терроризмом, «Оценка террористической угрозы в Нидерландах», Министерство юстиции и безопасности, 14 мая 2020 г., https://english.nctv.nl/topics/terrorist-threat-assessment-netherlands
New Zealand Security Intelligence Service. Служба безопасности и разведки Новой Зеландии, «Национальный уровень террористической угрозы», https://www.nzsis.govt.nz/our-work/countering-violent-extremism-and-terrorism/national-terrorism-threat-level/ (дата обращения: 5 июня 2024 г.).

5.5 Сбор и анализ информации об угрозах

Неотъемлемым компонентом эффективных оценок субъектов и сценариев угроз, а также процесса управления угрозами являются сбор и анализ информации об угрозах. Ниже приведены примеры передовой практики по сбору и анализу информации об угрозах, которые были взяты из документов государств-членов.

58 Национальный координационный центр по безопасности и борьбе с терроризмом, «Оценка террористической угрозы в Нидерландах», Министерство юстиции и безопасности, 14 мая 2020 г.), URL: https://english.nctv.nl/topics/terrorist-threat-assessment-netherlands

59 См., например, Национальный координационный центр по безопасности и борьбе с терроризмом, «Оценка террористической угрозы NCTV: угроза в Нидерландах и для Нидерландов стала более сложной и глобальной — Раздел «Новости» — Национальный координационный центр по безопасности и борьбе с терроризмом», Министерство юстиции и безопасности, 7 ноября 2022 г.), URL: https://english.nctv.nl/latest/news/2022/11/07/nctvs-terrorist-threat-assessment-threat-in-and-to-the-netherlands-has-become-more-multifaceted-and-diffuse

Одним из таких примеров для специалистов-практиков, проводящих оценку угроз, связанных с использованием новых технологий в террористических целях, является анализ оперативной информации о киберугрозах (CTI). Британская модель CTI определяет такой анализ как ситуационную оценку, которая учитывает как потенциальные угрозы, так и стоящие за ними субъекты угроз, поскольку речь идет об использовании технологий и злоупотреблении им[60]. Одним из методов сбора CTI является использование OSINT — формы оперативной информации, которая по своей природе более доступна для заинтересованных сторон и требует меньших ресурсов для ее сбора, чем другие виды данных. К дополнительным методикам, которые могут применяться для сбора CTI, относится сотрудничество с представителями частного сектора, технологических компаний и научных кругов для сбора и анализа имеющихся данных о потенциальных угрозах. В рамках сбора и анализа CTI важно регулярно разрабатывать информационные материалы, содержащие оценку собранных данных и соответствующий отчет, чтобы заинтересованные стороны могли в любой момент ознакомиться с результатами ситуационной оценки различных угроз[61].

В отчете, опубликованном Европейской комиссией, CIVI.POL Conseil и Королевским объединенным институтом оборонных исследований (RUSI), также представлен передовой опыт по сбору и анализу информации об угрозах. В нем подчеркивается важность проведения «контекстного анализа» наряду с анализом угроз. Такой подход предполагает «учет любых политических, экономических, экологических аспектов и вопросов безопасности на местном, национальном и региональном уровнях» [62]. Стандарт ISO 31000 также предусматривает контекстно-ориентированный подход к управлению рисками[63]. Согласно его положениям понимание «внутренней» и «внешней» среды помогает заинтересованным сторонам «адаптировать» принимаемые меры реагирования под определенную группу и понять, каким образом контекст определенных угроз может повлиять на связанный с ними риск[64]. Использование такого подхода при проведении анализа субъектов угроз и разработке сценариев угроз позволит заинтересованным сторонам получить более полное представление об угрозах до начала процесса анализа рисков.

5.6 Непрерывная оценка

Оценки угроз и рисков должны регулярно пересматриваться. Равно как субъекты угроз могут развиваться и эволюционировать с течением времени и с появлением новых технологий, так и страны могут развивать и актуализировать свои усилия по противодействию угрозам. Пересмотр оценки угроз и рисков необходим, чтобы понять изменения, произошедшие на уровне конкретной угрозы в связи с принятием контртеррористических мер или другими изменениями[65]. Это непрерывный процесс, который сопровождается регулярными обзорами и обновлениями на основе новой оперативной информации и с учетом меняющихся обстоятельств, таких как развитие технологий. Кроме того, методология, с помощью которой угрозы оценивают и управляют ими, должна пройти оценку воздействия, чтобы подтвердить свою эффективность и актуальность в текущих реалиях, которые она призвана проанализировать.

Соединенные Штаты Америки оценивают эффективность операций и корректируют их с помощью ежегодной независимой стратегической оценки, которая строится на результатах исследований, оперативной информации и аналитических данных и призвана обеспечить измеримый прогресс в достижении стратегических целей. Она позволяет выявить недостатки в контртеррористической стратегии и внести в нее

60 Flanders et al., "Cyber Threat Intelligence in Government: A Guide for Decision Makers and Analysts" («Сбор и анализ оперативной информации о киберугрозах на государственном уровне: руководство для лиц, ответственных за принятие решений, и аналитиков»), 15.

61 Там же, 36.

62 CIVI.POL Conseil и Королевский объединенный институт оборонных исследований, «Оперативное руководство по подготовке и реализации мер, направленных на противодействие терроризму и насильственному экстремизму в третьих странах, при финансовой поддержке ЕС», 30.

63 Международная организация по стандартизации, ISO 31000 «Менеджмент риска. Принципы и руководство», второе издание (Швейцария: Международная организация по стандартизации, 2018 г.), 3 и 6, URL: https://shahrdevelopment.ir/wp-content/uploads/2020/03/ISO-31000.pdf

64 Там же.

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

соответствующие коррективы, чтобы опередить динамично развивающихся субъектов угроз. Она также направлена на обеспечение устойчивого прогресса в реализации стратегии и решение всего спектра современных проблем национальной безопасности[66]. Согласно контртеррористической стратегии США эта оценка является продуктом исследований, изучения оперативной информации и анализа данных, при этом каждая новая оценка опирается на результаты предыдущей. Ежегодный отчет об оценке угроз отражает связанные с угрозами изменения, выраженные с помощью таких показателей, как уровень угрозы, характер субъекта угрозы, доступные ему ресурсы, а также ресурсы, которыми располагает страна для борьбы с потенциальными угрозами. В Новой Зеландии уровень национальной террористической угрозы подлежит официальному пересмотру на ежегодной основе, при этом он может быть изменен в любое время на основании текущей оперативной информации.

5.7 Расширение обмена оперативной информацией

Обмен информацией и культура сотрудничества на междисциплинарном и многостороннем уровнях остаются залогом эффективной оценки угроз, которая может лечь в основу контртеррористической политики[67]. Они включают обмен оперативной информацией между государственными органами и с международными партнерами. Важно проводить повсеместное обучение по вопросам оценки угроз для обеспечения сотрудничества и понимания со стороны различных источников и субъектов, что позволит добиться более широкого эффекта[68]. Например, в контртеррористической стратегии Испании особое внимание уделено возможности использования данных, которые должны быть не только доступны тем, кому они необходимы, но и защищены от тех, кто не должен иметь доступ к этому типу информации[69]. Так, в стратегии говорится о необходимости шифрования данных для их последующего обмена между заинтересованными сторонами из различных сфер[70].

Одним из примеров надлежащей практики обмена информацией является модель Общей базы данных (CDB), применяемая бельгийской Координационной группой по анализу угроз (CUTA). Она позволяет различным государственным органам не только иметь доступ к данным в таких категориях, как иностранные боевики-террористы, внутренние боевики-террористы, пропагандисты ненависти, потенциально насильственные экстремисты и лица, осужденные за терроризм, но и пополнять эти данные[71].

Обмен информацией между заинтересованными сторонами, находящимися в разных точках, должен осуществляться с помощью защищенных средств для обеспечения безопасности операций в таких вопросах, как оценка субъектов угроз и реагирование на угрозы. Как и в испанской модели, безопасный обмен информацией в рамках модели CDB основан на принципе «служебной необходимости». Это означает, что пользователи имеют доступ к разным объемам данных (и возможность их пополнять) в зависимости от типа информации, относящейся к их конкретной функции[72]. Регулирование типа и объема доступной информа-

66 Там же.

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

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

69 Министерство внутренних дел Испании, *Национальная контртеррористическая стратегия*, 2019 г., 53–54, URL: https://www.dsn.gob.es/eu/file/4271/download?token=-K6uOf-C

70 Там же.

71 Координационная группа по анализу угроз (CUTA), «Общая база данных (CDB)», URL: https://cuta.belgium.be/the-common-database-cdb/ (дата обращения: 5 июня 2024 г.).

72 Там же.

ции с учетом специфики пользователей обеспечивает более высокий уровень безопасности операций, тем самым снижая вероятность попадания данных к пользователям, которые не должны иметь к ним доступ.

Еще один способ безопасного обмена таким реестром (базой данных) и содержащейся в нем информацией — это внедрение модели, аналогичной «кластерной», которая практикуется в Соединенном Королевстве. Кластерная модель — это форма регионального межсекторального сотрудничества между государственными органами, компаниями частного сектора и научными кругами. В рамках этой модели каждый регион имеет «кластер», который действует на полуавтономной основе в вопросе приоритизации угроз с учетом специфики его зоны ответственности (ЗО). Заинтересованные стороны в каждом кластере обмениваются информацией и передовым опытом. Сами кластеры выполняют функцию централизации на уровне отчетности и обмена информацией с национальными заинтересованными сторонами в отношении угроз[73]. Бельгийская Стратегическая записка «Экстремизм и терроризм» (Стратегия T.E.R.) содержит аналогичную модель активного участия специалистов-практиков на местах в деле борьбы с терроризмом. В рамках этой модели действует местная целевая группа, а также локальная группа по предотвращению радикализации[74]. Они подчиняются Национальной целевой группе (NTF), которая сотрудничает на более глобальном уровне с различными правительственными и военными организациями. Локализованный характер этой модели позволяет более дифференцированно подходить к оценке и приоритизации угроз применительно к ЗО, а также способствует формированию у национальных заинтересованных сторон глубокого представления о каждом из регионов, входящих в сферу их ответственности.

На уровне обмена информацией также важно упростить процесс передачи данных, особенно для представителей общественности в тех случаях, когда они хотят сообщить важные сведения об угрозах. Для этого общественность должна быть проинформирована об угрожающем поведении или действиях, а также о каналах, по которым она может обратиться, чтобы сообщить об инциденте, для дальнейшего рассмотрения вопроса заинтересованными сторонами, прошедшими соответствующую подготовку.

Для решения этой задачи можно организовать в школах и на рабочих местах обучение по выявлению признаков угрожающего поведения. Кроме того, платформа, с помощью которой представители общественности могут передавать информацию об угрозах компетентным органам, должна быть легкодоступной и простой в использовании, чтобы ее сложность не препятствовала получению обращений. Одним из примеров такой платформы, которая служит одновременно центральной и легкодоступной моделью для сообщения об угрозах, является специализированный сайт в Новой Зеландии. На нем представители общественности могут оценить степень серьезности информации об угрозе, а также поделиться своей оценкой с компетентными органами[75]. Сайт также позволяет оставлять информацию анонимной.

5.8 Исследования и инновации

Для того чтобы предвосхитить влияние современных технологий на террористические угрозы в текущих реалиях, требуется эффективное реагирование, которое выражается в наличии подходящих инструментов у правоохранительных органов. Исследования и инновации являются неотъемлемым компонентом эффективной оценки угроз, благодаря которому специалисты-практики смогут актуализировать свои знания о потенциальных угрозах и продолжать разрабатывать новые меры реагирования, исходя из понимания того, как с помощью новых технологий следует противодействовать угрозам, в том числе возникающим в результате злонамеренного использования таких технологий. В этой связи Европейская комиссия, CIVI.POL Conseil и Королевский объединенный институт оборонных исследований (RUSI) рекомендуют использовать этот компонент в качестве важного условия понимания сценариев угроз для обеспечения непрерывного изучения технологических достижений и потенциального воздействия, которое они могут оказать в случае

73 UK Cyber Cluster Collaboration (UKC3), «Операционная основа кибер-кластеров», UK Cyber Cluster Collaboration (блог) URL: https://ukc3.co.uk/cyber-cluster-operating-framework/ (дата обращения: 5 июня 2024 г.).

74 Координационная группа по анализу угроз (CUTA), «Стратегическая записка «Экстремизм и терроризм» (Стратегия T.E.R.)», URL: https://cuta.belgium.be/the-strategic-note-extremism-and-terrorism-strategy-t-e-r/ (дата обращения: 5 июня 2024 г.).

75 Служба безопасности и разведки Новой Зеландии, «Как можно помочь: форма участия общественности», URL: https://providinginformation.nzsis.govt.nz/ (дата обращения: 5 июня 2024 г.).

использования террористами (см. раздел 4.2.2)[76]. Такие исследования и инновации должны опираться на межведомственное и межсекторальное сотрудничество при участии представителей научных кругов и отрасли высоких технологий.

Исследования по вопросам безопасности, проводимые в ЕС, сосредоточены на разработке инициатив, направленных на повышение потенциала правоохранительных органов в таких сферах, как разработка аналитических решений для работы с большими массивами данных[77]. Кроме того, исследования в области безопасности, финансируемые ЕС, направлены на укрепление потенциала раннего обнаружения вероятных террористических угроз, в частности, путем изучения возможностей использования искусственного интеллекта для более эффективной и точной обработки больших объемов данных. Кроме того, в рамках будущей программы финансирования исследований и инноваций «Горизонт Европа» исследования будут еще более интегрированы в цикл политики безопасности, чтобы обеспечить получение ориентированного на воздействие результата, который отвечает выявленным потребностям правоохранительных органов[78].

76 CIVI.POL Conseil и Королевский объединенный институт оборонных исследований, «Оперативное руководство по подготовке и реализации мер, направленных на противодействие терроризму и насильственному экстремизму в третьих странах, при финансовой поддержке ЕС», 30, URL: https://ct-morse.eu/wp-content/uploads/2017/11/EU-CT-CVE-guidelines.pdf

77 Европейская комиссия, «Контртеррористическая повестка ЕС: предвидеть, предупреждать, защищать, реагировать».

78 См., например, проекты DANTE и TENSOR («Обнаружение и анализ онлайн-контента и финансовой деятельности, связанных с терроризмом»), Европейская комиссия: Информационная служба общественных исследований и разработок (CORDIS), https://cordis.europa.eu/project/id/700367 (дата обращения: 5 июня 2024 г.). «Поиск и анализ гетерогенного онлайн-контента для распознавания террористической деятельности», Европейская комиссия: CORDIS, URL: https://cordis.europa.eu/project/id/700024) (дата обращения: 5 июня 2024 г.).

[ПРИЛОЖЕНИЕ А]
Пример модели оценки для атрибуции угроз

A.1 Обзор

На рисунке ниже приведена модель, с помощью которой специалисты-практики могут оценить угрозу с целью ее дальнейшей атрибуции. В рамках этой модели атрибуция угрозы означает оценку риска на основе данных оценки самой угрозы[79]. Представленная модель опирается на оценку потенциала. Поскольку основное внимание в этом руководстве уделено новым технологиям, первоначальный фактор «информация, знания и возможности», который в целом описывает понятие «потенциал», был изменен на «технологический потенциал»[80].

Согласно модели, показанной на рисунке, сначала необходимо учесть технологический потенциал, намерения и мотивацию субъекта угрозы. Затем на основе полученных данных следует проанализировать вероятность совершения им террористической атаки и масштаб потенциального ущерба, который она может нанести. На следующем этапе специалисты-практики оценивают имеющиеся механизмы защиты и эффективность их использования для противодействия потенциальной угрозе[81]. Понимание текущего потенциала защиты от угроз влияет на уровень атрибуции угрозы. Чем больше эффективных мер защиты от угроз принято в стране, тем ниже будет атрибуция угрозы.

РИСУНОК 1[82]

79 Erez Magen and R., "Enabling Advancements in Security-Danger and Opportunities" («Новые достижения в области безопасности: опасности и возможности»), Maarachot (Systems) (blog), March 29, 2022.

80 Там же.

81 Там же.

82 Перевод и адаптация графики по материалам Erez Magen and R., "Enabling Advancements in Security-Danger and Opportunities" («Новые достижения в области безопасности: опасности и возможности»).

[ПРИЛОЖЕНИЕ B]
Пример неправомерного использования технологий террористами

B.1 Обзор

В таблице ниже приведены новые технологии и способы их потенциального использования террористами, а также потенциал их применения специалистами-практиками для противодействия терроризму. Понимание возможностей применения новых технологий в деле борьбы с терроризмом может помочь специалистам интегрировать эти возможности в меры реагирования на уровне контртеррористической политики.

Важно отметить, что таблица содержит точные сведения на момент составления настоящего документа, однако ее содержание подлежит регулярному пересмотру для обеспечения его точности и актуальности в случае использования. По мере непрерывного развития новых технологий будут появляться новые способы, с помощью которых террористы смогут использовать их в злонамеренных целях, а также новые методы применения технологий для противодействия терроризму.

ТАБЛИЦА 1. **Примеры**

Тип технологии	Злонамеренное использование террористами	Использование правоохранительными органами для борьбы с терроризмом
Интернет	• Вербовка в террористическую организацию через пропаганду, распространяемую в Интернете • Публикация в Интернете информации о способах совершения террористических актов[83] • Финансирование терроризма • Радикализация, ведущая к терроризму • Сбор оперативной информации о потенциальных объектах нападения • Распространение террористического контента и искаженных представлений • Связь, координация и иная поддержка террористических актов или деятельности • Информационные операции с применением кибертехнологий	• Противодействие насильственному экстремизму и террористическим идеям[84] • Сбор и анализ OSINT • Платформа для обмена информацией между заинтересованными сторонами • Выявление террористического контента в Интернете и пресечение его распространения • Группы по оценке интернет-контента, которые перенаправляют сообщения об экстремистском контенте в технологические компании, призванные бороться с ним на своих платформах • Выявление новых террористических групп и их намерений
Социальные сети	• Вербовка в террористические организации через пропаганду, распространяемую в социальных сетях • Дезинформационные кампании • Распространение террористического контента и искаженных представлений, пропаганды и (или) материалов для размещения в качестве пропаганды в социальных сетях по зашифрованным каналам[85] (см. резолюцию 2396 Совета Безопасности) • Радикализация, ведущая к терроризму • Службы обмена зашифрованными сообщениями позволяют вести переписку, которую сложнее отследить тем, кто не является ее участником.	• Сбор/мониторинг SOCMINT • Противодействие насильственному экстремизму и террористическим идеям • Перенаправление сообщений об экстремистском контенте в технологические компании • Предотвращение создания террористами новых учетных записей

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

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

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

Даркweб	• Хакерские форумы, на которых можно приобрести вредоносное ПО, вирусы-вымогатели и другие вредоносные программы для совершения кибератак • Приобретение оружия • Вербовка • Зашифрованные сообщения между членами террористической группы	• Сбор и анализ OSINT
Виртуальные активы (криптовалюты, NFT, электронные платежные системы и т. д.)	• Использование криптовалюты/NFT-токенов для финансирования терроризма • Использование криптовалюты/NFT-токенов в деятельности по отмыванию денег	• NFT-токены также можно использовать для контрпропаганды терроризма (известен пример использования NFT-токенов представителями ИГИЛ для распространения пропаганды)[86] • Фандрайзинг/краудфандинг в виртуальных активах может использоваться на низовом уровне в борьбе с терроризмом (например, для приобретения оборудования, необходимого на местах)
Распознавание лиц	• В настоящее время неизвестно — неприменимо	• Обнаружение аномалий (процесс интеллектуального анализа данных для выявления единиц данных, которые выходят за рамки или отклоняются от нормы) • Международная база данных террористов
3D-печать	• Производство оружия/компонентов оружия	• 3D-печать также можно использовать для печати деталей с целью их последующего применения в борьбе с терроризмом: например, деталей беспилотных авиационных систем, которые, в свою очередь, могут быть использованы для разведки, наблюдения и рекогносцировки (ISR).

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

Искусственный интеллект и машинное обучение	• Дезинформационные кампании и кибератаки с использованием ИИ[87] • Оружие с использованием ИИ[88] • Кампании социальной инженерии[89] • Может использоваться для обновления эксплойтов или написания вредоносного ПО для сложных кибератак	• Использование ИИ/машинного обучения для автоматизации мониторинга и анализа CTI (например, автоматическая сортировка сообщений в социальных сетях/онлайн-форумах)[90] • Анализ больших данных с использованием ИИ[91] • Использование методов обработки естественного языка (ОЕЯ) для выявления символов и шаблонов, применяемых террористическими группами в Интернете • Мониторинг распространения ложных сведений и дезинформации[92]

87 Контртеррористический центр Организации Объединенных Наций и Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия, «Алгоритмы и терроризм: злонамеренное использование искусственного интеллекта в террористических целях», совместный доклад (Организация Объединенных Наций, 2021 г.), 39–40, URL: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf

88 См. например, там же, 33–35.

89 Там же, 45.

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

91 Там же, 17.

92 Там же, 27–28.

[ПРИЛОЖЕНИЕ C]
Руководящие вопросы для проведения оценки угроз

C.1 Обзор

Ниже представлены вопросы, которыми заинтересованные стороны и правоохранительные органы могут руководствоваться в своей работе на различных этапах процесса оценки угроз и рисков, описанных выше. Они позволяют выделить значимые факторы, которые важно учитывать для обеспечения эффективной оценки угроз и рисков.

C.2 Руководящие вопросы

ТАБЛИЦА 1. **Общие вопросы для начального этапа процесса оценки угрозы**

Ландшафт угроз	• Какие новые технологии представляют интерес для контртеррористической деятельности? • Как эти технологии используются террористами или потенциальными субъектами угроз? • Каковы потенциальные риски и уязвимости, связанные с этими технологиями? • Существуют ли новые технологии, которые могут повысить уровень уязвимости или создать новые проблемы в области безопасности?
Идентификация угрозы	• Существуют ли какие-либо индикаторы или тревожные признаки, указывающие на возможность применения насилия или причинения вреда? • Какие объекты или места потенциально подвержены риску?
Сбор и анализ информации	• Какие источники информации доступны (например, оперативная информация из открытых источников, интервью, записи)? • Насколько надежны и достоверны источники информации? • Есть ли в имеющейся информации пробелы, которые необходимо устранить? • Какой информацией следует делиться с соблюдением конфиденциальности и правовых норм?

ТАБЛИЦА 2. **Оценка субъекта угрозы**

Намерения	• Кто (группа лиц/отдельные лица) планирует совершить атаку и каковы его/ее мотивы? • Какие мотивы могут побуждать террориста к совершению атаки? • Принадлежит ли террорист к определенной идеологической/политической группе (является ли ее сторонником)? • Чего хочет добиться субъект угрозы с помощью этой атаки (т. е. каковы его цели)? • Кто является потенциальными субъектами угрозы, вовлеченными в терроризм на основе технологий? • Есть ли какие-либо признаки радикализации или экстремистской идеологии, связанные с использованием технологий?
Потенциал	• К каким видам новых технологий имеет доступ субъект угрозы? • Насколько хорошо субъект угрозы знает, как использовать эти технологии? • Какие ресурсы доступны субъекту угрозы? • Имеет ли субъект угрозы опыт совершения атак? • Какой опыт/какое обучение имеет/прошел субъект угрозы? • Может ли субъект угрозы приобрести материалы или услуги, необходимые для совершения атаки? • Какой технический потенциал и опыт необходимо иметь для совершения атак с использованием технологий? • Существуют ли известные или новые субъекты угрозы или террористические группы, обладающие необходимым технологическим потенциалом? • Каков уровень знаний и доступа к ресурсам у потенциальных субъектов угроз?

ТАБЛИЦА 3. **Оценка субъекта угрозы**

Субъект угрозы	• Действует ли субъект угрозы в одиночку или в составе группы? • Какова принадлежность субъекта угрозы?
Вектор угрозы	• Является ли предполагаемая атака физической или кибератакой? • Если это кибератака, существует ли потенциальная угроза для критически важных объектов инфраструктуры? • Если это кибератака, то каковы вероятные механизмы (тактика, техника, процедуры) ее совершения атаки? • Если это кибератака, то какова ее цель (например, нарушение работы критически важных объектов инфраструктуры, получение финансовых средств с помощью вирусов-вымогателей и т. д.)?
Объекты угрозы	• Какие элементы критически важных объектов инфраструктуры могут быть уязвимы для атаки? • Какие категории лиц/места могут стать вероятными объектами атаки? • Нацелена ли атака на гражданское население?
Используемые технологии	• Предусмотрено ли использование новых технологий для совершения планируемой атаки? Если да, то какие технологии предполагается использовать? • Возможно ли применение новых технологий в рамках мер реагирования на планируемую атаку?

ТАБЛИЦА 4. **Оценка сценариев и определение приоритетности угроз**

Осуществимость	• Насколько вероятна реализация таких атак исходя из оперативной информации, исторических данных или других соответствующих факторов?
Вероятность	• Существуют ли какие-то конкретные факторы или события, которые могут повысить вероятность или серьезность атак с использованием технологий?
Последствия	• Каковы потенциальные последствия атак, совершенных с использованием технологий, с точки зрения количества жертв, ущерба, нанесенного инфраструктуре, или воздействия на общество?
Критичность	• Какими уязвимостями и недостатками обладают критически важные объекты инфраструктуры, системы или сети, которые могут быть использованы для совершения атак с применением технологий?

ТАБЛИЦА 5. **Реагирование на угрозы**

Национальная политика и план действий	• Какие планы реагирования и стратегии смягчения рисков должны быть реализованы в случае совершения атаки с использованием технологий? • Как можно использовать технологии для усиления потенциала реагирования — например, на уровне мониторинга в режиме реального времени, систем реагирования на инциденты или коммуникационных сетей? • Существуют ли какие-либо правовые или этические аспекты, которые необходимо учитывать при реагировании на угрозы, связанные с использованием технологий? • Какие процедуры документирования необходимо выполнять в процессе оценки угроз? • Как следует сообщать о результатах и рекомендациях и обмениваться ими с соответствующими сторонами?
Выделение ресурсов	• Насколько эффективны текущие меры безопасности для снижения или предотвращения этих уязвимостей? • Существуют ли новейшие технологии, которые могут повысить уровень уязвимости или создать новые проблемы в области безопасности? • Обладают ли сотрудники контртеррористических органов необходимыми знаниями и навыками для понимания и устранения угроз, связанных с использованием технологий? • Какие обучающие программы или инициативы по наращиванию потенциала необходимы для повышения уровня технической компетентности и осведомленности? • Каким образом партнерство с экспертами в области технологий, представителями научных кругов или частного сектора может способствовать непрерывному обучению специалистов и обмену знаниями?
Распределение функций и сфер ответственности	• Есть ли другие органы или заинтересованные стороны, с которыми необходимо проконсультироваться или которых следует проинформировать?

ТАБЛИЦА 6. **Оценка воздействия**

Оценка воздействия	• Насколько эффективны текущие меры безопасности для снижения или предотвращения этих уязвимостей? • Можно ли оценить эффективность воздействия с точки зрения снижения потенциала угрозы, снижения уязвимости, снижения последствий угрозы?

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)