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

INTERPOL

При финансовой поддержке Европейского союза

# Кибербезопасность и новые технологии


## Руководство по налаживанию сотрудничества между правоохранительными органами и технологическими компаниями в борьбе с терроризмом

---

**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.

---

# Содержание

# Совместное предисловие

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

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

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

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

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

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

**Стивен Кавана**
Исполнительный директор,
Полицейская служба Интерпола

# Выражение признательности

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

- **Гретхен Буерманн** — специалисту по исследованиям и анализу, Центр кибербезопасности Всемирного экономического форума;
- **Адаму Калабро** — руководителю группы по расследованию киберпреступлений, отдел неминуемых угроз, Google;
- **Нагам Эль Кархили** — руководителю по программированию и партнерству, Глобальный интернет-форум по противодействию терроризму (GIFCT);
- **Анне Краанен** — научному руководителю и ведущему специалисту по борьбе с терроризмом, платформа для анализа контента Tech Against Terrorism («Технологии против терроризма»);
- **Майклу Маффей** – старшему советнику по безопасности, Google; а также
- **Майклу О'Кифу** — специалисту по борьбе с терроризмом, Сектор по предупреждению терроризма Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН).

# Термины и определения

| | |
|---|---|
| **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[1]. |
| **Зеттабайт** | Один зеттабайт равен одному миллиарду терабайтов. |
| **ИКТ-компании** | Компании, работающие в сфере информационных и коммуникационных технологий (ИКТ), относятся к предприятиям, которые предоставляют продукты или услуги, связанные с информационными технологиями, телекоммуникациями, или и тем и другим. |
| **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. |

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

| | |
|---|---|
| **Новые технологии** | Термин «Новые технологии» охватывает широкий спектр различных технологий[2], 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[3]. |
| **Оперативная информация** | Информация, являющаяся результатом сбора, разработки, распространения, анализа и интерпретации данных, полученных из широкого круга источников, которая используется лицами, принимающими решения, в целях планирования последующих решений или действий на стратегическом, оперативном или тактическом уровнях. Сбор, хранение, использование оперативной информацией и обмен ею должны осуществляться в соответствии с обязательствами государств-членов по международному праву прав человека. |
| **Поставщики интернет-услуг** | Компании или организации, предлагающие услуги через Интернет. Эти услуги могут охватывать широкий спектр областей, таких как электронная почта, платформы социальных сетей, облачные хранилища, веб-хостинг, поисковые системы, платформы электронной коммерции и различные другие онлайн-коммуникативные или инфраструктурные услуги. |
| **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. |
| **Терроризм** | Преступные деяния, в том числе против гражданского населения, совершаемые с намерением причинить смерть или серьезные телесные повреждения, или акты захвата заложников, которые призваны вызвать состояние ужаса у широких слоев населения, группы лиц или отдельных лиц, запугать население или заставить правительство или международную организацию совершить или воздержаться от совершения какого-либо действия, и которые являются преступлениями в рамках и в соответствии с определениями международных конвенций и протоколов в области противодействия терроризму[4]. |
| **Технологические услуги** | Относится к использованию технологий и связанных с ними услуг для предложения решений пользователям ИКТ-компаний. |
| **Уголовное расследование** | Процесс сбора информации (или доказательств) для установления факта совершения преступления, выявления преступника и представления доказательств в поддержку обвинения в судебном разбирательстве. |
| **Уголовное правосудие** | Юридический процесс, который предусматривает предъявление обвинений в совершении уголовно наказуемого деяния физическому или юридическому лицу, проведение судебных слушаний, разрешение дела, назначение наказания, а также исправление и реабилитацию осужденных. |

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

3 Проектный документ CT TECH — Приложение I. Описание действий.

4 См. S/RES/1566 (2004), пункт 3 постановляющей части.

# Краткое содержание

Развитие сотрудничества между правоохранительными органами и компаниями, работающими в сфере информационных и коммуникационных технологий (ИКТ), имеет жизненно важное значение для обеспечения общественной безопасности. Технологический ландшафт и способы его использования переживают стремительное развитие, равно как и методы, которыми злоупотребляют террористы. В результате это сотрудничество имеет решающее значение для противодействия использованию новых и новейших технологий в террористических целях и использования возможностей ИКТ для обеспечения общественной безопасности.

Целью данного документа является содействие сотрудничеству и освещение передовых практик совместной работы правоохранительных органов и ИКТ-компаний в области предотвращения использования новых технологий в террористических целях.

Несмотря на то, что это начинание сопряжено с рядом неотъемлемых проблем, оно несет и ряд возможностей, которые могут быть эффективно использованы.

Предлагаемое руководство по передовым практикам работы с ИКТ-компаниями основано на четырех основных моделях сотрудничества:

- **Обмен информацией:** данная модель способствует обмену соответствующей информацией об угрозах, углубляет понимание тактики террористической деятельности и выявляет потенциальные угрозы, связанные со злоупотреблением услугами ИКТ-компаний. Она предоставляет правоохранительным органам и ИКТ-компаниям необходимые инструменты для активного и эффективного реагирования на террористическую деятельность.
- **Расширение возможностей:** многие коммерческие организации предлагают свои услуги разведывательному сообществу, используя свои технологические ресурсы в таких областях, как даркнет и криптовалюта. Взаимодействие с этими организациями может значительно повысить возможности правоохранительных органов по борьбе с терроризмом.
- **Бизнес-альянс/коллегия:** формирование бизнес-альянса расширяет возможности борьбы с терроризмом, способствуя обмену технологиями, методами и знаниями о потенциальных угрозах. Цель такого альянса — предвидеть и подготовиться к предстоящим вызовам, понимая потенциальные риски и возможности, предоставляемые будущими технологиями.
- **Активные расследования:** основная цель сотрудничества между правоохранительными органами и ИКТ-компаниями заключается в сборе информации, имеющей отношение к текущим террористическим расследованиям, и противодействию использованию ИКТ в террористических целях. Это сотрудничество вносит значительный вклад в повышение общественной безопасности посредством активного предотвращения и тщательного судебного преследования.

Содействие этому сотрудничеству может привести к существенному улучшению общественной безопасности и борьбы с терроризмом, несмотря на связанные с ним проблемы. Предлагаемые в данном руководстве передовые практики и руководящие принципы предназначены для того, чтобы проинформировать и сориентировать государства-члены в выполнении этой важной миссии.

[ 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)[5] 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)[6] и 2396 (2017)[7] Совета Безопасности призывают государства-члены сотрудничать при принятии национальных мер, призванных воспрепятствовать использованию террористами технологий и средств связи для совершения террористических атак. Резолюция 2396 (2017) Совета Безопасности также призывает государства-члены **расширять сотрудничество с частным сектором, особенно с компаниями, работающими в секторе информационно-коммуникационных технологий (ИКТ)**, в деле сбора цифровых данных и доказательств по делам, связанным с терроризмом.

В своем 30-м докладе Совету Безопасности Организации Объединенных Наций[8] 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[9].

5 Глобальная контртеррористическая стратегия Организации Объединенных Наций: седьмой обзор (A/RES/75/291), N2117570.pdf (un.org)

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

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

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

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

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

## 1.2 Инициатива CT TECH

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

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

РИСУНОК 1

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

| | |
|---|---|
| **Направление 1: принятие эффективных мер реагирования в рамках контртеррористической политики в ответ на вызовы и возможности новых технологий в борьбе с терроризмом при полном соблюдении прав человека и принципа верховенства права.** | |
|  Компонент 1.1 | Подготовка информационных материалов для разработки мер реагирования в рамках национальной контртеррористической политики в ответ на вызовы и возможности новых технологий в борьбе с терроризмом при полном 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 мер реагирования в рамках национальной контртеррористической политики для противодействия использованию террористами новых технологий и применения новых технологий в деле борьбы с терроризмом при полном соблюдении прав человека и принципа верховенства права. |
| **Направление 2: укрепление оперативного потенциала правоохранительных органов и органов уголовного правосудия для противодействия использованию новых технологий в террористических целях и применения новых технологий в деле предотвращения терроризма и борьбы с ним при полном соблюдении прав человека и принципа верховенства права.** | |
|  Компонент 2.1 | Предоставление практических инструментов и руководства для правоохранительных органов в целях противодействия использованию новых технологий в террористических целях и применения новых технологий в деле предотвращения терроризма и борьбы с ним при полном соблюдении прав человека и принципа верховенства права. |
|  Компонент 2.2 | Развитие у специалистов правоохранительных органов и органов уголовного правосудия государств-партнеров навыков, направленных на противодействие использованию новых технологий в террористических целях и применение новых технологий в деле предотвращения терроризма и борьбы с ним при полном 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

Целью данного документа является поддержка правоохранительных органов и ИКТ-компаний в создании механизмов сотрудничества и координации для противодействия использованию новых и новейших технологий в террористических целях.

Он предназначен для повышения осведомленности и предоставления обзора передовых практик для правоохранительных органов по установлению рабочих отношений с ИКТ-компаниями в рамках усилий по предотвращению насилия и борьбе с терроризмом.

## 1.3.1 Сфера охвата

Целью данного документа является предоставление практических советов и инструментов правоохранительным органам, особенно в странах с менее развитой экосистемой частного сектора, для эффективного сотрудничества с ИКТ-компаниями. ИКТ-компаниям также может быть полезно понять области сотрудничества, различные методы сотрудничества с правоохранительными органами и потенциальные проблемы, с которыми они могут столкнуться.

Кроме того, в данном документе не рассматривается местный контекст отдельных государств-членов с точки зрения юридических требований, соблюдения прав человека, принципа верховенства права, зрелости отрасли и доступа, среди прочего. Все это может повлиять на уровень сотрудничества между правоохранительными органами и ИКТ-компаниями.

### 1.3.2 Целевая аудитория

Настоящее руководство предназначено для правоохранительных органов и контртеррористических ведомств государств-членов, а также ИКТ-компаний.

### 1.3.3 Преимущества

Наладив хорошее и эффективное сотрудничество с технологическими компаниями, правоохранительные органы могут добиться следующего:

- получить лучшее представление о ключевых тенденциях использования технологических платформ и услуг в террористических целях;
- усилить координацию между правоохранительными органами и ИКТ-компаниями в целях активного и эффективного противодействия использованию технологических платформ и услуг в террористических целях;
- использовать технический опыт ИКТ-компаний в ходе осуществления контртеррористической деятельности;
- предоставить ИКТ-компаниям информацию на национальном уровне о контртеррористических операциях, чтобы помочь им сосредоточить свою деятельность и активно бороться с неправомерным использованием их платформ террористами;
- обеспечить доступ к более актуальной информации, чтобы быстрее и с большей вероятностью получать оперативную информацию и доказательства;
- улучшить обмен информацией об угрозах и взаимно укрепить обучение и понимание формирующихся угроз, расширяя возможности по принятию отраслевых решений в сфере борьбы с терроризмом.

### 1.3.4 Ограничения

Принимая во внимание тот факт, что как тактика террористической деятельности, так и технологический ландшафт являются динамичными системами и постоянно меняются, в данном документе не могут быть предугаданы, рассмотрены или предоставлены передовые практики для всех сценариев, платформ или технологий. Он предназначен для предоставления рекомендаций и подходов, основанных на современном понимании неправомерного использования и злоупотребления технологическими услугами в террористических целях.

Сотрудничество между ИКТ-компаниями и правоохранительными органами будет зависеть от местных правил, которые могут различаться в зависимости от юрисдикции, а также от методов обеспечения соблюдения прав человека и решения проблем конфиденциальности. Следует отметить, что данный документ не может комплексно охватить все юридические нюансы каждой юрисдикции и их влияние на возможности сотрудничества.

Его цель — помочь странам определить наиболее подходящие каналы для сотрудничества и предвидеть проблемы, которые могут возникнуть с течением времени.

[ II ]

# Подход

## 2.1 Обзор

Цель настоящего доклада заключается в том, чтобы предоставить государствам-членам поддержку и возможности для расширения сотрудничества между правоохранительными органами и ИКТ-компаниями в рамках усилий по противодействию использованию новых технологий в террористических целях, которые соответствуют Глобальной контртеррористической стратегии Организации Объединенных Наций и реализуются при полном уважении прав человека и принципа верховенства права.

## 2.2 Руководящая основа

РИСУНОК 2

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

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

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

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

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

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

| 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, принимающих решения, в целях планирования последующих решений или действий на стратегическом, оперативном или тактическом уровнях. Сбор, хранение, использование и обмен оперативной информацией должны осуществляться в соответствии с обязательствами государств-членов по 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, предпринимаемые 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 консультации с заинтересованными сторонами, кабинетные исследования, документы проекта CT TECH, совещания экспертных групп (СЭГ), данные внутреннего анализа и внутренние руководства, а также руководящая основа, описанная выше в разделе 2.2. Ключевые результаты этой деятельности включают определение различных моделей сотрудничества, предложение подхода, который следует учитывать при реализации модели сотрудничества, а также практические рекомендации по запросу информации у поставщиков интернет-услуг.

## 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. Цель их проведения заключалась в обсуждении эффективных стратегий противодействия использованию новых технологий в террористических целях, применении новых технологий в рамках проводимой работы, определении передовых практик, а также обсуждении рисков, проблем и неудачного опыта, требующих внимания и осторожности.

## 2.3.2 Обзор справочных материалов

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

### ТАБЛИЦА 3. Справочные материалы

| | |
|---|---|
| 1 | Совет Безопасности Организации Объединенных Наций (ИДКТК), «Состояние международного сотрудничества в области законного доступа к цифровым доказательствам», 2022 г. |
| 2 | Отделение Организации Объединенных Наций в Вене, «Система раскрытия данных. Общие практики, разработанные международными поставщиками услуг в ответ на запросы зарубежных правительств о предоставлении данных», 2021 г. |
| 3 | Отделение Организации Объединенных Наций в Вене, «Практическое руководство по порядку запроса электронных доказательств из других стран», 2021 г. |
| 4 | Интерпол, «Рекомендации по сбору электронных доказательств», 2018 г. |
| 5 | Директива (ЕС) 2017/541 о противодействии терроризму: влияние на основные права и свободы, 2021 г. |
| 6 | Совет Европы, Главное управление по правам человека и правовым вопросам Управления по борьбе с экономической преступностью Франции, «Сотрудничество между правоохранительными органами и поставщиками интернет-услуг в борьбе с киберпреступностью: к общим руководящим принципам» (пересмотренное исследование и руководящие принципы)», 2020 г. |
| 7 | Глобальная сеть по экстремизму и технологиям (GNET), Королевский колледж в Лондоне, «Совместная борьба с террористическим контентом в Интернете: сотрудничество между правоохранительными органами по борьбе с терроризмом и технологическими компаниями», профессор Стюарт Макдоналд и Эндрю Стэнифорт, 2023 г. |
| 8 | Фонд ICT4Peace и ИДКТК, «Участие частного сектора в реагировании на использование Интернета и ИКТ в террористических целях», 2016 г. |

[ III ]

# Введение

## 3.1 Обзор

Во все более взаимосвязанном мире, в котором цифровой ландшафт постоянно эволюционирует, борьба с терроризмом требует многогранного и совместного подхода. Настоящее руководство направлено на выявление, разработку и продвижение передовых практик по установлению сотрудничества между ИКТ-компаниями и правоохранительными органами в рамках глобальных усилий по борьбе с терроризмом.

ИКТ-компании играют решающую роль в этой борьбе, учитывая огромные объемы данных, с которыми они работают, и их потенциал выступать в качестве каналов для обмена жизненно важной информацией. В то же время правоохранительные органы находятся на переднем крае борьбы с терроризмом, в значительной степени полагаясь на анализ данных и оперативную информацию для предотвращения потенциальных угроз.

Однако эффективное сотрудничество между ними зачастую может быть осложнено в силу различных операционных процедур, юридических ограничений и проблем конфиденциальности данных. Поэтому становится крайне важно создать оптимальную основу, которая будет способствовать взаимопониманию и упорядоченному сотрудничеству.

Данное руководство направлено на то, чтобы помочь разобраться в этих сложностях и построить надежную модель партнерства, которая учитывает как операционные требования правоохранительных органов, так и бизнес-протоколы ИКТ-компаний. Основываясь на мнениях таких организаций, как Исполнительный директорат Контртеррористического комитета (ИДКТК), и руководящих принципах международных организаций, таких как Организация Объединенных Наций и Интерпол, это руководство направлено на создание устойчивой и эффективной среды сотрудничества, которая повышает наш коллективный потенциал в борьбе с терроризмом.

Установление партнерских отношений с ИКТ-компаниями может оказаться непростой задачей, учитывая, что каждая компания действует в соответствии с отдельными процедурами и протоколами сотрудничества при взаимодействии с правоохранительными органами. Кроме того, многочисленные ИКТ-компании предоставляют уникальные платформы, специально предназначенные для обработки запросов от правоохранительных органов, причем каждая из них имеет свое собственное контактное лицо. Организация Объединенных Наций опубликовала полезное руководство[10], призванное облегчить процесс запроса электронных доказательств через международные границы. Государствам-членам рекомендуется использовать это руководство в качестве полезного ресурса, поскольку в нем собрана всесторонняя информация, имеющая отношение к сотрудничеству со всеми ведущими ИКТ-компаниями.

Существуют различные стратегии установления отношений сотрудничества с ИКТ-компаниями. Хотя наш метод отличается от некоторых других, мы включили в него элементы ключевых принципов сотрудничества, почерпнутые из опыта Исполнительного директората Контртеррористического комитета (ИДКТК)[11]. Последний предоставил полезную информацию о различных методах работы, которые ИКТ-компании используют в рамках сотрудничества с правоохранительными органами.

10 Отделение Организации Объединенных Наций в Вене, «Практическое руководство по порядку запроса электронных доказательств из других стран», 2021 г.

11 Совет Безопасности Организации Объединенных Наций (ИДКТК), «Состояние международного сотрудничества в области законного доступа к цифровым доказательствам», 2022 г.

## 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[12], из которых более 93 процентов — это пользователи социальных сетей[13]. По оценкам, в 2022 году в мире будет создано более 97 зеттабайт[14] информации[15]. В то время как подобные технологические достижения способствуют преобразованию общества во имя всеобщего блага, террористы используют эти технологии в своих злонамеренных целях. Применение новых технологий в террористических целях ставит перед государствами-членами серьезные задачи по борьбе с терроризмом. Использование новых технологий обеспечивает анонимность и позволяют координировать действия и действовать удаленно.

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

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

### 3.2.1 Борьба с использованием новых технологий в террористических целях

Достижения в области ИКТ и их доступность сделали привлекательным для террористических и насильственных экстремистских групп использование Интернета и социальных сетей для совершения широкого спектра противоправных действий, включая подстрекательство, радикализацию, вербовку, обучение, планирование, сбор информации, коммуникацию, подготовку, пропаганду и финансирование. Кроме того, в своих целях террористические группировки умело используют гендерный фактор — неравенство, нормы и роли, включая агрессивную маскулинность, — и манипулируют им. Так, ИГИЛ эффективно вербует женщин через социальные сети, адаптируя свои послания для обращения к лицам женского пола, говорящим на разных языках и живущим в разных социальных, экономических и культурных условиях в Западной Европе, Центральной Азии, на Ближнем Востоке и в Северной Африке, и нередко эксплуатируя опыт женщин в области гендерного неравенства. Террористы также используют зашифрованные коммуникации и даркнет 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: борьба с терроризмом и правоохранительная деятельность

Новые технологии открывают перед правоохранительными органами безграничные возможности для эффективного противодействия терроризму при соблюдении международного права прав человека. Правоохранительные органы могут применять новые технологии для выявления, расследования, судебного

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

13 Инфорграфика Data Never Sleeps от компании Domo, Data Never Sleeps 10.0 | Domo

14 Один зеттабайт равен одному миллиарду терабайтов.

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

преследования и разрешения дел о преступлениях, связанных с терроризмом, новыми и более эффективными способами.

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

Эти практические идеи, основанные на использовании новых технологий, могут 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 предусматривает 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 информа-

ционно-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 правоприменение

Понятие «гендер» охватывает роли, поведение, занятия и качества, которые в конкретном обществе в определенный период времени считаются подходящими для мужчин и женщин, девочек и мальчиков. Помимо социальных атрибутов и возможностей, ассоциируемых с принадлежностью к мужскому или женскому полу, гендер связан с отношениями между женщинами и мужчинами, девочками и мальчиками. Гендер является частью более широкого социокультурного контекста и пересекается с другими факторами идентичности, включая пол, социальный класс, расовую принадлежность, уровень бедности, этническую принадлежность, половую ориентацию, возраст и т. д. Мужчины, женщины, девочки и мальчики, а также лица с различной гендерной идентичностью и самовыражением испытывают безопасность по-разному и в соответствии с их конкретными потребностями, уязвимостью и возможностями[16]. В частности, в контексте использования новых технологий. Несмотря на то что отсутствие иерархической структуры в Интернете позволяет устранить гендерные ограничения и предоставить возможности для расширения прав и возможностей женщин, оно также повышает вероятность их вербовки или активного взаимодействия с воинствующими экстремистскими и террористическими группировками в Интернете[17]. Имеющиеся данные также свидетельствуют о том, что террористические группы используют гендерную проблематику в своих онлайн-сообщениях; например, ИГИЛ стратегически использовало противоречивые с гендерной точки зрения послания при вербовке и распространении информации, изменяя свой дискурс в соответствии с целевой группой[18]. Еще один ключевой аспект, касающийся гендера и новых технологий, касается цифрового гендерного разрыва, в результате которого во всем мире доступ женщин к Интернету, по оценкам, составляет 85 процентов от аналогичного показателя у мужчин, и при этом приблизительно 1,7 миллиарда женщин в странах Глобального Юга не имеют доступа к Интернету. Это неравенство создает проблему прав человека, лежащую в основе всех аспектов кибербезопасности, включая потенциальную подверженность риску, отсутствие безопасности или участие в структуре управления[19].

Таким образом, интеграция гендерных аспектов в деятельность правоохранительных органов имеет решающее значение для оценки террористических намерений и потенциальных целей, а также для разработки соответствующих мер реагирования, учитывающих особые потребности и уязвимости лиц разной гендерной идентичности, принимая во внимание пересекающиеся факторы, такие как возраст, инвалидность, этническая принадлежность, язык, национальность, расовая принадлежность, религия, сексуальная ориентация или любой другой фактор идентичности и их сочетание.

16 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

17 ИДКТК, «Гендерные аспекты мер реагирования, принимаемых в связи с возвращением иностранных боевиков-террористов: перспективы исследований», февраль 2019 г.

18 Нелли Лахуд, «Расширение прав и возможностей или подчинение: анализ гендерно ориентированных сообщений ИГИЛ» (Структура «ООН-женщины», июнь 2018 г.).

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

# [IV] Модели сотрудничества

## 4.1 Обзор

Были определены четыре широкие модели сотрудничества, в рамках которых правоохранительные органы и ИКТ-компании могут эффективно работать вместе для достижения общей цели: противодействия использованию новых технологий в террористических целях. В этой главе подробно описаны модели сотрудничества, ключевые проблемы и возможности, а также ключевые руководящие принципы сотрудничества.

Первая модель, «Обмен информацией», облегчает обмен информацией об угрозах в режиме реального времени. Подобный обмен повышает ситуационную осведомленность и дает представление о ключевых тенденциях, что позволяет применять упреждающий подход к борьбе с терроризмом и формировать эффективную коммуникационную сеть, которая дает ИКТ-компаниям возможность предотвращать неправомерное использование их услуг для осуществления потенциальных угроз.

Вторая модель, «Расширение возможностей», позволяет правоохранительным органам передавать конкретные потребности на аутсорсинг, тем самым работая с повышенной эффективностью и гибкостью ресурсов. Эта модель использует технические возможности ИКТ-компаний, эффективно расширяя возможности правоохранительных органов и позволяя им быстро адаптироваться к изменяющемуся ландшафту потенциальных угроз.

Третья модель, «Бизнес-альянс/коллегия», способствует более широкому сотрудничеству. Эта модель побуждает правоохранительные органы и ИКТ-компании преодолевать изоляцию, повышая их коллективную осведомленность и позволяя им расставлять приоритеты в тех областях, которые представляют взаимный интерес. В ней подчеркивается совместная стратегия, общая ответственность и общие цели в борьбе с терроризмом.

И, наконец, четвертая и наиболее распространенная модель сотрудничества — «Активное расследование». Эта модель подразумевает поддержку проведения активных расследований путем предоставления данных и технологической помощи как для пресечения террористической деятельности, так и для преследования террористов. В ней участвуют ИКТ-компании, работающие напрямую с правоохранительными органами, предоставляющие данные и техническую помощь в режиме реального времени, в результате чего повышается скорость и эффективность расследований.

Эти четыре модели, каждая со своими уникальными преимуществами и областями применения, обеспечивают комплексную основу для укрепления сотрудничества между правоохранительными органами и ИКТ-компаниями в рамках усилий по борьбе с терроризмом.

РИСУНОК 4


ТАБЛИЦА 4. **Модели сотрудничества**

| | |
|---|---|
| **Обмен информацией** | Содействует двустороннему обмену информацией, включая актуальную информацию об угрозах, понимание террористических тенденций и тактики использования технологий в злонамеренных целях, оповещение и принятие мер в случае подозрительных или противоправных действий. Кроме того, важно расставить приоритеты в выявлении угроз, связанных со злоупотреблением услугами, платформами или продуктами ИКТ-компаний со стороны террористов. Первостепенное внимание к этим аспектам позволяет эффективно решать проблемы, связанные с террористической деятельностью, в рамках сотрудничества. |
| **Расширение возможностей** | Коммерческие компании предоставляют соответствующим службам услуги по сбору оперативной информации за определенную плату, инвестируя ресурсы и технологии в различные области, такие как даркнет или криптовалюта. Сотрудничество с такими компаниями может быть полезным для обеих сторон, поскольку многие из них имеют такие возможности, которые правоохранительные органы могут использовать для более эффективной борьбы с терроризмом. |
| **Бизнес-альянс/ коллегия** | Создание бизнес-альянса направлено на расширение возможностей борьбы с терроризмом путем обмена технологиями и методами, а также получения знаний о потенциальных угрозах. Такое сотрудничество может помочь правоохранительным органам лучше подготовиться к предстоящим угрозам и дать им представление о перспективных разработках для снижения террористических рисков. В основные задачи такой коллегии входит изучение потенциальных рисков и возможностей, которые могут нести в себе перспективные технологии. |
| **Активное расследование** | Основная цель сотрудничества между правоохранительными органами и ИКТ-компаниями заключается в сборе данных, связанных с расследованием террористической деятельности, и предотвращение злоупотребления предоставляемыми ими услугами со стороны террористических группировок. Это сотрудничество имеет решающее значение для повышения общественной безопасности посредством активного предотвращения и тщательного судебного преследования. |

## 4.2 Общие проблемы сотрудничества

Зачастую правоохранительные органы и ИКТ-компании имеют благие намерения и желание работать вместе в борьбе с терроризмом. Однако существуют общие проблемы, которые ограничивают эффективность и уровень сотрудничества между ними. Из-за присущих им различий в мотивации и интересах правоохранительные органы и ИКТ-компании могут иметь противоречивое видение, которое затрудняет сотрудничество. Каждая из сторон имеет свой образ мышления и свои подходы, которые могут создавать препятствия для эффективного сотрудничества. Ниже представлены некоторые общие проблемы, которые влияют на сотрудничество:

## ТАБЛИЦА 5. **Общие проблемы**

| Общие проблемы | |
|---|---|
| **Проблемы в области конфиденциальности и прав человека** | Сотрудничество между правоохранительными органами и ИКТ-компаниями может быть сопряжено с серьезными проблемами в области конфиденциальности, особенно в отношении обмена персональными данными. Представители частного сектора могут неохотно делиться конфиденциальной информацией с правоохранительными органами из-за опасений по поводу возможных нарушений прав на неприкосновенность частной жизни. Например, шифрование обеспечивает конфиденциальность и безопасность, необходимые для свободы выражения мнений в Интернете, особенно в случае социально уязвимых групп населения. ИКТ-компании должны защищать данные пользователей и предоставлять такую информацию только при соблюдении соответствующих законов и правил, особенно когда запрос предполагает удаление контента, что может выглядеть как нарушение свободы слова. Поэтому ИКТ-компаниям следует внедрить прозрачную политику и практику, которые обеспечат информирование пользователей о том, как их данные собираются, хранятся и передаются правоохранительным органам. |
| **Недостаток знаний и осведомленности или недопонимание** | Одной из наиболее существенных проблем межведомственного сотрудничества является отсутствие координации ожиданий. У правоохранительных органов зачастую имеются нереалистичные ожидания или недопонимание относительно возможностей ИКТ-компаний с точки зрения характера сохраняемых данных, периода их хранения, объема, предоставления, а также удаления контента. Это может привести к невозможности исполнения, задержкам или отказу от сотрудничества со стороны ИКТ-компаний. С другой стороны, ИКТ-компании могут не понимать, каким образом террористические группы злоупотребляют их услугами и какие данные необходимы правоохранительным органам для предотвращения или расследования такой деятельности. |
| **Коллидирующие интересы** | У ИКТ-компаний могут быть иные интересы, чем у правоохранительных органов, например, защита своих коммерческих интересов или конфиденциальности пользователей. Влияние сотрудничества с государством на их репутацию можно рассматривать по-разному. Это может приводить к задержкам или трудностям в обработке запросов на предоставление информации и ресурсов, что повлияет на время ответа компаний и их мотивацию к сотрудничеству с правоохранительными органами. |
| **Правовые требования** | Несовместимость законов и правил разных стран и регионов зачастую ограничивает возможности правоохранительных органов и компаний по обмену соответствующей информацией или сотрудничеству в расследованиях, особенно в случаях, связанных с подстрекательством к насилию или разжиганием ненависти. Одни компании могут ссылаться на законы в области обеспечения национальной безопасности или правила конфиденциальности для защиты данных своих пользователей, в то время как другие могут заявлять, что свобода слова является защитой от цензуры или преследования. Эти правовые конфликты могут препятствовать усилиям правоохранительных органов по предотвращению или преследованию за использование ИКТ в террористических целях. |
| **Технические проблемы** | Технические проблемы также могут препятствовать сотрудничеству между правоохранительными органами и ИКТ-компаниями. Помимо дифференцированной классификации компьютерных систем и методических процедур, различные технологии и системы могут затруднять эффективный обмен информацией и ресурсами для обеих сторон. Более того, правоохранительным органам может не хватать необходимого оборудования, навыков или подготовки для проведения цифровой криминалистической экспертизы или расследований с использованием открытых источников (OSINT). |
| **Приоритеты** | Противоречивые точки зрения могут приводить к разному восприятию рисков и ответственности. Правоохранительные органы могут рассматривать конкретный инцидент, связанный с использованием ИКТ в террористических целях, как непосредственную угрозу общественной безопасности, требующую немедленных действий, а ИКТ-компании могут воспринимать его как потенциально низкий риск, который не оправдывает угрозу конфиденциальности данных их пользователей. Правоохранительные органы, имеющие опыт оценки рисков, несут юридическую ответственность за защиту общественности, в то время как ИКТ-компании нуждаются в большем понимании и доверии к конкретным вопросам и собеседникам со стороны правоохранительных органов. Это может привести к отсутствию сотрудничества или даже конфликту между двумя сторонами. Более того, ИКТ-компании могут быть сосредоточены на предоставлении услуг и информации, которые отвечают потребностям и ожиданиям их клиентов, вместо активного мониторинга злоупотреблений их услугами, в то время как правоохранительные органы должны всегда быть начеку в отношении потенциальных угроз. Этот разный образ действий может поставить под угрозу сотрудничество между двумя сторонами в отношении их функций и обязанностей в обеспечении общественной безопасности. |
| **Ресурсы** | Небольшие компании могут не располагать достаточными ресурсами, чтобы предложить серьезное сотрудничество с правоохранительными органами, и они могут не решаться на такое сотрудничество, чтобы сохранить свои ресурсы. |

# 4.3 Мотивация к сотрудничеству

Террористы все чаще полагаются на технологические платформы и поставщиков услуг для осуществления своей злонамеренной деятельности, и поэтому правоохранительные органы зачастую сталкиваются с техническими проблемами в борьбе, преследовании и привлечении террористов к ответственности. К таким проблемам относятся получение соответствующих данных, которые хранятся ИКТ-компаниями, работа с ограниченными ресурсами, преодоление технологических пробелов и сложный характер самой угрозы. Мотивация правоохранительных органов к сотрудничеству с ИКТ-компаниями обусловлена следующими факторами:

ТАБЛИЦА 6. **Мотивация правоохранительных органов к сотрудничеству**

| Мотивация правоохранительных органов | |
|---|---|
| **Сбор информации и доказательств** | Сотрудничество между правоохранительными органами и ИКТ-компаниями имеет важное значение для получения ценных доказательств или оперативной информации, которыми располагают эти компании. Например, ИКТ-компании могут предоставлять доступ к пользовательским данным, контенту, метаданным, данным о местоположении и т. д., что может помочь правоохранительным органам в выявлении и расследовании действий отдельных террористов и террористических сетей. |
| **Доступ к передовым технологиям** | ИКТ-компании зачастую имеют доступ к новейшим технологиям и опыту, которые могут помочь правоохранительным органам в сборе доказательств, отслеживании и мониторинге потенциальных угроз и реагировании на инциденты. Например, ИКТ-компании могут предоставлять инструменты для шифрования, дешифрования, анализа данных, «добычи» данных, визуализации, цифровой криминалистической экспертизы, анализа данных с использованием искусственного интеллекта и т. д. Это может расширить возможности правоохранительных органов в борьбе с терроризмом. |
| **Улучшение координации и реагирования** | Совместные усилия правоохранительных органов и ИКТ-компаний могут привести к улучшению координации и более эффективному реагированию на инциденты. Например, ИКТ-компании могут предоставлять критически важные данные, инфраструктуру, ресурсы и опыт, которые могут содействовать усилиям правоохранительных органов по реагированию на террористические инциденты. |
| **Экономически эффективные решения** | Сотрудничество между правоохранительными органами и ИКТ-компаниями может обеспечить экономически эффективные решения для борьбы с угрозой терроризма. За счет объединения ресурсов обеих сторон, правоохранительные органы могут эффективно распределять свои ресурсы, бюджеты, средства, рабочую силу, оборудование, материалы и т. д., таким образом снижая затраты на борьбу с терроризмом благодаря уникальной ценности сотрудничества. |
| **Повышение степени общественного доверия** | Эффективное партнерство между правоохранительными органами и ИКТ-компаниями может повысить степень уверенности общества в способности правоохранительных органов противостоять угрозе терроризма. Это может помочь укрепить общественное доверие и поддержать усилия правоохранительных органов по борьбе с терроризмом. |
| **Промежуточное хранение и противодействие использованию Интернета и социальных сетей в террористических целях** | Расширение сотрудничества между правоохранительными органами и ИКТ-компаниями препятствует использованию террористами Интернета и социальных сетей в террористических целях. |

Кроме того, сотрудничество между правоохранительными органами и ИКТ-компаниями может нести прямую или косвенную выгоду для ИКТ-компаний. Такое сотрудничество может оказать положительное влияние на бизнес этих компаний в долгосрочной перспективе. Мотивация ИКТ-компаний к сотрудничеству обусловлена следующими факторами:

ТАБЛИЦА 7. **Мотивация ИКТ-компаний к сотрудничеству**

| Мотивация ИКТ-компаний | |
|---|---|
| **Репутация и имидж бренда** | Сотрудничество с правоохранительными органами может повысить репутацию и имидж бренда компании. Компания может повысить свой авторитет и репутацию среди клиентов, заинтересованных сторон и широкой общественности, продемонстрировав свою приверженность принципам обеспечения безопасности и защиты населения. Это сотрудничество может улучшить пользовательский опыт для их клиентов и создать более безопасную среду, что позволит повысить привлекательность платформы и увеличить доход. |
| **Общественная безопасность** | Это сотрудничество может улучшить пользовательский опыт для их клиентов и создать более безопасную среду, что позволит повысить репутацию платформы и увеличить доход. |
| **Правовые обязательства** | ИКТ-компании могут иметь юридические обязательства по сотрудничеству с правоохранительными органами, например, в ответ на обоснованный законный запрос на предоставление информации или в соответствии с национальными или международными нормами и правилами. |
| **Повышенная безопасность** | Сотрудничество с правоохранительными органами может помочь ИКТ-компаниям повысить безопасность предоставляемых продуктов и услуг. Это может помочь предотвратить использование их технологий в преступной или террористической деятельности, а также смягчить последствия инцидентов, связанных с использованием их технологий. |

## 4.4 Ключевые руководящие принципы сотрудничества

Чтобы укрепить сотрудничество между правоохранительными органами и ИКТ-компаниями, обеим сторонам необходимо придерживаться ключевых принципов сотрудничества, таких как общие цели в борьбе с терроризмом, полное соблюдение принципа верховенства права, взаимное доверие и уважение, а также защита конфиденциальности данных и прав человека. Ключевые принципы, перечисленные в приведенной ниже таблице, служат основой для построения прочного и долгосрочного сотрудничества между правоохранительными органами и ИКТ-компаниями в борьбе с терроризмом.

ТАБЛИЦА 8. **Руководящие принципы сотрудничества**

| Ключевые принципы | |
|---|---|
| **Общая цель борьбы с терроризмом** | Сотрудничество между правоохранительными органами и ИКТ-компаниями должно носить характер партнерства. Обе стороны должны прикладывать усилия для достижения общих целей, вкладывать свои силы и ресурсы для поддержки друг друга, принимая во внимание различные интересы и потребности обеих сторон. |
| **Всеобщее уважение принципа верховенства права** | Сотрудничество должно соответствовать применимым законам и правилам, включая национальные и международные законы о конфиденциальности и защите данных. Это позволит ИКТ-компаниям оказывать эффективную помощь и укреплять доверие. |
| **Взаимное доверие и уважение** | Сотрудничество между правоохранительными органами и ИКТ-компаниями должно основываться на взаимном доверии и уважении. |
| **Конфиденциальность** | Сотрудничество должно осуществляться с соблюдением принципа конфиденциальности данных и ресурсов, которыми обмениваются правоохранительные органы и ИКТ-компании. Конфиденциальная информация должна передаваться только по принципу служебной необходимости и должна быть защищена от несанкционированного доступа. Если данные могут быть представлены в суде и могут стать общеизвестными, компания должна быть предупреждена об этом.<br><br>ИКТ-компаниям требуется полное обоснование запроса на предоставление данных, при этом некоторые из них могут иметь правило уведомления — как только они предоставят данные любым правоохранительным органам, они автоматически уведомят об этом клиента. |

| Ключевые принципы | |
|---|---|
| **Прозрачность** | Уведомление соответствующих сторон о существовании и объеме такого сотрудничества. Некоторые компании могут делиться с правоохранительными органами информацией об условиях использования или публиковать ежегодный отчет с описанием степени своего сотрудничества, чтобы повысить прозрачность своей работы. |
| **Компетенции** | Правоохранительные органы и ИКТ-компании должны быть в полной мере осведомлены о процедурах обмена информацией. Представители правоохранительных органов должны понимать, что может предложить каждая компания, какие ресурсы ей потребуются для предоставления этих данных, сколько времени может потребоваться для ответа на запрос и каким образом он должен быть выполнен. Взаимное удовлетворение ожиданий обеих сторон имеет основополагающее значение для успешного сотрудничества. |

# 4.5 Прочие соображения

Существуют дополнительные аспекты, которые следует учитывать при налаживании сотрудничества между правоохранительными органами и ИКТ-компаниями в борьбе с терроризмом. Во-первых, характер сотрудничества, которое может быть либо долгосрочным, либо разовым. Во-вторых, количество сторон, принимающих участие в сотрудничестве, которое может быть либо двусторонним, либо многосторонним, охватывающим несколько государств-членов. Эти аспекты оказывают значительное влияние на условия сотрудничества и должны учитываться при выборе соответствующей модели. Они влияют на имеющиеся ресурсы, сроки достижения результатов и подход к сотрудничеству.

## 4.5.1 Характер сотрудничества

В зависимости от целей правоохранительных органов и оперативных требований характер сотрудничества с отдельными ИКТ-компаниями может различаться. В частности, правоохранительные органы могут сотрудничать с ИКТ-компаниями в ограниченном объеме на разовой основе с учетом конкретного случая или требования.

Это может включать в себя обращение к ИКТ-компаниям с просьбой предоставить техническую помощь или доступ к данным в рамках конкретного расследования или операции, и очевидно, что такое сотрудничество является редким случаем и может не повториться в ближайшем будущем.

Как правило это случаи, имеющие чрезвычайный характер и не подразумевающие наличия ранее установленных отношений между правоохранительными органами и конкретной ИКТ-компанией. В подобной ситуации попросту нет времени для установления доверительных отношений между сторонами, и координация усилий может оказаться более сложной задачей. Поскольку в подобной ситуации долгосрочных отношений между сторонами не предвидится, общение между ними будет ограничено конкретным случаем.

В таких случаях правоохранительным органам следует придерживаться следующего порядка действий:

1. **Определить соответствующее контактное лицо в компании:** обычно лучше всего начать с юридических отделов, поскольку они знают юридические требования и процедуры для ордеров и чрезвычайных случаев. Они также могут направить правоохранительные органы к соответствующему лицу, которое может помочь с запросом. После определения метода сотрудничества можно обсудить то, на какие данные оно распространяется.

2. **Согласовать характер и средства сотрудничества:** установление реалистичных целей — лучший способ направить конкретные ожидания в правильное русло, четко определить степень срочности и время, которое потребуется ИКТ-компании для получения запрошенных данных после обсуждения согласованных средств их предоставления.

При этом необходимо принять во внимание тот факт, что в данном случае отсутствие сотрудничества в прошлом ограничивает доверие, и может возникнуть необходимость предоставления допол-

нительной информации о последовательности событий и фактах в подтверждение запроса. Один из способов сделать это — предоставить всю соответствующую информацию при первом контакте и обновлять ее по мере необходимости. При наличии задержек или трудностей следует рассмотреть возможность предоставления данных, разбитых на несколько пакетов, вместо того, чтобы ожидать формирования полного набора данных.

Еще одним фактором сотрудничества является то, что проведение долгосрочного сотрудничества между правоохранительными органами и ИКТ-компаниями требует тщательного рассмотрения различных факторов и механизмов. Это наиболее распространенный тип сотрудничества между сторонами, построенный на заранее определенных принципах.

Крайне важно поддерживать постоянные каналы связи, при этом наличие специально назначенного контактного лица будет способствовать установлению эффективного сотрудничества. Создание инфраструктуры, включающей взаимное обучение, периодические встречи, обмен данными, безопасные линии связи и стандартные процедуры для различных сценариев, может быть выгодным вложением для обеих сторон.

### 4.5.2 Двустороннее и многостороннее сотрудничество

Многостороннее сотрудничество предполагает сотрудничество между несколькими сторонами, в некоторых случаях даже на международном уровне. В рамках многостороннего сотрудничества основное внимание уделяется решению более широких проблем, затрагивающих множество сторон, и такое сотрудничество может привести к формированию общих ресурсов и передовых практик. В то время как двустороннее сотрудничество является более простым и быстрым, многостороннее сотрудничество может привести к разработке более комплексных и эффективных решений в долгосрочной перспективе.

Самое важное, что следует учитывать, это то, стороны могут иметь разные ценности, ресурсы и правовую ситуацию. Диверсификация может быть мудрым решением, однако при этом следует убедиться, что все стороны сосредоточены на главных целях.

Многостороннее сотрудничество лучше подходит для общих альянсов, которые сосредоточены на продвижении концепций и выявлении рисков и возможностей, а не на конкретных оперативных расследованиях. С другой стороны, двустороннее сотрудничество обычно используется для решения оперативных задач, связанных с текущими делами.

[V]

# Модель сотрудничества № 1 — Обмен информацией

## 5.1 Цель

Обмен информацией является важнейшим аспектом сотрудничества между ИКТ-компаниями и правоохранительными органами в борьбе с терроризмом. ИКТ-компании имеют доступ к ценным данным и знаниям на своих платформах, которые могут помочь в выявлении и предотвращении террористической деятельности. Например, они могут обнаруживать модели подозрительного поведения, выявлять контент, нарушающий их условия предоставления услуг, или сообщать об учетных записях, связанных с известными террористами и террористическими организациями. С другой стороны, правоохранительные органы могут предоставлять ИКТ-компаниям рекомендации и обратную связь о способах улучшения принимаемых ими мер безопасности. Своевременный и эффективный обмен информацией позволяет обеим сторонам извлекать выгоду из сильных сторон и ресурсов друг друга, соблюдая при этом конфиденциальность данных и права своих пользователей.

## 5.2 Задачи

Цель состоит в том, чтобы установить рабочие отношения между ИКТ-компаниями и правоохранительными органами для облегчения двустороннего обмена информацией. В частности, обмен информацией позволяет обеспечить следующее:

- обмен информацией об угрозах, которая может быть актуальной для правоохранительных органов и ИКТ-компаний;
- понимание ключевых тенденций, идентификаторов, тактики и способов использования технологий для осуществления террористической деятельности;
- оповещение и принятие мер в отношении подозрительного или незаконного поведения и действий, которые могут потребовать расследования;
- определение приоритетов угроз, связанных со злоупотреблением услугами, платформами или продуктами ИКТ-компаний со стороны террористов.

## 5.3 Подход к сотрудничеству

Обмен информацией является важнейшим аспектом сотрудничества между ИКТ-компаниями и правоохранительными органами в борьбе с терроризмом. ИКТ-компании имеют доступ к ценным данным и знаниям на своих платформах, которые могут помочь в выявлении и предотвращении террористической деятельности. Например, они могут определять модели подозрительного поведения, выявлять подозрительный контент, при этом правоохранительные органы могут предоставлять обратную связь по этим вопросам.

1. Определение наиболее подходящих ИКТ-компаний для сотрудничества является важным начальным шагом в установлении сотрудничества с правоохранительными органами. Эта модель сотрудничества должна быть приоритетной и использоваться в отношениях с как можно большим количеством ИКТ-компаний.

   Команда, отвечающая за данную задачу, должна также выявить компании, которые могут быть уязвимыми, и предоставить им соответствующую информацию. Рекомендуется передавать несекретные данные как можно большему количеству соответствующих компаний, тогда как секретные данные следует передавать выборочно и с соответствующей осторожностью.

2. Мотивация к активному сотрудничеству между правоохранительными органами и ИКТ-компаниями имеет решающее значение, поскольку такое сотрудничество опирается на активное предоставление информации со стороны этих компаний. Одним из способов побуждения к обмену информацией является предоставление отзывов о результатах действий правоохранительных органов в соответствующих случаях. Подобные отзывы могут помочь укрепить доверие между двумя сторонами и стимулировать ИКТ-компании к дальнейшему обмену информацией, которая может помочь в борьбе с терроризмом.

   Кроме того, информация, предоставляемая правоохранительными органами, помогает ИКТ-компаниям в обеспечении безопасности своих платформ и может выступать в качестве мотивирующего фактора.

3. Постоянное взаимодействие с соответствующими компаниями может помочь в поддержании их активного сотрудничества и обеспечить своевременное предоставление необходимых данных, что, в свою очередь, позволит повысить безопасность их платформ.

4. Одним из эффективных способов активного мониторинга социальных сетей на предмет подозрительной террористической деятельности является мониторинг силами самих компаний. Некоторые компании уже создали механизмы для отслеживания и предотвращения такой деятельности[20]. Рекомендуется оказывать этим компаниям любую возможную поддержку, например, путем обмена известными индикаторами террористической деятельности. Примеры таких индикаторов включают факторы радикализации, запрещенные группы, названия активных групп и псевдонимы, запланированные дни действий, лозунги и символическое содержание. Если раньше для мониторинга активности использовались ключевые слова, то теперь для сканирования платформ и выявления новых форм угроз используются возможности ИИ. Однако, поскольку данная технология все еще является новой и незрелой, рекомендуется сочетать ее с традиционными методами.

5. Существует множество НПО и международных организаций, которые занимаются мониторингом различных аспектов онлайн-деятельности террористических групп. Объединение усилий с этими организациями может расширить возможности по превентивному предотвращению угроз и поддержанию общественной безопасности на оптимальном уровне.

   Необходимо определить эти организации и начать обмениваться с ними информацией, опытом и ресурсами. Партнерская сеть может повысить эффективность и результативность усилий по борьбе с терроризмом.

20 Одним из примеров такого сотрудничества является The Christchurch Call — сообщество, объединяющее более 120 правительств, поставщиков онлайн-услуг и организаций гражданского общества, действующих вместе для устранения террористического и насильственного экстремистского контента в Интернете.

# [VI] Модель сотрудничества № 2 — Расширение возможностей

## 6.1 Цель

Многочисленные коммерческие компании предлагают свои услуги по сбору оперативной информации за определенную плату. Эти компании инвестируют значительные ресурсы и технологии для приобретения уникального опыта в различных областях, таких как даркнет или криптовалюта.

Существует множество компаний, которые вложили значительные ресурсы в развитие возможностей, которые правоохранительные органы могли бы использовать для более эффективной борьбы с терроризмом. Сотрудничество с этими компаниями может быть выгодным для обеих сторон.

## 6.2 Задачи

Цель состоит в том, чтобы расширить возможности правоохранительных органов за счет использования знаний и опыта ИКТ-компаний. В частности, такое расширение возможностей позволяет правоохранительным органам:

- экономить на НИОКР за счет сотрудничества с компаниями, которые уже вложили средства в соответствующие технические возможности;
- содействовать экономически эффективной диверсификации штата правоохранительных органов путем включения в него людей с различными навыками и опытом;
- получить быстрый доступ к передовым технологиям и ценным базам данных оперативной информации;
- корректировать штат и квалификацию своих сотрудников в соответствии с насущными потребностями.

## 6.3 Подход к сотрудничеству

1. ИКТ-компании функционируют в рамках гражданского ландшафта и часто происходят из разных юрисдикций, каждая из которых имеет свой собственный набор правил, потенциально упуская из виду местные культурные нюансы и сталкиваясь с языковыми препятствиями. Более того, некоторые компании могут не обладать необходимым пониманием или опытом работы с местными правовыми нормами и этическими стандартами.

   Поэтому крайне важно обеспечить соответствие любого сотрудничества с такими компаниями требованиям местного законодательства, этическим соображениям и процедурным методам при соблюдении международного законодательства. Эти компании должны соблюдать правовые ограничения, придерживаться этических принципов, сохранять целостность доказательств и следовать любым другим соответствующим директивам.

Чтобы обеспечить соблюдение предусмотренных законом процедур в рамках сотрудничества, рекомендуется провести комплексную юридическую проверку потенциальных партнеров до оформления с ними официальных соглашений о сотрудничестве. Это становится особенно важным в случае сотрудничества с компаниями, которые занимаются сбором оперативной информации на возмездной основе.

2. В нынешнюю эпоху наблюдается резкий рост числа частных коммерческих организаций, которые сосредотачивают свои усилия на сборе оперативной информации через Интернет, уделяя особое внимание крупномасштабному сбору и анализу данных. Некоторые из этих компаний предлагают ценные услуги по предоставлению оперативной информации. Они освоили технологии и отточили специализированный опыт, который правоохранительные органы могут использовать для обеспечения общественной безопасности.

   Эти компании зачастую могут быть более эффективными благодаря своей способности инвестировать значительные ресурсы, что позволяет им распространять оперативную информацию в глобальном масштабе, хотя и ради собственной прибыли. Ярким примером является даркнет — теневая платформа с глобальным охватом. Определенному ведомству с конкретным географическим мандатом может потребоваться анализ данных, не связанных с его юрисдикцией. И наоборот, коммерческая компания может проанализировать все данные и поделиться соответствующей информацией с заинтересованными странами.

   Рекомендуется определить подходящих поставщиков услуг, которые смогут наилучшим образом поддержать конкретные инициативы. Чтобы эффективно устранить недостатки в сборе данных или технологических возможностях, рекомендуется сначала провести исчерпывающую оценку и установить степень приоритетности этих недостатков совместно с экспертами в области извлечения оперативной информации. После выявления критических пробелов следующим шагом является исследование рынка в поисках потенциальных компаний, предлагающих решения, предназначенные для устранения этих пробелов.

[VII]

# Модель сотрудничества № 3 — Бизнес-альянс/коллегия

## 7.1 Цель

Целью создания бизнес-альянса является создание консорциума организаций, способных расширить возможности борьбы с терроризмом путем обмена новыми технологиями и методами работы. Благодаря такому сотрудничеству правоохранительные органы могут получить информацию о потенциальных угрозах до того, как они достигнут рынка и попадут в руки террористических группировок. Понимание новых технологий, несущих с собой эти угрозы, позволит правоохранительным органам лучше подготовиться к предстоящим угрозам или разработать рекомендации по предотвращению реализации таких угроз. Более того, такой альянс может дать представление о будущих событиях, которые позволят смягчить террористические риски. В основные задачи такой коллегии входит изучение потенциальных рисков и возможностей, которые могут нести в себе перспективные технологии.

## 7.2 Задачи

Цель данной модели сотрудничества заключается в создании альянса, который будет работать как совместное предприятие по актуальным вопросам. В частности, такой альянс позволяет:

- подготовиться к будущим угрозам путем прогнозирования появления новых технологий до того, как ими воспользуются террористы;
- предотвратить будущие угрозы, изучая упреждающие меры, необходимые для обеспечения общественной безопасности;
- использовать инновационные технологии в качестве самых передовых инструментов для борьбы с терроризмом;
- обеспечить широкое информирование компаний о потенциальных рисках, которое позволит им снижать риски за счет согласованных усилий.

## 7.3 Подход к сотрудничеству

1. Поскольку основной целью такого консорциума является использование новых технологий, рекомендуется постоянно искать инновационные компании, которые могут внести свой вклад в работу бизнес-альянса.
2. Возможность создания нового бизнес-альянса следует рассматривать только в том случае, если существующего консорциума нет или если рассматриваемый вопрос касается проблем, требующих решения на местном уровне. Рекомендуется искать и присоединяться к уже существующему бизнес-альянсу, а не пытаться создать новый, поскольку компании могут не решаться одновременно вступать в несколько бизнес-альянсов.

3. Принимая во внимание, что наиболее инновационными компаниями могут быть небольшие стартапы, важно обеспечить, чтобы такой бизнес-альянс был открыт для них, и чтобы они знали о его существовании.

4. Рекомендуется создавать бизнес-альянс постепенно. Для этого следует составить перечень представляющих интерес ИКТ-компаний и первоначально обращаться с предложением о сотрудничестве только к некоторым из них. После создания бизнес-альянса будет легче добиться вступления в него новых членов.

5. Существуют различные тематические бизнес-альянсы, которые правоохранительные органы могут инициировать или к которым могут присоединиться, однако особо отличаются те из них, которые посвящены ИИ. Такие альянсы состоят из множества стран, которые используют разнообразие, необходимое для создания объективного и эффективного ИИ. Поэтому рекомендуется изучить существующие группы, которые уже работают по этому вопросу. Несмотря на то что ИИ обладает огромным потенциалом для усиления профилактических мер, он также создает значительные риски, которые необходимо устранять, а диверсифицированный альянс может дать в этом отношении лучшие результаты.

6. Следует рассмотреть возможность изучения существующих международных альянсов, которые уже доказали свою эффективность, и направить запрос о присоединении к ним или использовании результатов совместной работы их членов[21].

21 GIFCT — Глобальный интернет-форум по борьбе с терроризмом, JCAT — Объединенная группа по оценке борьбы с терроризмом, InfraGard — партнерство между ФБР и частным сектором.

[VIII]

# Модель сотрудничества № 4 — Активное расследование

## 8.1 Цель

Это наиболее распространенная и востребованная форма сотрудничества между правоохранительными органами и ИКТ-компаниями. Основная цель сотрудничества между правоохранительными органами и ИКТ-компаниями заключается в сборе данных, связанных с расследованием террористической деятельности, и предотвращение злоупотребления предоставляемыми ими услугами со стороны террористических группировок. Это сотрудничество имеет решающее значение для повышения общественной безопасности посредством активного предотвращения и тщательного судебного преследования.

## 8.2 Задачи

Цель такого сотрудничества — помочь правоохранительным органом в преследовании террористов посредством активных расследований с участием ИКТ-компаний. В частности, такое сотрудничество позволяет:

- осуществлять активный мониторинг данных для отслеживания потенциальных террористических атак;
- удалять контент, связанный с терроризмом, с общедоступных платформ;
- осуществлять сбор данных для предотвращения террористических атак или выявления новых террористических группировок;
- осуществлять сбор доказательств, необходимых для судебного преследования.

## 8.3 Подход к сотрудничеству

1. Решающим фактором, который может существенно повлиять на успех сотрудничества между правоохранительными органами и ИКТ-компаниями, является наличие единой точки контакта. Обе стороны получают выгоду от наличия специального подразделения, которое поддерживает тесные отношения с представителем компании и осведомлено об их данных, организации, процедурах и ожидаемых сроках доступа к ним. Централизация всех необходимых протоколов для эффективного сотрудничества в рамках одной организации может быть залогом успеха.

   **ПРИМЕЧАНИЕ. Чтобы обеспечить круглосуточную доступность, как правило рекомендуется использовать единый (постоянно проверяемый) адрес электронной почты.**

2. Инфраструктура является важным компонентом успешного сотрудничества между правоохранительными органами и ИКТ-компаниями. Крайне важно обеспечить безопасность каналов связи и защитить конфиденциальность и целостность передаваемых данных. Также важно обеспечить своевременное и эффективное предоставление данных с соблюдением норм международного права, чтобы обеспечить

приемлемость любой предоставленной информации в качестве доказательств в судебном разбирательстве. Многие глобальные компании оказывают поддержку правоохранительным органам через специальный портал, созданный специально для запросов правоохранительных органов.

После регистрации правоохранительные органы могут войти в систему и загрузить официальные запросы на предоставление данных. Такие компании также предлагают обучение для правоохранительных органов по использованию их порталов. Важно отметить, что портал служит постоянной платформой для сотрудничества, но не может выступать в качестве единственной линии коммуникаций.

3. Чтобы обеспечить эффективное сотрудничество, важно установить конкретные протоколы для различных ситуаций. Эти протоколы могут включать в себя рекомендации по действиям в чрезвычайных ситуациях, например, определение того, что представляет собой чрезвычайную ситуацию, и установление временных рамок для принятия необходимых мер. Установив четкие протоколы, стороны смогут более эффективно сотрудничать друг с другом и рационализировать свои усилия по предотвращению террористических угроз и реагированию на них.

   Предварительное установление процедур позволит обеспечить тщательно структурированное и эффективное сотрудничество. Сюда входит определение процесса запроса, указание необходимой информации для каждого типа запроса, описание условий использования, а также определение юридического процесса и необходимых разрешений. Для облегчения сотрудничества может быть разработан набор соответствующих форм. При работе с местными компаниями принято подписывать меморандум о взаимопонимании (MOU), в котором указываются сроки реагирования и расстановка приоритетов, формат данных, протокол экстренной помощи, контактные лица, доступность и соглашение об уровне обслуживания. Крупные международные ИКТ-компании уже имеют для этой цели специальные порталы.

4. Для поддержки обеих сторон должны быть созданы взаимовыгодные программы обучения. Правоохранительные органы могут провести обучение представителей ИКТ-компаний по юридическим процедурам, этике, вопросам кибербезопасности и терминологии. С другой стороны, ИКТ-компании могут проводить обучение правоохранительных органов по их технологиям, политике хранения данных, протоколам, условиям использования, уведомлениям и способам отправки запросов о предоставлении данных. Между правоохранительными органами и ИКТ-компаниями следует планировать проведение регулярных встреч для решения проблем, повышения прозрачности и улучшения процесса обращения за помощью. Подобные встречи также могут помочь правоохранительным органам узнать о новых технологиях в ИКТ-компаниях, которые могут оказаться полезными в борьбе с терроризмом и выявлении любого потенциального злоупотребления технологиями со стороны террористов.

5. Учитывая, что эти компании являются коммерческими организациями, важно продумать механизм компенсации, покрывающий их расходы, сопряженные с осуществлением соответствующих операций в ходе сотрудничества с правоохранительными органами, особенно при работе с небольшими компаниями.

6. Рекомендуется отдавать приоритет запросам на хранение данных, направляемым в адрес международных компаний. Это гарантирует, что данные будут храниться в течение определенного периода, необходимого для направления официального запроса. Также важно настроить напоминание о необходимости продления срока хранения данных в случае, если процесс направления официального запроса затягивается.

   Необходимо обеспечить своевременное принятие последующих мер посредством направления официального запроса или сообщить компании об отсутствии необходимости дальнейшего хранения данных, если запрос был выполнен или больше не актуален.

7. Сотрудники правоохранительных органов, отвечающие за сотрудничество с ИКТ-компаниями, должны иметь доступ к соответствующим техническим ресурсам, таким как адреса электронной почты, которые четко указывают на их принадлежность к соответствующему ведомству, и другим инструментам, необходимым для безопасного получения электронной информации от контрагента.

8. Любой запрос, направленный в адрес ИКТ-компаний, должен быть подкреплен официальным письменным документом. Это имеет особое значение в экстренных случаях. Подобное документальное

оформление гарантирует соблюдение соответствующих процедур, а также повышает доверие и прозрачность в рамках партнерства.

9. Должностным лицам рекомендуется свести к минимуму использование экстренных и срочных запросов и избегать любого злоупотребления этими процедурами. Такое злоупотребление может стать помехой нормальному ходу ведения коммерческой деятельности ИКТ-компаний.

10. Крайне важно проявлять особую осторожность при направлении запросов на удаление данных, особенно в таких случаях, как пропаганда терроризма, вербовка и подстрекательство.

    Серьезной проблемой в этих случаях является потенциальное расхождение во взглядах между правоохранительными органами и ИКТ-компаниями. В то время как правоохранительные органы могут воспринимать определенное событие как непосредственную угрозу, ИКТ-компании могут считать его проявлением свободы слова — преодоление этого расхождения во мнениях имеет решающее значение. Местные компании могут довольствоваться ордером, тогда как международные компании могут потребовать предоставить дополнительные доказательства угрозы.

    Для таких ситуаций в большинстве стран установлены руководящие принципы и правовые основы. Они позволяют обеим сторонам рассмотреть отдельные случаи, избегая при этом каких-либо нарушений прав человека.

    Когда дело доходит до удаления контента, коммерческие компании серьезно относятся к этому вопросу и с большей вероятностью будут сотрудничать, если им будет предоставлено надлежащее обоснование запроса.

    Поэтому крайне важно предоставить компании все сведения о соответствующем случае и принять во внимание, что во многих случаях необходимые подтверждающие данные являются не известными широкой публике и должны быть переданы.

    Прежде чем приступить к удалению контента, важно обеспечить сохранность всех данных, необходимых для судебного преследования. Во многих случаях в результате удаления контента также могут быть удалены файлы журналов и документация, необходимые для судебного преследования правонарушителей.

    Крупные корпорации, такие как Meta, Google и Microsoft, установили свои собственные протоколы удаления контента и разработали превентивные меры для выявления случаев, в которых следует их применять. Рекомендуется обратиться в эти компании и ознакомиться с их рекомендациями по эффективному разрешению подобных ситуаций.

    В некоторых случаях правоохранительные органы решают отложить удаление определенного контента в целях сбора оперативной информации. Например, если контент может предоставить важную информацию, которую невозможно получить никакими другими способами. Однако в таких случаях важно оценить потенциальное влияние существующей угрозы на общественную безопасность и скоординировать свои действия с вовлеченной ИКТ-компанией, принимая во внимание потенциальные последствия для нее.

    Следует рассмотреть возможность рекомендовать компаниям помечать запросы на удаление контента как законные запросы властей. Это позволит им поддерживать прозрачность в отношениях со своими пользователями и сохранять нейтралитет.

### 8.3.1 Особые соображения касательно сбора доказательств

1. Чтобы поддерживать целостность данных в рамках «цепочки обеспечения сохранности»[22], правоохранительным органам крайне важно координировать свою работу с ИКТ-компаниями и гарантировать, что данные надежно хранятся и остаются в целости на протяжении всего процесса, от места хранения

22 Он относится к отслеживаемому и документированному процессу обращения, сохранения и владения цифровыми доказательствами от момента их сбора до их использования, обеспечивая их подлинность, надежность и допустимость в судебном разбирательстве.

до конечного пункта назначения в суде. Рекомендуется создать механизм проверки идентичности отправляемых данных исходным данным, хранящимся в компании. Одним из эффективных способов такой проверки является использование цифровых подписей — компания подписывает файлы цифровой подписью перед их отправкой, и подпись служит доказательством того, что копия идентична оригиналу. Сохранность цифровой подписи обеспечит возможность проверки его подлинности в рамках юридических процедур.

2. Необходимо поддерживать безопасную «цепочку обеспечения сохранности» на протяжении всего процесса. Файлы должны надежно храниться, а для дополнительной безопасности и целостности цифровая подпись может храниться отдельно.

3. При необходимости сбора доказательств в сотрудничестве с международными компаниями для получения доказательств может потребоваться прохождение процедуры проверки в рамках договора о взаимной правовой помощи (MLAT). Несмотря на то что данный процесс зачастую является бюрократизированным и занимает значительное время, он может являться единственным способом получения данных от международных компаний, который является приемлемым в судебном разбирательстве. Однако следует учитывать, что в некоторых компаниях может допускаться использование нескольких типов запросов в отношении одних и тех же данных. Это означает, что данные запрашиваются на основании MLAT для официального использования в ходе судебного преследования, и параллельно те же данные запрашиваются непосредственно у компании для осуществления предупредительных мероприятий. После получения данных на основании MLAT они также могут быть использованы для целей судебного преследования.

4. Если в соответствующей компании не предусмотрен порядок направления параллельных запросов[23], рекомендуется оперативно разделить запросы и отдать приоритет получению необходимых данных для осуществления предупредительных мероприятий. В то же время следует инициировать юридический процесс по запросу данных, необходимых для доказательства, на основании MLAT. Подобный подход позволяет ускорить сбор данных для уменьшения угрозы в процессе ожидания получения официальных данных, которые впоследствии можно будет использовать для судебного преследования.

23 Некоторые компании утверждают, что данные подписчиков могут быть предоставлены без прохождения процедуры MLAT, а запросы на предоставление контента должны проходить процедуру MLAT.

# [ ПРИЛОЖЕНИЕ A ]
# Практические указания по запросу данных у поставщиков интернет-услуг

## A.1 Обзор

Террористы и воинствующие экстремисты все чаще используют Интернет в качестве инструмента для осуществления своей противоправной деятельности. Следовательно, важно, чтобы правоохранительные органы были осведомлены о различных доступных им вариантах запроса и получения данных, связанных с Интернетом, от ИКТ-компаний и поставщиков интернет-услуг в рамках процесса расследования и судебного преследования. Цель данного раздела заключается в предоставлении пошаговых инструкций по направлению запросов на предоставление данных или доказательств в адрес поставщиков интернет-услуг, а также в описании передовых практик, которые повысят шансы на получение информации по запросу и в необходимые сроки.

## A.2 Типы информации

Существует два основных типа цифровой информации: хранимая информация и информация, поступающая в режиме реального времени.

1. **Хранимая информация.** Это информация, которая уже хранится на серверах поставщиков интернет-услуг до момента направления запроса.
2. **Информация, поступающая в режиме реального времени.** Это информация, которая еще не хранится на серверах, но которая может быть получена в режиме реального времени; например, время и место входа человека в свою учетную запись.

   Как хранимую информацию, так и информацию, поступающую в режиме реального времени, можно разделить на:

   - основную информацию об абоненте и сведения о входе в систему;
   - данные о трафике;
   - контент.

## ТАБЛИЦА 1. Сравнение основной информации об абоненте/сведений о входе в систему и данных о трафике

| | |
|---|---|
| **Основная информация об абоненте и сведения о входе в систему** | Основная информация об абоненте включает в себя всю информацию, предоставленную абонентом поставщику интернет-услуг при создании учетной записи, а также его IP-адрес на соответствующий момент времени. Информация об абоненте как правило включает в себя следующее:<br>• имя абонента, почтовый или географический адрес, IP-адреса, номер телефона и другой номер доступа, адрес электронной почты, информацию о выставлении счетов и оплате, доступные на основании договора или соглашения об оказании услуг. ПРИМЕЧАНИЕ. Эти данные могут быть сфальсифицированы, поскольку они генерируются на стороне абонента;<br>• учетную запись или логин абонента;<br>• вид используемой услуги связи, принятые к ней технические условия и срок предоставления услуги;<br>• любую иную информацию о месте установки оборудования связи, доступной на основании договора оказания услуг.<br>Сведения о входе в систему включают дату, время и IP-адреса каждого входа в систему. |
| **Данные о трафике** | Чаще всего данные о трафике включают отправителя и получателя сообщений, их IP-адреса, дату, время и продолжительность общения, а также перечень веб-сайтов, которые посетил абонент.<br>Типы данных о трафике включают следующее:<br>• информацию о соединении: пункт назначения или источник соединения; время и дату подключения; время и дату отключения; способ подключения к системе (например, telnet, ftp, http); объем передачи данных (например, в байтах); и информацию о маршрутизации;<br>• источник или место назначения любых сообщений электронной почты, отправленных или полученных учетной записью: «заголовок» электронного письма или поля «Кому» и «От»; дату, время и длину сообщения;<br>• информацию, касающуюся любых изображений или других документов, загруженных в учетную запись: даты и время загрузки, а также размеры файлов, но не включая их содержимое;<br>• имя и другие идентификационные данные лиц, которые получили доступ к определенному изображению, файлу или веб-странице в течение определенного периода времени или в определенную дату.<br>Одним из примеров данных о трафике является журнал сообщений Facebook между двумя людьми. Следует иметь в виду, что этот журнал не включает непосредственное содержание сообщений. |

Сбор информации, не включающей контент, в режиме реального времени заключается в направлении поставщиком интернет-услуг сообщений следующего содержания в правоохранительные органы:

- время и IP-адрес входа подозреваемого в свою учетную запись для определения его местоположения; и (или)
- тот факт, что подозреваемый отправил кому-то сообщение или получил сообщение от кого-то. Номера телефонов/адреса электронной почты других подозреваемых также могут быть получены с целью идентификации этих других возможных подозреваемых в режиме реального времени (но без какого-либо контента).

3. **Контент.** Все, что не является данными об абоненте или трафике. Сюда могут входить письменные сообщения, встроенные фотографии и прикрепленные файлы. Примеры контента:
   - электронная почта: содержание всех электронных писем, хранящихся в учетной записи, включая копии электронных писем, отправленных с учетной записи, и черновики.
   - учетные записи социальных сетей: все публикации, посты и сообщения, отправленные или полученные пользователем, включая личные сообщения и вложения, а также такие элементы, как список друзей, ожидающие запросы на добавление в друзья, отметки «нравится» и членство в группах.

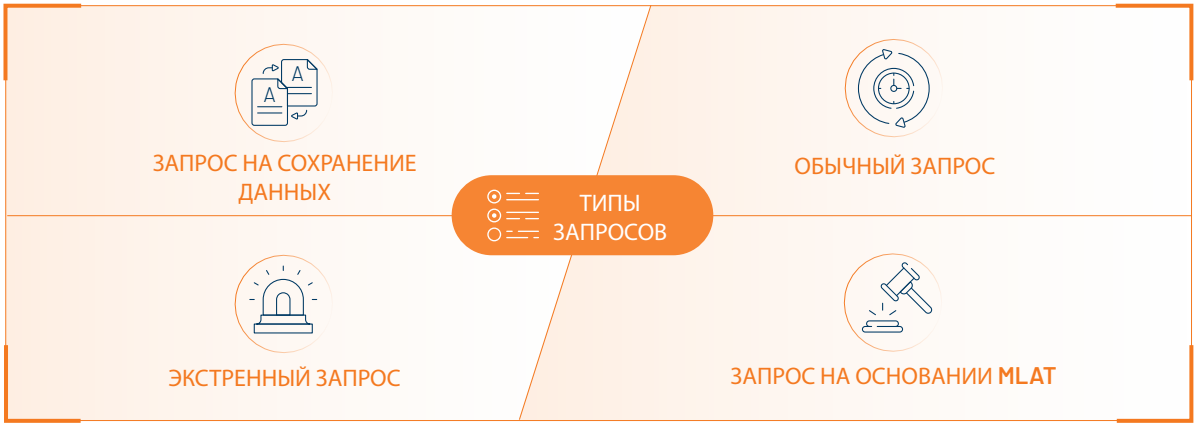
# A.3 Типы запросов

Запросы на предоставление цифровых доказательств можно разделить на различные типы в зависимости от характера доказательств, требований расследования и степени срочности. Каждый из этих типов выполняет определенную функцию и регулируется разными правовыми принципами.

Как правило выделяется четыре категории запросов информации у поставщика интернет-услуг:

- **запрос на сохранение данных:** запрос на сохранение цифровых данных, которые могут служить в качестве доказательств, в их первоначальном состоянии, без удалений или изменений;
- **обычный запрос:** стандартный запрос, соответствующий установленным юридическим процессам и протоколам;
- **экстренный запрос:** направляется только в срочных ситуациях, когда немедленный доступ к цифровым доказательствам необходим для предотвращения неминуемого вреда или защиты общественной безопасности;
- **запрос на основании MLAT:** обычно направляется, когда следственный орган или юридическое лицо пытается получить цифровые доказательства, находящиеся в другой стране.

РИСУНОК 1




## A.3.1 Запрос на сохранение данных

Запрос на сохранение данных предназначен для обеспечения защиты и сохранности цифровых доказательств параллельно с оформлением основного официального запроса на предоставление данных.

ПРИМЕЧАНИЕ. **Запросы на сохранение данных рекомендуется направлять на систематической основе, перед каждым запросом на предоставление данных. Если этого не сделать, запрашиваемые данные могут быть изменены или удалены до выполнения запроса на предоставление данных.**

Запросы на сохранение данных могут быть сделаны правоохранительными органами напрямую или по дипломатическим каналам страны юрисдикции поставщика интернет-услуг.

Как правило, запрос на сохранение данных должен включать следующее:

- идентификацию запрашивающего органа: имя, номер жетона или служебного удостоверения, адрес электронной почты (большинство поставщиков принимают запросы только от должностных лиц с четким государственным адресом электронной почты), номер телефона, адрес;
- основные факты расследования (очень краткое описание);

- описание данных, которые необходимо сохранить: тип данных (основная информацию об абоненте, данные о трафике или контент), уникальный идентификатор конкретной учетной записи или IP-адрес/веб-сайт, а также период времени для запрошенных данных;
- заявление о том, что запрос на предоставление данных будет отправлен после сохранения данных;
- требование сохранить конфиденциальность всех запросов в случае если абонент не должен быть уведомлен о расследовании.

ПРИМЕЧАНИЕ. **Запросы на сохранение данных предполагают сохранение данных только в течение ограниченного времени и не продлеваются поставщиками интернет-услуг автоматически. Необходимо своевременно направить запрос на продление срока хранения — в противном случае сохраненные данные будут утеряны.**

### A.3.2 Обычный запрос

Обычный запрос на предоставление цифровых доказательств относится к стандартной или регулярной процедуре поиска конкретных цифровых доказательств в рамках расследования или судебного разбирательства. Это обычный и ожидаемый шаг при сборе доказательств по различным типам дел.

Обычные запросы обычно не являются срочными и позволяют выполнить стандартные юридические процедуры. Обычные запросы как правило осуществляются в соответствии с установленными юридическими процедурами, такими как выдача ордеров на обыск, постановлений суда или повесток в суд, чтобы обеспечить соблюдение действующего законодательства и защиту прав отдельных лиц.

Если обычные запросы на предоставление цифровых доказательств представляют собой стандартную процедуру, то экстренные запросы и запросы на основании MLAT касаются более экстренных или трансграничных ситуаций, которые требуют срочных действий или международного сотрудничества.

### A.3.3 Экстренные запросы на предоставление информации

Запросы на экстренное предоставление информации направляются в чрезвычайных ситуациях, чтобы предотвратить неминуемый вред. Они представляют собой экстраординарную процедуру, которая может быть использована только в крайних случаях. Экстренные запросы могут направляться в обход определенных стандартных юридических процедур для ускорения процесса, однако они все равно требуют наличия надлежащих разрешений и соблюдения критериев, определенных законом.

В случае непосредственной угрозы физической неприкосновенности цифровые доказательства могут быть запрошены немедленно и непосредственно у поставщика интернет-услуг в обход MLAT. У крупных поставщиков интернет-услуг, таких как Facebook или WhatsApp, как правило имеется контактное лицо, доступное круглосуточно и без выходных, а на их веб-сайтах представлены формы экстренного запроса помощи, которые необходимо заполнить («Форма экстренного запроса на предоставление информации»).

Если прямой контакт с поставщиком интернет-услуг не представляется возможным, допускается использовать каналы взаимодействия между правоохранительными органами (например, сеть Интерпола I-24/7, сеть «Большой семерки» 24/7, сеть Совета Европы 24/7 или сотрудничество в рамках двустороннего меморандума о взаимопонимании между странами).

После того как поставщик интернет-услуг получает запрос, он как правило хранит данные в течение 90 или 180 дней. Этот период продлевается каждые 90 или 180 дней, пока не будет выполнен запрос на предоставление данных. ПРИМЕЧАНИЕ. Запрос не продлевается автоматически — необходимо направить запрос на продление. Если запрос не будет продлен до истечения установленного срока, цифровые доказательства будут удалены. Кроме того, поскольку хранение данных не является обязательным, некоторые поставщики интернет-услуг могут отказаться делать более одного или двух продлений.

Большинство поставщиков направляют ответ в течение нескольких дней и сообщают свой регистрационный номер. Чтобы связать официальный запрос с сохраненными данными, необходимо указать этот регистрационный номер.

Информация, которую поставщик интернет-услуг может добровольно предоставить иностранным государственным организациям посредством данной процедуры, представляет собой основную информацию об абоненте, данные недавнего входа в систему и другую сохраненную информацию, за исключением

контента. С другой стороны, контент может быть раскрыт только правоохранительным органам страны юрисдикции поставщика интернет-услуг. Если требуется предоставление контента, может быть полезно предварительно обсудить этот вопрос с лицами, ответственными за связь и взаимодействие, а в случае направления запроса — по дипломатическим каналам.

Экстренные запросы на предоставление информации как правило направляются при соблюдении следующих трех условий:

ТАБЛИЦА 2. **Критерии соответствия**

| | |
|---|---|
| **Срочность, требующая предоставления информации без промедления** | Запрос должен содержать обоснование невозможности применения стандартной процедуры, например, в силу необходимости предотвращения теракта, при том, что стандартная процедура требует слишком много времени. Большинство поставщиков интернет-услуг строго интерпретируют слово «непосредственный», поэтому поставщик может отказаться от предоставления информации в рамках такого запроса при отсутствии непосредственный угрозы физической неприкосновенности. |
| **Реальная опасность** | В запросе должно быть четко объяснено, почему к угрозе следует относиться серьезно. Гипотетическая возможная опасность не является достаточным основанием. Например, если установлен факт общественно опасного поведения подозреваемого или имеется достоверный источник, указывающий на неминуемость совершения теракта. |
| **Физическая неприкосновенность** | Согласно политике большинства поставщиков интернет-услуг, чрезвычайная ситуация должна предполагать непосредственную угрозу смерти или серьезных телесных повреждений любому человеку или группе лиц. |

Поставщик интернет-услуг сам решает, выполняются ли эти критерии, однако их соблюдение не является обязательным. Поэтому важно привести поставщику интернет-услуг достаточно убедительные аргументы, особенно в тех случаях, когда поставщики интернет-услуг в меньшей степени осведомлены о срочности ситуации, чем запрашивающие правоохранительные органы. Чем больше контекста предоставлено для удовлетворения упомянутых критериев, тем выше вероятность готовности поставщика интернет-услуг выполнить процедуру, удовлетворяющую интересам обеих сторон.

Кроме того, сотрудник правоохранительных органов должен иметь возможность идентифицировать себя в достаточной степени, например, с помощью копии служебного удостоверения или официального адреса электронной почты. Если поставщик интернет-услуг отказывается добровольно передать данные правоохранительным органам в соответствии с данной процедурой, рекомендуется установить контакт по дипломатическим каналам или начать обычную процедуру запроса на предоставление основной информации об абоненте и сведений о входе в систему.

Если поставщик интернет-услуг отказывается добровольно передать данные правоохранительным органам в соответствии с процедурой экстренного запроса на предоставление информации, рекомендуется начать обычную процедуру запроса на предоставление информации об абоненте и сведений о входе в систему, использовать судебный запрос о представлении документов или установить контакты по дипломатическим каналам.

- **Национальный судебный запрос о представлении документов**. Выдается по запросу судебного органа страны или по официальному запросу правоохранительных органов. Если поставщик интернет-услуг принимает повестку в суд от правительства запрашивающей страны, это самый простой и быстрый способ получения основной информации об абоненте и сведений о входе в систему.
- **Судебный запрос о представлении документов, выданный иностранным правительством.** Правоохранительные органы некоторых иностранных правительств имеют право направлять официальные судебные запросы для рассмотрения своих национальных дел в четко определенных законом случаях.

Если выдача национального судебного запроса о представлении документов не представляется возможной, стоит связаться с лицами, ответственными за связь и взаимодействие в стране юрисдикции поставщика интернет-услуг, или использовать дипломатические каналы, чтобы узнать, могут ли власти иностранного государства открыть собственное дело и использовать свои административные полномочия по направлению

судебных запросов. Это может дать более быстрый результат и помочь избежать трудоемкой и дорогостоящей процедуры на основании MLAT.

### A.3.4 Договор о взаимной правовой помощи (MLAT)

Договор о взаимной правовой помощи (MLAT) — это двустороннее соглашение, обеспечивающее сотрудничество между двумя странами. Цель такого договора заключается в содействии сотрудничеству и взаимной правовой помощи между двумя странами по трансграничным правовым вопросам, включая обмен цифровыми доказательствами.

Запросы на предоставление цифровых доказательств в рамках MLAT как правило используются в тех случаях, когда направление обычных или экстренных запросов не представляется возможным. Они включают следующие сведения:

- обстоятельства дела, искомые доказательства и значимость запрошенных данных для расследования;
- сроки (т. е. даты) запрошенных записей и крайний срок, к которому должны быть представлены искомые доказательства;
- описание предполагаемых или вменяемых правонарушений, которые должны являться уголовными преступлениями;
- процедуры, которым необходимо следовать при выполнении запроса.

Имеются два важных нюанса относительно данного типа запросов:

- судья, выдающий ордер, должен быть убежден в том, что в учетной записи, скорее всего, все еще будут содержаться доказательства расследуемой преступной деятельности. Если ранее был запрос на сохранение данных и запрашивающая страна сейчас добивается предоставления этих сохраненных данных, существует высокая вероятность того, что эти записи все еще существуют, что позволяет избежать проблемы «устаревших» данных;
- должно существовать разумное основание полагать, что преступление было совершено или совершается и что доказательства преступления могут содержаться в запрашиваемых данных.

В этом плане необходимо продемонстрировать следующее:

- информация должна быть достаточно достоверной: информация считается заслуживающей доверия, если источником ее предоставления является сотрудник правоохранительных органов, другое государственное должностное лицо или гражданин, обладающий достаточным уровнем знаний. Если источник анонимен или является преступником, необходимо предоставить дополнительную поддержку для доказательства достоверности его информации; например, показав, что информация, полученная от этого человека в прошлом, заслуживала доверия;
- кроме того, должно быть предоставлено подробное описание источника доказательств и объяснение того, почему соответствующий орган пришел к таким выводам;
- в запросе необходимо пояснить, что доказательства будут находиться в материалах поставщика онлайн-услуг и связаны с уголовным расследованием.

СОВЕТ. **Если прокурор или полицейский орган страны юрисдикции поставщика онлайн-услуг уже знаком с запросом и заинтересован в его исполнении, рекомендуется предоставить эту информацию, чтобы обеспечить более быструю координацию и исполнение.**

ПРИМЕЧАНИЕ. **В случае запросов в рамках MLAT страна юрисдикции поставщика онлайн-услуг может оказаться не в состоянии помочь, если преступная деятельность, расследуемая в запрашивающей стране, защищена ее конституцией. Например, разжигание ненависти защищено конституцией некоторых государств.**

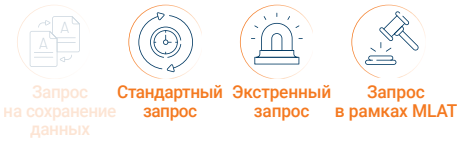
## A.3.5 Выбор правильного типа запроса

В зависимости от ситуации и типа запрашиваемой информации следует использовать соответствующий тип запроса. Чем больше информации запрашивается, тем больше вероятность того, что потребуется MLAT.

ПРИМЕЧАНИЕ. **Запрос данных в рамках MLAT выполняется крайне медленно. Поэтому рекомендуется сначала использовать другие типы запросов, если это возможно. Обратите внимание, что MLAT не отменяет другие запросы, поэтому, например, можно запросить экстренные данные для предотвращения атаки и в то же время отправить запрос в рамках MLAT на данные, предназначенные для использования в целях судебного преследования.**

### a. Запрос информации об абоненте и сведений о входе в систему:

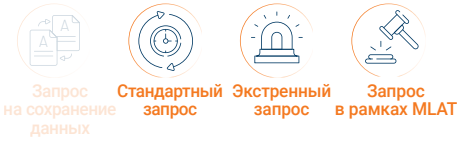
Типы запросов:




Многие юрисдикции прямо не запрещают поставщикам онлайн-услуг предоставлять эту информацию иностранным судебным органам или правоохранительным органам без соответствующего постановления суда. В то же время по закону поставщики онлайн-услуг не обязаны предоставлять такие данные без постановления суда. Другими словами, политика поставщиков онлайн-услуг различается, и если одни поставщики онлайн-услуг могут принимать прямые запросы на предоставление информации об абонентах и сведений о входе в систему, то другие не будут разглашать какие-либо сведения без распоряжения суда.

### b. Данные о трафике:

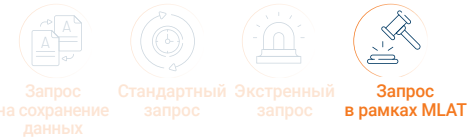
Типы запросов:




Подобно данным об абоненте и сведений о входе в систему, большая часть данных о трафике является информацией, не включающей контент, и может быть предоставлена поставщиками онлайн-услуг без соответствующего постановления суда. Однако большинство поставщиков онлайн-услуг не желают раскрывать эту информацию без постановления суда, поэтому в большинстве случаев необходимо сделать запрос в рамках MLAT.

### c. Контент:

Типы запросов:




Как правило, поставщики онлайн-услуг не предоставляют информацию, включающую контент, без предварительного ордера на обыск, который можно получить только по запросу в рамках MLAT.

ПРИМЕЧАНИЕ. **В чрезвычайных ситуациях контент может быть раскрыт только правоохранительным органам страны юрисдикции поставщика онлайн-услуг. В этом случае в запрос необходимо включить следующую информацию:**

- **достоверные факты, свидетельствующие о совершении преступления, в том числе:**
  - **на какие источники опираются власти в своей информации о преступлении?**
  - **когда было совершено преступление?**

**Достоверные факты, указывающие на то, что целевая учетная запись будет содержать доказательства, связанные с преступлением, в том числе:**

- **каким образом была идентифицирована учетная запись?**
- **как она была сопоставлена с подозреваемым?**
- **была ли учетная запись использована для дальнейшего совершения преступления?**
- **когда и как учетная запись была использована для дальнейшего совершения преступления?**

СОВЕТ. **Факты должны быть достаточно недавними, чтобы судья мог прийти к выводу, что доказательства, вероятно, все еще находятся в учетной записи. Поэтому следует в обязательном порядке указывать даты.**

ПРИМЕР ИЗ ПРАКТИКИ. ***Почему вполне вероятно, что учетная запись в сети Facebook будет содержать доказательства террористической деятельности?***

***Согласно имеющейся информации, террористы, как правило, используют сеть Facebook для общения, что не является достаточно веской причиной для поставщика онлайн-услуг, чтобы предоставить такую информацию правоохранительным органам.***

***Данные о трафике, которыми располагают следователи, показывают, что в период с 12 марта 2022 года по 9 февраля 2023 года подозреваемый обменивался сообщениями в Facebook Messenger с учетными записями, которые, как известно, принадлежали существующей террористической организации, что достаточно для того, чтобы добиться желаемых действий от поставщика онлайн-услуг.***

### d. Информация, поступающая в режиме реального времени

Типы запросов:


Запросы на предоставление информации в режиме реального времени как правило следует направлять в рамках MLAT.

**Информация, не включающая контент.** Обязательным условием для получения необходимой информации является указание значимости учетной записи для расследования. Поскольку это дорогостоящий и трудоемкий процесс, необходимо предоставить следующие обоснования:

- почему считается, что целевая учетная запись принадлежит подозреваемому;
- что подозреваемый, скорее всего, снова воспользуется этой учетной записью; например, из-за частого недавнего использования. Это может быть доказано путем предварительного запроса информации о недавних входах в систему, а затем — с помощью процедуры перехвата и отслеживания/прослушивания.

После вынесения судом постановления правоохранительные органы могут собирать информацию в режиме реального времени в течение 60 дней и продлевать запрос еще на 60 дней, если это необходимо и одобрено судом. Чтобы получить такое продление, судья должен быть убежден в продолжающейся значимости расследования. ПРИМЕЧАНИЕ. Примерно через 40 дней необходимо начать дополнительную процедуру в рамках MLAT, чтобы было достаточно времени для завершения всей процедуры.

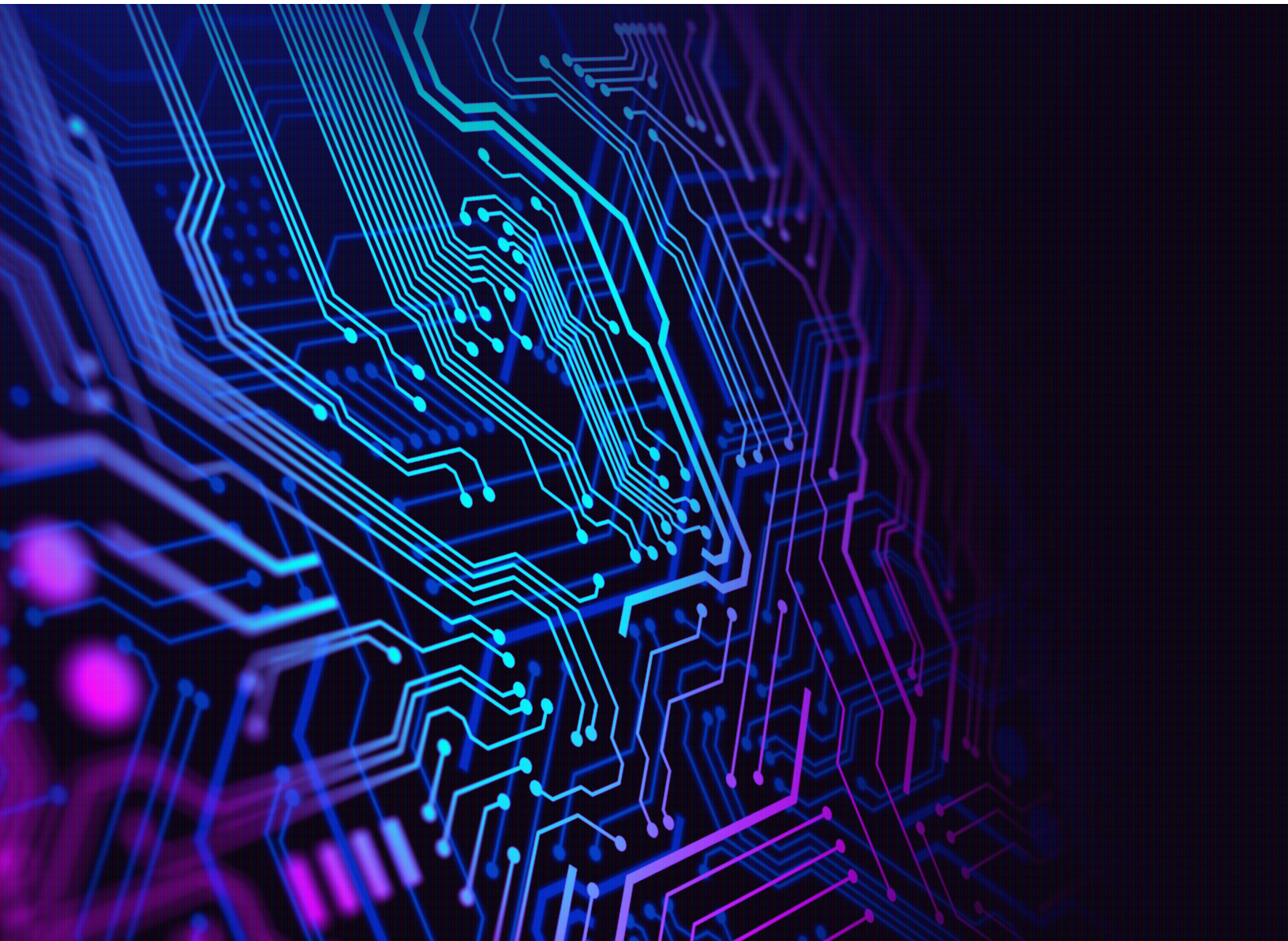
**Информация, включающая контент.** Судья может выдать предписание о раскрытии информации в режиме «перехвата контента в режиме реального времени» только в рамках текущего внутреннего расследования, а не по ходатайству из-за пределов страны юрисдикции поставщика онлайн-услуг.

## A.3.6 Действия перед отправкой запросов

ТАБЛИЦА 3. **Действия, которые необходимо совершить перед отправкой запроса**

| | |
|---|---|
| **1. Можно ли доверять поставщику онлайн-услуг?** | Если опыт предыдущего взаимодействия с поставщиком онлайн-услуг отсутствует, важно проверить его надежность и убедиться, что он не управляется террористической организацией или связанным с ней лицам. Кроме того, сегодня существует множество поставщиков «надежных хостинговых услуг», которые могут быть замешаны в преступной деятельности. |
| **2. Данные еще доступны?** | Каждый поставщик онлайн-услуг имеет свою собственную политику хранения данных, поэтому следует с ней ознакомиться перед отправкой запроса.<br>Примечание. В некоторых случаях могут существовать нормативные требования по хранению данных. Например, Регламент ЕС «Террористический контент в Интернете» (TCO) вступил в силу 7 июня 2022 года и применяется ко всем поставщикам услуг хостинга, предлагающим свои услуги в ЕС. Статья 6 Регламента требует от поставщиков сохранять контент, который был удален или доступ к которому был заблокирован, в течение шести месяцев. |

| | |
|---|---|
| **3. Какова политика поставщика онлайн-услуг?** | У большинства поставщиков онлайн-услуг есть онлайн-руководства для правоохранительных органов, которые включают конкретные требования, которым правоохранительные органы должны следовать, чтобы поставщик мог предоставить им запрашиваемые данные. Например, поставщики онлайн-услуг могут потребовать URL-адрес или идентификационный номер учетной записи, а не указанное в самой учетной записи имя, для раскрытия информации. |
| **4. Уведомляет ли поставщик онлайн-услуг пользователя?** | В соответствии с политикой некоторые поставщики онлайн-услуг уведомляют владельцев учетных записей о любых действиях, предпринятых от имени правоохранительных органов. Целесообразно поинтересоваться у поставщика онлайн-услуг (без упоминания конкретных учетных записей), уведомляет ли компания своих клиентов о запросах правоохранительных органов.<br><br>Если запрос должен быть конфиденциальным, необходимо включить в запрос прямую просьбу не информировать пользователя о запросе на предоставление информации или сотрудничестве в рамках MLAT с указанием конкретной причины или, если применимо, правового обоснования, объясняющего, почему пользователь не должен быть проинформирован. |
| **5. В какой стране находятся данные?** | Некоторые поставщики онлайн-услуг имеют серверы в разных странах. При этом может применяться право той страны, в которой хранятся данные. Важно выяснить этот вопрос путем обращения к соответствующему поставщику онлайн-услуг. |
| **6. Сохранение данных** | Поскольку сохранение данных является добровольной практикой и продолжительность сохранения варьируется в зависимости от поставщика онлайн-услуг, данный запрос следует направлять сразу после обеспечения доступности данных. После удаления информации ее, как правило, невозможно восстановить. Однако запросы на сохранение должны использоваться ограниченно и разумно. |



## A.3.7 Передовые практики направления запросов

### ТАБЛИЦА 4. Действия, которые необходимо совершить перед отправкой запроса

| | |
|---|---|
| **Единая точка контакта (ЕТК)** | Запросы, особенно экстренные, скорее всего, будут рассмотрены ЕТК и быстро выполнены, если запросы будут последовательно подаваться одними и теми же экспертами на национальном уровне (ЕТК). |
| **Актуальность** | Запрашиваемые данные должны иметь отношение к расследованию. Важно подробно объяснить, почему данное лицо является подозреваемым, какие преступления оно предположительно совершило, какова его/ее роль, почему считается, что оно является пользователем учетной записи и какая запрашиваемая информация имеет отношение к расследованию. |
| **Конфиденциальность** | Некоторые поставщики онлайн-услуг уведомляют своих клиентов о запросах данных. Если запрос должен быть конфиденциальным, необходимо включить в запрос прямую просьбу не информировать пользователя учетной записи о запросе. По запросам в рамках MLAT можно получить постановление о неразглашении информации в суде.<br><br>Запрос должен содержать сведения о том, почему такое неразглашение необходимо, например:<br>• создание угрозы жизни или физической безопасности человека;<br>• бегство от преследования;<br>• уничтожение или подделка доказательств;<br>• запугивание потенциальных свидетелей; и (или)<br>• в противном случае это серьезно поставит под угрозу расследование или неоправданно затянет судебное разбирательство.<br><br>Можно также потребовать, чтобы запрос был запечатан, что, в случае удовлетворения, скроет документы и подтверждающую документацию, представленные в суд, от публичного просмотра на определенный период времени. |
| **Сфера охвата** | Чтобы увеличить вероятность получения данных и увеличить скорость выполнения запроса, рекомендуется использовать как можно более узкую область запроса. |
| **Временные рамки** | Укажите точные временные рамки для запрашиваемых данных. Например, данные о трафике за период с 10 по 12 августа 2023 года. |
| **Официальный адрес электронной почты** | Обязательно используйте официальный адрес электронной почты правительства/правоохранительных органов — в противном случае поставщик онлайн-услуг может попросту отклонить запрос. |
| **Соблюдение требований** | Убедитесь, что запрос соответствует:<br>• законодательству страны юрисдикции поставщика онлайн-услуг;<br>• законодательству запрашивающей страны;<br>• нормам международного права;<br>• политике поставщика онлайн-услуг. |

# A.4 Наиболее распространенные платформы

У каждого поставщика онлайн-услуг имеется своя политика обработки персональных данных. Поскольку она часто обновляется, рекомендуется ознакомиться с ее содержимым перед направлением любого запроса. Список некоторых наиболее известных поставщиков онлайн-услуг, а также ссылки на их порталы и инструкции для правоохранительных органов приводятся в таблице ниже.

ТАБЛИЦА 5. **Руководства по наиболее распространенным платформам**

| | |
|---|---|
|  | **Facebook**<br>Запросы: https://www.facebook.com/records/login/<br>Руководства: https://about.meta.com/actions/safety |
|  | **Instagram**<br>Запросы: https://www.facebook.com/records/login/<br>Руководства: https://www.facebook.com/help/instagram/494561080557017 |
|  | **WhatsApp**<br>Запросы: https://www.whatsapp.com/records/login/<br>Руководства: https://faq.whatsapp.com/444002211197967 |
|  | **Google (Alphabet)**<br>Запросы: https://lers.google.com/signup_v2/landing<br>Руководства: https://policies.google.com/terms/information-requests |
|  | **YouTube**<br>Запросы: https://lers.google.com/signup_v2/landing<br>Руководства: https://policies.google.com/terms/information-requests |
|  | **TikTok**<br>Запросы: https://www.tiktok.com/legal/report/lawenforcementrequest<br>Руководства: https://www.tiktok.com/legal/page/global/law-enforcement/en |
|  | **Snapchat**<br>Запросы: https://less.snapchat.com/<br>Руководства: https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf |
|  | **Twitter**<br>Запросы: https://legalrequests.twitter.com/forms/landing_disclaimer<br>Руководства: https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support |
|  | **Telegram**<br>Руководства: https://telegram.org/faq<br>https://telegram.org/privacy?setln=it |
|  | **LinkedIn**<br>Запросы: https://app.kodex.us/linkedin/signin<br>Руководства: https://www.linkedin.com/help/linkedin/answer/a1340284/linkedin-law-enforcement-data-request-guidelines?lang=en |
|  | **Pinterest**<br>Запросы: https://help.pinterest.com/en/law-enforcement<br>Руководства: https://help.pinterest.com/en/article/law-enforcement-guidelines |

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

**www.un.org/counterterrorism**

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

24-09818