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

INTERPOL

При финансовой поддержке
Европейского союза

Кибербезопасность и новые технологии

Руководство для персонала оперативного реагирования по изъятию цифровых устройств на поле боя

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:

- **г-ну Адриану Винкарту** — эксперту по цифровой криминалистике ЮНИТАД;
- **г-же Сесилии Наддео** — сотруднику по правовым вопросам и координатору уголовного правосудия Исполнительного директората Контртеррористического комитета (ИДКТК);
- **г-же Мари Паулюс** — штабному офицеру Контртеррористического отдела Управления новых вызовов безопасности НАТО; а также
- **г-ну Уинтропу Уэллсу** — руководителю программ, Международный институт правосудия и верховенства права (IIIJ).

Термины и определения

Действия правоохранительных органов	Этот термин, как правило, описывает основанные на законных полномочиях действия правоохранительных органов, предпринимаемые для противодействия угрозе, которые могут включать задержание отдельных лиц, пресечение деятельности злоумышленников (например, удаление контента, арест активов) и т. д.
Зеттабайт	Один зеттабайт равен одному миллиарду терабайтов.
Искусственный интеллект	Под этим термином обычно понимают дисциплину, занимающуюся разработкой технологических инструментов, позволяющих имитировать когнитивные функции человеческого мозга, такие как планирование, обучение, рассуждение и анализ.
Новые технологии	Термин «Новые технологии» охватывает широкий спектр различных технологий[1], однако для целей данного документа под новыми технологиями понимается использование и злоупотребление такими новыми технологиями, как Интернет, социальные сети, криптовалюты, системы распознавания лиц и даркнет[2].
Оперативная информация	Информация, являющаяся результатом сбора, разработки, распространения, анализа и интерпретации данных, полученных из широкого круга источников, которая используется лицами, принимающими решения, в целях планирования последующих решений или действий на стратегическом, оперативном или тактическом уровнях. Сбор, хранение, использование и обмен оперативной информацией должны осуществляться с соблюдением обязательств государств-членов по международному праву прав человека.
Персонал оперативного реагирования	Отдельные лица или группы представителей уполномоченных органов, которые прибывают на место террористической атаки после или вместе с персоналом экстренных служб и которым поручено изъятие цифровых устройств в силу их полномочий в рамках контртеррористической политики. Этот термин не распространяется на сотрудников экстренных служб, таких как пожарные и медицинские работники. Для целей настоящего документа персоналом оперативного реагирования являются любые военные или гражданские сотрудники национальной, региональной или международной правительственной организации, которые первыми прибывают на место преступления террористического характера и чьи полномочия включают изъятие цифровых устройств. Сотрудники неправительственных организаций также могут присутствовать на поле боя и собирать цифровые устройства, но для целей настоящего документа они не рассматриваются как персонал оперативного реагирования.

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

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

Поле боя	Для целей настоящего документа под термином «поле боя» подразумевается описание среды, в которой происходят контртеррористические действия и в которой военнослужащие могут быть первыми, кто реагирует на угрозу в силу неуправляемых или недостаточно управляемых аспектов данной среды. Для целей настоящего документа термин «поле боя» иллюстрирует разницу между обычным местом преступления и особыми обстоятельствами, при которых персоналу оперативного реагирования необходимо действовать и корректировать свою деятельность в соответствии со своими исходными полномочиями. Употребление термина «поле боя» в настоящем документе не влияет на какие-либо определения, используемые в работе национальных или региональных организаций или в национальном или региональном законодательстве.
Реабилитация	В контексте уголовного судопроизводства 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.
Сортировка	Процесс оценки, проверки и определения приоритетности цифровых устройств или носителей данных на месте для их дальнейшего изучения и анализа. Зачастую это первый шаг на месте проведения цифровой криминалистической экспертизы, который помогает следователям быстро найти соответствующие носители данных. Для целей настоящего документа сортировка включает идентификацию и определение приоритетности цифровых устройств на поле боя для их последующего изъятия на основании таких факторов, как их ценность для контртеррористических расследований и ценность хранимых на них данных. Для целей настоящего документа сортировка не включает в себя онлайн-процессы или доступ к данным на устройстве со стороны персонала оперативного реагирования[3].
Сортировка в режиме реального времени	Для целей настоящего документа, процесс оценки, проверки и определения приоритетности цифровых устройств или носителей данных на месте для их дальнейшего изучения и анализа путем доступа и цифрового поиска информации, хранящейся на рабочем устройстве, на месте с целью копирования хранящейся на нем информации или определения, имеет ли соответствующий носитель данных отношение к контртеррористическому расследованию, без полного копирования всех данных, хранящихся на устройстве.
Судебное преследование/ разрешение дел	Юридический процесс, который предусматривает предъявление обвинений в терроризме физическому или юридическому лицу, проведение судебных слушаний, вынесение решения или приговора по делу и назначение наказания осужденному.
Сумки Фарадея	Сумка Фарадея — это чехол из проводящего материала, например, металлической сетки, который блокирует электромагнитные поля. Это делает ее идеальной для защиты электронных устройств от радиочастотных помех. Сумки Фарадея зачастую используются для защиты мобильных телефонов, ноутбуков и других чувствительных устройств от взлома или отслеживания.
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].

3 Более подробную информацию о сортировке в режиме реального времени с доступом к данным, хранящимся на устройстве, на поле боя см. в Руководстве Интерпола для персонала оперативного реагирования в области цифровой криминалистики, март 2021 г., URL: https://www.interpol.int%2Fcontent%2Fdownload%2F16243%2Ffile%2FGuidelines_to_Digital_Forensics_ First_ Responders_V7.pdf. Дополнительную информацию об эволюции процессов сортировки цифровых устройств см. в публикации Carrier, B. (2011). Digital triage forensics: A field guide for first responders («Сортировка в цифровой криминалистике: полевое руководство для персонала оперативного реагирования», Syngress.

4 См. S/RES/1566 (2004), пункт 3.

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.
Уголовное расследование	Процесс сбора информации (или доказательств) для установления факта совершения преступления, выявления преступника и представления доказательств в поддержку обвинения в судебном разбирательстве.
Цепочка обеспечения сохранности	Хронологические записи о том, как были изъяты и обработаны доказательства. Любая запись должна, по крайней мере, указывать, какая информация была изъята, когда и кем, кто обрабатывал информацию и когда она была передана в правоохранительные или судебные органы[5].
Цифровая криминалистика	Направление в криминалистике, которое занимается выявлением, сбором, обработкой, анализом и составлением отчетов по информации, хранящейся в электронном виде. Основная цель цифровой криминалистики — извлечь данные из электронного устройства, превратить их в ценную информацию и представить результаты для целей судебного преследования. Во всех процессах цифровой криминалистики используются надежные криминалистические методы, обеспечивающие допустимость использования их результатов в судебном разбирательстве[6].
Цифровые устройства	Электронные устройства, которые предназначены для хранения или обработки информации в электронном виде. Примеры цифровых устройств включают, помимо прочего, смартфоны, ноутбуки, планшеты, внешние жесткие диски, устройства удаленного хранения данных, беспилотные летательные системы, корабельное оборудование. Цифровые устройства могут содержать различные типы электронной информации, например документы, изображения, видео- и аудиозаписи, системную информацию, журналы и метаданные.
Электронные доказательства	«Доказательство» — 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 является исходной, «сырой» формой доказательств[7]. Электронная форма доказательств — это любая информация, хранящаяся в электронном виде, которая потенциально может быть использована в качестве доказательств в судебном разбирательстве или процессуальных действиях.

Краткое содержание

Поле боя требует от персонала оперативного реагирования осуществления оперативных действий в сложных и постоянно меняющихся условиях. Динамика поля боя зачастую характеризуется срочностью, неопределенностью, хаосом и высоким уровнем риска. Термин «поле боя» иллюстрирует разницу между обычным местом преступления и особыми обстоятельствами, при которых персоналу оперативного реагирования необходимо действовать и корректировать свою деятельность в соответствии со своим исходным мандатом. Для целей настоящего доклада персоналом оперативного реагирования являются любые военные или гражданские сотрудники национальной, региональной или международной правительственной организации, которые первыми прибывают на место преступления террористического характера и чьи полномочия включают в себя изъятие цифровых устройств. Сотрудники неправительственных организаций также могут присутствовать на поле боя и проводить изъятие цифровых устройств, однако для целей настоящего документа они не рассматриваются как персонал оперативного реагирования.

5 Руководство ИДКТК по содействию в использовании и обеспечении допустимости в качестве доказательства в национальных уголовных судах информации, собранной, обработанной, сохраненной и предоставленной вооруженными силами для привлечения к ответственности за преступления террористического характера (2019 г.), URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_military_evidence_guidelines.pdf

6 ИНТЕРПОЛ — Цифровая криминалистика, URL: https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics

7 Руководство ИДКТК по содействию в использовании и обеспечении допустимости в качестве доказательства в национальных уголовных судах информации, собранной, обработанной, сохраненной и предоставленной вооруженными силами для привлечения к ответственности за преступления террористического характера (2019 г.) URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org. securitycouncil.ctc/files/files/documents/2021/Jan/cted_military_evidence_guidelines.pdf

Борьба с терроризмом на поле боя представляет собой ряд ключевых задач для персонала оперативного реагирования. Изъятие цифровых устройств на поле боя для доказательственных целей — одна из таких новых и незнакомых задач.

Если персоналу оперативного реагирования не хватает знаний и осведомленности о рисках и передовых методах изъятия цифровых устройств, его действия в ходе изъятия и обращения с цифровыми устройствами на поле боя могут нанести потенциальный вред безопасности членов группы, безопасности других лиц и окружающей среды, а также могут поставить под угрозу уголовное судопроизводство по делам о преступлениях террористического характера.

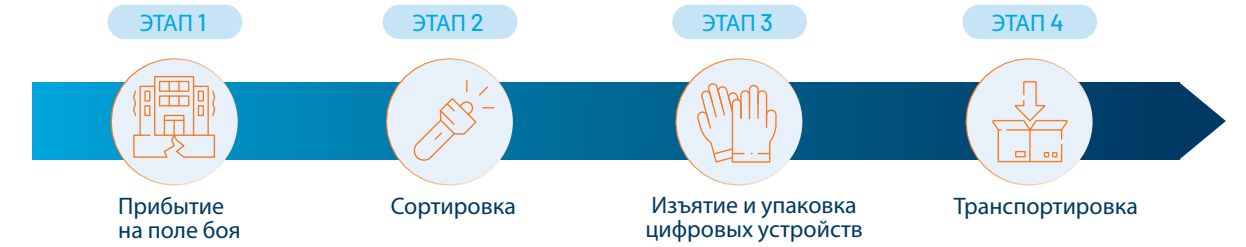
Целью данного документа является предоставление практического руководства для персонала оперативного реагирования по изъятию цифровых устройств на поле боя для расследования, судебного рассмотрения и разрешения дел о преступлениях террористического характера. В нем изложены практические и технологические аспекты и принципы, которые должен знать и соблюдать персонал оперативного реагирования, чтобы обеспечить свою безопасность, безопасность других, а также подлинность и надежность цифровых устройств в качестве доказательств.

В данном документе изложены действия, которые должны быть предприняты персоналом оперативного реагирования на поле боя для обеспечения безопасности и сохранности группы, а также безопасности и сохранности других лиц, изъятия и обращения с цифровыми устройствами на поле боя, а также осуществления необходимых действий до передачи цифровых устройств в криминалистическую лабораторию для их дальнейшего изучения таким образом, чтобы гарантировать допустимость информации и данных, которые хранятся на цифровых устройствах, в качестве доказательств в уголовном судопроизводстве.

Это практическое руководство предназначено для персонала оперативного реагирования, который имеет очень ограниченные знания или опыт в изъятии цифровых устройств или цифровых доказательств, но которому поручено изъятие цифровых устройств на поле боя в целях борьбы с терроризмом.

Данное руководство построено вокруг четырех этапов, связанных с изъятием цифровых устройств на поле боя для целей уголовного правосудия: (1) прибытие на поле боя; (2) сортировка; (3) изъятие и упаковка цифровых устройств; и (4) транспортировка цифровых устройств с поля боя.

РИСУНОК 1



Чтобы помочь персоналу оперативного реагирования, в документе представлен перечень предлагаемых действий для каждого этапа, а также спецификации и шаблоны документации в виде приложений.

[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)[8] 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)[9] и 2396 (2017)[10] 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[11] Группа по аналитической поддержке и наблюдению за санкциями отметила, что «многие государства-члены подчеркнули растущую роль социальных сетей и других онлайн-технологий в финансировании терроризма и распространении пропаганды». Платформы, на которые ссылаются государства-члены, включают Telegram, Rocket.Chat, Hoop и TamTam, среди прочих. В докладе также говорится о том, что **сторонники ИГИЛ используют платформы в даркнете** для хранения учебных материалов, размещать которые другие сайты отказываются, и доступа к ним, а также **для приобретения новых технологий**.

Противодействие использованию новых и новейших технологий в террористических целях обсуждалось на специальном заседании Контртеррористического комитета (КТК) Совета Безопасности Организации Объединенных Наций, которое состоялось 28–29 октября 2022 года в Нью-Дели и завершилось принятием документа, не имеющего обязательной силы и известного как Делийская декларация[12].

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

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

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

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

12 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 2

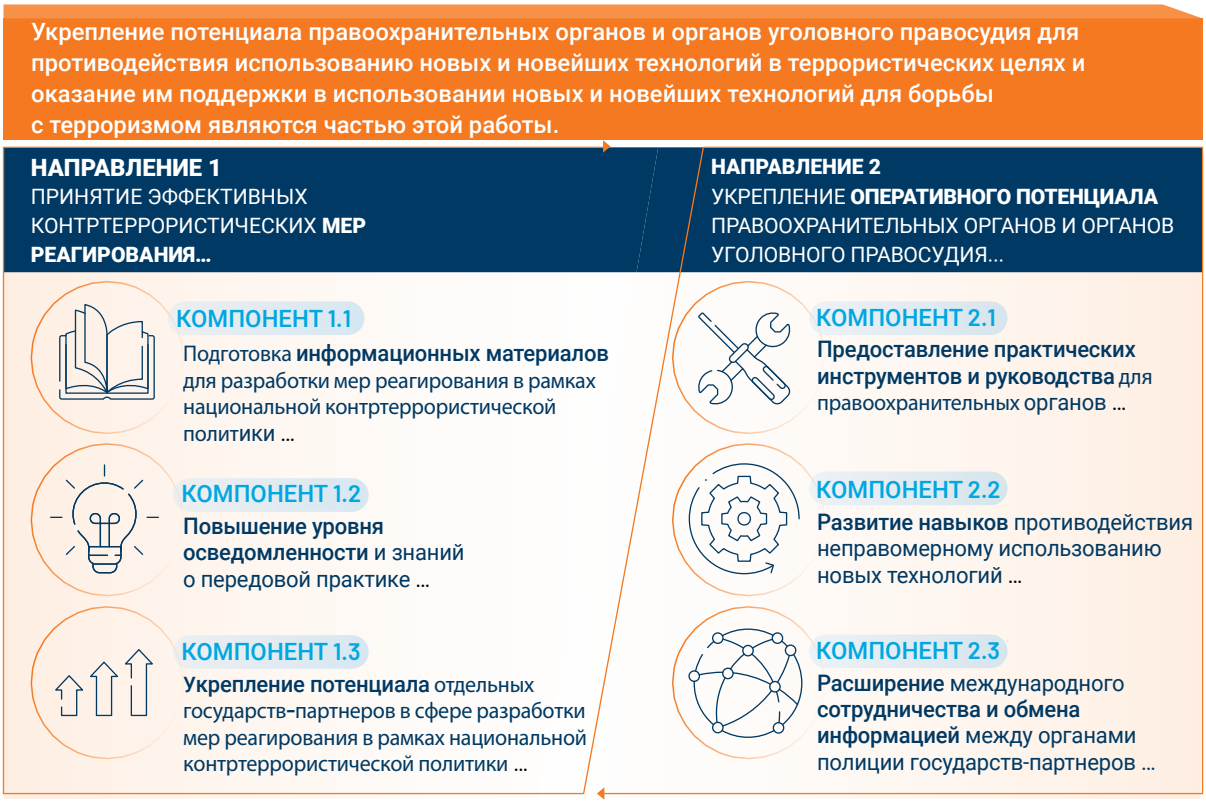


ТАБЛИЦА 1. **Направления и компоненты CT TECH**

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

1.3 Цель и назначение документа

Целью данного документа является предоставление практического руководства для персонала оперативного реагирования по изъятию цифровых устройств на поле боя для дальнейшего расследования, судебного преследования и разрешения дел о преступлениях террористического характера. В нем изложены практические и технологические аспекты и принципы, которые должен знать и соблюдать персонал оперативного реагирования, чтобы обеспечить свою безопасность, безопасность других, а также подлинность и надежность цифровых устройств в качестве доказательств.

1.3.1 Сфера охвата

В настоящем документе изложены действия, которые рекомендуется предпринимать персоналу оперативного реагирования на поле боя, чтобы обеспечить:

- собственную безопасность и сохранность, а также безопасность и сохранность других лиц;
- обнаружение и надлежащее изъятие цифровых устройств на поле боя;
- надлежащее обращение с любыми изъятыми устройствами до их прибытия в криминалистическую лабораторию для дальнейшего изучения.

Общая цель состоит в том, чтобы гарантировать допустимость информации и данных, содержащихся в цифровых устройствах, в качестве доказательств в уголовном процессе.

Правовая основа, касающаяся использования и допустимости информации, полученной на поле боя, в качестве доказательств в национальных уголовных судах при судебном преследовании за совершение преступлений террористического характера, рассматривается в *Руководстве ИДКТК по содействию в использовании и обеспечении допустимости в качестве доказательства в национальных уголовных судах информации, собранной, обработанной, сохраненной и предоставленной вооруженными силами для привлечения к ответственности за преступления террористического характера*[13] и должна быть разработана с учетом всех необходимых правовых условий.

Данный документ не предназначен для использования персоналом оперативного реагирования в качестве справочного руководства по методологии цифровой криминалистики или в качестве основы цепочки обеспечения сохранности. Цель настоящего документа состоит в том, чтобы оказать поддержку персоналу оперативного реагирования, не имеющему опыта изъятия и обращения с цифровыми устройствами, путем обучения тому, как следует изымать и транспортировать цифровые устройства с поля боя в специальную криминалистическую лабораторию.

1.3.2 Целевая аудитория

Это практическое руководство предназначено для персонала оперативного реагирования, который имеет очень ограниченные знания или опыт в изъятии цифровых устройств или цифровых доказательств, но которому поручено изъятие цифровых устройств на поле боя в целях борьбы с терроризмом.

Настоятельно рекомендуется включать специалистов в области цифровой криминалистики в состав групп оперативного реагирования, однако настоящий документ учитывает профессиональные и технические пробелы, с которыми сталкиваются многие государства-члены, и нацелен на любой персонал, которому могут быть поручены функции оперативного реагирования и изъятия цифровых устройств на поле боя.

1.3.3 Преимущества

Данный документ предоставляет персоналу оперативного реагирования четкий и структурированный процесс изъятия цифровых устройств на поле боя для содействия расследованию, судебному преследованию и разрешению дел о преступлениях террористического характера в рамках системы уголовного правосудия. В частности, настоящее руководство может способствовать совершенствованию навыков и повышению готовности персонала оперативного реагирования путем ознакомления с основными принципами и требованиями по изъятию цифровых устройств для доказательственных целей и снижения рисков, связанных с безопасностью и сохранностью группы. Следуя приведенным рекомендациям, персонал оперативного реагирования может повысить свою эффективность и соблюдение принципов цепочки обеспечения сохранности, повысить допустимость цифровых устройств и содержащейся на них информации в качестве доказательств в производстве по делам о преступлениях террористического характера, а также добиться успешного привлечения виновных к ответственности за преступления террористического характера.

1.3.4 Ограничения

Настоящий документ не содержит рекомендаций по юридическим аспектам, связанным с изъятием цифровых устройств на поле боя. Данный документ предполагает, что все необходимые правовые условия были соблюдены, и что персонал оперативного реагирования действует в полном соответствии с принципом верховенства права. Именно суд определяет окончательную допустимость любых доказательств, включая (потенциальные) доказательства, полученные из цифровых устройств, изъятых на поле боя.

13 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, разработанное Исполнительным директоратом Контртеррористического комитета ООН, 2019 г., URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_military_evidence_guidelines.pdf

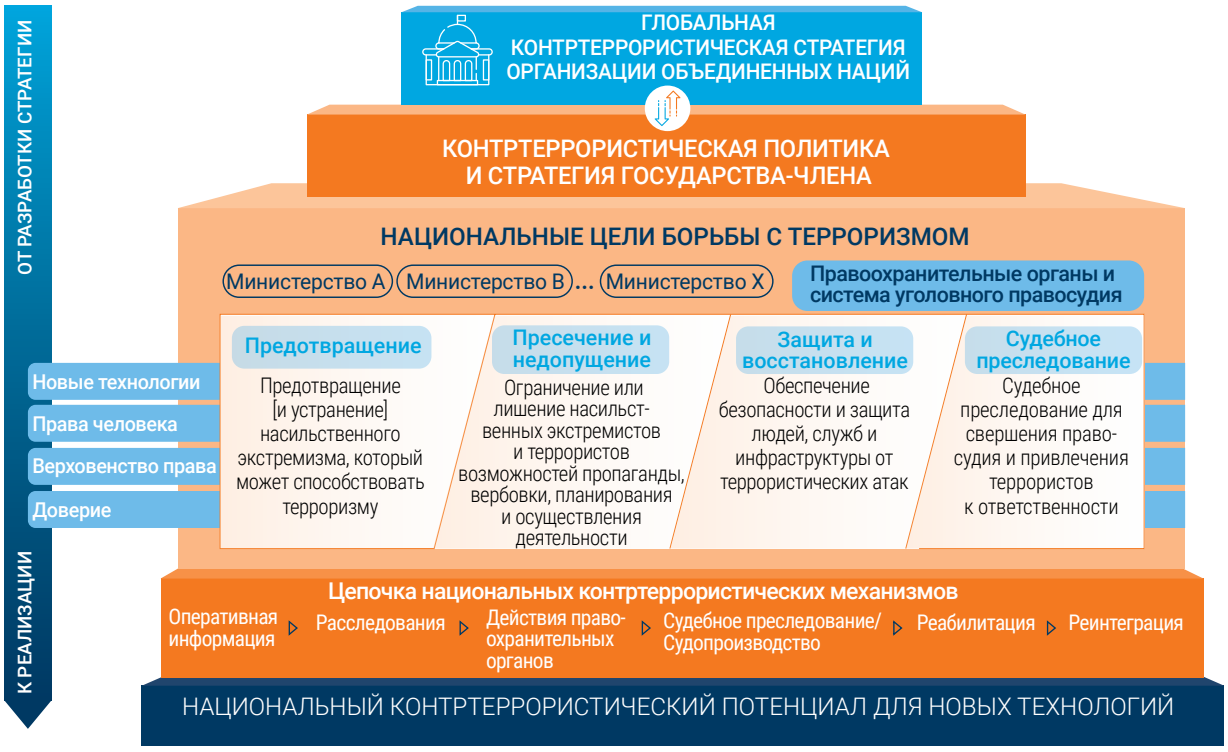
[II] Подход

2.1 Обзор

Цель настоящего доклада заключается в том, чтобы предоставить государствам-членам поддержку и возможности в виде спектра предлагаемых решений для изъятия цифровых устройств на поле боя, которые соответствуют Глобальной контртеррористической стратегии Организации Объединенных Наций и реализуются при полном уважении прав человека и принципа верховенства права.

2.2 Руководящая основа

РИСУНОК 3



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**

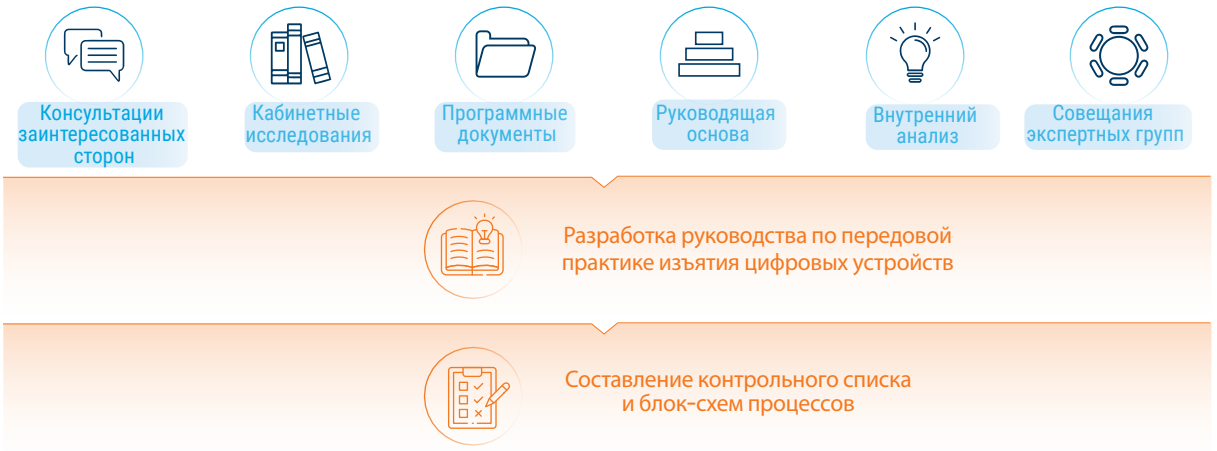
Механизм	Описание
Уголовное правосудие	Юридический процесс, который предусматривает предъявление обвинений в терроризме физическому или юридическому лицу, проведение судебных слушаний, разрешение дела и назначение наказания, а также исправление и реабилитацию осужденных.
Оперативная информация	Результат 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, предпринятые для противодействия угрозе, которые могут включать задержание отдельных лиц, пресечение деятельности злоумышленников (например, удаление контента, арест активов) и т. д.
Реабилитация	В контексте уголовного правосудия термин «реабилитация» используется для обозначения мероприятий, проводимых исправительной системой с целью изменения взглядов или поведения правонарушителей, для того чтобы снизить вероятность повторного совершения ими преступления, а также подготовить и обеспечить их реинтеграцию в общество.
Реинтеграция	Комплексный процесс возвращения человека в социальную и (или) функциональную среду.

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

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

2.3 Методология

РИСУНОК 4



В качестве информационных источников при разработке и составлении настоящего документа был использован широкий спектр материалов, включая документы проекта CT TECH, консультации с заинтересованными сторонами, данные внутреннего анализа, кабинетные исследования, совещания экспертных групп (СЭГ), сотрудничество с различными структурами в рамках Глобального договора по координации контртеррористической деятельности, а также руководящая основа, описанная выше в разделе 2.2.

2.3.1 Совещания экспертных групп и консультации

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

2.3.2 Обзор справочных материалов

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

ТАБЛИЦА 3. Справочные материалы

1	Руководство Исполнительного директората Контртеррористического комитета ООН (ИДКТК) по содействию в использовании и обеспечении допустимости в качестве доказательства в национальных уголовных судах информации, собранной, обработанной, сохраненной и предоставленной вооруженными силами для привлечения к ответственности за преступления террористического характера («Руководство по военным доказательствам»), декабрь 2019 г., https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_military_evidence_guidelines.pdf
2	Глобальный контртеррористический форум (ГКФ), Абуджийские рекомендации по сбору, использованию и обмену доказательствами в целях уголовного преследования подозреваемых в терроризме, сентябрь 2018 г., https://theiij.org/wp-content/uploads/2021/09/GCTF-Abuja-Recommendations_ENG.pdf
3	Евроюст, Меморандум о доказательствах на поле боя, сентябрь 2020 г., https://www.eurojust.europa.eu/publication/eurojust-memorandum-battlefield-evidence
4	Евроюст, «Анализ ситуации по борьбе с терроризмом: выводы за 2020–2021 гг.», декабрь 2021 г., https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_casework_on_ct_insights_2020_2021.pdf
5	Совет Европы, Рекомендация Комитета министров государствам-членам об использовании информации, собранной в зонах конфликтов, в качестве доказательств в уголовном судопроизводстве по делам о преступлениях террористического характера, CM/Rec (2022) 8, 30 марта 2022 г., https://search.coe.int/cm?i=0900001680a5fe10
6	Государственный департамент, Министерство юстиции и Министерство обороны США, «Необязательные руководящие принципы США по использованию доказательств с поля боя в гражданском уголовном процессе», https://theiij.org/wp-content/uploads/2021/09/USG-Non-Binding-Guiding-Principles-on-Use-of-Battlefield-Evidence-EN-1.pdf
7	Женевская академия международного гуманитарного права и прав человека и Международный комитет Красного Креста (МККК), «Руководство по расследованию нарушений международного гуманитарного права: закон, политика и передовая практика», сентябрь 2019 г., https://www.geneva-academy.ch/
8	Battlefield Digital Forensics Digital Intelligence and Evidence Collection in Special Operations («Цифровая криминалистика поля боя: цифровая разведка и сбор доказательств в специальных операциях»), Christian Braccini, Teemu Väisänen, Michal Sadloň, Hayretdin Bahşi, Agostino Panico, Kris van der Meij, Mario Huis in 't veld, 2016.
9	INTERPOL, Guidelines for Digital Forensics First Responders, Best Practices for Search and Seizure of Electronic and Digital Evidence («Рекомендации для персонала оперативного реагирования в области цифровой криминалистики: передовые практики поиска и изъятия электронных и цифровых доказательств»), март 2021 г.

Введение

3.1 Обзор

По мере ускорения технологического прогресса террористы все чаще злоупотребляют инновациями в этой сфере для реализации своих разрушительных планов. Быстрое распространение коммуникационных платформ, социальных сетей, шифровальных методов и новейших технологий создает серьезные проблемы для правоохранительных органов. Поскольку террористы все чаще используют технологии для коммуникации для вербовки и планирования, цифровые следы становятся ценными источниками информации для раскрытия их деятельности. Цифровая криминалистика включает систематический сбор, сохранение, анализ и представление цифровых доказательств, что позволяет следователям реконструировать события, идентифицировать преступников и ликвидировать террористические сети. Целью настоящего руководства является предоставление рекомендаций по изъятию и обращению с цифровыми устройствами, которые могут содержать ценную информацию, таким образом, чтобы свести к минимуму нарушение работы таких устройств в их текущем состоянии. Такой упреждающий подход не только помогает предотвращать террористические атаки, но и способствует судебному преследованию лиц, причастных к террористической деятельности.

3.2 Новые технологии и борьба с терроризмом

Развитие цифровых технологий, инноваций в области обработки и передачи данных и Интернета привело к созданию гиперсвязанного мира, в котором доступ к информации, обмен ею и ее получение происходят практически мгновенно. По состоянию на 2022 год почти 70 процентов населения мира пользуется Интернетом[14], из которых более 93 процентов — это пользователи социальных сетей[15]. По оценкам, в 2022 году в мире будет создано более 97 зеттабайт[16] информации[17]. В то время как подобные технологические достижения способствуют преобразованию общества во имя всеобщего блага, террористы используют эти технологии в своих злонамеренных целях. Применение новых технологий в террористических целях ставит перед государствами-членами серьезные задачи по борьбе с терроризмом, в частности, по противодействию использованию технологий, которые обеспечивают анонимность и позволяют координировать действия и действовать удаленно.

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

Противодействие использованию новых технологий в террористических целях зависит от понимания механизмов такого использования, разработки эффективной правовой основы и мер реагирования на уровне по-

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

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

16 Один зеттабайт равен одному миллиарду терабайтов.

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

литики, а также наращивания оперативного потенциала для противодействия применению таких технологий в террористических целях, включая освоение и использование новых технологий.

3.2.1 Вызовы: использование новых технологий в террористических целях

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

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

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

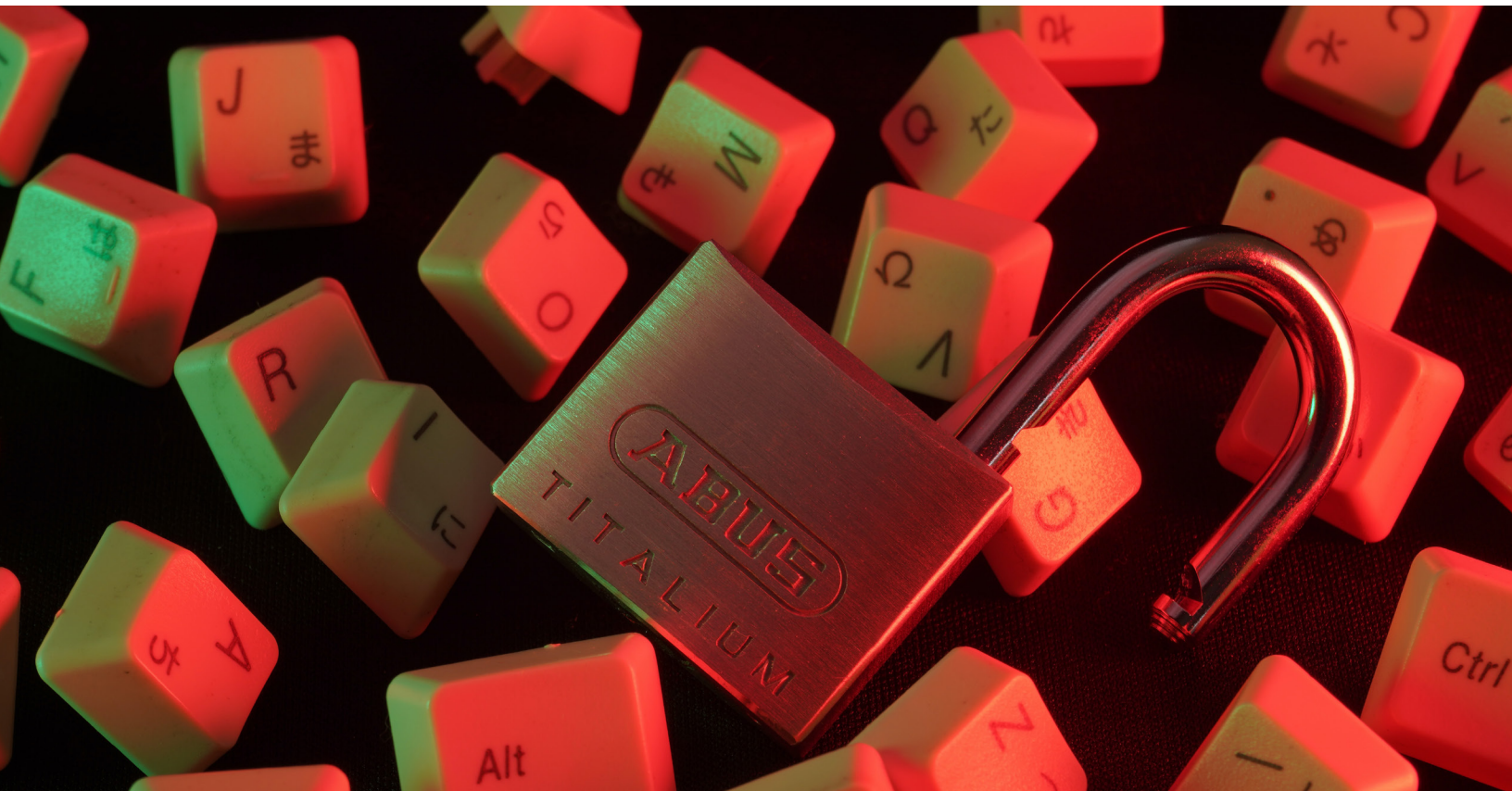
Использование новых технологий может способствовать более эффективному распределению ограниченных ресурсов правоохранительных органов. При этом крайне важно, чтобы эти технологии использовались с учетом этических норм и при строгом соблюдении права на неприкосновенность частной жизни, прав человека и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

3.2.3 Права человека и новые технологии

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

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

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



[IV] Изъятие цифровых устройств на поле боя

4.1 Обзор

В данной главе представлена концепция цифровой информации на поле боя и приводятся практические рекомендации для персонала оперативного реагирования по сбору и обращению с цифровыми устройствами на поле боя и их транспортировке в криминалистическую лабораторию таким образом, чтобы обеспечить безопасность и сохранность персонала оперативного реагирования и других людей и окружения, а также гарантировать доказательственную ценность устройств (и полученной из них информации) для их потенциального использования в уголовном процессе.

Поскольку технологии продолжают стремительно развиваться, важно, чтобы потенциальное влияние новых достижений на практику и процедуры, предлагаемые в настоящем документе, учитывалось персоналом оперативного реагирования при применении данного руководства.

Данное руководство построено вокруг четырех этапов, связанных с изъятием цифровых устройств на поле боя для обеспечения допустимости их использования в рамках последующего уголовного процесса: 1) прибытие на поле боя; 2) сортировка; 3) изъятие и упаковка цифровых устройств; и 4) транспортировка цифровых устройств с поля боя.

Каждый этап включает перечень предлагаемых действий для персонала оперативного реагирования и их описание:

- словами **«ОБЯЗАТЕЛЬНО»** или **«ДОЛЖНЫ»** обозначены действия, которые должны быть предприняты персоналом оперативного реагирования, чтобы сохранить доказательственную ценность цифрового устройства или в случаях, когда соответствующее действие необходимо выполнить перед тем как перейти к следующему действию;
- словом **«СЛЕДУЕТ»** обозначены рекомендуемые действия и передовая практика, которым должен следовать персонал оперативного реагирования, чтобы обеспечить полное соответствие методологии цифровой криминалистики. Исключения могут быть сделаны, когда время, необходимое для выполнения этих действий, может поставить под угрозу персонал оперативного реагирования или других лиц;
- словами **«ПО ВОЗМОЖНОСТИ»** обозначены примеры передовой практики, которым должен следовать персонал оперативного реагирования. Они не являются обязательными и не влияют на допустимость цифровых устройств в качестве доказательств в уголовном процессе.

Рекомендации, изложенные в настоящем руководстве, позволят персоналу оперативного реагирования обеспечить допустимость цифровых устройств, изъятых на поле боя, и данных, полученных из них, в качестве доказательств в уголовном процессе.

Эти руководящие принципы должны быть реализованы в соответствии с протоколами защиты и безопасности, которым следует персонал оперативного реагирования. Если группа подозревает наличие взрывчатых веществ или заминированных устройств на поле боя, ее члены **ДОЛЖНЫ** соблюдать протокол действий при угрозе взрыва.

4.2 Цифровая информация на поле боя

Стремительное распространение цифровых устройств и развитие ИКТ предоставили террористам и террористическим организациям новые инструменты для вербовки, финансирования, обучения, планирования и осуществления нападений, в том числе кибератак. Эти действия часто оставляют цифровые следы на используемых устройствах, документируя их деятельность, включая работу в Интернете и коммуникационную активность.

Цифровая информация может помочь предотвратить террористические акции и террористическую деятельность, выявить виновных, раскрыть доказательства их деятельности, выявить их сторонников и привлечь их к ответственности. Государствам-членам рекомендуется использовать цифровую информацию, собранную на поле боя, в качестве цифровых доказательств для расследования, судебного преследования и вынесения судебных решений по делам о преступлениях террористического характера. Для облегчения сбора, использования и обмена такими доказательствами был разработан ряд руководств и рекомендаций, включая, помимо прочего, 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 («Руководство по военным доказательствам»)[18], разработанное Исполнительным директоратом Контртеррористического комитета Организации Объединенных Наций (ИДКТК) и Абуджийские рекомендации по сбору, использованию и обмену доказательствами для целей уголовного преследования подозреваемых в терроризме («Абуджийские рекомендации»), разработанные Глобальным контртеррористическим форумом (ГКФ)[19].

Информация и доказательства, содержащиеся в цифровых устройствах, нестабильны, легко изменяются, повреждаются или уничтожаются, они также чувствительны ко времени и не подпадают под территориальную юрисдикцию. Цифровой информацией можно легко манипулировать или бесследно удалить ее.

Среда поля боя создает дополнительные проблемы, когда речь идет об изъятии, обращении и сохранении цифровых устройств, а также обеспечении возможности использования и допустимости содержащейся на них информации в качестве доказательств в судебном разбирательстве, особенно при отсутствии опыта в области цифровой криминалистики и наличии рисков для безопасности и сохранности.

Действия персонала оперативного реагирования, связанные с изъятием и обращением с цифровыми устройствами, обнаруженными на поле боя, имеют особое значение и во многих случаях определяют, является ли информация, содержащаяся в цифровых устройствах, допустимой в качестве доказательств в уголовном процессе по делам о борьбе с терроризмом.

В Абуджийских рекомендациях признается эта особая проблема, связанная с обеспечением того, чтобы информация, полученная военными и другими признанными субъектами в (пост)конфликтных ситуациях, соответствовала правовым требованиям, позволяющим использовать ее в качестве доказательств в уголовном процессе в соответствии с правовой системой различных государств. Необходимо соблюдать строгие правовые критерии, закрепленные в национальных уголовных кодексах, которые включают допустимость доказательств, сохранение цепочки обеспечения сохранности и доказательств, а также уважение принципов справедливого судебного разбирательства[20].

В данной главе рассказывается об уникальных обстоятельствах и проблемах, связанных с изъятием цифровых устройств персоналом оперативного реагирования на поле боя, а также с использованием информации, содержащейся на этих цифровых устройствах, в качестве допустимых доказательств в судебных разбирательствах по делам о преступлениях террористического характера.

18 Руководство Исполнительного директората Контртеррористического комитета ООН (ИДКТК) по содействию в использовании и обеспечении допустимости в качестве доказательства в национальных уголовных судах информации, собранной, обработанной, сохраненной и предоставленной вооруженными силами для привлечения к ответственности за преступления террористического характера («Руководство по военным доказательствам», 9 декабря 2019 г.).

19 Глобальный контртеррористический форум (ГКФ), Абуджийские рекомендации по сбору, использованию и обмену доказательствами в целях уголовного преследования подозреваемых в терроризме, сентябрь 2018 г.

20 Там же, с.17, п. V, Рекомендации по сбору, использованию и обмену доказательствами военными.

4.2.1 Поле боя и цифровые устройства

Поле боя требует от персонала оперативного реагирования осуществления оперативных действий в сложных и постоянно меняющихся условиях. Динамика поля боя зачастую характеризуется срочностью, неопределенностью, хаосом и высоким уровнем риска. Борьба с терроризмом на поле боя характеризуется необходимостью быстрого выявления и нейтрализации террористических угроз при минимизации сопутствующего ущерба и сохранении безопасности гражданского населения и окружающей среды при полном уважении прав человека и принципа верховенства закона. Иногда она также включает изъятие цифровых устройств на поле боя, которые могут содержать данные и информацию, важные или имеющие отношение к расследованию, судебному преследованию и разрешению дел о преступлениях террористического характера.

4.2.2 Действующие лица на поле боя

Для целей настоящего документа под термином «поле боя» подразумевается описание среды, в которой происходят контртеррористические действия и в которой военнослужащие могут быть первыми, кто реагирует на угрозу в силу неуправляемых или недостаточно управляемых аспектов данной среды. В число персонала оперативного реагирования зачастую входят как военные, так и гражданский персонал национальных, региональных и международных организаций, уполномоченных осуществлять контртеррористическую деятельность. На поле боя также могут присутствовать сотрудники неправительственных организаций.

Термин «поле боя» иллюстрирует разницу между обычным местом преступления и особыми обстоятельствами, при которых персоналу оперативного реагирования необходимо действовать и корректировать свою деятельность в соответствии со своими исходными полномочиями.

Для целей настоящего доклада персоналом оперативного реагирования являются любые военные или гражданские сотрудники национальной, региональной или международной правительственной организации, которые первыми прибывают на место преступления террористического характера и чьи полномочия включают изъятие цифровых устройств. Этот термин не распространяется на сотрудников экстренных служб, таких как пожарные и медицинские работники.

Действия и функции персонала оперативного реагирования по изъятию цифровых устройств на поле боя имеют первостепенное значение для обеспечения того, чтобы изъятые устройства были допустимы в качестве доказательств в уголовном процессе, и членам группы необходимо осознавать последствия, связанные с неправильным изъятием и транспортировкой цифровых устройств как на поле боя, так и за его пределами.

4.2.3 Информационная ценность — оперативная информация и доказательства

Цифровая информация стала важнейшим источником оперативной информации для военных и доказательств для правоохранительных органов. Цифровая информация, собранная на поле боя, может быть использована в качестве оперативной информации для борьбы с терроризмом и в качестве доказательств в уголовном процессе по делам о борьбе с терроризмом.

Использование цифровой информации в разведывательных или других военных целях не затрагивает систему уголовного правосудия и не входит в сферу охвата настоящего доклада. В этом документе основное внимание уделяется использованию цифровой информации в качестве доказательств в уголовных процессах по делам о преступлениях террористического характера и юридическим пределам, которые должны быть соблюдены, включая допустимость доказательств, сохранение цепочки обеспечения сохранности и доказательств, а также уважение принципов справедливого судебного разбирательства[21].

21 Там же, с.17, п. V, Рекомендации по сбору, использованию и обмену доказательствами военными.

4.2.4 Основные проблемы

Борьба с терроризмом на поле боя сопряжена с целым рядом сложных проблем для персонала оперативного реагирования. Изъятие цифровых устройств на поле боя для целей правоохранительной деятельности и судебного производства — одна из таких новых и незнакомых задач.

Если персоналу оперативного реагирования не хватает знаний и осведомленности о рисках и передовых методах изъятия цифровых устройств, его действия в ходе изъятия и обращения с цифровыми устройствами на поле боя:

- могут нанести потенциальный вред их безопасности, безопасности других людей и окружающей среды;
- могут повлиять на допустимость информации, содержащейся на цифровых устройствах, в качестве доказательств в уголовном процессе по делам о борьбе с терроризмом.

Например, беспилотные летательные аппараты (БПЛА) — это цифровые устройства, которые персоналу оперативного реагирования может быть поручено изъять на поле боя. Террористы могут минировать БПЛА в попытке нанести вред персоналу оперативного реагирования, который пытается вскрыть устройство на поле боя, или могут использовать его для вторичной атаки после прибытия группы на место взрыва. В 2016 году БПЛА взорвался, когда военные пытались вскрыть его после того, как он якобы упал на землю, в результате чего двое солдат погибли и еще двое получили ранения.

Персонал оперативного реагирования должен быть осведомлен о потенциальных рисках, связанных с цифровыми устройствами, оставленными на поле боя, таких как опасность взрыва, возможность отслеживания со стороны противника и другие средства, которые могут поставить под угрозу безопасность персонала.

Чтобы информация, полученная с цифровых устройств, изъятых на поле боя, могла быть использована в качестве доказательств в уголовном процессе, персонал оперативного реагирования должен соблюдать ряд требований цифровой криминалистики, которые позволят обеспечить соблюдение цепочки обеспечения сохранности и гарантировать допустимость извлеченной информации в качестве доказательств.

Надлежащее документирование сведений о поле боя, цифровом устройстве и действиях, предпринятых для изъятия и обращения с устройством до его передачи на хранение или в криминалистическую лабораторию, обеспечивает соблюдение цепочки обеспечения сохранности и допустимость цифрового устройства и информации в качестве доказательства в судебном разбирательстве.

Персоналу оперативного реагирования, действующему на поле боя, зачастую не хватает подготовки, опыта и ресурсов для выполнения надлежащих требований к документации, в результате чего в цифровые устройства могут быть внесены изменения, которые сделают их недопустимыми в качестве доказательств. Например, включение или выключение цифрового устройства или доступ к его содержимому приводят к изменению источника доказательств.

4.3 Руководящие принципы

Приведенные ниже руководящие принципы составляют основу разработанного документа и руководства по изъятию цифровых устройств на поле боя.

ТАБЛИЦА 4. **Руководящие принципы**

Руководящие принципы	
Непричинение вреда	Чтобы обеспечить безопасность группы, окружения, устройства и следственных систем, необходимо действовать осторожно при приближении к цифровому устройству, прикосновении, внесении изменений или подключении цифрового устройства, обнаруженного на поле боя, к сетям или следственным системам.
Надежность	Чтобы цифровое устройство было допустимо в качестве доказательства, необходимо продемонстрировать, что полученная с него информация может быть воссоздана. Таким образом, действия, выполняемые с цифровым устройством на месте, могут повлиять на его надежность и изменить даты или другие данные, хранящиеся на устройстве. Например, «непрочитанные сообщения».
Целостность	Чтобы обеспечить допустимость информации, полученной с цифрового устройства, в качестве доказательства, необходимо продемонстрировать, что данные не были подделаны или изменены каким-либо образом, который мог бы изменить их значение или контекст.
Подлинность	Подлинность означает уверенность в том, что цифровые доказательства не были подделаны или каким-либо образом изменены и что они являются тем, чем они должны быть. Это важный аспект в вопросе о допустимости устройства и хранящейся на нем информации в качестве доказательств. В некоторых случаях для изъятия цифрового устройства требуется внести в него определенные изменения, при этом сама процедура и предпринятые действия должны быть задокументированы.
Достоверность	Достоверность подразумевает надежность и правдоподобность цифровых доказательств в глазах суда или присяжных. Достоверные доказательства — это доказательства, которые подкреплены другими фактами и доказательствами и могут быть приняты как правдивые.
Соблюдение цепочки обеспечения сохранности	Допустимость цифрового устройства в качестве доказательства означает соответствие доказательств, полученных из цифрового устройства, юридическим требованиям допустимости в судебном разбирательстве. Критерии допустимости могут различаться в зависимости от юрисдикции, но, как правило, доказательства должны быть относимыми, существенными, полученными законным путем и с соблюдением цепочки обеспечения сохранности.

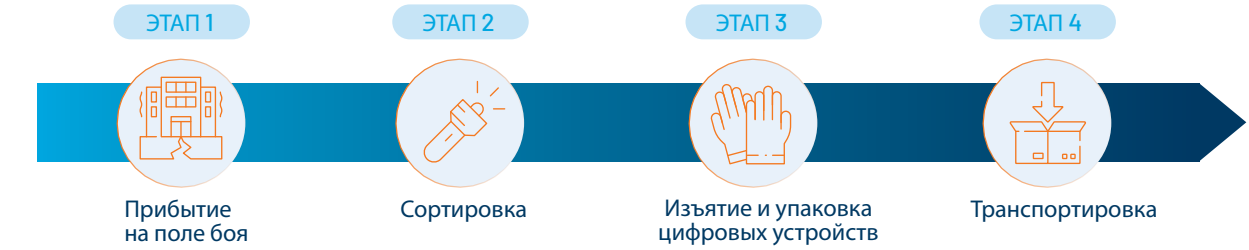
[V] Изъятие цифровых устройств на поле боя

5.1 Обзор

В данной главе представлены практические рекомендации для персонала оперативного реагирования по изъятию цифровых устройств на поле боя таким образом, чтобы свести к минимуму нарушения и обеспечить целостность цифровых устройств, которые могут содержать ценную информацию, включая потенциально компрометирующие доказательства, которые суд может счесть допустимыми в судебном разбирательстве. Данное руководство включает четыре ключевых этапа:

- Этап 1 — Прибытие на поле боя
- Этап 2 — Сортировка
- Этап 3 — Изъятие и упаковка цифровых устройств
- Этап 4 — Транспортировка

РИСУНОК 5



5.2 Этап 1 — Прибытие на поле боя

5.2.1 Планирование и подготовка

Заблаговременное планирование может значительно улучшить возможности и эффективность действий персонала оперативного реагирования, осуществляющего изъятие цифровых устройств на поле боя, а также улучшить сортировку цифровых устройств на поле боя. Подготовка может повысить эффективность работы персонала оперативного реагирования при изъятии цифровых устройств, а также сократить время пребывания на поле боя и воздействия угроз безопасности.

В ходе планирования и подготовки персонал оперативного реагирования **по возможности** определяет приоритеты в отношении того, какие цифровые устройства должны быть изъяты в первую очередь, доступную техническую поддержку, а также то, какой дополнительный технический персонал и оборудование могут потребоваться. Список приоритетных цифровых устройств, подлежащих изъятию, приведен в Приложении I.

5.2.2 Прибытие на поле боя

По прибытии на поле боя персонал оперативного реагирования **ДОЛЖЕН** совершить несколько быстрых действий, которые необходимы для обеспечения безопасности группы и других лиц и которые иногда называют «обработкой поля боя»:

Персонал оперативного реагирования **ДОЛЖЕН** обследовать поле боя на предмет потенциальных опасностей и идентифицировать цифровые устройства, осуществляющие передачу в режиме реального времени.

РЕКОМЕНДУЕТСЯ провести документирование поля боя, за исключением случаев, когда существует непосредственная угроза безопасности и сохранности персонала оперативного реагирования, других людей и окружающей среды, а также провести быструю оценку поля боя.

ТАБЛИЦА 5. **Краткое описание действий**

Действие	Цель	Уровень значимости
Обследование поля боя	Мера безопасности	ОБЯЗАТЕЛЬНО
Идентификация цифровых устройств, передающих данные в режиме реального времени	Мера безопасности	ОБЯЗАТЕЛЬНО
Документирование	Документирование	СЛЕДУЕТ
Быстрая оценка поля боя	Обращение	СЛЕДУЕТ

5.2.3 Обследование поля боя

ВСТАВКА 1. **Указания**

Это действие **ДОЛЖНО** быть выполнено до входа на поле боя и должно являться первым действием по прибытии группы.

ПРИМЕЧАНИЕ. Обследование поля боя может быть совмещено со следующим действием — идентификацией цифровых устройств, передающих данные в режиме реального времени (см. п. 5.2.4 ниже).

Цифровые устройства, оставленные террористами на поле боя, могут представлять физическую угрозу для персонала, работающего на поле боя, и окружающей среды. Были случаи, когда террористы планировали двойную атаку, нацеленную на персонал оперативного реагирования, работающий на поле боя, его платформы и технологические инструменты.

Цифровые устройства могут быть заминированы и взорваны террористами с помощью датчиков, распознающих приближение группы, при физическом контакте с цифровым устройством, когда персонал оперативного реагирования касается или поднимает устройство, или с помощью дистанционного управления, когда территория или устройство контролируются террористами. Быстрое обнаружение электронных устройств может оказаться полезным для дальнейшей обработки поля боя.

Неисчерпывающий список устройств, на которые следует обращать место при обследовании поля боя, включает следующее:

- камеры (активные или неактивные);
- БПЛА (летающие, включенные или выключенные);
- датчики;
- сетевое оборудование: роутеры, серверы, сетевые кабели;
- компьютеры;
- планшеты;
- мобильные телефоны;
- карты памяти;
- флеш-накопители;
- цифровые устройства хранения данных.

a. Цель

- Обеспечить безопасность и сохранность персонала оперативного реагирования, другого персонала, отдельных лиц и окружающей среды.
- Обеспечить понимание того, сколько цифровых устройств необходимо изъять.

b. Действия

Визуально обследовать или осмотреть поле боя для обнаружения видимых глазом цифровых устройств, не входя на поле боя.

c. Результаты

После завершения обследования поля боя персонал оперативного реагирования может выявить угрозы безопасности и сохранности, исходящие от цифровых устройств, оставленных на поле боя, их технологическую сложность и возможность удаленного мониторинга объекта террористами. Наличие камер, БПЛА, датчиков и сетевых устройств указывает на возможность удаленной активации обнаруженных устройств, и персонал оперативного реагирования не должен входить на поле боя до тех пор, пока не будут обеспечены условия для безопасного входа.

Кроме того, персонал оперативного реагирования может получить представление о количестве и типе цифровых устройств, которые необходимо изъять с поля боя.

5.2.4 Идентификация цифровых устройств, передающих данные в режиме реального времени, и заминированных устройств

Террористы могут удаленно контролировать объекты на поле боя и предпринимать действия, направленные против персонала оперативного реагирования удаленно, без ведома последних. Это создает угрозу для безопасности персонала оперативного реагирования, других людей и окружающей среды, а также данных, которые можно найти на цифровых устройствах на поле боя. Подключенные и активные цифровые устройства, передающие данные в режиме реального времени, находящиеся на поле боя, могут предупредить террористов о прибытии на место персонала оперативного реагирования и позволить им осуществить атаку.

Цифровые устройства, передающие данные в режиме реального времени, такие как сотовые телефоны, планшеты и компьютеры, также могут быть активированы террористами удаленно с целью их взрыва, удаления или шифрования данных.

Летающий БПЛА может указывать на то, что его оператор находится поблизости. В рамках действия «Быстрая оценка» (см. п. 5.2.6 ниже) персоналу оперативного реагирования **СЛЕДУЕТ** рассмотреть возможность вызова эксперта по БПЛА и выполнить осмотр прилегающей области, чтобы определить местонахождение пилота БПЛА в реальном времени.

Следует отметить, что по мере развития технологий этот индикатор нахождения оператора поблизости должен быть пересмотрен и не должен восприниматься как нечто само собой разумеющееся.

Передающие камеры могут фиксировать действия персонала оперативного реагирования и использоваться против них не только в режиме реального времени, но и в качестве источника сведений о тактических действиях группы, и их следует избегать.

Рекомендуется выполнить поиск активных камер до выхода группы на поле боя, при этом следует учитывать возможность наличия скрытых камер.

Закрытие объектива камеры не влияет на цифровые материалы, но может повлиять на другие криминалистические меры, такие как сбор образцов ДНК. Закрывать объективы фотоаппаратов следует **ПО ВОЗМОЖНОСТИ** с использованием антистатических перчаток.

Если персонал оперативного реагирования отдает приоритет сбору образцов ДНК с цифровых устройств и других объектов на поле боя, **СЛЕДУЕТ** использовать антистатические перчатки и отключить **камеру** от источника питания, чтобы остановить передачу данных и подготовить камеру к изъятию.

При отключении камер от источника питания **СЛЕДУЕТ** убедиться, что это не влияет на полное или частичное электроснабжение поля боя, а также на питание ближайшего цифрового видеорегистратора или устройства хранения данных. Это можно сделать, тщательно убедившись, что отключаемый источник питания подсоединен непосредственно к соответствующей камере и только к ней. Если камера работает от батареи, отключите батарею. Данный этап необходим из соображений безопасности. На следующем этапе «Быстрой оценки» (см. п. 5.2.6 ниже) группа может рассмотреть возможность более широкого отключения электропитания или сетевого подключения.

Использование портативных глушителей беспроводной связи ближнего радиуса действия[22] может остановить передачу данных с цифровых устройств в удаленное место. Нарушение передачи данных может предотвратить взрыв заминированных устройств с дистанционным управлением и препятствовать удаленному наблюдению за действиями персонала оперативного реагирования на поле боя.

a. Цель

- Обеспечить безопасность и сохранность персонала оперативного реагирования, другого персонала, отдельных лиц и окружающей среды.
- Определить наличие на поле боя подключенных цифровых устройств, которые могут представлять угрозу безопасности и сохранности группы, и по возможности остановить передачу данных.

22 Battlefield Digital Forensics Digital Intelligence and Evidence Collection in Special Operations, Christian Braccini, Teemu Väisänen, Michal Sadloň, Hayretdin Bahşi, Agostino Panico, Kris van der Meij, Mario Huis in 't veld, («Цифровая криминалистика поля боя: цифровая разведка и сбор доказательств в специальных операциях», Центр НАТО по сотрудничеству в сфере кибероборонь, Таллин, 2016 г.) p. 39.

- Выявить подключенные устройства, которыми террористы могут удаленно управлять, и препятствовать им в этом.

b. Действия

1. Персонал оперативного реагирования **ДОЛЖЕН** идентифицировать работающие камеры и БПЛА и оценить их возможности передачи данных. Следующие признаки могут указывать на то, что цифровое устройство является подключенным:
   - устройство работает, летает, мигает;
   - устройство использует кабельное или беспроводное подключение (Wi-Fi, сотовая связь, спутник и т. д.).
2. Персоналу оперативного реагирования **СЛЕДУЕТ** закрывать лица, чтобы предотвратить фотосъемку или видеозапись с помощью подключенных устройств.
3. **ПО ВОЗМОЖНОСТИ** следует прекратить передачу и запись и обеспечить цифровую изоляцию поля боя. Передача связи может быть прервана следующими способами:
   - использование глушителей передачи сетей и сигналов, включая GPS;
   - отключение всего поля боя от кабельных сетей, выключение маршрутизаторов и беспроводных генерирующих или расширяющих устройств;
   - отключение устройства от источника питания.

c. Результаты

По результатам обследования поля боя персонал оперативного реагирования может выявить угрозы безопасности и сохранности, исходящие от цифровых устройств, оставленных на поле боя, их технологическую сложность и возможность удаленного мониторинга объекта террористами. Наличие камер, БПЛА, датчиков и сетевых устройств указывает на возможность удаленной активации обнаруженных устройств, и персонал оперативного реагирования не должен входить на поле боя до тех пор, пока не будут обеспечены условия для безопасного входа.

5.2.5 Документирование

ВСТАВКА 2. **Указания**

Этот шаг **СЛЕДУЕТ** предпринять перед переходом к следующему этапу.

Документация является ключевым элементом в соблюдении цепочки обеспечения сохранности. На данном этапе документация также полезна для следующих целей:

- содействия принятию решений на месте, особенно в отношении цифрового устройства и того, может ли оно быть использовано и должно ли оно быть изъято;
- содействия дальнейшему использованию цифровых устройств в лаборатории цифровой криминалистики. Документация может помочь лаборатории понять несоответствия, которые эксперты по цифровой криминалистике обнаруживают в цифровом устройстве, идентифицировать владельца цифрового устройства и т. д.;
- документирования действий персонала оперативного реагирования на поле боя, если последние будут оспорены в ходе судебного разбирательства.

В рамках процесса документирования персонал оперативного реагирования может использовать видеокамеры для регистрации поля боя и цифровых устройств. Видеозапись может предоставить всю или большую часть информации, необходимой для документирования на более позднем этапе. В качестве альтернативного варианта персонал оперативного реагирования может начертить план поля боя.

Любые изменения, вносимые персоналом оперативного реагирования на поле боя, должны осуществляться только по соображениям безопасности, при этом видеорегистрация в режиме реального времени может обеспечить достоверность действий и соблюдение цепочки обеспечения сохранности цифровых устройств.

Если не удалось произвести видеорегистрацию всех изменений, внесенных персоналом оперативного реагирования, рекомендуется дополнить запись письменным отчетом. Если видеозапись недоступна, группа может оформить документацию в письменном виде, используя шаблон, представленный в Приложении B1.

a. Цель

- Обеспечить соблюдение цепочки обеспечения сохранности и содействие дальнейшим процессам цифровой криминалистики.

b. Действия

1. Персоналу оперативного реагирования **СЛЕДУЕТ** документировать в письменной форме или с помощью видеозаписи окрестности поля боя и обнаруженные на нем цифровые устройства.
2. В документацию на данном этапе **СЛЕДУЕТ** включать:
   - общее описание поля боя;
   - местоположение цифрового устройства;
   - описание и состояние устройства — работает, летает, мигает;
   - состояние подключения — наличие сетевого подключения — по кабелю или с помощью устройств беспроводного подключения (Wi-Fi, сотовая связь, спутниковая связь и т. д.);
   - действия, предпринятые для изоляции цифрового устройства, передающего данные в режиме реального времени, и поля боя — использование глушителей, отключение электропитания и т. п.
   - информацию, отображаемую на экране найденного устройства;
   - подтвержденный список всех свидетелей, присутствующих на поле боя по прибытии группы — с указанием имени, фамилии, любых признаков, вызывающих подозрения — видимое состояние сознания.
3. См. «Шаблон документации по прибытии на поле боя», приведенный в Приложении B1.

c. Результаты

Документирование или видеозапись поля боя с описанием поля боя, местоположения, внешнего вида и состояния устройств, состояния подключения устройств, действий персонала оперативного реагирования по отключению устройств и любых свидетелей, присутствующих на поле боя.

5.2.6 Быстрая оценка поля боя

ВСТАВКА 3. **Указания**

Это действие **СЛЕДУЕТ** предпринять перед переходом к следующему этапу, чтобы обеспечить полное соответствие методологии цифровой криминалистики. Исключения могут быть сделаны в тех случаях, когда длительное пребывание на поле боя может подвергнуть опасности персонал оперативного реагирования или другой персонал.

Этот шаг является последним шагом этапа прибытия на поле боя и запускает следующий этап — сортировку цифровых устройств.

Он ограничивается отключением видеокамер и БПЛА от электропитания или сети, поскольку они представляют наибольший риск удаленного мониторинга.

Некоторая информация может быть потеряна при отключении цифрового устройства от источника питания или сети, но это не является основным фактором для видеокамер и БПЛА.

Изоляция поля боя имеет важное значение для безопасности персонала оперативного реагирования. Цифровая изоляция поля боя осуществляется путем отключения цифровых устройств от источника питания и сети.

Если на поле боя расположены онлайн-камеры или летающие БПЛА, рекомендуется связаться с экспертом по цифровой криминалистике или вызвать его на поле боя.

Персоналу оперативного реагирования следует определить все БПЛА, подлежащие изъятию. Стационарные камеры как правило не хранят много данных, при этом сама камера менее важна, чем соответствующий компьютер для хранения данных (цифровой видеорегистратор или сетевой видеорегистратор).

Камеры являются объектами с низким приоритетом для изъятия.

Если персонал оперативного реагирования считает, что поле боя находится под наблюдением или заминировано, решение покинуть поле боя или войти на него **ДОЛЖНО** быть принято в соответствии с применимыми протоколами безопасности и защиты.

a. Цель

- Изолировать поле боя от дистанционного видеонаблюдения.

b. Действия

1. Персонал оперативного реагирования **ДОЛЖЕН** решить, какие цифровые устройства следует отключить от источника питания или сети.
2. Персонал оперативного реагирования **ДОЛЖЕН** решить, нужно ли вызывать специального эксперта на поле боя (например, эксперта по цифровой криминалистике, БПЛА, взрывным устройствам).
3. Персонал оперативного реагирования **ДОЛЖЕН** идентифицировать цифровые устройства, подлежащие сортировке.

c. Результаты

Цифровые устройства отключаются от источника питания или сети и идентифицируются для дальнейшей сортировки. Соответствующие эксперты вызываются на поле боя в безопасной или благоприятной обстановке.

5.3 Этап 2 — Сортировка цифровых устройств

Сортировка является важным элементом процесса изъятия цифровых устройств персоналом оперативного реагирования. Сортировка предполагает оценку, проверку и определение приоритетности цифровых устройств или носителей данных на месте для их изъятия в целях дальнейшего изучения и анализа. Это помогает персоналу оперативного реагирования сосредоточить свои усилия и сэкономить время.

Для целей настоящего документа сортировка включает в себя идентификацию и определение приоритетности цифровых устройств на поле боя для их последующего изъятия на основании таких факторов, как их ценность для контртеррористических расследований и ценность хранимых на них данных.

На этом этапе персонал оперативного реагирования **ДОЛЖЕН** обнаружить все цифровые устройства на месте и **ДОЛЖЕН** определить, какие устройства подлежат изъятию для дальнейшего использования и анализа, в каком порядке, при этом также **СЛЕДУЕТ** документировать все действия и провести быструю оценку поля боя.

Следует отметить, что не все цифровые устройства содержат данные, которые с высокой вероятностью могут быть использованы в уголовном процессе по делам о преступлениях террористического характера. Некоторые данные, хранящиеся на цифровых устройствах, могут быть неотносимыми, поэтому приоритет изъятия цифровых устройств должен быть определен в соответствии со всеми обстоятельствами и соображениями группы.

Для целей настоящего документа сортировка не включает в себя онлайн-процессы или доступ к данным на устройстве со стороны персонала оперативного реагирования[23].

23 Более подробную информацию о сортировке в режиме реального времени с доступом к данным, хранящимся на устройстве, на месте см. в Руководстве Интерпола для персонала оперативного реагирования в области цифровой криминалистики, март 2021 г. Дополнительную информацию об эволюции процессов сортировки цифровых устройств см. в публикации Carrier, B. (2011). Digital triage forensics: A field guide for first responders («Сортировка в цифровой криминалистике: полевое руководство для персонала оперативного реагирования»). Syngress.

ТАБЛИЦА 6. **Краткое описание действий**

Действие	Цель	Уровень значимости
Обнаружение всех цифровых устройств на поле боя	Обращение	ОБЯЗАТЕЛЬНО
Определение цифровых устройств, подлежащих изъятию	Документирование	СЛЕДУЕТ
Документирование	Документирование	СЛЕДУЕТ
Быстрая оценка поля боя	Мера безопасности	СЛЕДУЕТ

5.3.1 Обнаружение всех цифровых устройств на поле боя

Персоналу оперативного реагирования следует выполнить поиск всех цифровых устройств на поле боя, включая скрытые устройства. Неисчерпывающий список наиболее актуальных цифровых устройств, хранящих большое количество данных и содержащих файлы, которые могут быть использованы в качестве доказательств в уголовном процессе по делам о преступлениях террористического характера, выглядит следующим образом:

- мобильные телефоны;
- компьютеры — стационарные и ноутбуки;
- серверы;
- планшеты;
- USB-накопители;
- цифровые устройства хранения данных;
- карты памяти;
- SIM-карты;
- камеры;
- БПЛА.

Если персонал оперативного реагирования обнаруживает на поле боя стационарные камеры, он **ДОЛЖЕН** выполнить поиск компьютера (цифрового видеорегистратора или сетевого видеорегистратора), на который эти камеры отправляют информацию. Такой компьютер хранит все данные, которые записывают камеры до тех пор, пока они не будут отключены, и он должен находиться поблизости, в некоторых случаях подключен к интернет-устройству с помощью кабеля, и отслеживание кабелей может позволить обнаружить все цифровые устройства, подключенные к Интернету с помощью сетевого кабеля. Эти компьютеры обычно хранят записанные данные в течение короткого периода времени и перезаписывают предыдущие записи. Другой метод — обнаружение компьютера-хранилища камеры, следуя за кабелями питания. Этот метод позволяет обнаружить дополнительные цифровые устройства, подключенные к тому же источнику питания.

Состояние цифрового устройства определяет меры, необходимые для его изъятия.

На этом этапе группа **ДОЛЖНА** только проверить состояние цифрового устройства. Документация будет подготовлена на следующем этапе (см. п. 5.3.3 ниже).

Основным элементом сортировки является принятие решения о том, какие устройства следует изъять, и с каким приоритетом. Персоналу оперативного реагирования **СЛЕДУЕТ** воздерживаться от проведения поиска внутри устройств, если состав группы не включает эксперта по цифровой криминалистике. Чтобы решить, какие устройства подлежат изъятию и в каком порядке приоритета, персонал оперативного реагирования **ДОЛЖЕН** оценить потенциальную значимость данных, хранящихся на цифровом устройстве, для контртеррористических расследований и состояние цифрового устройства.

ТАБЛИЦА 7. **Краткое описание соображений**

Параметр	Факторы для учета	Значимость	Степень срочности
Потенциальная значимость данных, хранящихся на цифровом устройстве, для контртеррористических расследований	Владелец или пользователь устройства подозревается в причастности к террористической деятельности	Высокая значимость для дальнейшего изучения и использования данных	-
	Данные на цифровых устройствах содержат файлы, действия пользователя, пользовательские данные, сообщения	Высокая значимость для дальнейшего изучения и использования данных	-
Состояние цифрового устройства	Устройство повреждено, защищено паролем, зашифровано.	Использование данных затруднено	-
	Устройство выключено, не повреждено	Более легкое изъятие	Не срочно
	Устройство включено, защищено паролем, предположительно зашифровано	Необходимо вызвать специалиста по цифровой криминалистике	Очень срочно

Общая оценка значимости цифрового устройства поможет группе определить, какие цифровые устройства необходимо обработать в первую очередь, какие — во вторую, а какие лучше вообще не трогать.

При наличии подозрений в том, что на поле боя находятся СВУ или устройства-ловушки, персонал оперативного реагирования **ДОЛЖЕН** соблюдать соответствующие процедуры и протоколы безопасности.

a. Цель

- Обнаружение всех цифровых устройств на поле боя и определение приоритетов их изъятия.

b. Действия

1. Персонал оперативного реагирования **ДОЛЖЕН** обыскать поле боя и обнаружить все цифровые устройства.
2. Если персонал оперативного реагирования обнаруживает на поле боя стационарные камеры, он **ДОЛЖЕН** выполнить поиск компьютера (цифрового видеорегистратора или сетевого видеорегистратора), на который эти камеры отправляют информацию.
3. Персонал оперативного реагирования **ДОЛЖЕН** определить состояние цифровых устройств, обнаруженных на поле боя:
   - устройство работает;
   - устройство выключено;
   - устройство подключено/отключено от сети;
   - устройство подключено/отключено от источника питания;
   - устройство повреждено;
   - устройство зашифровано;
   - устройство защищено паролем.
4. Персонал оперативного реагирования **ДОЛЖЕН** оценить значимость устройства для расследования, судебного преследования и вынесения судебных решений по делам о преступлениях террористического характера.

c. Результаты

1) Обнаружение местоположения всех цифровых устройств на поле боя.
2) Определение состояния и приоритизация цифровых устройств с точки зрения их значимости для расследования, судебного преследования и разрешения дел о преступлениях террористического характера.

5.3.2 Определение цифровых устройств, подлежащих изъятию

Персоналу оперативного реагирования **СЛЕДУЕТ** изымать сотовые/мобильные телефоны, БПЛА и их пульты дистанционного управления, портативные компьютеры, выключенные стационарные компьютеры, хранилища данных, такие как USB-накопители, карты памяти и жесткие диски, поскольку они обычно имеют небольшую массу и могут содержать много цифровых материалов, необходимых для расследования и привлечения к ответственности за преступления террористического характера. Периферийные устройства, такие как клавиатуры, мыши, принтеры, мониторы, как правило не представляют интереса в контексте цифровой информации и цифровых доказательств.

ВСТАВКА 4. **Указания**

Цифровые устройства, расположенные на поле боя, помимо цифровой информации, могут иметь и другую ценность для следствия. Они могут хранить образцы ДНК, отпечатки пальцев или остатки взрывчатых материалов, которые могут иметь значение для расследования и привлечения к ответственности за преступления террористического характера, и должны учитываться при принятии решения о том, какие цифровые устройства подлежат изъятию.

Если на поле боя обнаружены серверы или стационарные включенные компьютеры, специалистам оперативного реагирования **СЛЕДУЕТ** проконсультироваться (удаленно) с экспертом по цифровой криминалистике перед их изъятием. На данном этапе сортировки консультации должно быть достаточно, и она может стать основанием для вызова эксперта по цифровой криминалистике на поле боя для проведения изъятия. Определение значимости серверов требует сортировки хранимой на них информации, при этом такое действие может нанести ущерб доказательственной ценности информации, которая будет изъята. Решение о сортировке должно основываться на значимости цифрового устройства для расследования и привлечения к ответственности за преступления террористического характера, а также на способности персонала оперативного реагирования обеспечить безопасность поля боя и дождаться прибытия эксперта по цифровой криминалистике.

Выключение работающего компьютера или сервера, скорее всего, повлияет на возможность восстановления хранящихся на них данных, и этого **СЛЕДУЕТ** избегать, если на поле боя может прибыть эксперт по цифровой криминалистике.

При отсутствии эксперта по цифровой криминалистике, с которым можно было бы проконсультироваться, персоналу оперативного реагирования **СЛЕДУЕТ** отключить цифровое устройство от сети, однако при этом **СЛЕДУЕТ** поддерживать его в рабочем состоянии до тех пор, пока не будет получен совет от эксперта по цифровой криминалистике. Если персонал оперативного реагирования должен срочно покинуть поле боя или если оставаться на поле боя не представляется возможным из соображений безопасности и защиты, персоналу оперативного реагирования **СЛЕДУЕТ** выключить работающие компьютеры или устройства и в любом случае произвести их изъятие. Оставление работающих компьютеров и серверов на поле боя является наименее рекомендованным вариантом.

ПО ВОЗМОЖНОСТИ персоналу оперативного реагирования следует выполнить поиск поврежденных цифровых устройств и оценить их значимость и необходимость их изъятия. Поврежденные цифровые устройства — это устройства, которые выглядят сломанными, сгоревшими, не целыми и т. д.

Персонал оперативного реагирования должен проверить целостность блока хранения данных поврежденного цифрового устройства. Если цифровое устройство явно находится в плохом состоянии, например, разбилось на куски, полностью сгорело, персонал оперативного реагирования не сможет определить, целы ли данные на этом устройстве. Если цифровое устройство полностью сломано, его восстановление представляется нецелесообразным, и устройство **СЛЕДУЕТ** оставить на поле боя.

При определении приоритетности подлежащих изъятию цифровых устройств персоналу оперативного реагирования **СЛЕДУЕТ** учитывать значимость хранящихся на них данных для задач группы и их относимость для расследования и судебного преследования за преступления террористического характера, а также возможность восстановления поврежденного или поломанного цифрового устройства, его массу, необходимую упаковку и меры по его транспортировке.

При сортировке персоналу оперативного реагирования **СЛЕДУЕТ** обеспечить маркировку как цифровых устройств, которые подлежат изъятию, так и тех цифровых устройств, которые будут оставлены на поле боя. Маркировка цифровых устройств в ходе сортировки позволит различать устройства, найденные на поле боя, и может помочь в документировании поля боя, первоначального местоположения цифровых устройств и их окружения.

ВСТАВКА 5. **Указания**

Иногда СВУ могут выглядеть как забытые или поврежденные устройства. Персоналу оперативного реагирования **СЛЕДУЕТ** использовать все меры безопасности для обнаружения взрывчатых веществ на поле боя и следовать протоколу действий при угрозе взрыва.

a. Цель

- Принятие решения об изъятии цифровых устройств, а также порядке или приоритете их изъятия.

b. Действия

1. Персоналу оперативного реагирования **СЛЕДУЕТ** определить цифровые устройства, подлежащие изъятию, из приведенного ниже перечня:
   - мобильные телефоны ;
   - БПЛА и их пульты дистанционного управления;
   - ноутбуки;
   - выключенные стационарные компьютеры;
   - хранилища данных, такие как USB-накопители, карты памяти, жесткие диски;
   - SIM-карты.
2. **ПО ВОЗМОЖНОСТИ** персоналу оперативного реагирования следует определить цифровые устройства, подлежащие изъятию, из приведенного ниже перечня:
   - серверы;
   - включенные стационарные компьютеры.
3. **ПО ВОЗМОЖНОСТИ** персоналу оперативного реагирования следует провести оценку поврежденных цифровых устройств.
4. Персоналу оперативного реагирования **СЛЕДУЕТ** выполнить маркировку цифровых устройств, подлежащих изъятию.

c. Результаты

Определение и маркировка цифровых устройств, подлежащих изъятию.

5.3.3 Документирование

Документирование сортировки обеспечивает понимание процесса принятия решений на поле боя на более позднем этапе, а также помогает отслеживать недостающие компоненты при дальнейшем использовании цифрового устройства в криминалистической лаборатории. Персоналу оперативного реагирования **СЛЕДУЕТ** документировать сортировку только в том случае, если это не ставит под угрозу безопасность и защиту группы. Если эксперт по цифровой криминалистике входит в состав персонала оперативного реагирования и выполняет сортировку в режиме реального времени, все действия **ДОЛЖНЫ** быть задокументированы в соответствии с методами цифровой криминалистики.

Эта документация будет относимой, если допустимость цифровых устройств, изъятых с поля боя, будет оспорена в суде, или они потребуются для последующего судебного рассмотрения. Сортировка также может быть задокументирована на более позднем этапе. Персоналу оперативного реагирования **СЛЕДУЕТ** выполнить маркировку всех цифровых устройств, подлежащих изъятию, с помощью простых наклеек. Для этих целей могут использоваться любые простые небольшие наклейки, которые обеспечивают видимость и понимание их значения группой.

a. Цель

- Документирование поля боя и всех цифровых устройств, обнаруженных на поле боя, и маркировка цифровых устройств, подлежащих изъятию.

b. Действия

1. Персоналу оперативного реагирования **СЛЕДУЕТ** задокументировать поле боя, сфотографировав его и все обнаруженные цифровые устройства, включая те, которые не подлежат изъятию.
2. Персоналу оперативного реагирования **СЛЕДУЕТ** выполнить маркировку всех цифровых устройств, подлежащих изъятию.

c. Результаты

Все цифровые устройства, обнаруженные на поле боя, документируются и маркируются для изъятия.

5.3.4 Проведение быстрой оценки поля боя

ВСТАВКА 6. **Указания**

Это действие **СЛЕДУЕТ** предпринять перед переходом к следующему этапу, чтобы обеспечить полное соответствие методологии цифровой криминалистики. Исключения могут быть сделаны в тех случаях, когда длительное пребывание на поле боя может подвергнуть опасности персонал оперативного реагирования или другой персонал.

Персоналу оперативного реагирования **СЛЕДУЕТ** оценить необходимость вызова других экспертов, прежде чем приступать к изъятию цифровых устройств. Эти решения должны быть приняты с учетом времени, в течение которого группа может находиться на поле боя, и складывающихся обстоятельств.

Если будет обнаружен работающий компьютер или сервер, выключение устройства, скорее всего, повлияет на способность группы цифровой криминалистики восстановить данные, хранящиеся на этом устройстве. Таким образом, персоналу оперативного реагирования **СЛЕДУЕТ** рассмотреть возможность вызова эксперта по цифровой криминалистике на поле боя для сбора информации с рабочих компьютеров или серверов, чтобы гарантировать строгое соблюдение процедур цифровой криминалистики и цепочки обеспечения сохранности.

Сбор информации с компьютера или поиск информации в мобильном телефоне без надлежащего обучения и оборудования может нанести вред как данным, так и устройству, повлиять на надежность, целостность и подлинность доказательств, а также сделать их недопустимыми в уголовном процессе и никогда не должен выполняться персоналом оперативного реагирования, который не обучен методам цифровой криминалистики.

При обнаружении работающего компьютера или сервера персоналу оперативного реагирования **ПО ВОЗМОЖНОСТИ** следует вызвать эксперта по цифровой криминалистике на поле боя для сортировки и копирования информации в режиме реального времени в рамках процедур цифровой криминалистки. Если персонал оперативного реагирования подозревает, что некоторые цифровые устройства могут быть заминированы, следует вызвать саперов.

По завершении сортировки персонал оперативного реагирования будет знать, какие цифровые устройства подлежат изъятию, и может оценить наличие достаточных ресурсов для упаковки и транспортировки всех цифровых устройств, подлежащих изъятию. Если персоналу оперативного реагирования не хватает ресурсов, следует запросить доставку дополнительных ресурсов на поле боя или соответствующим образом изменить сортировку. Персоналу оперативного реагирования **СЛЕДУЕТ** помнить об угрозах, исходящих от СВУ или заминированных цифровых устройств. Всегда **ДОЛЖНЫ** соблюдаться соответствующие протоколы безопасности и защиты.

a. Цель

- Вызов дополнительных специалистов перед изъятием цифровых устройств и оценка физических возможностей группы изъять все цифровые устройства, подлежащие изъятию.

b. Действия

1. Персоналу оперативного реагирования **СЛЕДУЕТ** решить, есть ли необходимость в консультации или приезде на поле боя эксперта по цифровой криминалистике.
2. Персоналу оперативного реагирования **СЛЕДУЕТ** решить, следует ли проконсультироваться с другими экспертами или вызвать их на поле боя.
3. Персонал оперативного реагирования **ДОЛЖЕН** оценить физическую способность группы изъять все цифровые устройства на поле боя с учетом имеющегося в наличии упаковочного оборудования и возможностей по транспортировке.

c. Результаты

1) Эксперты по цифровой криминалистике или другие эксперты вызываются на поле боя по мере необходимости перед изъятием цифровых устройств;
2) Персонал оперативного реагирования имеет достаточные ресурсы для упаковки и транспортировки цифровых устройств, подлежащих изъятию.

5.4 Изъятие и упаковка цифровых устройств

На поле боя в распоряжении персонала оперативного реагирования имеется значительно меньше времени на изъятие цифровых устройств. Поэтому персонал оперативного реагирования всегда должен изымать компьютеры и цифровые устройства в тех случаях, когда они обнаружены, и никогда не открывать их на месте.

Цифровые устройства следует изымать с осторожностью, чтобы не допустить их загрязнения и обеспечить их сохранность. Например, использование антистатических перчаток персоналом оперативного реагирования увеличивает шансы на восстановление отпечатков пальцев с цифровых устройств с использованием традиционных методов криминалистики.

ТАБЛИЦА 8. **Краткое описание действий**

Действие	Цель	Уровень значимости
Обращение	Обращение	ОБЯЗАТЕЛЬНО
Документирование поля боя	Документирование	ОБЯЗАТЕЛЬНО
Упаковка	Обращение	ОБЯЗАТЕЛЬНО

5.4.1 **Обращение**

ВСТАВКА 7. **Указания**

Этот шаг **ДОЛЖЕН** быть предпринят перед переходом к следующим этапам.

«Цифровая изоляция устройства» — действие, направленное на предотвращение отправки и приема сигналов цифровым устройством.

Персонал оперативного реагирования **ДОЛЖЕН** отключить все цифровые устройства от сети. Это можно сделать путем изъятия кабеля, переключения устройства в авиарежим или отключения его от сети. Все эти действия позволяют изолировать цифровое устройство от удаленного окружения.

После отключения устройства от сети персонал оперативного реагирования **ДОЛЖЕН** учитывать, что цифровое устройство может продолжать передавать сигналы. Даже в авиарежиме сотовое устройство продолжает отправлять сигналы GPS и может указывать точное местоположение персонала оперативного реагирования или лаборатории цифровой криминалистики, куда персонал оперативного реагирования доставляет устройство.

Чтобы обеспечить блокировку сигналов, персонал оперативного реагирования **ДОЛЖЕН** упаковать все подлежащие изъятию цифровые устройства в сумку Фарадея как можно скорее после их отсоединения от сети (дополнительную информацию см. в разделе «Упаковка» (п. 5.4.3 ниже). Во избежание путаницы между устройствами, а в некоторых случаях и между различными полями боя, персонал оперативного реагирования должен обеспечить маркировку цифровых устройств с помощью наклеек и упаковать их в отдельные сумки.

При этом маркировка **ДОЛЖНА** включать следующую информацию:

- обозначение «ЦИФРОВОЕ УСТРОЙСТВО»;
- дату и время изъятия;
- уникальный идентификационный номер цифрового устройства;
- полное имя члена группы, изъявшего устройство;
- уникальное и точное определение места, где было обнаружено устройство;
- метку, указывающую, следует ли клонировать или копировать данное устройство.

При обращении с **работающими устройствами**, оборудованными камерами, персонал оперативного реагирования **ДОЛЖЕН** всегда отводить камеру от лица. Это предотвратит запись террористами действий персонала оперативного реагирования с помощью автоматических устройств, которые как правило также отправляют фотографии на удаленные устройства. Персонал оперативного реагирования **ДОЛЖЕН** убедиться, что при приближении к устройству на объектив камеры наклеена небольшая наклейка, закрывающая объектив.

Если **сотовый телефон** включен и открыт, персоналу оперативного реагирования **СЛЕДУЕТ** отменить пароль, установленный на нем, чтобы обеспечить к нему доступ на более позднем этапе.

Все модели телефонов после 2013 года следует считать зашифрованными и **СЛЕДУЕТ** обращаться с ними соответствующим образом на поле боя (см. п. 5.3.4 выше). **ПО ВОЗМОЖНОСТИ** персоналу оперативного реагирования не следует выключать сотовые телефоны, и следует изымать их с поля боя в том состоянии, в котором они были обнаружены. **ПО ВОЗМОЖНОСТИ** персоналу оперативного реагирования следует поддерживать работу мобильных телефонов с помощью альтернативного источника питания (внешнего аккумулятора), пока они не будут доставлены в криминалистическую лабораторию для дальнейшей работы с ним.

Если поблизости нет криминалистической лаборатории, персоналу оперативного реагирования **СЛЕДУЕТ** вызвать эксперта по цифровой криминалистике для работы с цифровым устройством на поле боя (см. п. 5.3.4 выше).

Если персоналу оперативного реагирования известен пароль от цифрового устройства или удается его отменить, цифровое устройство может быть отключено. Если ожидается, что изъятый сотовый телефон будет доставлен в криминалистическую лабораторию через несколько дней после изъятия, персоналу оперативного реагирования следует **ПО ВОЗМОЖНОСТИ** снабдить цифровое устройство этикеткой с указанием пароля, и выключить его перед упаковкой.

Для отключения шифрования мобильного телефона требуются ресурсы современной лаборатории цифровой криминалистики. Если такая лаборатория недоступна, персоналу оперативного реагирования **СЛЕДУЕТ** попытаться идентифицировать хозяина устройства и получить пароль от него. Эти действия **ДОЛЖНЫ** осуществляться в соответствии с принципом верховенства права и, при необходимости, сопровождаться судебным контролем или ордером.

Мобильные телефоны **СЛЕДУЕТ** изымать вместе с зарядными кабелями, если последние были обнаружены на поле боя.

Если на поле боя обнаруживается БПЛА, независимо от того, находится ли он в рабочем состоянии или выключен, он может использоваться персоналом оперативного реагирования для получения оперативной информации. Однако осмотр БПЛА **ДОЛЖЕН** проводиться экспертом по цифровой криминалистике, которого **СЛЕДУЕТ** вызвать на поле боя (см. п. 5.3.4 выше)[24].

Если есть подозрение, что **устройство хранения данных** зашифровано, персоналу оперативного реагирования **СЛЕДУЕТ** найти пароль на поле боя и допросить соответствующих свидетелей. Все действия **ДОЛЖНЫ** осуществляться в соответствии с принципами верховенства права и соблюдения прав человека. Если ситуация является неотложной, любое недобровольное предоставление информации о пароле должно подлежать судебному контролю.

Если устройство представляет собой работающий **компьютер** с зашифрованным хранилищем данных, персоналу оперативного реагирования следует **ПО ВОЗМОЖНОСТИ** сфотографировать информацию, отображаемую на экране устройства, и вызвать эксперта по цифровой криминалистике для консультации (см. п. 5.3.4 выше). Информация, отображаемая на экране устройства, может быть недоступна после его выключения. Персонал оперативного реагирования **ДОЛЖЕН** проконсультироваться со специалистом по цифровой криминалистике, прежде чем выключить устройство или компьютер или отключать его от источника питания.

Компьютерные мониторы имеют большие размеры, их трудно транспортировать, и они обычно не содержат цифровой информации, имеющей значение для целей расследования и судебного преследования. Если это обычный компьютерный монитор, персоналу оперативного реагирования **НЕ СЛЕДУЕТ** его изымать, лучше оставить его на поле боя. При этом персоналу оперативного реагирования **СЛЕДУЕТ** убедиться, что соответствующий монитор не является моноблочным компьютером.

Монитор моноблочного компьютера **ДОЛЖЕН** считаться компьютером, и персонал оперативного реагирования **ДОЛЖЕН** изъять его с поля боя, если он выключен, или проконсультироваться со специалистом по цифровой криминалистике, если он включен.

Если на поле боя обнаружен смарт-телевизор, персоналу оперативного реагирования **СЛЕДУЕТ** проконсультироваться с экспертом по цифровой криминалистике, чтобы решить, подлежит ли он изъятию.

Принтеры как правило не хранят никакой дополнительной информации. Большая часть данных о распечатанных документах хранится на отправляющем устройстве, и персоналу оперативного реагирования **СЛЕДУЕТ** изымать цифровые устройства, такие как компьютеры или сотовые телефоны, а задаче изъятия принтеров **СЛЕДУЕТ** отдавать низкий приоритет. Однако иногда принтеры хранят данные последних напечатанных документов. Документ может храниться на принтере в частичном виде, без указания времени и даты или без привязки к пользователю, отправившему документ в печать. Специалистами группы оперативного реагирования **СЛЕДУЕТ** изымать принтеры с поля боя только в том случае, если другие цифровые устройства недоступны.

Прежде чем прикоснуться к цифровому устройству или поднять его, персоналу оперативного реагирования следует убедиться, что оно не подключено к источнику питания или не заминировано.

a. Цель

- Обеспечить целостность, подлинность и достоверность цифровых устройств, изъятых на поле боя, соблюдения цепочки обеспечения сохранности информации или устройства и их допустимости в качестве доказательства в суде.

24 Также см. Интерпол, «Рекомендации для персонала оперативного реагирования в области цифровой криминалистики: передовые практики поиска и изъятия электронных и цифровых доказательств», март 2021 г., сс. 41–42.

b. Действия

1. Персонал оперативного реагирования **ДОЛЖЕН** обеспечить цифровую изоляцию устройства.
2. Персонал оперативного реагирования **ДОЛЖЕН** обеспечить маркировку всех цифровых устройств.
3. Персонал оперативного реагирования **ДОЛЖЕН** изымать цифровые устройства с осторожностью, чтобы не допустить их загрязнения и обеспечить их сохранность.

c. Результаты

Цифровые устройства изымаются с поля боя для упаковки и транспортировки в криминалистическую лабораторию или на специализированный объект.

5.4.2 Документирование

ВСТАВКА 8. **Указания**

Этот шаг **ДОЛЖЕН** быть предпринят перед переходом к следующим этапам.

Первое прикосновение к цифровому устройству — наиболее важный этап в процедурах цифровой криминалистики. Документирование на этом этапе имеет решающее значение для обеспечения целостности, подлинности и достоверности цифрового устройства, а также для соблюдения цепочки обеспечения сохранности доказательств. Помимо этого **ДОЛЖНА** быть обеспечена допустимость цифровых устройств в качестве доказательства в уголовном процессе.

Каждое изъятое цифровое устройство должно сопровождаться документированной информацией на каждом этапе цепочки обеспечения сохранности, в том числе при хранении, передаче в криминалистическую лабораторию, а также при дальнейшем изучении цифровыми криминалистами.

Обязательная документация может быть дополнена заранее размеченными наклейками, видеозаписями, заметками на месте, шаблонами отчетов, контрольными списками и т. д.

Как показано в таблице 9 ниже, часть документации может быть заполнена на более позднем этапе, а не на поле боя, при условии, что соответствующая информация может быть получена до того, как персонал оперативного реагирования передаст цифровое устройство другой группе. Персоналу оперативного реагирования **СЛЕДУЕТ** документировать следующие параметры:

ТАБЛИЦА 9. **Краткое описание действий**

Документируемая информация	Предлагаемые меры
Дата и время изъятия. Эта информация должна быть максимально точной.	Структурированная форма для регистрации даты и времени. Может быть заполнена на более позднем этапе.
Полное имя и идентификатор члена группы, который осуществлял обращение с цифровым устройством при сортировке, сборе, упаковке и транспортировке.	Каждому члену группы могут быть предоставлены идентификационные наклейки, которые могут быть использованы для маркировки и документирования цифровых устройств на всех этапах процесса, а также для целей документирования на более позднем этапе.
Местоположение: район, поле боя, местоположение цифрового устройства на поле боя, подключенные устройства или кабели.	Устройство может быть сфотографировано перед изъятием, а дополнительная информация может быть добавлена на более позднем этапе.
Описание: тип цифрового устройства, производитель или модель, цвет, номер этикетки и т. д.	Устройство может быть сфотографировано до/во время изъятия, а дополнительная информация может быть добавлена на более позднем этапе с помощью средств оптического распознавания символов. Для этого цифровое устройство должно сопровождаться фотографией или формой с заполненными данными.

Состояние цифрового устройства: включено/выключено, передает/не передает данные, заблокировано/разблокировано физическое состояние.	Структурированная форма поможет персоналу оперативного реагирования выбрать соответствующие параметры из предварительно подготовленного списка.
Действия, предпринимаемые на поле боя: изменения, которые персонал оперативного реагирования вносит в цифровое устройство, например, отмена пароля, выключение, подключение к аккумулятору, отключение от сети.	Текстовые поля для описания всех изменений, внесенных в изъятое устройство, для соблюдения цепочки обеспечения сохранности. Вполне возможно, что описанные действия изменят устройство и могут повлиять на его подлинность или иметь другие непредвиденные последствия. Эта информация должна быть указана максимально точно.
Подробности: известный владелец, время и дата на экране, предполагаемые материалы, которые следует искать на устройстве.	Данная информация может быть заполнена на более позднем этапе и будет способствовать дальнейшему расследованию и использованию материалов.

a. Цель

- Обеспечить целостность, подлинность и достоверность цифровых устройств, изъятых на поле боя, соблюдение цепочки обеспечения сохранности устройства и его допустимости в качестве доказательства.

b. Действия

- Персонал оперативного реагирования **ДОЛЖЕН** документировать все действия, выполненные с устройством для извлечения из него информации.

c. Результаты

Все изъятые цифровые устройства документируются, чтобы гарантировать их допустимость в качестве доказательства.

5.4.3 Упаковка

Прежде чем упаковывать любое цифровое устройство, персонал оперативного реагирования **ДОЛЖЕН** убедиться, что все изъятые устройства снабжены соответствующими наклейками с уникальной маркировкой (см. п. 5.4.2 выше).

Каждое цифровое устройство **ДОЛЖНО** быть упаковано отдельно от других цифровых устройств, но вместе с кабелями или другими дополнительными устройствами, подключенными к нему при обнаружении.

При изъятии компьютеров персоналу оперативного реагирования **СЛЕДУЕТ** изъять их вместе с футлярами, в которых они были обнаружены, и **НЕ СЛЕДУЕТ** разбирать их на поле боя.

Чтобы предотвратить электростатический разряд, который может нанести вред цифровому устройству или его окружению или даже вызвать самовзрыв, персоналу оперативного реагирования **СЛЕДУЕТ** использовать антистатические пакеты. Антистатические пакеты являются дешевыми и легкими, и их следует рассматривать как часть базового снаряжения персонала оперативного реагирования. Вместо антистатических пакетов можно использовать бумажные пакеты или конверты, которые могут быть запечатаны.

Персоналу оперативного реагирования **СЛЕДУЕТ** знать, что сотовые устройства продолжают отправлять сигналы GPS, даже когда они находятся в авиарежиме, и позволяют террористам определить точное местоположение персонала оперативного реагирования на поле боя, в ходе транспортировки, а также местоположение криминалистической лаборатории. Чтобы цифровые устройства не передавали сигналы, в качестве упаковочного материала рекомендуется использовать мешки Фарадея.

Прежде чем прибыть на место, персонал оперативного реагирования должен убедиться, что использованная ранее сумка Фарадея работает должным образом. В качестве альтернативного варианта персонал оперативного реагирования может обернуть цифровое устройство алюминиевой фольгой (не менее трех раз) после его упаковки в антистатический пакет.

Чтобы предотвратить тряску и физический вред изъятым цифровым устройствам, персоналу оперативного реагирования следует упаковать их в чехлы с мягкой подкладкой. При этом допускается использование любого типа подкладки при условии, что цифровое устройство упаковано в антистатический пакет.

Персоналу оперативного реагирования следует **ПО ВОЗМОЖНОСТИ** упаковывать цифровые устройства в оригинальную упаковку[25].

Все цифровые устройства **ДОЛЖНЫ** быть упакованы вместе с документацией, указанной в п. 5.4.2.

Персонал оперативного реагирования **ДОЛЖЕН** заклеить упаковку клейкой лентой, чтобы обеспечить сохранность документов, кабелей и аксессуаров, упакованных вместе с цифровым устройством.

Персонал оперативного реагирования должен снабдить упаковки маркировкой, и маркировка **ДОЛЖНА** включать следующую информацию:

- обозначение «ЦИФРОВОЕ УСТРОЙСТВО»;
- обозначение «УСТРОЙСТВО В РАБОЧЕМ СОСТОЯНИИ», если применимо;
- обозначение «ОПАСНОСТЬ ВЗРЫВА — СОДЕРЖИТ АККУМУЛЯТОРНУЮ БАТАРЕЮ», если устройство оснащено внешним аккумулятором или содержит батарею;
- дату и время изъятия;
- уникальный идентификационный номер цифрового устройства;
- уникальное и точное определение места, где было обнаружено устройство;
- место или название группы оперативного реагирования;
- конечный пункт следования упаковки.

Использование альтернативного источника питания (внешнего аккумулятора) для транспортировки цифрового устройства в рабочем состоянии может быть опасным и увеличивает риск взрыва батареи.

Об использовании внешнего аккумулятора и транспортировке устройства в рабочем состоянии **СЛЕДУЕТ** всегда информировать весь персонал, работающий с устройством.

Если цифровое устройство перевозится в рабочем состоянии с внешним аккумулятором или без него, оно **НЕ ДОЛЖНО** подвергаться воздействию экстремальных температур.

Прежде чем принять решение о том, следует ли перевозить цифровое устройство с внешним аккумулятором, персонал оперативного реагирования **ДОЛЖЕН** учесть ожидаемое время транспортировки в лабораторию цифровой криминалистики, ожидаемую температуру во время транспортировки и расчетное время прибытия.

a. Цель

- Упаковать все изъятые цифровые устройства для подготовки к транспортировке.

b. Действия

1. Персонал оперативного реагирования **ДОЛЖЕН** упаковывать все небольшие цифровые устройства в отдельные антистатические пакеты.
2. Персонал оперативного реагирования **ДОЛЖЕН** использовать сумки Фарадея по мере необходимости.
3. Персонал оперативного реагирования **ДОЛЖЕН** обернуть все цифровые устройства, не имеющие защитных чехлов (помещенные в антистатический пакет), воздушно-пузырчатой пленкой.
4. Персонал оперативного реагирования **ДОЛЖЕН** упаковывать все цифровые устройства, обернутые воздушно-пузырчатой пленкой, в коробку, конверт или сумку.
5. Персонал оперативного реагирования **ДОЛЖЕН** упаковывать все цифровые устройства вместе с копией соответствующей документации.
6. Персонал оперативного реагирования **ДОЛЖЕН** запечатать упаковку перед транспортировкой.
7. Персонал оперативного реагирования **ДОЛЖЕН** снабдить упаковку соответствующей маркировкой перед транспортировкой.

25 Также см. Интерпол, «Рекомендации для персонала оперативного реагирования в области цифровой криминалистики: передовая практика поиска и изъятия электронных и цифровых доказательств», март 2021 г., с. 20.

c. Результаты

Все собранные цифровые устройства имеют уникальную маркировку и надлежащим образом упакованы.

5.5 Транспортировка

Изъятые цифровые устройства необходимо как можно скорее вывезти за пределы поля боя в безопасное место для хранения и дальнейшего изучения.

Цифровые устройства могут транспортироваться как самим персоналом оперативного реагирования, так и другими группами. Учитывая, что не все цифровые устройства могут быть доставлены непосредственно в лабораторию цифровой криминалистики, устройства должны быть доставлены в хранилище, а затем, как можно скорее, в лабораторию цифровой криминалистики для дальнейшего изучения.

Если цифровые устройства передаются на хранение, персонал оперативного реагирования **ДОЛЖЕН** подготовить все необходимые документы перед транспортировкой. Изъятые цифровые устройства **НЕ ДОЛЖНЫ** быть оставлены без присмотра.

Документация, подготовленная на предыдущих этапах настоящего руководства, **ДОЛЖНА** быть приложена к соответствующим устройствам.

Цифровые устройства **СЛЕДУЕТ** перемещать в чехлах с мягкой подкладкой, в закрытом виде и как можно дальше от группы, осуществляющей транспортировку, чтобы свести к минимуму возможность записи активными записывающими устройствами.

ТАБЛИЦА 10. **Краткое описание действий**

Действие	Цель	Уровень значимости
Документирование	Документирование	ОБЯЗАТЕЛЬНО
Транспортировка цифровых устройств	Мера безопасности	ОБЯЗАТЕЛЬНО
Передача	Обращение	ОБЯЗАТЕЛЬНО

5.5.1 Документирование

ВСТАВКА 9. **Указания**

Данное действие **ДОЛЖНО** быть выполнено.

Транспортировка **ДОЛЖНА** быть задокументирована с указанием членов группы, которые прикасались к цифровому устройству, а также конкретного пункта назначения, такого как криминалистическая лаборатория, хранилище и т. д.

В документацию **СЛЕДУЕТ** включать краткое описание цифрового устройства и цели его транспортировки, чтобы обеспечить возможность быстрой обработки цифровых устройств принимающей стороной.

Цифровое устройство должно сопровождаться копией документации, подготовленной персоналом оперативного реагирования в ходе его изъятия.

5.5.2 Транспортировка цифровых устройств

Во время перевозки цифровых устройств члены группы, осуществляющей перевозку, должны осознавать риски, связанные с тем, что цифровые устройства могут осуществлять передачу данных. Члены группы, осуществляющей транспортировку, ни при каких условиях **НЕ ДОЛЖНЫ** распаковывать изъятые цифровые устройства, поскольку это может подвергнуть их опасности со стороны террористов, которые могут продол-

жать отслеживать цифровые устройства. Распакованные цифровые устройства могут передавать сигналы и раскрывать местоположение транспорта, записывать разговоры и передавать данные террористам. Это, в свою очередь, может привести к целенаправленным атакам, раскрытию маршрутов транспортировки и местонахождения специальных объектов.

Распаковка сотовых телефонов может привести к записи лиц членов группы и передачи этих данных в облако.

Члены группы, осуществляющей транспортировку, также должны осознавать риск самовзрывающихся устройств, таких как аккумуляторные батареи, внешние аккумуляторы, сотовые телефоны и т. д., и принимать необходимые меры предосторожности.

Цифровые устройства **СЛЕДУЕТ** перемещать в соответствующей упаковке. Запрещается класть их на колени члену группы.

Необходимо следить за температурой транспортировки, чтобы не допустить перегрева цифровых устройств. Перегрев может произойти в экстремальных погодных условиях или когда цифровое устройство находится рядом с источником тепла во время транспортировки.

5.5.3 Передача

ДОЛЖНА соблюдаться цепочка обеспечения сохранности, а передача собранных цифровых устройств **ДОЛЖНА** быть задокументирована, и соответствующая документация должна быть приложена к цифровому устройству.

Группа, передающая устройство, **ДОЛЖНА** проинструктировать группу, осуществляющую транспортировку, о мерах безопасности и механизмах транспортировки, а также убедиться, что вся необходимая документация и маркировка приложены к цифровому устройству перед его передачей. Это необходимо для предотвращения нарушения цепочки обеспечения сохранности и предотвращения потери устройств, недоразумений и путаницы в будущем.

[ПРИЛОЖЕНИЕ A]
Контрольный список базового снаряжения

A.1 Контрольный список

Ниже приводится контрольный список базового снаряжения персонала оперативного реагирования:

- ☐ видеокамера;
- ☐ антистатические перчатки;
- ☐ маркировочные наклейки — с уникальной маркировкой или предназначенные для записи; перманентные маркеры (для маркировки);
- ☐ небольшие наклейки для закрытия объектива камеры;
- ☐ переносные глушители передачи данных, включая Wi-Fi, сотовую связь и GPS;
- ☐ антистатические пакеты, пакеты с застежкой-молнией или бумажные конверты с заклейкой;
- ☐ запечатывающие устройства;
- ☐ сумки Фарадея или пакеты из алюминиевой фольги или алюминиевая фольга для обертывания;
- ☐ воздушно-пузырьковая пленка для обертывания;
- ☐ чехлы с мягкой подкладкой;
- ☐ картонные коробки для упаковки;
- ☐ шаблоны документации:
  - документация по прибытии на поле боя;
  - документация по изъятию цифровых устройств.

[ПРИЛОЖЕНИЕ B]
Шаблоны документации

B.1 Шаблон — документация по прибытии на поле боя

Персоналу оперативного реагирования следует документировать в письменной форме или с помощью видеозаписи окрестности поля боя и обнаруженные цифровые устройства.

Заполняется для каждого места изъятия:			
Дата и время прибытия:			
Дата		Время	
Подробная информация о поле боя:			
Район		Поле боя	
Общее описание			
Лицо, заполняющее документацию: Полное имя и удостоверение личности члена группы, заполняющего форму, и командира на поле боя			
Полное имя	Удостоверение личности		Описание
Полное имя	Удостоверение личности		Описание

Описание и состояние устройства:				
№ п/п	**Описание и состояние устройства: включено/выключено/неисправно/летает**	**Состояние подключения устройства**	**Местоположение на поле боя**	**Нужна ли консультация специалиста по цифровой криминалистике для изъятия устройства?**
		☐ Вкл. ☐ Выкл.		☐ Да ☐ Нет
		☐ Вкл. ☐ Выкл.		☐ Да ☐ Нет
		☐ Вкл. ☐ Выкл.		☐ Да ☐ Нет
		☐ Вкл. ☐ Выкл.		☐ Да ☐ Нет
		☐ Вкл. ☐ Выкл.		☐ Да ☐ Нет
		☐ Вкл. ☐ Выкл.		☐ Да ☐ Нет

Действия, предпринимаемые на поле боя:

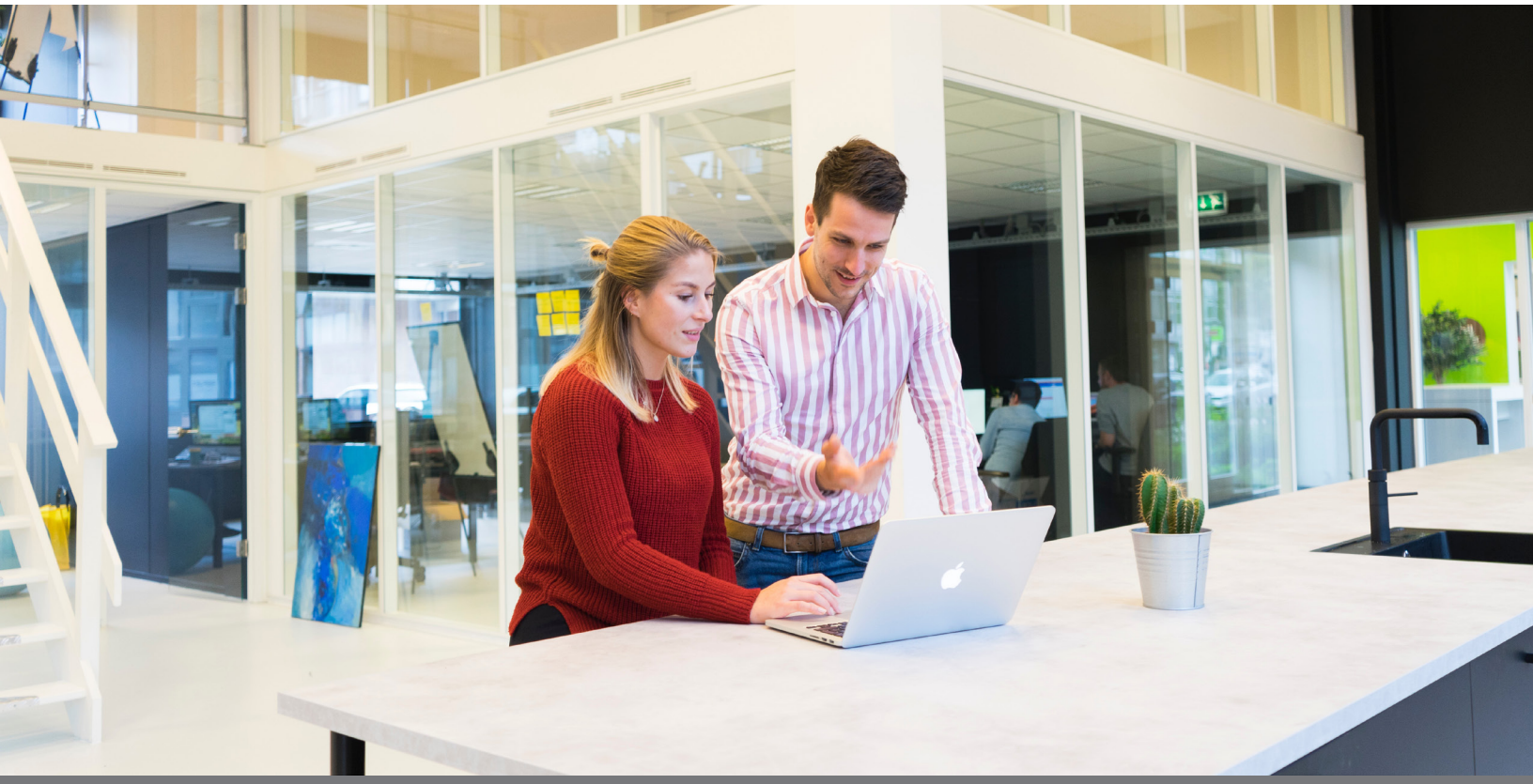
Указать любые изменения, внесенные группой на поле боя с точки зрения изоляции сетевого подключения, передачи данных и устройств. Здесь следует указать любые действия по обращению с устройством, такие как отмена пароля, выключение, подключение к внешнему аккумулятору, отключение от сети и т. д.

Свидетели

Полное имя	Удостоверение личности	Описание
Полное имя	Удостоверение личности	Описание
Полное имя	Удостоверение личности	Описание
Полное имя	Удостоверение личности	Описание

Примечания:

- Описание и состояние устройства — информация, отображаемая на экране устройства. Укажите, работает ли устройство, находится ли оно в полете, мигает ли оно и т. д.
- Состояние подключения — наличие сетевого подключения — по кабелю или с помощью устройств беспроводного подключения (Wi-Fi, сотовая связь, спутниковая связь и т. д.).
- Действия, предпринятые для изоляции цифрового устройства, передающего данные в режиме реального времени, и поля боя — использование глушителей, отключение электропитания и т. п.
- Подтвержденный список всех свидетелей, присутствующих на поле боя по прибытии группы — с указанием имени, фамилии, любых признаков, вызывающих подозрения — видимое состояние сознания.



B.2 Шаблон — документация по изъятию цифровых устройств

Цифровые устройства следует изымать с осторожностью, чтобы не допустить их загрязнения и обеспечить их сохранность. Данный шаблон предназначен для документирования каждого изъятого устройства. Часть документации может быть заполнена на более позднем этапе, а не на поле боя, при условии, что соответствующая информация может быть получена до того, как персонал оперативного реагирования передаст цифровое устройство другой группе.

Приложите заполненную форму к изъятому устройству и упакуйте ее вместе с устройством.

На каждое изъятое цифровое устройство необходимо заполнить следующую документацию:

Номер устройства, присвоенный по прибытии на поле боя, или его маркировка
Убедитесь, что номер соответствует маркировке на устройстве.

Дата и время изъятия:		
Дата	Время	
Специалист, взаимодействующий с устройством: Полное имя и удостоверение личности члена группы, который работал с устройством, вносил изменения или отбирал его для сортировки, сбора и упаковки.		
Полное имя	Удостоверение личности	Описание
Полное имя	Удостоверение личности	Описание
Полное имя	Удостоверение личности	Описание
Полное имя	Удостоверение личности	Описание
Место изъятия:		
Район	Поле боя	
Местоположение цифрового устройства на поле боя		
Присоединенные устройства или кабели		
Описание изъятого устройства:		
Тип устройства		
Производитель или модель		
Цвет	Номер маркировки	
Состояние:	☐ Включено	☐ Выключено
Передача данных	☐ Да ☐ Заблокировано	☐ Нет ☐ Разблокировано
Физическое состояние		

Действия, предпринимаемые на поле боя:

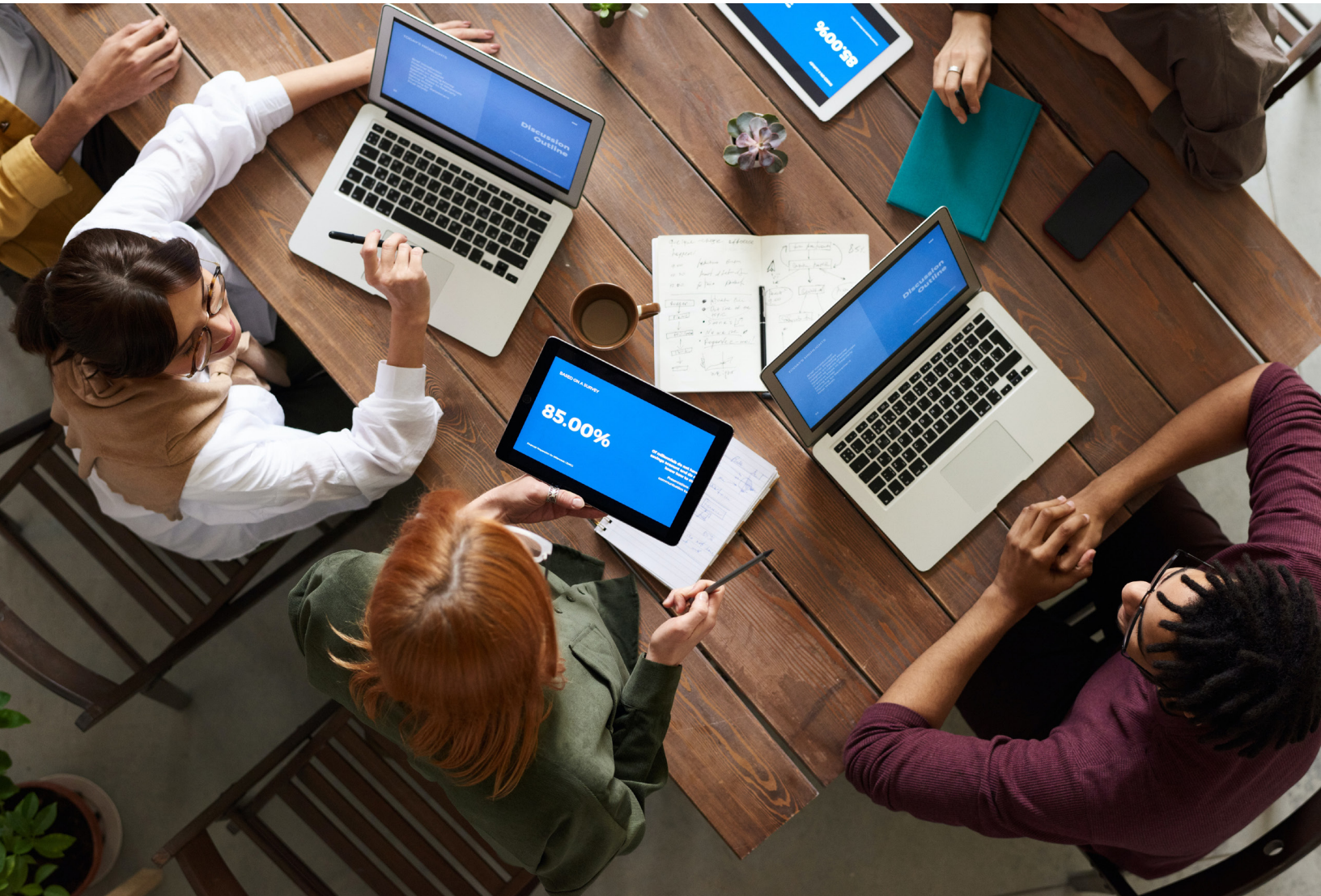
Здесь следует указать любые действия с устройством, предпринимаемые группой, такие как удаление пароля, выключение, подключение к внешнему аккумулятору, отключение от сети и т. д.

Дополнительные сведения:

Известный владелец устройства

Дата и время, отображаемые на экране устройства

Примечания.



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)

24-09823