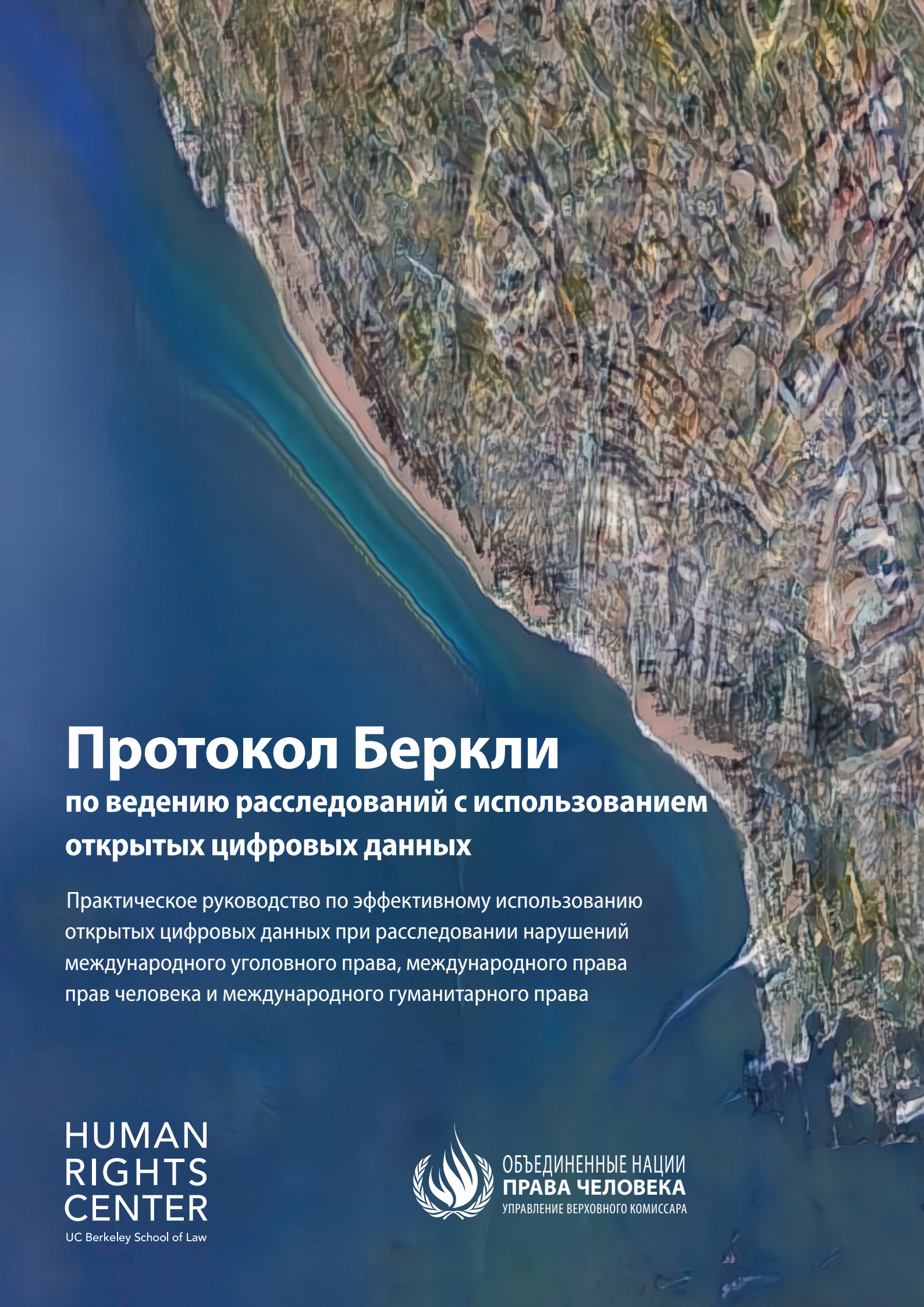


Протокол Беркли

по ведению расследований с использованием открытых цифровых данных

Практическое руководство по эффективному использованию открытых цифровых данных при расследовании нарушений международного уголовного права, международного права прав человека и международного гуманитарного права

HUMAN RIGHTS CENTER
UC Berkeley School of Law

ОБЪЕДИНЕННЫЕ НАЦИИ
ПРАВА ЧЕЛОВЕКА
УПРАВЛЕНИЕ ВЕРХОВНОГО КОМИССАРА

Протокол Беркли

по ведению расследований с использованием открытых цифровых данных

Практическое руководство по эффективному использованию открытых цифровых данных при расследовании нарушений международного уголовного права, международного права прав человека и международного гуманитарного права

HUMAN RIGHTS CENTER
UC Berkeley School of Law

ОБЪЕДИНЕННЫЕ НАЦИИ
ПРАВА ЧЕЛОВЕКА
УПРАВЛЕНИЕ ВЕРХОВНОГО КОМИССАРА

Нью-Йорк и Женева, 2022 год

HR/PUB/20/2
ISBN: 978-92-1-154249-3
eISBN: 978-92-1-005348-8
В продаже под номером: R.20.XIV.4

Данная работа опубликована совместно Организацией Объединенных Наций — от имени Управления Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ) — и Центром по правам человека при Школе права Калифорнийского университета в Беркли.

Обозначения, используемые в настоящей публикации, и изложение материала не подразумевают выражения со стороны Секретариата Организации Объединенных Наций какого бы то ни было мнения в отношении правового статуса той или иной страны, территории, города или района, или их органов власти, или делимитации их границ.

Условные обозначения документов Организации Объединенных Наций состоят из прописных букв и цифр. Когда такое обозначение встречается в тексте, оно служит указанием на соответствующий документ Организации Объединенных Наций.

Изображение обложки: дипфейк спутникового изображения, созданный Ахмедом Эль-Гамалем с помощью платформы искусственного интеллекта Playform.

Центр по правам человека при Школе права Калифорнийского университета в Беркли благодарит за финансовую поддержку следующих доноров: Фонд Сигрид Раузинг (Sigrid Rausing Trust); Фонд Оук (Oak Foundation); отдельных доноров в Калифорнийском университете в Беркли; фонды «Открытое общество»; Центр Фонда Рокфеллера в Белладжо.

Содержание

Предисловие

С начала 1990-х годов цифровые инструменты и Интернет, как до них фотоаппарат и телефон, произвели революцию в получении, сборе и распространении информации о нарушениях прав человека и других серьезных нарушениях международного права, включая международные преступления.

Сегодня лица, проводящие расследования, могут получить данные о потенциальных нарушениях прав человека и других серьезных нарушениях международного права, включая международные преступления, из огромного количества общедоступных спутниковых изображений, видео и фотографий, включая материалы, загруженные в Интернет со смартфонов, и посты на платформах социальных сетей. Это помогает расследователям обойти государственные и другие традиционные структуры, контролирующие поток информации, и получить, в том числе в режиме реального времени, доступ к ключевой информации о правонарушениях, которая в противном случае осталась бы скрытой от общественности.

Однако цифровые данные из открытых источников используются в основном ситуативно, поскольку правозащитные организации, межправительственные органы, механизмы расследований и суды порой сталкиваются с трудностями при адаптации своей рабочей практики для включения в нее новых цифровых методов установления и анализа фактов. Одна из самых серьезных проблем — это обнаружение и верификация соответствующих материалов в условиях растущего объема информации в Интернете, особенно снятых на смартфоны и другие мобильные устройства фотографий и видео, некоторые из которых могли оказаться объектом манипуляций или быть неверно атрибутированы.

Между тем появление международных уголовных судов и механизмов расследований, а также национальных подразделений по расследованию военных преступлений еще больше усилило потребность в общих стандартах для сбора, сохранения и анализа открытых данных, которые могут быть представлены в качестве доказательств в уголовных процессах. Для того чтобы такие открытые данные могли быть приняты в качестве доказательства в суде, обвинители и защитники, как правило, должны иметь возможность установить их подлинность и цепочку обеспечения их сохранности. Надлежащее использование и обработка этих материалов значительно повысят вероятность того, что они могут быть использованы обвинителями и защитниками. Однако, если применяются ненадежные методы сбора и сохранения информации, она не может считаться достоверной для целей установления фактов по делу. Для судов и механизмов расследований будут полезны четкие критерии оценки весомости открытых данных в качестве доказательства либо причастности к преступлению, либо его совершения. Кроме того, общие методологические стандарты в области подтверждения подлинности и верификации станут подспорьем для миссий по установлению фактов в области прав человека, которые также все чаще используют открытые цифровые данные в своих расследованиях. Комиссии по расследованию, правозащитные компоненты операций по поддержанию мира, отделения Управления Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ) на местах и другие усилия Организации Объединенных Наций по мониторингу и расследованию нарушений прав человека могут извлечь пользу из надежных методологических принципов и подходов для обеспечения обоснованности и весомости своих выводов.

Для решения этой задачи наши учреждения, Центр по правам человека при Школе права Калифорнийского университета в Беркли и УВКПЧ, объединили усилия для публикации «Протокола Беркли по ведению расследований с использованием открытых цифровых данных: практическое руководство по эффективному использованию открытых цифровых данных при расследовании нарушений международного уголовного права, международного права прав человека и международного гуманитарного права». Путь, приведший к этой публикации, начался в кампусе Беркли в 2009 году, когда Центр по правам человека собрал вместе экспертов в области права, создателей технологий, журналистов и активистов для разработки стратегий использования цифровых технологий и методик для выявления и документирования нарушений прав человека. С тех пор Центр по правам человека провел серию междисциплинарных рабочих совещаний в сотрудничестве с рядом экспертов по техническим, правовым и методологическим вопросам, в том числе из УВКПЧ, для коллективного обсуждения, разработки новых инструментов и определения и уточнения критериев, стандартов и методов выяв-

ления, оценки, проверки и сохранения открытых цифровых данных для документирования нарушений прав человека и привлечения виновных к ответственности. Этот процесс хорошо согласуется с усилиями УВКПЧ по разработке руководств и инструментов для поддержки и консультирования комиссий по расследованию и миссий по установлению фактов Организации Объединенных Наций, а также сотрудников УВКПЧ в их все более широком использовании открытых данных в работе по установлению фактов и расследованиях.

В разработке Протокола Беркли приняли участие специалисты с различным профессиональным опытом, юридическим и культурным бэкграундом, разной гендерной принадлежности и разных национальностей; было проведено более 150 консультаций с экспертами и получены материалы от основных заинтересованных сторон, включая специалистов Организации Объединенных Наций по расследованию нарушений прав человека. Кроме того, в основу этой публикации положен опыт специализированных рабочих групп из Секции по вопросам методологии, образования и профессиональной подготовки УВКПЧ и Канцелярии Прокурора Международного уголовного суда. В соответствии с международными стандартами разработки новой методологии УВКПЧ и Центр по правам человека провели тщательное рецензирование, редактирование и проверку Протокола Беркли.

Исходя из совместного подхода в Протоколе Беркли сформулированы международные стандарты проведения онлайн-расследований предполагаемых нарушений международного права прав человека, международного гуманитарного и уголовного права. В нем содержатся также рекомендации по методологии и профессиональному, юридически корректному и этичному проведению процедур сбора, анализа и сохранения цифровой информации. Наконец, Протокол Беркли устанавливает меры, которые могут принять специалисты по онлайн-расследованиям для защиты цифровой, физической и психосоциальной безопасности их самих и других лиц, включая свидетелей, жертв и лиц, первыми реагирующих на нарушения (например, граждан, активистов и журналистов), которые рискуют своим благополучием, документируя нарушения прав человека и серьезные нарушения международного права.

Протокол Беркли следует по стопам двух предыдущих протоколов Организации Объединенных Наций: Миннесотского протокола по расследованию предположительно незаконного лишения жизни (1991 год, обновлен в 2016 году) и Руководства по эффективному расследованию и документированию пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения и наказания (Стамбульский протокол) (1999 год, обновлен в 2004 году). Миннесотский протокол, разработанный юристами и судмедэкспертами, занимавшимися поиском исчезнувших лиц в 1980-х годах, устанавливает международные стандарты и процедуры проведения медико-юридических расследований подозрительных смертей или смертей без свидетелей, а также служит инструментом оценки достоверности результатов таких расследований. Аналогичным образом Стамбульский протокол содержит руководящие указания для практикующих врачей и юристов о том, как распознавать и документировать физические и психосоциальные последствия пыток, чтобы документация могла служить веским доказательством в суде или в других контекстах, включая расследования и мониторинг нарушений прав человека. Все три протокола основаны на убеждении, что наука, технологии и право могут — и должны — работать вместе на благо прав человека. Как и предыдущие протоколы, Протокол Беркли будет доступен на официальных языках Организации Объединенных Наций, чтобы облегчить его использование и применение во всем мире.

Мы надеемся, что в мире, который становится все более цифровизирован, Протокол Беркли поможет специалистам, ведущим расследования в Интернете, будь то юристы, правозащитники, журналисты или другие лица, разработать и внедрить эффективные процедуры документирования и проверки нарушений международного права прав человека, международного гуманитарного и уголовного права, максимально используя открытые цифровые данные, чтобы лица, виновные в таких нарушениях, могли быть справедливо привлечены к ответственности.

Эрик Стовер
директор факультета, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Мишель Бачелет
Верховный комиссар Организации Объединенных Наций по правам человека

Резюме

Расследования с использованием открытых цифровых данных — это расследования, которые полностью или частично опираются на общедоступную информацию для проведения формального и систематического онлайн-поиска информации о предполагаемом правонарушении. Сегодня большие объемы общедоступной информации имеются в Интернете, где быстро развивающаяся цифровая среда способствует появлению новых видов и источников информации, которые могут помочь в расследовании предполагаемых нарушений прав человека и серьезных международных преступлений. Возможность расследования таких предполагаемых нарушений представляет особую ценность для следователей, которые физически не могут своевременно добраться до места преступления, как это часто бывает при проведении международных расследований.

Открытые данные могут служить основой версий, подтверждать разведывательную информацию и служить прямым доказательством в судах. Однако для их использования в официальных процессах расследований, включая юридические расследования, миссии по установлению фактов и комиссии по расследованию, расследователи должны использовать последовательные методы, которые как повышают точность их выводов, так и позволяют судьям и другим лицам, устанавливающим факты, лучше оценить качество самого процесса расследования. Протокол Беркли по ведению расследований с использованием открытых цифровых данных был разработан для установления международных стандартов и предоставления рекомендаций специалистам, занимающимся расследованиями в области международного уголовного правосудия и прав человека. Такие лица представляют различные учреждения, включая СМИ, группы гражданского общества и неправительственные организации, международные организации, суды, а также национальные и международные следственные органы. Установление последовательных и измеримых стандартов для поддержки этой междисциплинарной сферы позволяет перевести на профессиональную основу практику проведения расследований с использованием открытых цифровых данных.

Хотя руководства и обучение, посвященные использованию конкретных инструментов и программного обеспечения, являются важной частью повышения качества расследований с использованием открытых цифровых данных, Протокол Беркли посвящен не конкретным технологиям, платформам, программному обеспечению или инструментам, а скорее основополагающим принципам и методикам, которые могут последовательно применяться даже при изменении самой технологии. В этих принципах изложены минимальные правовые и этические стандарты проведения эффективных расследований с использованием открытых данных. Следуя указаниям Протокола Беркли, лица, ведущие расследования, смогут обеспечить качество своей работы, минимизируя при этом физические, психосоциальные и цифровые риски для себя и других.

Протокол Беркли разработан в качестве учебного пособия и справочника для лиц, проводящих расследования с использованием открытых данных. Три главы, следующие за введением, посвящены всеобъемлющим основам, включая принципы, правовые соображения и безопасность. В остальных главах идет речь о самом процессе расследования. Эта часть Протокола Беркли начинается с главы о подготовке и стратегическом планировании, за которой следует глава, посвященная различным необходимым этапам расследования, а именно: онлайн-поиску, предварительной оценке, сбору, сохранению, верификации и расследовательскому анализу. Документ завершается главой, посвященной методологии и принципам составления отчета о результатах расследования с использованием открытых цифровых данных.

Авторы и участники

Координационный комитет Протокола Беркли

Алекса Кёниг, исполнительный директор, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Эрик Стовер, директор факультета, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Линдси Фримен, старший научный сотрудник по правовым вопросам, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Редакционный комитет Протокола Беркли

Сарета Ашраф, старший юридический консультант; адвокат Адвокатской палаты «Гарден корт» (Garden Court Chambers); бывший старший аналитик Следственной группы Организации Объединенных Наций по содействию привлечению к ответственности за преступления, совершенные ДАИШ/«Исламским государством Ирака и Леванта»

Бет Ван Шаак, приглашенный профессор по правам человека, Стэнфордская школа права; бывший заместитель посла по особым поручениям по вопросам военных преступлений, Управление глобального уголовного правосудия Государственного департамента США

Кристиан Венавезер, Постоянный представитель Лихтенштейна при Организации Объединенных Наций; бывший председатель Ассамблеи государств — участников Римского статута Международного уголовного суда

Сьюзан Волфинбаргер, сотрудник по иностранным делам и руководитель группы аналитиков Государственного департамента США; бывший старший директор проекта по геопространственным технологиям Американской ассоциации по развитию науки

Ричард Голдстоун, бывший судья Конституционного суда Южной Африки; бывший главный обвинитель Международного трибунала по бывшей Югославии и Международного уголовного трибунала по Руанде

Аликс Данн, исполнительный директор международной организации Engine Room

Мишель де Смедт, директор Отдела расследований Канцелярии Прокурора Международного уголовного суда

Таня Каранасиос, директор по программам, организация WITNESS («СВИДЕТЕЛЬ»)

Энрике Пирасез, руководитель программы «СМИ и права человека», Центр науки прав человека, Университет Карнеги — Меллон

Алан Тигер, старший судебный защитник Специализированной прокуратуры по Косову; в прошлом бывший старший защитник, Международный трибунал по бывшей Югославии

Алекс Уайтинг, руководитель отдела расследований Специализированной прокуратуры по Косову; практикующий профессор Гарвардской школы права; бывший координатор судебного преследования и координатор расследований Канцелярии Прокурора Международного уголовного суда

Бренда Дж. Холлис, международный сообвинитель Чрезвычайных палат в судах Камбоджи; бывший главный прокурор Остаточного механизма Специального суда по Сьерра-Леоне

Консультативный комитет Протокола Беркли

Федерика д'Алессандра, исполнительный директор Оксфордской программы по международному миру и безопасности, Оксфордский университет; редактор «Справочника по документированию гражданским обществом серьезных нарушений прав человека: принципы и передовая практика» Группы по вопросам международного публичного права и политики

Винсент Иакопино, старший медицинский советник организации «Врачи за права человека»; член основного авторского коллектива Руководства по эффективному расследованию и документированию пыток и других жестоких,

бесчеловечных или унижающих достоинство видов обращения и наказания (Стамбульский протокол)

Стюарт Кейси-Маслен, почетный профессор юридического факультета Университета Претории, соавтор Миннесотского протокола по расследованию предположительно незаконного лишения жизни (2016)

Элисон Коул, советник-специалист по правам человека Департамента внутренних дел Новой Зеландии

Ханни Мегалли, член Независимой международной комиссии по расследованию событий в Сирийской Арабской Республике; старший научный сотрудник Центра международного сотрудничества Нью-Йоркского университета

Хуан Мендес, приглашенный профессор права прав человека, Вашингтонский колледж права; бывший Специальный докладчик по вопросу о пытках и других жестоких, бесчеловечных или унижающих достоинство видах обращения и наказания; координатор универсального протокола о ведении следственного допроса и процессуальных гарантиях

Келли Мэтисон, старший адвокат и руководитель программы организации WITNESS; автор практического руководства «Видео как доказательство» (Video as Evidence Field Guide)

Арье Найер, почетный президент фондов «Открытое общество»

Нави Пиллэй, председатель Международной комиссии по отмене смертной казни; бывший Верховный комиссар Организации Объединенных Наций по правам человека; бывший судья Международного уголовного суда; бывший председатель Международного уголовного трибунала по Руанде

Паулу Сержиу Пиньейру, председатель Независимой международной комиссии по расследованию событий в Сирийской Арабской Республике; бывший Специальный докладчик по вопросу о положении в области прав человека в Бурунди; бывший Специальный докладчик по вопросу о положении в области прав человека в Мьянме

Томас Проберт, внештатный лектор Центра по правам человека Университета Претории; научный сотрудник Центра управления и прав человека Кембриджского университета; соавтор Миннесотского протокола по расследованию предположительно незаконного лишения жизни (2016)

Стивен Рапп, заслуженный научный сотрудник Центра Саймона-Скьодта по предотвращению геноцида, Мемориальный музей Холокоста США; бывший посол по особым поручениям по вопросам военных преступлений, Управление глобального уголовного правосудия, Государственный департамент США; бывший прокурор Специального суда по Сьерра-Леоне

Кристина Рибейро, координатор расследований Канцелярии Прокурора Международного уголовного суда

Патрисия Селлерс, специальный советник по гендерным вопросам Прокурора Международного уголовного суда; приглашенный научный сотрудник Келлог-колледжа Оксфордского университета; бывший юридический консультант и судебный защитник Международного трибунала по бывшей Югославии и Международного уголовного трибунала по Руанде

Кристоф Хейнс, профессор права в области прав человека Университета Претории; член Комитета по правам человека; бывший Специальный докладчик по вопросу о внесудебных казнях, казнях без надлежащего судебного разбирательства или произвольных казнях; координатор Миннесотского протокола по расследованию предположительно незаконного лишения жизни (2016)

Франсуаза Хэмпсон, почетный профессор Школы права Эссекского университета; член Комиссии по расследованию событий в Бурунди

Участники рабочих совещаний

Рабочее совещание по новой криминалистике: использование открытых данных для расследования тяжких преступлений (Белладжо, Италия, 2017)

Хади Аль Хатиб, Сирийский архив

Стюарт Кейси-Маслен, Университет Претории

Алекса Кёниг, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Стив Костас, правовая инициатива фондов «Открытое общество»

Иван Куйперс, Международный уголовный суд

Андреа Лампрос, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Фелим Макмахон, Международный уголовный суд

Келли Мэтисон, организация WITNESS

Джулиан Николлс, Международный уголовный суд

Томас Проберт, Кембриджский университет

Кристина Рибейро, Международный уголовный суд

Эрик Стовер, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Алан Тигер, Международный трибунал по бывшей Югославии

Марк Уотсон, «Комиссия по международному правосудию и привлечению к ответственности»

Гай Уиллоуби, Ассоциация по изучению военных преступлений

Линдси Фримен, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Гэвин Шеридан, Vizlegal

Скотт Эдвардс, организация Amnesty International

Рабочее совещание, посвященное созданию этической основы для расследований с использованием открытых данных (Эссекский университет, Великобритания, 2019)

Фред Абрахамс, организация Human Rights Watch

Лина Бассуни, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Джефф Гилберт, Эссекский университет

Сэм Дабберли, организация Amnesty International

Федерика д'Алессандра, Оксфордский университет

Габриэла Ивенс, стипендиат фонда Mozilla и WITNESS

Дженнифер Истердей, организация JustPeace Labs

Алекса Кёниг, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Лорна Макгрегор, Эссекский университет

Мэтт Махмуди, Кембриджский университет

Дараг Мюррей, Эссекский университет

Вивиан Нг, Эссекский университет

Энрике Пирасез, Центр науки о правах человека, Университет Карнеги-Меллон

Зара Рахман, организация Engine Room

Саша Робехмед, организация Engine Room

Илия Сиатица, благотворительная организация Privacy International

Кристофер «Кип» Хейл, «Комиссия по международному правосудию и привлечению к ответственности»

Эванна Ху, Omelas

Линдси Фримен, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Скотт Эдвардс, организация Amnesty International

Представитель УВКПЧ из Секции по вопросам методологии, образования и профессиональной подготовки

Круглый стол по правовым вопросам, возникающим при проведении расследований с использованием открытых данных (Гаага, 2019)

Дэвид Акерсон, Следственная группа Организации Объединенных Наций по содействию привлечению к ответственности за преступления, совершенные ДАИШ/«Исламским государством Ирака и Леванта»

Сарета Ашраф, Адвокатская палата «Гарден корт»

Ракель Васкес Льоренте, благотворительная организация eyeWitness to Atrocities

Бастиан Ван Дер Лаакен, Международный беспристрастный и независимый механизм для содействия проведению расследований в отношении лиц, которые несут ответственность за наиболее серьезные преступления по международному праву, совершенные в Сирийской Арабской Республике с марта 2011 года, и их судебному преследованию

Федерика д'Алессандра, Оксфордский университет

Нико Декенс, интернет-издание Bellingcat

Мишель Джарвис, Международный беспристрастный и независимый механизм для содействия проведению расследований в отношении лиц, которые несут ответственность за наиболее серьезные преступления по международному праву, совершенные в Сирийской Арабской Республике с марта 2011 года, и их судебному преследованию

Эдвард Джереми, Международный уголовный суд

Эшли Джордана, фонд Global Rights Compliance

Эмма Ирвинг, Лейденский университет

Алекса Кёниг, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Санг-Мин Ким, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Алан Кларк, Международный уголовный суд

Николас Кумджян, Независимый механизм по расследованию для Мьянмы

Дирбла Миноуг, Global Legal Action Network (Глобальная сеть правовых действий)

Ник Ортис, Лейденский университет

Стивен Паулс, Адвокатская палата «Доути Стрит» (Doughty Street Chambers); Комитет по военным преступлениям Международной ассоциации юристов

Матевж Пездирк, Сеть по предупреждению геноцида Агентства Европейского союза по сотрудничеству в области уголовного правосудия

Саня Попович, Специализированная прокуратура по Косову

Стивен Рапп, Центр Саймона-Скьодта по предотвращению геноцида, Мемориальный музей Холокоста США

Кристина Рибейро, Международный уголовный суд

Марк Робсон, «Комиссия по международному правосудию и привлечению к ответственности»

Далила Сеоане, Civitas Maxima

Карстен Стан, Лейденский университет

Брэд Сэмюэлс, SITU Research

Мелинда Тейлор, Международный уголовный суд

Алан Тигер, Специализированная прокуратура по Косову

Линдси Фримен, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Даня Чайкель, Специализированная прокуратура по Косову

Крис Энгельс, «Комиссия по международному правосудию и привлечению к ответственности»

Дополнительные эксперты-рецензенты

Элиз Бейкер, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Шон Брукс, Центр долгосрочной кибербезопасности, Калифорнийский университет в Беркли

Ракель Васкес Льоренте, благотворительная организация eyeWitness to Atrocities

Сэм Дабберли, организация Amnesty International

Габриэла Ивенс, организация Human Rights Watch

Стефани Крофт, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Фелим Макмахон, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Дараг Мюррей, Эссекский университет

Ивонн Нг, организация WITNESS

Зара Рахман, организация Engine Room

Марк Робсон, «Комиссия по международному правосудию и привлечению к ответственности»

Джастин Сейтц, Hunchly

Андреа Тревиннард, Центр по правам человека при Школе права Калифорнийского университета в Беркли

Стив Труш, Центр долгосрочной кибербезопасности, Калифорнийский университет в Беркли

Кристофер «Кип» Хейл, «Комиссия по международному правосудию и привлечению к ответственности»

Томас Эдвин, Центр перспективных оборонных исследований

Особая благодарность

Особая благодарность членам Рабочей группы по онлайн-расследованиям Канцелярии Прокурора Международного уголовного суда.

Выражаем также признательность многим коллегам в УВКПЧ, чьи усилия способствовали появлению этой совместной публикации*.

* В соответствии с политикой УВКПЧ, вклад в его публикации не приписывается лицам, работающим в Управлении.

Аббревиатуры и сокращения

ИКТ	информационно-коммуникационные технологии
ИП	интернет-провайдер
МККК	Международный комитет Красного Креста
НПО	неправительственная организация
УВКПЧ	Управление Верховного комиссара Организации Объединенных Наций по правам человека
HTML	язык разметки гипертекста
IP	межсетевой протокол
PDF	формат переносимых документов
URI	унифицированный идентификатор ресурса
URL	унифицированный указатель ресурса
VPN	виртуальная частная сеть

1

ВВЕДЕНИЕ

КРАТКОЕ СОДЕРЖАНИЕ ГЛАВЫ

- Цель
- Целевая аудитория
- Определения

1. В Протоколе Беркли по ведению расследований с использованием открытых цифровых данных описаны профессиональные стандарты, которые должны применяться при выявлении, сборе, сохранении, анализе и представлении открытых цифровых данных и их использовании в международных уголовных расследованиях и расследованиях нарушений прав человека. Открытые данные — это данные, которые любой представитель общественности может наблюдать, приобретать или запрашивать без необходимости наличия специального правового статуса или получения несанкционированного доступа. Открытые цифровые данные — это общедоступные данные в цифровом формате, которые обычно можно получить в Интернете. К ним относятся как созданные пользователем, так и автоматически сгенерированные данные, и они могут включать, например, контент, размещенный в социальных сетях; документы, изображения, видео- и аудиозаписи на веб-сайтах и платформах обмена информацией; спутниковые изображения; и опубликованные правительством данные[1]. Расследования с использованием открытых цифровых данных — это расследования, основанные на цифровой информации из открытых источников. Для удобства чтения в Протоколе цифровая информация из открытых источников и расследования с использованием цифровой информации из открытых источников будут далее обозначаться как «открытые данные» и «расследования с использованием открытых данных» соответственно.

2. Хотя использование открытых данных в расследованиях не является чем-то новым, объем и разнообразие открытых источников расширились в результате все более активного использования Интернета и других цифровых ресурсов для обмена информацией, включая распространение социальных сетей. В Протоколе рассматриваются как трудности, возникающие при работе с цифровой информацией, так и уникальные проблемы, связанные с оценкой источников и проверкой информации, найденной на открытых онлайн-форумах.

3. Несмотря на то, что все большее число лиц, проводящих международные расследования по уголовным делам и по делам о нарушениях прав человека, в настоящее время используют Интернет для облегчения своей работы, универсальных справочников, руководств или стандартов для расследований с использованием открытых данных сейчас не существует. Протокол призван восполнить этот пробел путем изложения принципов и видов практики, которые помогут следователям осуществлять свою работу на профессиональном уровне и способствовать, где это необходимо, сохранению открытых данных для их потенциального использования механизмами привлечения к ответственности.

4. В Протоколе уделяется особое внимание расследованиям с использованием открытых данных, которые проводятся в целях обеспечения международного правосудия и привлечения виновных к ответственности и которые в широком смысле включают: документирование нарушений прав человека, сохранение, сбор доказательств и установление фактов; расследования комиссий по расследованию и миссий по установлению фактов[2]; другие виды расследований и работы по установлению фактов, проводимых в соответствии с международным мандатом[3]; процессы установления истины и примирения; гражданское судопроизводство; и уголовное судопроизводство, включая международные уголовные процессы. Поскольку расследования с использованием открытых источников могут внести вклад в различные виды усилий по обеспечению привлечения к

[1] Данный перечень не является исчерпывающим.

[2] Комиссии по расследованию и миссии по установлению фактов — это органы, которые могут быть созданы правительствами или международными организациями для расследования различных вопросов. Комиссии по расследованию или миссии по установлению фактов сообщают фактические данные, делают юридические заключения и дают рекомендации. Хотя заключения международных комиссий по расследованию или миссий по установлению фактов не имеют обязательной юридической силы, они могут иметь большое влияние. Однако в некоторых юрисдикциях заключения национальных комиссий по расследованию могут иметь обязательную силу. Более подробную информацию о международных комиссиях по расследованию и миссиях по установлению фактов см. в документе Совета по правам человека «Международные комиссии по расследованию, комиссии по правам человека, миссии по установлению фактов и другие расследования». URL: www.ohchr.org/ru/hr-bodies/hrc/co-is.

[3] См., например, доклад Верховного комиссара Организации Объединенных Наций по правам человека о положении в области прав человека в Боливарианской Республике Венесуэла (A/HRC/41/18), представленный в соответствии с резолюцией 39/1 Совета по правам человека. См. также резолюцию 41/2 Совета, в которой Совет просил Верховного комиссара подготовить доклад о положении в области прав человека на Филиппинах.

ответственности[4], требования к методологии и документации, изложенные в Протоколе, могут быть более строгими, чем те, которые традиционно используются в других областях, таких как журналистика и правозащитная деятельность. Независимо от цели расследования, придерживаясь изложенных в Протоколе методологических принципов, которые разработаны на основе общих правовых стандартов, лица, ведущие расследования с использованием открытых данных, обеспечат высокое качество своей работы и максимально расширят потенциальное использование собранной информации в судах, трибуналах и других процессах для обеспечения привлечения виновных к ответственности.

5. Кроме того, в Протоколе особое внимание уделяется стандартам расследования нарушений международного права, в том числе нарушений прав человека, и нарушений международного уголовного права, включая военные преступления, преступления против человечности и геноцид. Более того, рекомендации, содержащиеся в Протоколе, могут быть применены к другим видам расследований, в том числе для национальных или муниципальных судов.

6. В конечном счете Протокол призван помочь лицам, проводящим расследования с использованием открытых данных, осуществлять свою работу в соответствии с профессиональной методологией, которая в целом соответствует правовым требованиям и этическим нормам. Он также направлен на то, чтобы помочь различным «конечным пользователям» процесса расследования, включая адвокатов, судей и других лиц, принимающих решения, лучше понять и оценить методы расследования с использованием открытых данных. Протокол в равной степени предусматривается как ресурс для опытных практиков и как учебное и методическое пособие для тех, кто хочет научиться проводить расследования предполагаемых нарушений международного права с использованием открытых данных[5].

A. Цель

7. Хотя расследователи уже давно полагаются на открытые данные, их систематическое использование активизировалось в начале–середине XX века, когда основное внимание уделялось извлечению разведданных из иностранных радиопередач и печатных газет[6]. С появлением Всемирной паутины в 1990-х годах, а затем популяризацией социальных сетей и смартфонов в 2000-х годах количество и качество открытых данных резко изменилось. Сегодня любой человек, имеющий смартфон и доступ к Интернету, может создавать и распространять цифровой контент по всему миру, хотя и разного качества, разной степени истинности и прозрачности. Растущий объем данных и скорость, с которой они передаются и распространяются, создали новые возможности для лиц, проводящих расследования с использованием открытых данных, для сбора и анализа информации о международных преступлениях и нарушениях прав человека. В то же время создатели контента теперь могут распространять дезинформацию и манипулировать цифровыми данными с относительной легкостью. Протокол представляет собой попытку отреагировать на эту новую среду и сложности, связанные с такими возможностями и вызовами.

8. Открытые данные полезны во всех видах расследований, но они играют особенно важную роль в международных расследованиях уголовных преступлений и нарушений прав человека. Это верно по ряду причин. Во-первых, основанные на международном мандате расследования, в том числе проводимые комиссиями по расследованию и миссиями по установлению фактов Организации Объединенных Наций или санкционированные Международным уголовным судом, зависят

[4] Например, открытые данные использовались независимой международной миссией по установлению фактов относительно Мьянмы наряду с информацией из первоисточников и другой информацией в процессе проверки и в ее выводах и заключениях. Итоговый доклад независимой международной миссии по установлению фактов (A/HRC/42/50) стал одним из факторов, приведших к созданию Советом по правам человека Независимого механизма по расследованию для Мьянмы, которому был предоставлен мандат на проведение судебных расследований. Миссии по установлению фактов было также поручено передать имеющуюся у нее информацию, включая материалы расследований с использованием открытых данных, Независимому механизму по расследованию для Мьянмы. Кроме того, доклады миссии по установлению фактов использовались в иске, направленном в Международный Суд Гамбией против Мьянмы в связи с нарушением последней Конвенции о предупреждении преступления геноцида и наказании за него. Это демонстрирует, как информация, собранная для одной цели, может в конечном итоге способствовать другому юридическому процессу привлечения к ответственности.

[5] Кроме того, Протокол содержит несколько шаблонов для проведения расследований с использованием открытых данных, а также глоссарий (см. главу VIII ниже).

[6] Nikita Mehandru and Alexa Koenig, "ICTs, social media, & the future of human rights", Duke Law & Technology Review, vol. 17, No. 1, p. 129.

от правовых и политических процессов, позволяющих проводить расследования[7]. Таким образом, они часто проводятся спустя долгое время после событий. Во-вторых, часто структуры, проводящие международные расследования, могут не иметь доступа к физическому месту, где произошли расследуемые инциденты, например из-за отказа государства сотрудничать или предоставить доступ. В-третьих, даже в случае предоставления доступа в регион или на территорию для расследователей может быть ограничен физический доступ к интересующему их месту или они могут быть лишены возможности проводить расследования или личные опросы на месте из-за обеспокоенности по поводу защиты. Наконец, большинство расследователей не будут иметь полных правоохранительных полномочий на территориях, на которых произошли предполагаемые преступления или нарушения, и поэтому могут оказаться не в состоянии собрать необходимую информацию. Даже в случае сотрудничества государств трансграничный сбор доказательств может быть трудным процессом, замедленным в связи с обременительными бюрократическими процедурами. Все эти факторы показывают, почему методы расследования с использованием открытых данных, которые могут проводиться удаленно и осуществляться одновременно с происходящими событиями, являются действенными и необходимыми.

9. Протокол предназначен для разнообразной группы расследователей, работающих в различных условиях с различными мандатами, расследовательскими полномочиями и ресурсами. Поэтому в нем избран гибкий подход, который предполагает, что расследователи будут проводить свою работу не одинаково, а скорее станут при необходимости адаптировать методики для каждых уникальных условий работы. Более того, поскольку технологии, инструменты и методы, способствующие проведению расследований с использованием открытых данных, постоянно развиваются, в Протоколе сделан акцент не на конкретные инструменты, платформы, веб-сайты, программное обеспечение или источники, которые могут меняться, а на основополагающие принципы и процедуры, которыми следует руководствоваться при проведении расследований с использованием открытых данных.

10. Протокол задуман с целью стандартизации процедур и обеспечения методических указаний для различных расследований, учреждений и юрисдикций, чтобы помочь лицам, занимающимся расследованиями с использованием открытых данных, понять важность:

a) отслеживания происхождения онлайн-контента и по возможности указания его первоисточника;

b) оценки достоверности и надежности онлайн-источников;

c) проверки онлайн-контента и оценки его истинности и надежности;

d) соблюдения требований законодательства и этических норм;

e) минимизации любого риска причинения вреда себе, своим организациям и третьим лицам;

f) усиления защиты прав человека источников, включая право на неприкосновенность частной жизни.

B. Целевая аудитория

11. Целевая аудитория Протокола включает лиц и организации, которые выявляют, собирают, сохраняют и/или анализируют открытые данные для расследования международных преступлений или нарушений прав человека в целях обеспечения правосудия и привлечения к ответственности. К ним относятся следователи, юристы, архивисты и аналитики, работающие в международных, региональных и гибридных уголовных трибуналах; национальных подразделениях по расследованию военных преступлений; комиссиях по расследованию; миссиях по установлению фактов; независимых механизмах по расследованию; международных организациях; механизмах правосудия переходного периода; и неправительственных организациях (НПО). Другие лица, которые могут извлечь пользу, — это лица, работающие в различных международных и региональных механизмах, которые проводят судебные и квазисудебные расследования нарушений международного права с

[7] Комиссии по расследованию и миссии по установлению фактов, уполномоченные Организацией Объединенных Наций, были созданы, в частности, Советом Безопасности, Генеральной Ассамблеей, Советом по правам человека и Генеральным секретарем. Что касается Международного уголовного суда, то Канцелярия Прокурора может начать расследование по представлению государств-участников или Совета Безопасности, либо по собственной инициативе и с санкции судей.

использованием открытых данных[8]. Протокол может быть также познавателен для цифровых организаций оперативного реагирования, таких как общественные организации и независимые исследователи, которые часто первыми публикуют выводы, основанные на открытых данных, и чья работа часто играет ключевую роль в инициировании других официально санкционированных расследований с использованием открытых данных. Целевая аудитория включает также лиц и организации, которые оказывают помощь жертвам в подаче гражданских исков против отдельных лиц, совершивших преступление, или государств. Кроме того, Протокол может в целом помочь тем, кто формулирует фактические или юридические выводы на основе расследований с использованием открытых данных, позволяя им лучше оценить материалы любых расследований с использованием открытых данных, на которые они опираются или которые они анализируют.

12. Другие потенциальные заинтересованные стороны могут включать поставщиков услуг на базе Интернета, таких как платформы социальных сетей, которые хранят большие объемы данных и могут играть ключевую роль в сохранении данных, и разработчиков, которые предоставляют программное обеспечение для поддержки методов и процессов расследования с использованием открытых данных.

C. Определения

13. Для обеспечения практических стандартов и руководящих указаний для проведения расследований с использованием открытых данных следователи должны иметь общее понимание конкретных терминов. В данном разделе разъясняется ключевая терминология, используемая в Протоколе, включая различия между часто отождествляемыми понятиями[9].

1. Открытые данные и закрытые данные

14. Открытые данные включают в себя общедоступные данные, которые любой представитель общественности может наблюдать, приобретать или запрашивать, без необходимости наличия специального правового статуса или получения несанкционированного доступа. Закрытые данные — данные, доступ к которым ограничен или защищен законом[10], но которые могут быть получены законным путем по частным каналам, например в ходе судебных процессов, или предложены добровольно. Несмотря на простое определение, установить, что представляют собой открытые данные в контексте онлайн-контента, сложнее, чем кажется на первый взгляд. В Интернете растет объем данных, которые обнародуются без согласия их владельцев, например вследствие взлома, утечки, раскрытия из-за уязвимости системы безопасности или размещения третьей стороной без соответствующего разрешения. Хотя такие данные находятся в открытом доступе и, следовательно, технически считаются открытыми, тем не менее, могут существовать юридические и этические ограничения на некоторые виды их конечного использования. Кроме того, цифровая информация может быть доступна лицам со специальными техническими навыками и подготовкой, которые могут получить доступ к сетям и данным, которые недоступны или вряд ли будут доступны для обычного человека[11]. Одним из примеров является информация, которую можно получить только в дарквебе, а именно в той части Интернета, которая доступна только с помощью определенного программного обеспечения, такого как браузер Tor[12]. Хотя дарквеб обеспечивает анонимность, что делает его привлекательным местом для незаконной деятельности, использование браузера Tor и поиск в дарквебе является законным в большинстве стран. В Протоколе идет речь о данных в пределах «открытых источников» при условии отсутствия несанкционированного доступа к информации. Самое явное различие заключается в том,

[8] См., например, сообщения и доклады о посещениях специальных процедур Совета по правам человека. Размещены по адресу: www.ohchr.org/ru/special-procedures-human-rights-council. См. также работу комитетов по санкциям, созданных Советом Безопасности. URL: www.un.org/securitycouncil/ru/content/repertoire/sanctions-and-other-committees.

[9] Более подробную подборку соответствующих терминов и определений см. в главе VIII.

[10] Например, конфиденциальная информация и секретная информация.

[11] Некоторые действия могут нарушать условия оказания веб-сайтом услуг, но сами по себе не являются незаконными. Например, нарушение условий оказания веб-сайтом услуг с целью извлечения данных является несанкционированным поведением и может повлечь за собой запрет на его использование.

[12] Дарквеб относится к той части Интернета, доступ к которой возможен только с помощью специализированного программного обеспечения. Браузер Tor является одним из примеров такого программного обеспечения.

что открытые данные не предполагают взаимодействия с отдельными пользователями Интернета или запрашивания у них информации[13]. Получение данных от других пользователей Интернета посредством общения с ними считается закрытым источником.

15. Открытые цифровые данные[14] — это данные из открытых источников в Интернете, доступ к которым можно получить, например, на публичных веб-сайтах, из онлайн-баз данных или на платформах социальных сетей. Ниже перечислены различные способы получения данных из открытых источников.

2. Получение открытых цифровых данных

a) Наблюдение

16. Контент на многих платформах можно получить, просто перейдя на соответствующий сайт с помощью любого из бесплатных веб-браузеров. Другие онлайн-платформы требуют от пользователей входа в аккаунт или регистрации для доступа и просмотра контента. Такой контент считается открытым, если эти процессы открыты для всех пользователей в юрисдикциях, в которых доступ к ним легален, и при доступе или просмотре не нарушается конфиденциальность или меры безопасности. Однако некоторые материалы, отвечающие этому определению, не могут считаться открытыми данными, например конфиденциальная, секретная или иным образом защищенная законом информация. В таких случаях, хотя информация доступна любому представителю общественности, ее использование в качестве доказательства в судебном процессе может быть ограничено. Кроме того, могут возникнуть этические или методологические проблемы при использовании таких материалов, например невозможность атрибутировать или проверить их содержание.

b) Приобретение

17. Некоторые источники данных для расследований с использованием открытых данных находятся на платформах, требующих оплаты или использующих комбинированную бесплатную и премиальную модель, в которой дополнительные функции и доступ к данным предоставляются за плату. Растет число компаний, которые агрегируют общедоступные данные и предлагают как бесплатные, так и платные сервисы для доступа к ним. Большая часть информации, которую лица, проводящие расследования с использованием открытых данных, найдут полезной, находится в базах данных и на платформах, доступных только за плату. Для целей Протокола открытые данные включают платные сервисы, доступные всем представителям общественности, но не сервисы, доступ к которым имеют только определенные группы, такие как сотрудники правоохранительных органов или лицензированные частные детективы.

c) Запрос

18. В данном контексте термин «запрос» относится к запросам, которые могут быть сделаны любым лицом для получения общедоступной информации от государственных учреждений в соответствии с законами о свободе информации или доступе к информации. Он не относится к запросам к частным лицам, компаниям или организациям о добровольной передаче их информации, а ограничивается запросами к государственным структурам, которые имеют юридические обязательства отвечать одинаковым образом всем лицам. Расследования с использованием открытых данных могут привести к другим расследовательским действиям в Интернете, таким как взаимодействие с внешними источниками с использованием служб обмена сообщениями, чатов, форумов или электронной почты. Такое взаимодействие выходит за рамки расследований с использованием открытых данных, рассматриваемых в Протоколе.

3. Разведывательные данные из открытых источников

19. Разведывательные данные из открытых источников относятся к подкатегории открытых данных, которые собираются и используются с конкретной целью оказания помощи в разработке политики и принятии решений, чаще всего в военном или политическом контексте. В то время как открытые данные включают всю общедоступную информацию, которую любой человек может получить законным путем, разведданные из открытых источников — это разновидность

[13] Хотя приобретение информации из частной базы данных или подача запроса на информацию в государственное учреждение требуют определенной степени онлайн-обмена, часто это автоматизированный процесс, который отличается от описанного здесь типа взаимодействия с другими индивидуальными пользователями Интернета.

[14] В Протоколе открытые данные могут также называться онлайн-контентом, онлайн-материалами или онлайн-данными.

такой информации, «которая своевременно собирается, используется и распространяется среди соответствующей аудитории с целью удовлетворения конкретной потребности в разведданных»[15]. В контексте международных уголовных дел и дел о нарушениях прав человека разведданные из открытых источников используются в качестве исходной информации для принятия решений — например, для содействия деятельности, связанной с обеспечением безопасности, такой как защита свидетелей и членов группы, которые выезжают на место, или отслеживание лиц, представляющих интерес, — а не для сбора информации, связанной с процессом расследования, например установления состава различных преступлений.

4. Расследование с использованием открытых данных

20. Расследование с использованием открытых данных означает использование данных из открытых источников для сбора информации и доказательств.

5. Открытые данные в качестве доказательства

21. Термин «доказательство» следует отличать от термина «информация»[16]. Доказательства обычно определяются в разных юрисдикциях как подтверждение факта (фактов), используемое в расследовании или представленное на слушании, например в суде. Открытые данные в качестве доказательства — это информация из открытых источников, которая имеет доказательную силу и может быть принята для установления фактов в ходе судебного разбирательства. Важно не злоупотреблять термином «доказательство» и не использовать его чрезмерно, когда речь идет об «информации» в целом.

6. Открытые данные и открытое программное обеспечение

22. Термин «открытое/открытый» часто используется для описания программного обеспечения или кода, которые свободно доступны для использования и переиздания без ограничений, предусмотренных авторским правом, патентами или другими правовыми механизмами контроля. Открытое программное обеспечение создается из исходного кода, который любой человек, имеющий доступ, может изучить, изменить и усовершенствовать[17]. Он обычно не виден пользователям, но может быть скорректирован и адаптирован программистом. Открытое программное обеспечение отлично от открытых данных, хотя открытое программное обеспечение и инструменты часто используются лицами, ведущими расследования с использованием открытых данных, для поиска, сбора, сохранения и анализа открытой информации.

7. Достоверность и надежность

23. Когда речь идет о свидетельских показаниях в международных уголовных процессах, судьи оценивают «достоверность показаний свидетеля» и «надежность его или ее показаний»[18]. При проведении расследований комиссиями по расследованию и миссиями по установлению фактов Организации Объединенных Наций и аналогичных расследований руководство предусматривает, что «лицо, проводящее опрос, должно оценить достоверность и надежность показаний опрашиваемого»[19]. В руководстве уточняется, что «при оценке учитывается относимость информации к предмету расследования. В нем также рассматривается надежность источника и правдивость или правильность информации»[20]. В Протоколе эти термины используются следующим образом:

a) «достоверность» означает правдоподобность или убедительность;

b) «надежность» означает способность делать что-либо последовательно, стабильно или в соответствии с ожиданиями;

c) «истинность» или «правдивость» означает точность, правильность или соответствие фактам.

---

15 National Open Source Enterprise, Intelligence Community Directive No. 301, 11 July 2006, p. 8 (сноска опущена).

16 Federica D'Alessandra and others, eds., *Handbook on Civil Society Documentation of Serious Human Rights Violations: Principles & Best Practices* (The Hague, Public International Law and Policy Group, 2016), p. 17.

17 См. Opensource.com, "What is open source?".

18 International Criminal Court, *Prosecutor v. Bosco Ntaganda*, Case No. ICC-01/04-02/06, Judgment of 8 July 2019, para. 53.

19 OHCHR, *Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law: Guidance and Practice* (New York and Geneva, 2015), p. 52. URL: www.ohchr.org/Documents/Publications/CoI_Guidance_and_Practice.pdf.

20 Ibid., p. 59.

II

Принципы

КРАТКОЕ СОДЕРЖАНИЕ ГЛАВЫ

- **Для соблюдения профессиональных принципов, касающихся расследований с использованием открытых цифровых данных, расследователи должны нести ответственность за свои действия, быть компетентными и объективными и выполнять свою работу в соответствии с законом и с должным учетом соображений безопасности.**
- **Расследователи должны также продумывать методы, которые они используют на всех этапах расследования. Соответствующие методологические принципы включают по крайней мере точность, минимизацию данных, сохранение данных и встроенные меры безопасности.**
- **Наконец, всем лицам, проводящим расследования, следует руководствоваться этическими соображениями. К ним относятся как минимум защита достоинства всех лиц, участвующих в расследовании или вовлеченных в него, а также обеспечение самокритичности, инклюзивности, независимости и прозрачности.**

24. В то время как технологии, инструменты и методы, применяемые в расследованиях с использованием открытых данных, будут меняться, определенные всеобъемлющие методологические и этические принципы должны сохраниться. Определение таких принципов является важным шагом на пути к профессионализации области расследований с использованием открытых данных. Следующие принципы являются основополагающими в обеспечении качества расследований с использованием открытых данных, что, в свою очередь, повысит достоверность, надежность и потенциальную полезность их результатов для целей привлечения виновных к ответственности и минимизации потенциального ущерба для различных заинтересованных сторон.

A. Профессиональные принципы

1. Ответственность

25. Лица, проводящие расследования с использованием открытых данных, должны нести ответственность за свои действия, что часто может быть обеспечено с помощью подробной документации, ведения учета и надзора. Прозрачность методов и процедур расследования является важным элементом обеспечения подотчетности. Таким образом, насколько это возможно и целесообразно, лицам, проводящим расследования с использованием открытых данных, следует вести учет своей деятельности. Этапы расследования с использованием открытых данных — от выявления соответствующих материалов до сбора, анализа и составления отчета — следует последовательно и четко документировать. Любым лицам, занимающимся сбором или обработкой онлайн-информации, необходимо знать о том, что их методы могут стать предметом изучения, включая возможность вызова для дачи показаний в суде. Документирование расследований с использованием открытых данных может выполняться вручную или с помощью автоматизированных процессов, предоставляемых различным программным обеспечением. При условии, что документация является последовательной и достаточно подробной, можно использовать как неавтоматизированные, так и автоматизированные методы. Автоматизированные процессы и программное обеспечение должны быть понятны пользователям, и пользователи или разработчики должны уметь объяснить их в суде. Кроме того, лицам, проводящим расследования с использованием открытых данных, следует вести записи обо всех инструментах и программном обеспечении, которые используются в ходе работы.

2. Компетенция

26. Лица, проводящие расследования с использованием открытых данных, должны иметь соответствующую подготовку и технические навыки для осуществления деятельности, которой они занимаются. Они должны вести онлайн-деятельность профессионально и этично: избегать присвоения чужой работы; указывать всех участников расследования (когда это безопасно и когда этого хотят сами участники); и точно представлять данные, включая признание любых пробелов, которые могут существовать в онлайн-контенте. Лица, проводящие расследования с использованием открытых данных, и процессы таких расследований также должны оставаться гибкими, расследователи должны следить за новыми разработками и внедрять новые технологии и методы по мере необходимости. Кроме того, организации и расследовательские группы должны располагать механизмами для обеспечения последовательного внедрения и соблюдения процедур.

3. Объективность

27. Объективность — это основополагающий принцип, который применяется ко всем расследованиям, будь то онлайн или офлайн. Лицам, проводящим расследования с использованием открытых данных, следует понимать возможность влияния личных, культурных и структурных предубеждений на их работу и необходимость принятия контрмер для обеспечения объективности. Такие лица должны убедиться, что они подходят к своим расследованиям объективно, разрабатывая и развивая несколько рабочих гипотез и не отдавая предпочтение какой-либо конкретной теории для объяснения обстоятельств дел. Для расследований с использованием открытых данных, проводимых онлайн, объективность особенно важна в связи тем, как структурируется информация в Интернете и предоставляется пользователям. Используемые браузер, поисковая система, поисковые запросы и синтаксис могут привести к совершенно разным результатам, даже если исходная поисковая задача одна и та же. Предвзятость, присущая архитектуре Интернета и алгоритмам, используемым поисковыми системами и веб-сайтами, может угрожать объективности результатов по-

иска[21]. На результаты поиска также может влиять ряд технических факторов, включая используемое устройство и его местоположение, а также предыдущая история поиска и активность пользователя в Интернете. Лицам, проводящим расследования с использованием открытых данных, следует уравновешивать такие предубеждения, применяя методики, обеспечивающие максимальное разнообразие результатов поиска, например выполняя несколько поисковых запросов и используя различные поисковые системы и браузеры[22]. Им следует знать, что на результаты поиска могут влиять и другие факторы, в том числе перекосы цифровой среды, когда онлайн-информация может неравномерно поступать от определенных групп или слоев общества[23]. Наконец, они всегда должны стремиться понимать и корректировать свои собственные предубеждения, которые могут быть как осознанными, так и неосознанными[24].

4. Законность

28. Лицам, проводящим расследования с использованием открытых данных, следует соблюдать действующее законодательство, что означает, что им необходимо иметь базовое представление о законах, применимых к их работе. В частности, им следует знать о законах о защите данных и праве на неприкосновенность частной жизни, которое защищено международным правом прав человека[25]. Даже если информация может быть общедоступной, это не означает, что ее сбор и использование не влияют на неприкосновенность частной жизни. Лица, проводящие расследования с использованием открытых данных, должны учитывать последствия своих действий для конфиденциальности, включая разумные ожидания лиц в отношении конфиденциальности в различных цифровых пространствах. Им следует также помнить об «эффекте мозаики», когда открытые данные, даже анонимизированные,

21 См. Safiya Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York, New York University Press, 2018); Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York, Picador, 2019).

22 См., например, Paul Myers, "How to conduct discovery using open source methods", in *Digital Witness, Using Open Source Information for Human Rights Investigation, Documentation and Accountability*, Sam Dubberley, Alexa Koenig and Daragh Murray, eds. (Oxford, Oxford University Press, 2020) (обсуждение того, как выбор поисковых систем и поисковых запросов может исказить результаты расследований с использованием открытых данных).

23 См., например, Alexa Koenig and Ulic Egan, "Hiding in plain site: using online open source information to investigate sexual violence and gender-based crimes", in *Technologies of Human Rights Representation*, James Dawes and Alexandra S. Moore, eds. (готовится к изданию) (обсуждение того, как относительно ограниченный доступ к смартфонам у женщин и использование закодированного языка в Интернете жертвами сексуального и гендерного насилия может снизить количество и доступность открытых данных, касающихся таких преступлений, а также того, как преобладание мужчин на должностях, связанных с информационными технологиями, и среди следователей по делам о военных преступлениях может негативно повлиять на вероятность того, что автоматизированные и/или неавтоматизированные процессы выявления дадут открытые данные, связанные с гендерными преступлениями). Более подробную информацию о предвзятости см. в главе II.C ниже об этических принципах и главе V.B ниже об оценке цифровой среды.

24 См., например, Forensic Science Regulator, *Cognitive Bias Effects Relevant to Forensic Science Investigations*, *FSR-G-217* (Birmingham, United Kingdom, 2015) (обсуждение различных категорий когнитивных предубеждений, которые могут негативно повлиять на качество расследования, включая влияние ожидания, предпочтение информации, подтверждающей сложившуюся точку зрения, эффект привязки, ситуативные предубеждения, а также эффекты роли и реконструкции); Wayne A. Wallace, *The Effect of Confirmation Bias on Criminal Investigative Decision Making* (Minneapolis, Walden University ScholarWorks, 2015) (объяснение предпочтения информации, подтверждающей сложившуюся точку зрения, как процесса, в ходе которого следователи ищут информацию, которая поддерживает их предпочтительную гипотезу, «игнорируя или отвергая не подтверждающие ее доказательства», и доверяют ей); Michael Pittaro, "Implicit bias within the criminal justice system", Psychology Today, 21 November 2018 (обсуждение предубеждений, которые могут влиять на уголовные расследования в целом, и предложение известных методов развенчания предубеждений); Jon S. Byrd, "Confirmation bias, ethics, and mistakes in forensics", Forensic Pathways, 21 March 2020 (обсуждение различных когнитивных и этических ошибок, которые могут исказить результаты судебной экспертизы, а также методов избегания таких ошибок). См. также Yvonne McDermott, Daragh Murray and Alexa Koenig, "Digital accountability symposium: whose stories get told, and by whom? Representativeness in open source human rights investigations", Opinio Juris, 19 December 2019 (обсуждение того, как методы расследований с использованием открытых данных могут негативно повлиять на «типы нарушений, о которых сообщается, на жертв и свидетелей, которые получают возможность высказаться, и на то, как строится изложение массовых нарушений прав человека»); и проект под руководством Ивонн МакДермотт под названием "The future of human rights investigations: using open source intelligence to transform the documentation and discovery of human rights violations" («Будущее расследований по правам человека: использование разведданных из открытых источников для преобразования документов и выявления нарушений прав человека»).

25 Статья 12 Всеобщей декларации прав человека предусматривает, что никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств. Международный пакт о гражданских и политических правах предусматривает в статье 17, что никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию. В статье 17 также говорится, что каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств.

могут быть повторно идентифицированы, если существует достаточно опубликованных или объединенных наборов данных, содержащих аналогичную или дополнительную информацию[26]. Кроме того, расследователям необходимо знать, что в некоторых юрисдикциях постоянный и непрерывный мониторинг лиц в Интернете или систематический сбор и долгосрочное хранение персональных данных могут потребовать дополнительных разрешений и гарантий в связи с повышенной озабоченностью по поводу конфиденциальности в связи с такой деятельностью[27].

5. Знание и понимание мер безопасности

29. В то время как встроенные меры безопасности[28] касаются структуры и инфраструктуры расследования и любых сопутствующих мероприятий, в основе принципа знания и понимания мер безопасности лежат соображения, которые лица должны принимать во внимание в ходе своей работы, в частности осведомленность о своем поведении в сети. Всем лицам, проводящим расследования в Интернете, необходимо обладать базовыми знаниями в области оперативной безопасности, чтобы минимизировать свой цифровой след и знать о потенциальных рисках. Организациям, проводящим расследования с использованием открытых данных, следует обеспечить прохождение их расследователями обучения по информационной безопасности, чтобы они понимали риски, с которыми они могут столкнуться, и чтобы они имели представление о трех основных столпах информационной безопасности: a) конфиденциальность (например, предоставление доступа к данным только разрешенным пользователям); b) целостность (гарантия того, что данные не будут подделаны или иным образом изменены неавторизованными пользователями); и c) доступность (обеспечение доступности систем и данных для авторизованных пользователей, когда они им нужны). В рамках обучения также следует уделять внимание структуре регулирования Интернета. Оценки угроз и рисков следует проводить до начала расследования в Интернете и периодически пересматривать и корректировать по мере необходимости. Безопасность — это ответственность каждого, а не только подразделений информационных технологий или менеджеров по управлению рисками в области безопасности.

B. Методологические принципы

1. Точность

30. Существует методологическая и этическая необходимость обеспечивать точность — и, следовательно, качество — расследований посредством использования в них только достоверных материалов. Лицам, проводящим расследования с использованием открытых данных, следует стремиться быть максимально правдивыми и точными в ходе своих расследований и при представлении любых результатов, особенно когда речь идет о признании слабых мест в исходных данных или в деле в целом. Зачастую точность можно повысить за счет использования и проверки нескольких рабочих гипотез и/или экспертной оценки, что помогает минимизировать вероятность необъективного отбора, интерпретации и представления данных. Следует избегать преувеличений и гипербол в аналитических выводах. Использование четких, объективных, основанных на фактах формулировок и отказ от эмоциональных высказываний обеспечит фактическую и воспринимаемую объективность расследования и его результатов.

---

[26] «Понятие "эффект мозаики" заимствовано из мозаичной теории сбора разведданных, в которой разрозненные фрагменты информации — хотя по отдельности они имеют ограниченную полезность — становятся значимыми в сочетании с другими видами информации (Pozen 2005). Применительно к данным общественного пользования концепция эффекта мозаики предполагает, что даже анонимизированные данные, которые могут казаться не представляющими опасности в отдельности, могут быть повторно идентифицированы, если будет опубликовано достаточное количество наборов данных, содержащих аналогичную или дополнительную информацию». См. John Czajka and others, *Minimizing Disclosure Risk in HHS Open Data Initiatives* (Washington, D.C., Mathematica Policy Research, 2014), appendix E, p. E-7. URL: https://aspe.hhs.gov/system/files/pdf/77196/rpt_Disclosure.pdf. См. также David E. Pozen, "The mosaic theory, national security, and the Freedom of Information Act", *Yale Law Journal*, vol. 115, No. 3 (December 2005), pp. 628–679.

[27] Например, в Соединенном Королевстве Великобритании и Северной Ирландии закон предписывает, что «персональные данные, обрабатываемые для... правоохранительных целей, должны храниться не дольше, чем это необходимо для целей, для которых они обрабатываются» (Chapter 12 of the Data Protection Act 2018, part 3, chap. 3, sect. 39 (1)). Согласно Регламенту 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/EC (Общий регламент о защите персональных данных/General Data Protection Regulation/GDPR), персональные данные могут собираться только для «определенных, явных и законных целей», должны ограничиваться информацией, необходимой для целей, для которых они собираются, и должны оставаться идентифицируемыми только до тех пор, пока это необходимо для целей сбора (статьи 5–6).

[28] См. пункт 33 ниже.

2. Минимизация данных

31. Принцип минимизации данных предписывает, что сбор и обработку цифровых данных следует осуществлять только в том случае, если это: a) оправдано для четко сформулированной цели; b) необходимо для достижения этой цели; и c) пропорционально возможности выполнения этой цели[29]. В контексте расследований с использованием открытых данных онлайн-контент следует собирать только в том случае, если он имеет отношение к конкретному расследованию. Согласно этому принципу, предпочтение отдается детализированному, ручному, а не массовому, автоматизированному сбору, хотя и отмечается, что последний может быть уместен в некоторых случаях. Применение этого принципа к сбору онлайн-контента поможет избежать сбора избыточного объема данных, что важно по нескольким причинам. Сбор избыточного объема данных — что особенно важно при использовании автоматизированных процессов сбора информации — может повлечь или усугубить уязвимость системы безопасности[30], в частности если это приведет к тому, что лица, проводящие расследование, не будут знать о типах информации, находящейся в их распоряжении. Сбор избыточного объема данных может также вызвать проблемы в плане конфиденциальности и защиты данных, если автоматизированный процесс не различает тип контента. Наконец, предотвращение сбора избыточного объема данных служит практическим целям минимизации затрат на хранение данных и предупреждения помех на дальнейших этапах расследования, таких как рассмотрение, анализ и, в случае если расследование приводит к судебному разбирательству, раскрытие информации.

3. Сохранение

32. Предотвратить сбор недостаточного объема данных так же важно, как и избежать сбора избыточного объема соответствующей информации. Это может быть особенно значимо в контексте онлайн-информации, постоянство и доступность которой зачастую нестабильны. Цель принципа сохранения заключается в предупреждении сбора недостаточного объема данных, чтобы не допустить утраты значимых и потенциально убедительных доказательств. Платформы социальных сетей, например, могут удалить контент, нарушающий их условия предоставления услуг, даже если этот контент имеет потенциальную ценность для расследователей. Если платформе не будет направлен своевременный запрос о сохранении или контент не будет сохранен иным образом лицами, проводящими расследование, такая информация может быть утрачена навсегда. Кроме того, пользователи могут удалить или отредактировать свой собственный контент, сделав некогда общедоступную информацию недоступной. Помимо этого, информация в Интернете может быть легко деконтекстуализирована, утрачена, стерта или повреждена. Для того чтобы цифровые материалы оставались доступными и пригодными для использования в будущих механизмах привлечения к ответственности, их необходимо активно и тщательно сохранять как краткосрочно, так и долгосрочно[31].

4. Встроенные меры безопасности

33. Принцип применения встроенных мер безопасности требует, чтобы, насколько это возможно, цифровая информация и онлайн-операции были безопасными по умолчанию. Организациям, проводящим расследования с использованием открытых цифровых данных, следует осуществлять инвестиции в соответствующие технические и структурные меры для обеспечения того, чтобы по умолчанию инфраструктура — включая оборудование и программное обеспечение — была надлежащим образом анонимизирована и не могла быть атрибутирована, когда расследователи выходят в Интернет, и внедрять их. Все оборудование должно иметь актуальное программное обеспечение для защиты от вредоносных программ, а также соответствующие настройки конфиденциальности и безопасности. Меры безопасности следует принимать до начала расследования в Интернете; их следует постоянно контролировать,

[29] В Протоколе принцип минимизации данных заимствован из Общего регламента Европейского союза о защите персональных данных и адаптирован к контексту расследований с использованием открытых данных (см. статью 5 Регламента).

[30] Примеры уязвимостей в области безопасности см. ниже в главе IV о безопасности.

[31] Более подробную информацию см. ниже в главе VI.D о сохранении.

обновлять и корректировать по мере необходимости. Расследователи, расследовательские группы или организации могут пожелать организовать непрерывное тестирование, включая тестирование на проникновение[32], чтобы убедиться, что их системы безопасности работают согласно замыслу.

C. Этические принципы

1. Достоинство

34. Расследования следует проводить с осознанием и учетом любых основных вопросов, касающихся уважения достоинства, особенно тех интересов, которые защищены международным правом прав человека. Например, лицам, проводящим расследования, следует придерживаться принципов недискриминации, которые могут повлиять на предмет расследования, а также на то, кто занимается расследовательской работой или кто считается автором расследования, а также предусматривать гарантии, касающиеся цифровой, физической и психосоциальной безопасности свидетелей, пострадавших, других лиц, проводящих расследование, обвиняемых, а также прочих лиц, на которых оно может негативно отразиться. Соблюдение принципа достоинства может также повлиять на то, какая информация о расследовании сообщается общественности, в том числе в письменном виде и в любых визуальных форматах: например, не следует показывать всю степень страданий или насилия, если в этом нет необходимости. Этот принцип гарантирует, что нормы прав человека являются сводом руководящих стандартов для проведения этичных расследований с использованием открытых данных.

2. Самокритичность

35. Лицам, проводящим расследования с использованием открытых данных, необходимо быть самокритичными, признавать собственные ограничения и осознавать пробелы в своих знаниях. Для правильного понимания и интерпретации открытых данных может потребоваться специальная подготовка или консультации с экспертами. Самокритичность означает также принятие ответственности за ошибки. Если лица, проводящие расследование, обнаруживают, что допустили ошибку, ее следует исправить или сообщить о ней тем, кто может минимизировать причиненный вред. В идеале должен существовать механизм сообщения об ошибках и внесения исправлений, особенно для расследований, которые являются публичными и информация о которых широко распространена.

3. Инклюзивность

36. Лица, проводящие расследования с использованием открытых данных, должны обеспечить учет различных точек зрения и опыта при проведении расследований. Необходимо принимать во внимание факторы, которые могут повлиять на общую инклюзивность онлайн-расследования, включая его географический охват, расследуемые нарушения и/или международные преступления и осознание неоднородности онлайн-информации в отношении различных слоев общества[33]. Состав следственных групп также должен быть разнообразным, что включает обеспечение гендерного баланса. Кроме того, принцип инклюзивности, наряду с принципом достоинства, может повлиять на то, какие материалы лицо, проводящее расследование, решит собрать и использовать в расследовании и как они будут представлены различным аудиториям.

4. Независимость

37. Лицам, проводящим расследования с использованием открытых данных, следует защищать себя и свои расследования от ненадлежащего влияния. Им следует выявлять любые реальные или предполагаемые конфликты интересов и избегать их, а также внедрять гарантии для смягчения тех конфликтов, которых избежать невозможно. Прозрачность процесса, методов и финансирования может помочь в оценке независимости и защитить фактическую и ощущаемую независимость расследования.

[32] Тест на проникновение — это имитация кибератаки, которая санкционирована с целью проверки безопасности системы.

[33] См. ниже в главе V.B об оценке цифровой среды.

5. Прозрачность

38. В то время как принцип ответственности требует прозрачности методов и результатов расследования, этический принцип прозрачности касается того, как лица, проводящие расследования с использованием открытых данных, ведут себя в Сети и по отношению к внешнему миру. Это означает необходимость избегать выдачи себя за другое лицо[34]. Хотя анонимность и отсутствие атрибуции — включая использование виртуальных личностей[35] — могут быть важны с точки зрения безопасности, лицам, проводящим расследование, следует знать о возможных негативных последствиях выдачи себя за другое лицо, таких как нанесение ущерба репутации и авторитету расследования, группы или организации, или же подрыв доверия к собранной информации. Получение информации путем выдачи себя за другое лицо, может нарушить право человека, являющегося объектом расследования, на неприкосновенность частной жизни и/или повредить расследованию, особенно если выдача себя за другое лицо является незаконной в соответствующей юрисдикции (соответствующих юрисдикциях).

[34] Например, пытаясь вступить в закрытые группы или завести связи в социальных сетях под ложным предлогом.

[35] Вопрос виртуальных личностей рассматривается ниже в главе IV.C о соображениях, касающихся инфраструктуры.

III

ПРАВОВАЯ ОСНОВА

КРАТКОЕ СОДЕРЖАНИЕ ГЛАВЫ

- **Определение того, какие законы применяются, имеет решающее значение для принятия решения о том, что собирать и какими способами. Это будет зависеть от личности расследователей, личности объектов расследований, цели их расследований и юрисдикций, в которых находятся они, объекты, данные и осуществляются правовые процедуры.**
- **Сохранение цифровых материалов с поддержанием их подлинности и документированием цепочки обеспечения их сохранности повышает вероятность того, что они могут быть допущены в качестве доказательства в суде.**
- **Определение типа расследования и его конечной цели (например, уголовный процесс, гражданское судопроизводство, процесс правосудия переходного периода и др.) обусловит требования к доказательствам, которые должны быть применены.**
- **Нарушение права человека на частную жизнь может привести к исключению доказательств.**

39. Лица, проводящие расследования с использованием открытых данных, должны понимать правовые рамки, в которых они работают. Сюда относятся применимые нормы права, затрагивающие их расследования, и правовая база юрисдикций, в которых они проводят расследовательские действия. Знание материального права, применимого к расследованиям, включая элементы состава потенциальных нарушений[36] или преступлений, а также формы ответственности[37], может способствовать проведению более целенаправленных расследований и повысить вероятность того, что собранная информация и любые сделанные аналитические выводы будут полезны в усилиях по обеспечению правосудия и привлечению к ответственности. Аналогичным образом знание процессуального права и норм доказательственного права в соответствующих юрисдикциях позволит расследователям вести свою работу в соответствии с требованиями к использованию открытых данных в судебных разбирательствах.

40. Для международных уголовных расследований правовые рамки будут предписаны нормативными документами соответствующего трибунала, суда или судебной системы[38]. Для расследований, проводимых в соответствии с международным мандатом, например комиссиями по расследованию, механизм, учреждающий расследование, будет определять, среди прочих факторов, применимые своды правовых норм и географические и временные рамки расследования[39]. Для других расследований, включая расследования, проводимые НПО, организация, проводящая расследование, сама может определить свою правовую базу[40].

41. Настоящая глава была разработана для того, чтобы помочь лицам, проводящим расследования с использованием открытых данных, лучше оценить и понять потенциальное конечное использование их работы и соответствующим образом адаптировать свои методы расследования. Поскольку применимые законы различаются в зависимости от юрисдикции, типа расследования и правовых полномочий органа, проводящего расследование, в следующих разделах представлен обзор основных факторов, которые необходимо принять во внимание при расследовании потенциальных нарушений международного права. Лицам, проводящим расследования, рекомендуется, где это возможно, получать экспертную юридическую консультацию у юристов, знакомых с соответствующими юрисдикциями и предметом расследования.

---

[36] Например, при расследовании случаев ненавистнических высказываний и подстрекательства к насилию расследователи должны понимать, какого рода поведение достигает высокого порога, предусмотренного статьей 20 (пункт 2) Международного пакта о гражданских и политических правах. См. Рабатский план действий по запрещению пропаганды национальной, расовой или религиозной ненависти, представляющей собой подстрекательство к дискриминации, вражде или насилию (A/HRC/22/17/Add.4, приложение), пп. 11 и 29, и изложенный в нем правозащитный пороговый тест, доступный на 32 языках. URL: www.ohchr.org/ru/freedom-of-expression. О языке ненависти см. Стратегию и План действий Организации Объединенных Наций по борьбе с языком ненависти (2019). URL: www.un.org/en/genocideprevention/hate-speech-strategy.shtml.

[37] В уголовном праве виновные могут быть привлечены к ответственности на основании ряда форм ответственности, определенных соответствующим законом. Такие формы ответственности включают прямое и косвенное совершение преступления, соучастие, пособничество и подстрекательство, а также ответственность лиц, отдающих приказы. См. Jérôme de Hemptinne, Robert Roth and Elies van Sliedregt, eds., *Modes of Liability in International Criminal Law* (Cambridge, United Kingdom, Cambridge University Press, 2019).

[38] См., например, Международный уголовный суд, Правила процедуры и доказывания (2013 год); Международный трибунал по бывшей Югославии, Правила процедуры и доказывания (8 июля 2015 года); Международный уголовный трибунал по Руанде, Правила процедуры и доказывания (13 мая 2015 года); Остаточный Специальный суд по Сьерра-Леоне, Правила процедуры и доказывания (30 ноября 2018 года); Специальный трибунал по Ливану, Правила процедуры и доказывания (10 апреля 2019 года); Чрезвычайные палаты в судах Камбоджи, Внутренние правила (3 августа 2011 года).

[39] Например, независимая международная миссия по установлению фактов в Боливарианской Республике Венесуэла, которая была создана в сентябре 2019 года, уполномочена расследовать внесудебные казни, насильственные исчезновения, произвольные задержания и пытки и другие жестокие, бесчеловечные или унижающие достоинство виды обращения за период с 2014 года и представить Совету доклад о результатах своей работы (резолюция 42/25 Совета по правам человека, п. 24). Независимая международная комиссия по расследованию событий в Сирийской Арабской Республике, которая была создана в 2011 году, уполномочена расследовать все предполагаемые нарушения международного права прав человека, имевшие место в Сирийской Арабской Республике в период с марта 2011 года, установить факты и обстоятельства таких нарушений и совершенных преступлений и по возможности выявить виновных (резолюция Совета по правам человека S-17/1, п. 13). Международной группе экспертов, направленной в регион Касаи Демократической Республики Конго в 2017 году, было поручено собрать и сохранить информацию о предполагаемых нарушениях и ущемлениях прав человека и нарушениях международного гуманитарного права в регионах Касаи и препроводить судебным властям Демократической Республики Конго выводы по итогам этого расследования (резолюция 35/33 Совета по правам человека, п. 10).

[40] Некоторые организации, включая НПО, часто имеют свои внутренние методологии, которые предписывают им сосредотачиваться на определенной области права, например касающейся пыток или сексуального и гендерного насилия, и которые будут также содержать указания относительно направленности расследований.

A. Международное публичное право

42. В Протоколе основное внимание уделяется трем категориям международного публичного права, которые во многом пересекаются друг с другом: международному гуманитарному праву, международному праву прав человека и международному уголовному праву. Эти три категории взаимодополняют друг друга; действительно, применимость международного гуманитарного права и/или международного уголовного права не освобождает государства от выполнения своих обязательств по международному праву прав человека. Ниже приводится обзор каждой области практики, включая источники права и различия между областями практики, чтобы лица, проводящие расследования с использованием открытых данных, знали, чем следует руководствоваться в своей работе.

1. Международное гуманитарное право

43. Международное гуманитарное право, или «право вооруженных конфликтов», регулирует ведение боевых действий и решает гуманитарные вопросы, возникающие в контексте таких конфликтов, которые могут быть международными или немеждународными по своему характеру[41]. Международное гуманитарное право вступает в действие с началом вооруженного конфликта и действует до достижения мира, хотя эти границы не всегда однозначны и ясны[42]. Основными источниками международного гуманитарного права являются Гаагские конвенции 1899 и 1907 годов[43], Женевские конвенции от 12 августа 1949 года[44] и Дополнительные протоколы к ним 1977 года[45], а также несколько договоров, регулирующих применение определенных видов оружия[46]. Обычное право также является важным источником международного гуманитарного права, поскольку оно заполняет пробелы, оставленные договорами. Обычное международное гуманитарное право имеет обязательную силу для всех сторон конфликта и особенно актуально для немеждународных вооруженных конфликтов, поскольку связанные с ним нормы более детализированы, чем нормы международного гуманитарного права, основанного на договорах[47]. До начала 1990-х годов главными механизмами применения международного гуманитарного права были национальные военные трибуналы, в которых государства привлекали к ответственности своих рядовых и офицеров. С воз-

41 Различие между международным и немеждународным вооруженным конфликтом основано на двух факторах: структуре и статусе вовлеченных сторон. В международных вооруженных конфликтах участвуют суверенные государства. В немеждународных вооруженных конфликтах, напротив, участвуют государства и организованные вооруженные группы. См. Andrew Clapham, Paola Gaeta and Marco Sassòli, eds., *The 1949 Geneva Conventions, A Commentary* (Oxford, Oxford University Press, 2015), chaps. 1 and 19.

42 В то время как начало международного конфликта относительно ясно, поскольку он начинается с любого применения силы между двумя государствами, начало немеждународного вооруженного конфликта менее однозначно. Немеждународные вооруженные конфликты существуют только в том случае, если вооруженные группы достаточно организованны, а уровень насилия достигает определенной интенсивности — два фактора, которые требуют детального анализа фактов в каждом конкретном случае. См. Sylvain Vité, "Typology of armed conflicts in international humanitarian law: legal concepts and actual situations", *International Review of the Red Cross*, vol. 91, No. 873 (March 2009), pp. 72 and 76–77. Существуют также разногласия относительно того, когда заканчивается вооруженный конфликт и достигается мир. Хотя соглашения о прекращении огня или мире могут помочь продемонстрировать окончание вооруженного конфликта, они не являются диспозитивными. Для определения момента прекращения вооруженного конфликта предлагаются различные критерии, а именно: общее прекращение военных действий после достижения общего заключения мира, наличие мирного урегулирования и прекращение действия критериев, позволяющих определить существование конфликта. См. Nathalie Weizmann, "The end of armed conflict, the end of participation in armed conflict, and the end of hostilities: implications for the detention operations under the 2001 AUMF", *Columbia Human Rights Law Review*, vol. 47, No. 3 (2016), pp. 221–224.

43 Соответственно, Конвенция о законах и обычаях сухопутной войны (Гаагская конвенция II) и Конвенция о законах и обычаях сухопутной войны (Гаагская конвенция IV).

44 См. Женевскую конвенцию об улучшении участи раненых и больных в действующих армиях (Женевская конвенция I); Женевскую конвенцию об улучшении участи раненых, больных и лиц, потерпевших кораблекрушение, из состава вооруженных сил на море (Женевская конвенция II); Женевскую конвенцию об обращении с военнопленными (Женевская конвенция III); Женевскую конвенцию о защите гражданского населения во время войны (Женевская конвенция IV).

45 См. Дополнительный протокол 1949 года к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов (Протокол I); Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв вооруженных конфликтов немеждународного характера (Прокол II).

46 См., например, Конвенцию о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничтожении; Конвенцию о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие; Конвенцию о запрещении разработки, производства, накопления и применения химического оружия и о его уничтожении; Конвенцию о запрещении применения, накопления запасов, производства и передачи противопехотных мин и об их уничтожении; Конвенцию по кассетным боеприпасам. См. также International Committee of the Red Cross (ICRC), "Weapons", 30 November 2011. URL: www.icrc.org/en/document/weapons.

47 См. ICRC, "Customary international humanitarian law", 29 October 2010. URL: www.icrc.org/en/document/customary-international-humanitarian-law-0. См. также МККК, «Добро пожаловать в базу данных по обычному МГП». URL: https://ihl-databases.icrc.org/customary-ihl/rus/docs/home.

никновением международных уголовных трибуналов некоторые серьезные нарушения международного гуманитарного права были кодифицированы в учредительных уставах трибуналов как военные преступления[48], что создало новые возможности для обеспечения соблюдения международного гуманитарного права на международном уровне. Ряд государств также кодифицировали военные преступления в своем национальном законодательстве[49], чтобы такие дела могли рассматриваться в рамках обычных судебных систем, а не в военных судах. Национальные дела могут рассматриваться в стране конфликта или все чаще в других странах в соответствии с принципом универсальной юрисдикции[50]. Ряд государств создали специализированные подразделения по военным преступлениям для осуществления уголовного преследования по таким делам. Международные уголовные трибуналы и национальные суды вносят свой вклад в растущий массив правовой практики по международному гуманитарному праву, служащий также важным источником права, нормы которого могут быть обязательными в зависимости от юрисдикции.

2. Международное право прав человека

44. В соответствии с международным правом у государств есть обязательства и обязанности по соблюдению, защите и осуществлению прав человека. Основой международного права прав человека служит Всеобщая декларация прав человека, принятая в 1948 году. Хотя она носит рекомендательный характер и не является юридически обязывающей, ряд ее статей составляют часть обычного международного права[51]. Декларация также послужила источником двух пактов и большого свода договоров о правах человека[52]. Государства связаны только теми пактами и договорами, которые они подписали и ратифицировали, если только нормы, содержащиеся в этих документах, не приобрели статус обычного международного права[53]. Международное право прав человека также было интегрировано в уставы многих международных уголовных трибуналов. Кроме того, существует несколько региональных судов по правам человека, созданных на основании международных конвенций с мандатами по рассмотрению дел против государств-участников этих конвенций в связи с нарушениями международного права прав человека, включая Африканский суд по правам

[48] Например, статья 8 Римского статута Международного уголовного суда кодифицирует международное гуманитарное право в своем определении военных преступлений.

[49] См., например: Австралия (Закон о военных преступлениях 1945 года с поправками, раздел 7); Босния и Герцеговина (Уголовный кодекс, статьи 171–184); Кения (Закон о международных преступлениях 2008 года, раздел 6 (1) (c) и (2)–(4)); Новая Зеландия (Закон о международных преступлениях и Международном уголовном суде 2000 года, раздел 11); Южная Африка (Закон о выполнении Женевских конвенций 2012 года).

[50] В соответствии с «универсальной юрисдикцией» национальный суд может преследовать физических лиц за серьезные преступления против международного права — такие как преступления против человечности, военные преступления, геноцид и пытки, — которые произошли за пределами границ государства, исходя из принципа, что такие преступления наносят ущерб международному сообществу и самому международному порядку, который отдельные государства могут стремиться защитить. См. International Justice Resource Center, "Universal jurisdiction". URL: https://ijrcenter.org/cases-before-national-courts/domestic-exercise-of-universal-jurisdiction.

[51] Многие страны, должностные лица Организации Объединенных Наций и ученые заявили, что большинство статей Всеобщей декларации прав человека, если не все, представляют собой обычное международное право. В частности, запреты на рабство, произвольное лишение жизни, пытки, произвольное задержание и расовую дискриминацию, кодифицированные во Всеобщей декларации прав человека, признаются как составляющие обычное международное право. См., Hurst Hannum, "The status of the Universal Declaration of Human Rights in national and international law", *Georgia Journal of International and Comparative Law*, vol. 25, No. 1 (1996), pp. 322–332 and 341–346.

[52] См. Международную конвенцию о ликвидации всех форм расовой дискриминации; Международный пакт о гражданских и политических правах; Международный пакт об экономических, социальных и культурных правах; Конвенцию о ликвидации всех форм дискриминации в отношении женщин; Конвенцию против пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения и наказания; Конвенцию о правах ребенка. Дополнительную информацию об основных договорах Организации Объединенных Наций по правам человека см. в документе УВКПЧ "The core international human rights instruments and their monitoring. URL: www.ohchr.org/EN/ProfessionalInterest/Pages/CoreInstruments.aspx.

[53] Обычное международное право относится к международным обязательствам, вытекающим из сложившейся международной практики, в отличие от обязательств, вытекающих из официальных письменных конвенций и договоров. Оно является результатом общей и последовательной практики государств, которой они следуют из убежденности в правовой обязательности. Основополагающим элементом обычного международного права является jus cogens, который относится к определенным фундаментальным, главенствующим принципам международного права. См., например, Legal Information Institute, "Customary international law" and "Jus cogens", Cornell Law School. URL: www.law.cornell.edu/wex.

человека и народов[54], Европейский суд по правам человека[55] и Межамериканский суд по правам человека[56]. Существуют дополнительные органы по правам человека на региональном уровне, включая Африканскую комиссию по правам человека и народов, Европейский комитет по социальным правам и Межамериканскую комиссию по правам человека, все из которых продолжают развивать нормативную базу международного права прав человека.

45. Международные организации также играют ключевую роль в разработке и установлении стандартов обычного международного права прав человека[57]. Управление Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ), а также другие международные организации публикуют тематические доклады по областям права, которые способствуют установлению стандартов и развитию «мягкого» права. Договорные органы по правам человека[58] готовят доклады[59], формируют правовую практику[60] и другие виды руководящих указаний, включая замечания общего порядка и общие рекомендации[61], которые способствуют разработке и пониманию статей их соответствующих договоров. Аналогичным образом специальные процедуры Совета по правам человека играют определенную роль в эволюции устанавливающих стандарты норм в международном праве прав человека[62], как и другие механизмы, включая миссии по установлению фактов и комиссии по расследованию.

46. Как и международное гуманитарное право, международное право прав человека стало частью законодательной базы многих стран либо в результате монистических правовых традиций, которые предусматривают прямое применение международных обязательств на национальном уровне, либо путем прямой интеграции международного права в национальное законодательство или путем применения универсальной юрисдикции, тем самым развивая важную нормативную базу, касающуюся такого права[63].

3. Международное уголовное право

47. Международное уголовное право применяется как в мирное время, так и в период вооруженного конфликта, налагая уголовную ответственность на лиц, совершивших преступления по международному праву, включая военные преступления, преступления против человечности и геноцид[64].

---

54 Учрежден в соответствии с Африканской хартией прав человека и народов (Банжульская хартия).

55 Учрежден в соответствии с Конвенцией о защите прав человека и основных свобод (Европейская конвенция по правам человека).

56 Учрежден в соответствии с Американской конвенцией о правах человека (Пакт Сан-Хосе).

57 Примерами международных организаций являются Международный уголовный суд, Международная организация по миграции и Организация по запрещению химического оружия, а также правозащитные механизмы, такие как специальные процедуры и комиссии по расследованию Совета по правам человека или им подобные. Мандаты специальных процедур осуществляются в отношении всех государств — членов Организации Объединенных Наций; они не зависят от ратификации того или иного договора. Существуют различия в правовых нормах и структуре этих правозащитных механизмов, а также в методах и стандартах сбора информации. Например, основным методом работы Рабочей группы по произвольным задержаниям является получение информации об отдельных случаях от соответствующих лиц, членов их семей или их представителей, правительств, НПО и национальных учреждений. Затем Рабочая группа расследует случаи, о которых идет речь в сообщениях, в том числе путем посещения стран. Последние методы работы Рабочей группы см. в документе A/HRC/36/38. Комиссии по расследованию, напротив, создаются Советом по правам человека на специальной основе и, как правило, начинают собственные расследования в соответствии с условиями своих мандатов, часто путем посещения страны, в ходе которого они, в частности, проводят опросы свидетелей. См., например, круг ведения Комиссии по расследованию в Бурунди. URL: www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/CoIBurundi/TermsofreferenceCOIBurundiENGL.pdf.

58 См., например, УВКПЧ, «Договорные органы по правам человека». URL: www.ohchr.org/ru/treaty-bodies/videos-about-treaty-bodies.

59 Доклады могут быть в форме заключительных замечаний, когда договорный орган рассматривает доклады, представленные государствами-участниками и другими заинтересованными сторонами, о выполнении обязательств государств по конкретному договору. Некоторые договорные органы также могут выпускать доклады по результатам расследований. См., например, Комитет по ликвидации дискриминации в отношении женщин, «Процедура расследования». URL: www.ohchr.org/ru/treaty-bodies/cedaw/inquiry-procedure.

60 Договорные органы издают соображения по индивидуальным жалобам в связи с конкретными случаями. См. в целом УВКПЧ, «Договорные органы по правам человека — индивидуальные сообщения». URL: www.ohchr.org/ru/treaty-bodies/human-rights-treaty-bodies-individual-communications.

61 См. УВКПЧ, «Договорные органы по правам человека — Замечания общего порядка». URL: www.ohchr.org/ru/treaty-bodies/human-rights-treaty-bodies-general-comments.

62 См., в целом, УВКПЧ, «Специальные процедуры Совета по правам человека». URL: www.ohchr.org/ru/special-procedures-human-rights-council.

63 Amnesty International, *Universal Jurisdiction: A Preliminary Survey of Legislation Around the World — 2012 Update* (London, 2012), pp. 1–2.

64 Robert Cryer, Darryl Robinson and Sergey Vasiliev, *An Introduction to International Criminal Law and Procedure*, 4th ed. (Cambridge, United Kingdom, Cambridge University Press, 2019), chap. 15.

Вместе их иногда называют «зверствами»[65] или «серьезными международными преступлениями», и они были в основном кодифицированы в Римском статуте, который в целом считается отражением норм обычного международного уголовного права. Кроме того, международное уголовное право включает некоторые преступления, которые не кодифицированы в Римском статуте, например, терроризм[66]. Возможно, существует некоторое пересечение между международным уголовным правом и смежной областью транснационального уголовного права, которое криминализирует трансграничные деяния, такие как торговля людьми, наркотиками, оружием и другими незаконными товарами[67]. В отличие от международного гуманитарного права и международного права прав человека, в международном уголовном праве акцент сделан на индивидуальной уголовной ответственности, а не на ответственности государства. Дела о нарушениях международного уголовного права могут рассматриваться в национальных уголовных судах, смешанных уголовных трибуналах[68], международных уголовных судах или трибуналах[69], включая Международный уголовный суд, или в национальных судах, осуществляющих универсальную юрисдикцию. Источниками международного уголовного права являются учредительные документы судов и трибуналов (например, резолюции Совета Безопасности, уставы, правила процедуры и доказывания, регламенты судов) и национальное законодательство государств, осуществляющих юрисдикцию в отношении международных преступлений. Другим важным источником международного уголовного права являются судебные решения, которые могут быть юридически обязательными или служить в качестве аргумента в зависимости от юрисдикции[70].

B. Юрисдикция и ответственность

48. Юрисдикция — это юридический термин, означающий полномочия, предоставленные юридическому лицу, такому как суд или трибунал, для назначения наказания, вынесения решений и обеспечения соблюдения закона. Правосудие и ответственность определены в Протоколе широко и относятся к различным видам судебных и внесудебных процессов. Ответственность за международные преступления и нарушения международного права прав человека и/или международного гуманитарного права может наступить в результате судебного разбирательства, которое может быть уголовным, гражданским или административным по своему характеру, а также в результате не имеющих обязательной юридической силы процессов, таких как доклады о результатах международных расследований нарушений прав человека, в том числе комиссий по расследованию и миссий по установлению фактов, и других механизмов правосудия переходного периода, включая инициативы, направленные на поиск истины. Лица, проводящие расследования, должны стремиться по возможности учитывать спектр возможных юрисдикций, в которых можно добиваться привлечения к ответственности.

49. Лицам, проводящим расследования с использованием открытых данных, следует определить механизмы привлечения к ответственности, актуальные для их работы, и потенциальные места рассмотрения дела, где собранные доказательства могут быть допущены для установления фактов. Однако на ранних этапах международных расследований они могут быть неизвестны или неясны. Это особенно верно, если государство, в котором были совершены преступления, не имеет функционирующей судебной системы или когда международное сообщество еще

---

65 Хотя термин «этническая чистка» не включен в Римский статут и не определен как самостоятельное преступление в международном праве, он рассматривался как относящийся к категории «зверств». В этом контексте см. United Nations, "Framework of analysis for atrocity crimes: a tool for prevention", p. 1. URL: www.un.org/en/genocideprevention/documents/about-us/Doc.3_Framework%20of%20Analysis%20for%20Atrocity%20Crimes_EN.pdf.

66 См. резолюцию 1757 (2007) Совета Безопасности, приложение, Дополнение (Устав Специального трибунала по Ливану), статья 2.

67 Cryer, Robinson and Vasiliev, *An Introduction to International Criminal Law and Procedure*, chap. 15.

68 Этот термин включает, в частности, Чрезвычайные палаты в судах Камбоджи, Специальный суд по Сьерра-Леоне, Специальный трибунал по Ливану, Специальные судебные палаты и Прокуратуру по Косову и Специальный уголовный суд Центральноафриканской Республики.

69 Этот термин включает постоянно действующий Международный уголовный суд и специальный Международный трибунал по бывшей Югославии, Международный уголовный трибунал по Руанде и Международный остаточный механизм для международных уголовных трибуналов.

70 См. Rosa Theofanis, "The doctrine of res judicata in international criminal law", *International Criminal Law Review*, vol. 3, No. 3 (2003).

не в полной мере располагает возможностями для расследования соответствующего вопроса. Более того, невозможно предугадать все юрисдикции, которые могут быть актуальны в будущем. Когда лица, проводящие расследования с использованием открытых данных, не знают конкретного механизма или юрисдикции, они должны стремиться собирать и сохранять информацию таким образом, чтобы максимально использовать ее в самом широком круге потенциально актуальных юрисдикций. Если они знают о соответствующих требованиях к месту, в котором дело в конечном итоге будет рассматриваться, им следует адаптировать свои процессы к этим конкретным требованиям.

50. Юрисдикция может быть установлена следующими способами:

a) территориальная юрисдикция — это полномочия суда рассматривать дела, связанные с действиями, происходящими на определенной территории. Для международных трибуналов территориальная юрисдикция обычно ограничивается территориями государств, ратифицировавших учредительный договор;

b) временная юрисдикция — это полномочия суда рассматривать дела, в которых предполагаемые деяния произошли в течение установленного периода времени;

c) персональная юрисдикция — это полномочия суда принимать решения в отношении стороны разбирательства;

d) предметная юрисдикция — это полномочия суда рассматривать дела определенного типа или дела, относящиеся к определенному предмету;

e) универсальная юрисдикция — это утверждение власти суда над обвиняемым независимо от того, где было совершено предполагаемое преступление, и независимо от гражданства, страны проживания или любых других отношений обвиняемого с организацией, осуществляющей уголовное преследование.

C. Полномочия и обязанности при расследовании

51. Официальные следственные полномочия — это полномочия, которыми закон наделяет конкретный орган для проведения расследований в рамках определенной юрисдикции. Подобно ограничениям на судебные полномочия, судебные органы или прокуратура могут проводить расследования только в той мере, в какой они уполномочены на это законом[71]. Следственные полномочия могут включать в себя возможность принуждать свидетелей к даче показаний, требовать предоставить документы и выдавать постановления на обыск. Следственный орган может быть обязан по закону следовать строгим процедурам или в некоторых случаях может определять свои собственные процедуры[72].

52. Большинство других лиц, расследующих нарушения международного права, как правило, не будут наделены следственными полномочиями или обязательными для исполнения средствами сбора доказательств, такими как судебный запрос о предоставлении документов или постановление об обыске. Таким образом, они могут полностью полагаться на открытые данные и информацию, предоставленную добровольно, такую как документы, цифровые файлы и показания свидетелей.

53. Как правило, следственные полномочия сопровождаются четко определенными обязанностями[73]. Хотя некоторые лица, проводящие расследования, могут не иметь полицейских или иных законных полномочий, рекомендуется, насколько это возможно, чтобы все такие лица стремились выполнять основные обязанности следователей, чтобы обеспечить качество расследований. Общие обязанности и обязательства следователей и прокуроров включают обязанность расследовать уличающие и оправдывающие обстоятельства, обязанность защищать свидетелей, обязанность сохранять доказательства, обязанность обеспечивать справедливость судебного разбирательства и обязательство уважать права обвиняемых.

---

71 См. Justia, "Agency investigations". URL: www.justia.com/administrative-law/agency-investigations.

72 Ibid.

73 Например, статья 54 Римского статута определяет обязанности и полномочия Прокурора при расследовании, устанавливая, в частности, что Прокурор может проводить расследования, собирать и изучать доказательства, допрашивать потерпевших и свидетелей и сотрудничать с государствами и международными организациями.

54. В уголовных процессах прокуроры обязаны также раскрывать защите относящуюся к делу информацию и доказательства[74]. К ним относятся не только доказательства, допущенные в суде, но и любая информация, собранная в ходе расследования, которая является уличающей или оправдывающей, включая информацию, касающуюся достоверности показаний свидетелей[75]. Существуют определенные исключения, связанные с конфиденциальной информацией или информацией, которая может подвергнуть человека риску. Суд может вынести постановление о неразглашении личности пострадавшего или свидетеля, которые могут оказаться под угрозой в результате такого разглашения, но это никогда не гарантировано[76]. Во многих уголовных юрисдикциях действуют правила раскрытия информации, которые требуют от прокуроров передавать все, что потенциально может служить оправданию обвиняемого[77]. Лица, проводящие расследования с использованием открытых данных, работающие над любым делом, имеющим хоть малейший шанс оказаться в суде, должны учитывать эти обязательства по раскрытию информации при проведении своей работы[78]. Есть еще несколько причин, по которым они должны учитывать возможность раскрытия информации. Например, если прокуроры обязаны изучить все материалы, собранные в ходе расследования, лицам, проводящим расследования, следует остерегаться массового сбора информации, поскольку большой объем информации может оказаться чрезмерно обременительным или даже невозможным для изучения. Это также актуально, когда речь идет о сохранении и хранении собранной информации, включая надлежащую маркировку, что обеспечит значительные преимущества для тех, кто захочет получить и просмотреть эти материалы позже.

D. Правила процедуры и доказывания

55. При работе в контексте судебного расследования основной задачей лиц, проводящих расследование с использованием открытых данных, является сбор относящейся к делу и достоверной информации, чтобы на ее основе можно было сделать фактические и юридические выводы. В частности, в международных судах и трибуналах следователи должны стремиться к тому, чтобы любые собранные доказательства из открытых источников были допустимыми, а также относимыми, надежными и обладали доказательной силой. Уголовные расследования отличаются от расследований, проводимых в других целях, наличием более высокого применимого стандарта доказывания[79] и более строгими правилами процедуры и доказывания, включая допустимость, с целью защиты прав любого обвиняемого на надлежащую процедуру и справедливое судебное разбиратель-

[74] См., например, Международный трибунал по бывшей Югославии, Правила процедуры и доказывания, правило 66 (A); Международный уголовный трибунал по Руанде, Правила процедуры и доказывания, правило 66 (A); Специальный трибунал по Ливану, Правила процедуры и доказывания, правило 110 (A).

[75] См., например, Международный уголовный суд, Правила процедуры и доказывания, правила 76–84; Международный трибунал по бывшей Югославии, Правила процедуры и доказывания, правило 66 (A) (ii); Международный уголовный трибунал по Руанде, Правила процедуры и доказывания, правило 66 (A) (ii); Специальный суд по Сьерра-Леоне, Правила процедуры и доказывания, правило 66 (A) (ii); Специальный трибунал по Ливану, Правила процедуры и доказывания, правило 110 (A) (ii); Специальные коллегии по тяжким преступлениям в Восточном Тиморе, Временные правила уголовного судопроизводства, раздел 24.4.

[76] См., например, Международный уголовный суд, Правила процедуры и доказывания, правило 81 (4); Международный трибунал по бывшей Югославии, Правила процедуры и доказывания, правило 69; Международный уголовный трибунал по Руанде, Правила процедуры и доказывания, правило 69; Специальный суд по Сьерра-Леоне, Правила процедуры и доказывания, правило 69; Специальный трибунал по Ливану, Правила процедуры и доказывания, правила 115–116; Специальные коллегии по тяжким преступлениям в Восточном Тиморе, Временные правила уголовного судопроизводства, раздел 24.6.

[77] См., например, Международный трибунал по бывшей Югославии, Правила процедуры и доказывания, правило 68; Международный уголовный трибунал по Руанде, Правила процедуры и доказывания, правило 68; Специальный суд по Сьерра-Леоне, Правила процедуры и доказывания, правило 68; Специальный трибунал по Ливану, Правила процедуры и доказывания, правило 113; Римский статут Международного уголовного суда, статья 67 (2); Особые коллегии по тяжким преступлениям в Восточном Тиморе, Правила процедуры и доказывания, правило 24.4 (c). Оправдательные доказательства — это доказательства, которые могут исключить вину обвиняемого. В США применяется доктрина Брэйди — это правило досудебного раскрытия информации, установленное Верховным судом США и требующее, чтобы обвинение передавало все оправдательные доказательства ответчику по уголовному делу. См. *Brady v. Maryland*, 378 U.S. 83 (1963).

[78] Поскольку в соответствии с обязательствами по раскрытию информации может потребоваться, чтобы некоторые или все собранные материалы были переданы защите, способность лиц, проводящих расследования с использованием открытых данных, защищать личные данные и другую конфиденциальную информацию может быть сведена на нет.

[79] Например, в то время как международные суды обычно применяют уголовно-правовой стандарт доказывания «вне разумных сомнений», комиссии по расследованию и аналогичные органы чаще всего принимают более низкий стандарт «разумные основания полагать», на котором они основывают свои выводы. Дополнительную информацию см. в документе OHCHR, *Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law: Guidance and Practice*, pp. 62–63.

ство[80]. Хотя критерий допустимости доказательств в международных уголовных судах и трибуналах, как правило, ниже, чем в некоторых национальных судах, методы сбора доказательств в любом случае будут влиять на вес, который судьи придают доказательствам. Это справедливо для всех юрисдикций. В эпоху, характеризующуюся распространением цифровой информации, включая как ложные сведения, так и дезинформацию[81], крайне важно, чтобы следователи могли определить, являются ли открытые данные подлинными, и установить или опровергнуть их истинность с достаточной точностью[82].

56. Применительно к судебному разбирательству допустимость означает, может ли материал, представленный стороной разбирательства, быть приобщен к протоколу в качестве доказательства. Как правило, международные уголовные трибуналы оценивают допустимость представленного материала с помощью теста, учитывающего три фактора: a) относимость; b) доказательную силу; и c) доказательную силу в сопоставлении с любым предвзятым влиянием на справедливость судебного разбирательства[83]. Материал будет относимым, если он помогает сделать факт более или менее вероятным, в то время как его доказательная сила относится к тому, помогает ли он доказать или опровергнуть факт, о котором идет речь в деле. В случае внесудебного расследования применяется оценка, аналогичная оценке допустимости. Вся информация должна быть оценена с точки зрения ее надежности, относимости и доказательной силы, чтобы определить, следует ли ее использовать и каким образом ее следует использовать в составлении юридического и/или фактического заключения[84].

57. Весомость — это значение, придаваемое материалу, и степень, в которой на него в конечном итоге будут опираться при составлении юридического или фактического заключения. Оценка весомости должна быть целостной и частично зависеть от другой информации, которая может поддерживать, подтверждать или опровергать рассматриваемый факт. Во многих судебных разбирательствах допустимость и весомость оцениваются отдельно. В других контекстах, в ситуациях, когда допустимость доказательств не является фактором, специалисты по расследованию нарушений прав человека будут применять аналогичный подход при оценке весомости, которую следует придать информации.

58. Правила процедуры и доказывания, применимые к международному уголовному судопроизводству, можно найти в учредительных документах каждого суда, чаще всего в их правилах процедуры и доказывания. Судебная практика выступает в качестве дополнительного руководства. В зависимости от характера расследования, возможно, стоит обратиться за консультацией к специалисту в области права. Это особенно актуально, если расследование призвано способствовать судебному разбирательству.

59. Открытые данные могут представлять собой сочетание документальных доказательств и свидетельских показаний. Например, необходимо будет подтвердить подлинность видео, на котором человек делает заявления, а сделанные в нем заявления — проверить

---

80 International Criminal Court, *Prosecutor v. Jean-Pierre Bemba*, Case No. ICC-01/05-01/08 A, Judgment on the Appeal of Mr Jean-Pierre Bemba Gombo against Trial Chamber III's "Judgment pursuant to Article 74 of the Statute", 8 June 2018, Appeals Chamber, Separate Opinion of Judge Van den Wyngaert and Judge Morrison, para. 5.

81 Ложные сведения — это информация, которая является ложной, но она не направлена на причинение вреда. Например, лица, которые не знают, что какая-то информация является ложной, могут распространять ее в социальных сетях, пытаясь быть полезными. Дезинформация — это ложная информация, которая намеренно создается или распространяется с явной целью причинить вред. Лица, создающие дезинформацию, обычно имеют политические, финансовые, психологические или социальные мотивы. См. Claire Wardle, "Information disorder: the essential glossary" (Cambridge, Massachusetts, Shorenstein Center on Media, Politics and Public Policy, 2018). URL: https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x32994.

82 Ibid.

83 Согласно Римскому статуту (статьи 64 (9) (a) и 69 (4)), Судебная палата Международного уголовного суда имеет «право по ходатайству одной из сторон или по своей инициативе... в соответствии с Правилами процедуры и доказывания вынести решение об относимости или допустимости любых доказательств, принимая при этом во внимание, наряду с прочим, их силу, а также вред, который такие доказательства могут причинить проведению справедливого судебного разбирательства или справедливой оценке показаний свидетеля».

84 См., например, OHCHR, *Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law: Guidance and Practice*, в частности главу IV.C о сборе и оценке информации.

отдельно[85]. В связи с этим могут применяться способы подтверждения подлинности цифрового материала как документа или оценки его надежности и допустимости в качестве свидетельского показания. Лицам, проводящим расследования, следует знать, как каждая категория доказательств рассматривается в соответствующей юрисдикции. Документальные доказательства часто могут быть допущены, даже если автор неизвестен или не может дать показания. Они также могут быть допустимы без представления документа через свидетеля, который может подтвердить их подлинность, при условии, что предлагающая сторона может ясно и конкретно показать, где и как этот документ встраивается в дело[86].

60. В ситуациях, когда ответственность за преступления и нарушения возлагается на лиц, занимающих более высокое положение в структуре командования, собранная информация может использоваться не только для создания «базы преступлений» (см. ниже), но также может иметь значение для определения формы ответственности[87] предполагаемого конкретного исполнителя (исполнителей)[88]. Лица могут считаться ответственными, когда каждый элемент преступления или нарушения, включая физические действия (actus reus) и психическое состояние обвиняемого (mens rea), демонстрируется в соответствии с применимым стандартом доказывания. Для принятия такого решения лицо, устанавливающее факт, изучает информацию, представленную в отношении каждого элемента нарушения или преступления. Лицам, проводящим расследование, следует знать, о каких преступлениях или нарушениях может идти речь, элементы каждого из них, кого обвиняют в их совершении и по какой теории ответственности. В делах о нарушениях международного уголовного права специалисты-практики часто разделяют «доказательства совершения преступления» и «доказательства причастности». Эти два понятия объясняются следующим образом:

a) доказательства совершения преступления — это доказательства преступлений, на которых основаны обвинения, включая информацию о том, кто, что, где и когда совершил[89]. Например, если предполагаемый преступник обвиняется в убийстве как преступлении против человечности, любая информация, доказывающая, что имело место убийство, считается доказательством совершения преступления;

---

85 См. Human Rights Center, University of California, Berkeley, School of Law, *Digital fingerprints: using electronic evidence to advance prosecutions at the International Criminal Court* (Berkeley, 2014). URL: www.law.berkeley.edu/files/HRC/Digital_fingerprints_interior_cover2.pdf. Показания с чужих слов — это информация, не относящаяся к непосредственным знаниям свидетеля, дающего показания. В некоторых юрисдикциях показания с чужих слов являются недопустимыми, если только они не подпадают под определенное исключение. В других случаях они допустимы, но им не придается большого веса из-за того, что они не могут быть должным образом проверены в ходе перекрестного допроса ни обвинением, ни защитой. По данным Организации по безопасности и сотрудничеству в Европе, «в то время как показания с чужих слов обычно не допустимы в юрисдикциях общего права при отсутствии особых обстоятельств, на показания с чужих слов нет запрета в юрисдикциях гражданского права или в международных трибуналах». См. Organization for Security and Cooperation in Europe, Mission to Bosnia and Herzegovina, *Investigation Manual for War Crimes, Crimes Against Humanity and Genocide in Bosnia and Herzegovina* (Sarajevo, 2013), p. 26. URL: www.osce.org/bih/281491?download=true. Несмотря на отсутствие препятствий в юрисдикциях гражданского права и международных трибуналах, как правило, показания с чужих слов рассматриваются как особенно ненадежная категория косвенных доказательств, и судьи часто придают им относительно небольшой вес.

86 См., например, International Tribunal for the Former Yugoslavia, *Prosecutor v. Pavle Strugar*, Case No. IT-01-42-T, Decision on the Admissibility of Certain Documents, 26 May 2004, Trial Chamber II, and *Prosecutor v. Milan Milutinović et al*., Case No. IT-05-87-T, Decision on Prosecution Motion to Admit Documentary Evidence, 10 October 2006, Trial Chamber; International Criminal Tribunal for Rwanda, *Prosecutor v. Edouard Karemera et al*., Case No. ICTR-98-44-T, Decision on Joseph Nzirorera's Motion to Admit Documents from the Bar Table: Public Statements and Minutes, 14 April 2009, Trial Chamber III; International Criminal Court, *Prosecutor v. Thomas Lubanga Dyilo*, Case No. ICC-01/04/-01/06, Decision on the Admission of Material from the "Bar Table", 24 June 2009; International Tribunal for the Former Yugoslavia, *Prosecutor v. Radovan Karadžić*, Case No. IT-95-5/18-PT, Order on Prosecution Request for Clarification and Proposal concerning Guidelines for the Conduct of Trial, 20 October 2009, Trial Chamber, and *Prosecutor v. Radovan Karadžić*, Case No. IT-95-5/18-T, Decision on the Prosecution's First Bar Table Motion, 13 April 2010, Trial Chamber; International Criminal Court, *Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui*, Case No. ICC-01/04-01/07, Decision on the Prosecutor's Bar Table Motions, 17 December 2010, Trial Chamber II.

87 Cryer, Robinson and Vasiliev, *An Introduction to International Criminal Law and Procedure*, chap. 15.

88 См. OHCHR, *Who's Responsible? Attributing Individual Responsibility for Violations of International Human Rights and Humanitarian Law in United Nations Commissions of Inquiry, Fact-Finding Missions and Other Investigations* (New York and Geneva, 2018). URL: https://ohchr.org/Documents/Publications/AttributingIndividualResponsibility.pdf.

89 Kelly Matheson, *Video as Evidence Field Guide* (WITNESS, 2016), p. 42. URL: https://vae.witness.org/video-as-evidence-field-guide.

b) доказательства причастности — это доказательства ответственности предполагаемого преступника за совершенные преступления, что особенно важно, если он не был непосредственным исполнителем преступления[90]. Другими словами, это доказательства, которые связывают ответственное лицо с преступлением. Например, в случаях, когда утверждается, что вышестоящий руководитель не предотвратил предполагаемые нарушения, о которых ему было известно, или не наказал за них, доказательствами причастности являются доказательства, подтверждающие эту осведомленность или тот факт, что вышестоящий руководитель осуществлял «эффективный контроль» над непосредственным нарушителем.

E. Право на неприкосновенность частной жизни и защита данных

61. Право на неприкосновенность частной жизни — одно из основных прав человека[91]. Одним из его важных элементов является право на защиту персональных данных, сформулированное в различных законах о защите данных[92]. В частности, законы о защите данных и частной жизни приобретают все большую значимость для расследований, в ходе которых используются цифровые информационно-коммуникационные технологии (ИКТ). Ниже приводится краткий обзор концепций международного права человека на неприкосновенность частной жизни и глобальной нормативно-правовой базы по защите данных, безопасности данных и обмену данными, о которых следует знать лицам, проводящим расследования с использованием открытых данных. В цифровой среде информационная конфиденциальность, охватывающая существующую информацию о человеке или ту, которая может быть о нем получена, имеет особое значение[93].

62. Лица, проводящие расследования с использованием открытых данных, должны уважать права человека и уделять особое внимание праву на неприкосновенность частной жизни, вопрос о котором часто поднимается в контексте цифровой информации. Например, нарушение права на неприкосновенность частной жизни является одним из немногих оснований для исключения доказательств судьями Международного уголовного суда[94]. Неприкосновенность частной жизни лежит в основе человеческого достоинства и других ключевых ценностей, таких как свобода ассоциации и свобода выражения мнений, и позволяет защищать их. Некоторые из наиболее сильных толкований законов о неприкосновенности частной жизни появились благодаря практике Европейского суда по правам человека, и количество постановлений, касающихся вопросов цифровых прав, быстро растет. Нарушение столь фундаментальных прав неизбежно будет оспорено стороной защиты в уголовном процессе и даже может стать основанием для предъявления гражданского иска сторонам, ведущим расследование. Помимо законов о конфиденциальности, обеспечению безопасности персональных данных содействуют многочисленные законы и нормативные акты о защите данных. В частности, лицам, проводящим расследования с использованием открытых данных, следует знать о существовании Регламента 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент о защите персональных данных), а также о сформулированном в нем подходе к защите индивидуальных данных, поскольку этим законом был установлен вы-

90 Ibid.

91 Право на неприкосновенность частной жизни предусмотрено в многочисленных документах по правам человека и конституциях более чем 130 стран. См., например: Американскую декларацию прав и обязанностей человека, ст. V; Европейскую конвенцию по правам человека, ст. 8; Американскую конвенцию о правах человека, ст. 11; Конвенцию о правах ребенка, ст. 16; Международную конвенцию о защите прав всех трудящихся-мигрантов и членов их семей, ст. 14; Африканскую хартию прав и благополучия ребенка, ст. 10; Арабскую хартию прав человека, ст. 16 и 21; Декларацию Ассоциации государств Юго-Восточной Азии по правам человека, ст. 21. См. также Privacy International, "What is privacy?", 23 October 2017. URL: https://privacyinternational.org/explainer/56/what-privacy.

92 Законы о защите данных существуют в более чем 100 странах, а соответствующие нормы изложены также в многочисленных международных и региональных документах. См., например, Руководство по защите неприкосновенности частной жизни и трансграничной передаче персональных данных Организации экономического сотрудничества и развития, Конвенцию о защите физических лиц при автоматизированной обработке персональных данных Совета Европы, Хартию Европейского союза об основных правах, Рамки защиты частной жизни форума Азиатско-тихоокеанского экономического сотрудничества, Дополнительный закон о защите персональных данных в рамках Экономического сообщества западноафриканских государств.

93 Для общей информации см. A/HRC/39/29, п. 5.

94 См. Римский статут, ст. 69, п. 7.

сокий стандарт, и другие государства рассматривают возможность принятия аналогичного законодательства[95]. Вместе с тем нормы в отношении защиты данных в разных странах существенно различаются, а иногда даже вступают в прямое противоречие друг с другом. Лицам, проводящим расследования с использованием открытых данных, следует проконсультироваться с экспертом по правовым вопросам для получения информации о законах и нормах, применимых к защите данных в той юрисдикции, в которой они работают.

63. Наконец, лицам, проводящим расследования с использованием открытых данных, следует знать об общем запрете несанкционированного доступа к данным и сетям. Например, это может включать в себя использование пароля, полученного в результате взлома базы данных, для доступа к материалам ограниченного пользования, а также получение несанкционированного доступа к информации ограниченного пользования путем обмана и других форм социальной инженерии[96].

F. Прочие применимые правовые соображения

64. К расследованиям с использованием открытых источников могут быть применимы и другие законы. Ниже приводятся некоторые правовые соображения, о которых следует знать лицам, проводящим расследования с использованием открытых данных.

1. Нарушение условий оказания услуг

65. Некоторые распространенные методы расследований с использованием открытых данных влекут за собой нарушение условий оказания услуг веб-сайтов или платформ. Например, веб-скрейпинг или использование виртуальной личности (не принадлежащей какому-либо реальному человеку) нарушают условия оказания услуг различных платформ, в частности платформ социальных сетей[97]. Нарушение условий оказания услуг является нарушением договора. Лицам, проводящим расследование, следует проверять, не являются ли подобные действия также противозаконными в той юрисдикции, в которой они работают. Необходимость соблюдения принципов безопасности, которая может быть обеспечена с помощью использования виртуальных личностей, должна соотноситься с потенциальным ущербом из-за нарушения договора в подобных обстоятельствах, в которых наиболее распространенным средством правовой защиты является отключение для пользователя доступа к платформе. Вместе с тем, хотя виртуальные личности необходимы в тех случаях, когда они используются исключительно для поиска в открытых источниках и мониторинга в них, как отмечалось выше, их не следует использовать при попытках получения доступа к контенту, распространяемому в социальных сетях, который подлежит ограничительному контролю доступа, или же в попытках получения информации напрямую от того или иного лица под прикрытием вымышленной личности. Подобные действия выведут расследователя за допустимые границы расследования с использованием открытых источников, станут нарушением этических принципов[98], а также могут нарушать закон[99].

2. Законодательство об интеллектуальной собственности

66. Проводящим расследования лицам следует знать обо всех разрешениях на интеллектуальную собственность, ко-

[95] В упомянутом выше Регламенте ЕС указывается, что физические лица имеют права, связанные с защитой персональных данных, защитой обработки персональных данных и неограниченным обращением персональных данных в пределах Европейского союза. Подобные права предусмотрены также в Конвенции о защите физических лиц при автоматизированной обработке персональных данных и, в частности, Протоколе 2018 года к ней. Конвенция налагает обязательства не только на государства — члены Совета Европы, но и на ряд других государств.

[96] Согласно Национальному институту стандартов и технологии Соединенных Штатов, социальная инженерия — это «обманные действия в отношении того или иного лица с целью заставить его раскрыть информацию ограниченного доступа путем вступления во взаимодействие с таким лицом для вхождения в его доверие» (Paul A. Grassi, Michael E. Garcia and James L. Fenton, *Digital Identity Guidelines* (Gaithersburg, Maryland, National Institute of Standards and Technology, 2017), p. 54. См. также Michael Workman, "Gaining access with social engineering: an empirical study of the threat", *Information Systems Security*, vol. 16, No. 6 (2007). Более подробно вопрос о несанкционированном и полученном обманным путем доступе рассматривается в п. 65 ниже. Вопрос о маскировке пользователей рассматривается в п. 107 ниже.

[97] Например, пользовательским соглашением «Фейсбука» предусматривается требование к пользователям «указывать для своего аккаунта имя, которое вы используете в повседневной жизни», «указывать точную информацию о себе» и «создавать только один аккаунт (ваш собственный) и использовать хронику в личных целях». См. https://ru-ru.facebook.com/legal/terms. Выдача себя за другое лицо является нарушением Правил и политики «Твиттера». См. «Политику в отношении вводящих в заблуждение и поддельных личностей». URL: https://help.twitter.com/ru/rules-and-policies/twitter-impersonation-and-deceptive-identities-policy.

[98] Вопрос о выдаче себя за другое лицо рассматривался выше в главе II.C об этических принципах.

[99] См. выше в главе III.E о праве на неприкосновенность частной жизни и защите данных.

торые им могут понадобиться для законной публикации, распространения и/или иного использования информации, собранной ими в ходе расследования. Применимое законодательство отличается в разных юрисдикциях, хотя большинство из них предоставляют (как минимум) определенную форму защиты авторских прав создателю контента, например видео, фотографии или фрагмента текста, размещенного в Интернете. Под «создателем» обычно понимается лицо, которое фактически создало материал, например сделав фотографию, записав видео или написав оригинальный текст, а не загрузившее его лицо, хотя это может быть одно и тот же человек. Во избежание нарушения авторских прав конечный пользователь, возможно, должен получать согласие создателя на предполагаемое использование контента (например, в публично распространяемом докладе или журналистском материале); получения согласия загрузившего контент лица, если оно не является также его создателем, для избежания нарушения закона, как правило, недостаточно. Это еще одна причина для того, чтобы пытаться найти первоисточник каждого материала, который может быть получен лицами, проводящими расследование. В некоторых (но не всех) юрисдикциях предусматриваются исключения из необходимости получения согласия (часто такие виды использования называют исключениями в порядке «добросовестного использования» или «добросовестных действий») в случаях, когда видео, фотографии, текст и другая информация используются в определенных общественно полезных целях, таких как образование, правоохранительная деятельность или журналистика. Однако эти исключения, когда они применимы, часто являются довольно узкими, и поэтому никогда не следует заключать, что конкретное использование подпадает под такое исключение, без проведения тщательного анализа. Механизмы, которые в некоторых случаях могут способствовать минимизации вероятности и/или масштабов нарушения авторских прав, включают в себя встраивание ссылки на оригинальный контент в цифровой доклад без изъятия его из первоисточника, указание имени создателя, а также использование лишь небольшой части оригинального контента, что, однако, также зависит от контекста и юрисдикции. Информация, на которую распространяются лицензии Creative Commons или другие свободные лицензии, может иметь широкий спектр допустимого использования на безвозмездной основе. Однако в тех случаях, когда такие бесплатные лицензии применяются, важно соблюдать их условия и не рассматривать соответствующий контент как не требующий никаких разрешений.

IV

БЕЗОПАСНОСТЬ

КРАТКОЕ СОДЕРЖАНИЕ ГЛАВЫ

- За обеспечение безопасности расследования и тех, кого оно затрагивает, отвечают все, а не только специалисты по информационным технологиям.
- Для обеспечения безопасности следует рассматривать соображения двух родов: a) связанные с инфраструктурой, включая оборудование, программное обеспечение и сети; b) поведенческого характера, включая действия лиц, ведущих расследование, и всех тех, с кем они взаимодействуют.
- Оценки безопасности следует проводить на трех уровнях, в том числе на уровне организации, конкретного расследования/случая и конкретных мероприятий/задач.
- Следует разработать защитные меры в целях смягчения рисков и угроз, выявленных в ходе оценки рисков расследования.
- При оценке безопасности следует учитывать все виды ущерба, включая цифровой, финансовый, правовой, физический, психосоциальный и репутационный ущерб.
- Отдельные наиболее важные факторы уязвимости при расследованиях с использованием открытых источников связаны с интернет-соединениями/IP-адресами, устройствами и их функциями, а также поведением пользователей.
- Лицам и организациям, ведущим расследования, следует постоянно проводить повышение квалификации по вопросам безопасности и внедрять защитные меры, меняющиеся при изменении характера любых угроз или факторов уязвимости.

67. В этой главе содержится обзор соображений безопасности в режиме онлайн и офлайн, касающихся расследований с использованием открытых источников. При условии соответствующей подготовки, вложений и уделения внимания оценке угроз и смягчению рисков лица, проводящие расследования с использованием открытых данных, со всей вероятностью смогут минимизировать риск причинения ущерба людям, данным и другим активам. Инфраструктуру безопасности, включая аппаратное и программное обеспечение, и протоколы поведения пользователей следует, насколько это возможно, внедрять до начала расследования, регулярно оценивать и обновлять по мере необходимости. Размер и ресурсы организации могут повлиять на возможность принятия определенных защитных мер; соответственно, в данной главе приводятся гибкие стандарты, которые следует адаптировать к конкретным потребностям организации и расследования. Организациям, проводящим расследования повышенного риска (например, касающиеся особо уязвимых жертв или ситуаций, когда предполагаемыми нарушителями являются государственные субъекты и/или лица, которых возможно идентифицировать), следует обращаться к услугам опытных специалистов в области кибербезопасности. Кроме того, в составе надежной системы безопасности следует предусматривать какой-либо механизм независимого аудита и повышения квалификации, с тем чтобы пользователи могли получать информацию о новых технологических разработках и передовой практике.

A. Минимальные стандарты

68. Поскольку инфраструктура безопасности и передовая практика поведения пользователей постоянно меняются, в Протоколе предлагаются всеобъемлющие принципы, которые помогут разработать меры безопасности лицам, проводящим расследования с использованием открытых данных. Ведущие расследование лица должны обеспечивать собственную безопасность, в том числе оценивать уровень риска, связанного с их действиями, и принимать надлежащие меры по снижению риска и защите. Несмотря на необходимость специфического и индивидуального подхода к безопасности, существуют некоторые минимальные стандарты, которые лицам, проводящим расследования с использованием открытых данных, следует всегда применять в своей работе в целях соблюдения принципов безопасности:

a) лицам, проводящим расследования с использованием открытых данных, следует избегать раскрытия третьим лицам элементов, позволяющих идентифицировать их самих, их организации и любых партнеров или источников, если только это не входит в задачи расследования или обязанности в его рамках. Поэтому им следует сохранять свою анонимность в Интернете и обеспечивать в максимально возможной степени невозможность атрибутирования их действий в Интернете;

b) лицам, проводящим расследования с использованием открытых данных, следует вести деятельность в Интернете исходя из того, что ее могут отслеживать и анализировать третьи стороны. Поэтому им следует действовать в Интернете таким образом, который соответствует их виртуальным личностям, не раскрывает их реальную личность или цели расследования и не подвергает опасности лиц, являющихся их источниками информации, или других третьих лиц;

c) лицам, проводящим расследования с использованием открытых данных, следует знать, что чрезмерно активное использование одного онлайн-источника информации, например конкретного веб-сайта, может увеличить риск мониторинга и анализа со стороны третьих лиц. Поэтому им следует внедрять практику, направленную на минимизацию такой вероятности, например диверсифицировать цифровые источники;

d) лицам, проводящим расследования с использованием открытых данных, следует избегать идентифицируемых или предсказуемых моделей поведения, таких как повторяющиеся схемы поиска на идентифицируемых устройствах, которые могут позволить третьей стороне определить цели расследования, а также способствовать их превращению в более легкую мишень для фишинговых атак и других форм социальной инженерии[100];

e) лицам, проводящим расследования с использованием открытых данных, следует отделять свою профессиональную деятельность от действий в Интернете в личных целях. Личные онлайн-аккаун-

[100] Объяснение фишинговых атак и социальной инженерии см. ниже.

ты и, насколько это возможно, личное оборудование не следует использовать для профессиональных расследований, а профессиональное оборудование никогда не следует использовать для личных целей[101];

f) лицам, проводящим сразу несколько расследований с использованием открытых данных, не следует смешивать такие расследования. Поэтому им следует устанавливать разное время начала и окончания того или иного действия в рамках каждого расследования, хранить данные и документацию по каждому расследованию в разных местах и при необходимости использовать разные виртуальные личности[102];

g) лицам, проводящим расследования с использованием открытых данных, следует использовать технические системы или среды, разработанные таким образом, чтобы на них минимально влияло возможное внедрение враждебного или вредоносного программного обеспечения или другие нарушающие функционирование воздействия, с которыми они могут столкнуться в ходе работы.

B. Оценки безопасности

69. Для того чтобы разработать соответствующую и эффективную систему безопасности, лица, проводящие расследования с использованием открытых данных, должны понимать ключевые концепции кибербезопасности и управления рисками. Они также должны быть способны определять активы, которым необходима защита, и потенциальный ущерб, а также оценивать потенциальные угрозы, риски и уязвимости.

70. Риск — это возможность потери, повреждения или уничтожения актива в результате реализации потенциала того или иного фактора уязвимости той или иной угрозой. Каждый из этих трех терминов определен ниже. Поскольку расследования с использованием открытых источников, проводимые в Интернете, предполагают иные методы сбора информации, чем при традиционных расследованиях, они порождают иные виды рисков. Выявление и оценка этих рисков являются важнейшей частью планирования и подготовки расследования. В качестве примеров распространенных рисков при проведении расследований с использованием открытых источников можно назвать: технологические возможности и осведомленность о расследовании его объекта или поддерживающих такой объект лиц, которые могут уклониться от него или направить его по ложному пути; проблемы в технической конфигурации онлайн-среды, используемой для расследования, что может привести к раскрытию информации, способной поставить расследование под угрозу; вредоносное программное обеспечение или код, которые могут поставить под угрозу компьютерные системы проводящего расследование лица, его деятельность, личность или собранные данные; технические функции, такие как трекеры, куки, веб-маяки и аналитика, которые могут поставить под угрозу мероприятия в рамках расследования.

71. В следующем разделе приведены пояснения ключевых терминов и их применения к расследованиям с использованием открытых источников, образующие собой «дорожную карту» для проведения оценки угроз и рисков.

1. Активы

72. Активом является все, что нуждается в защите, включая людей[103], имущество и информацию. В контексте расследований с использованием открытых данных в состав лиц, нуждающихся в защите, могут входить лица или группы, проводящие расследование, включая всех, с кем они работают (т. е. внутренних коллег и внешних партнеров — как местных, так и полевых), авторы или источники информации, свидетели, жертвы, предполагаемые нарушители и случайные лица. В состав имущества входят материальные и нематериальные объекты, которым можно присвоить стоимость[104]. К материальным активам относятся здания, оборудование и документы, а нематериальные активы включают в себя репутацию и служебную информацию, такую как

[101] Если использование личного оборудования неизбежно, то пользователям следует использовать для профессиональных расследований и в личных целях разные онлайн-среды, например пользоваться виртуальной машиной для расследований.

[102] Помимо минимизации риска смешения расследований, такая практика содействует эффективному обеспечению сохранности доказательств.

[103] Обозначение людей в качестве активов приводится исключительно в контексте проведения оценки безопасности.

[104] См. Threat Analysis Group, "Threat, vulnerability, risk — commonly mixed up terms". URL: www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms.

цифровые данные, метаданные, базы данных, программный код и записи.

2. Ущерб

73. Ущерб — это физическое или психическое повреждение либо вред активам или их уничтожение. Он может включать в себя цифровой, финансовый, правовой, физический, психосоциальный или репутационный ущерб.

a) Цифровой ущерб

74. Цифровой ущерб — это повреждение любой цифровой информации или инфраструктуры. Потенциальный цифровой ущерб может включать в себя уничтожение данных, манипулирование ими или потерю доступа к ним, а также нарушение работы компьютерных систем и платформ.

b) Финансовый ущерб

75. Финансовый ущерб может проистекать из различных источников, включая правовой и репутационный ущерб, связанный с тем или иным расследованием. Такой ущерб могут понести как лица, проводящие расследование, так и его объекты и случайные лица. Кроме того, финансовый ущерб может быть нанесен в тех случаях, когда проводящие расследование лица неадекватно оценивают долгосрочные затраты на расследование.

c) Правовой ущерб

76. Лица, проводящие расследования с использованием открытых данных, могут понести правовую ответственность за процесс или за результаты своей работы. Проводящим расследования лицам следует знать о правовых ограничениях в отношении допустимых действий и о правовых последствиях их действий в целях минимизации рисков того, что они сами и/или третьи лица понесут правовую ответственность. Расследования также могут приводить к нанесению правового ущерба объектам таких расследований и даже посторонним лицам, которые могут оказаться вовлеченными в правонарушения, выявленные в ходе расследования[105].

d) Физический ущерб

77. Физический ущерб может включать в себя вред, наносимый людям или имуществу. Хотя лица, проводящие расследования с использованием открытых данных, обычно работают в офисе или из дома, а не «в поле», тем не менее, физический вред следует рассматривать как одно из возможных последствий деятельности в Интернете. Действия в киберпространстве могут привести к последствиям в реальном мире, о которых проводящим расследования лицам следует знать и к которым им следует быть готовыми. Например, лицам, проводящим расследования с использованием открытых данных, следует помнить о тех людях (будь то коллеги, интернет-пользователи в относящихся к рассматриваемому случаю странах или иные лица), которые могут находиться в небезопасной среде и подвергаться риску физического ущерба в результате действий проводящего расследование лица в Интернете. Проводящие онлайн-расследования лица несут этическую, а в некоторых случаях и юридическую обязанность проявлять заботу[106] по отношению к другим людям, чтобы не допустить усиления опасности в результате их деятельности для тех, кому угрожает физический вред. Физические риски следует рассматривать как часть комплексной оценки угроз до начала работы и переоценивать на протяжении всего жизненного цикла расследования.

e) Психосоциальный ущерб

78. Психосоциальный ущерб может принимать различные формы, от психологического стресса до травмы, и затрагивать любого члена проводящей расследование группы и/или лиц, иным образом вовлеченных в расследование или затрагиваемых им, включая объекты расследования и случайных лиц. Помимо морально-этической значимости защиты себя и других от психологического ущерба, в некоторых случаях человек может становиться наиболее слабым местом для эффективного функционирования любой организации. Человек, получивший психосоциальный ущерб, может оказаться особо уязвим, что создает новые возможности для действий субъектов, умышленно нарушающих информационную безопасность, или другие риски для физической и цифровой безопасности, особенно если негативные психологические последствия приводят к рабочим нарушениям, например ослаблению соблюдения протоколов безопасности. Известно, что просмотр большого количества видеоматериалов со сценами жестокости или иными натуралистическими подробностями воспри-

[105] См. также более подробный анализ соответствующих правовых соображений в главах IV.E и IV.F выше.

[106] Римский статут, ст. 54 (1) (b).

нимается особенно тяжело и может приводить к психологическому стрессу или травме, что, в свою очередь, может потребовать обращения за профессиональной помощью. Признаки вторичной травмы могут включать в себя изменения в поведении, перепады настроения, изменения режима питания или употребления напитков, бессонницу, увеличение продолжительности сна или кошмары[107]. Стратегии смягчения психосоциального ущерба описаны в разделе о подготовке и разработке плана повышения стрессоустойчивости и самопомощи[108].

f) Репутационный ущерб

79. Репутационный ущерб в контексте расследований с использованием открытых данных может быть наиболее значительным для лиц, проводящих расследования с использованием открытых данных, и/или их организаций, например в случае публикации ими ошибочной информации, нарушения этических норм или создания проблемного контента иного характера. Репутационный ущерб может быть нанесен также объектам расследования, которые могут подвергнуться остракизму за предположительно совершенные ими действия после того, как об этих действиях станет известно общественности. Это может становиться особенно проблематичным в тех случаях, когда в отношении тех или иных лиц или организаций выдвигаются обвинения, которые впоследствии оказываются ложными.

3. Защитные меры

80. Защитные меры — это усилия, которые прилагаются для предотвращения или минимизации факторов уязвимости и могут включать в себя меры физического, технологического и политического характера. Мерами физической защиты может являться установка замков в зданиях, помещениях или шкафах, в которых хранятся конфиденциальные материалы. Технологические меры могут включать в себя использование паролей, шифрование и многофакторную аутентификацию на устройствах или контроль доступа к системам данных. Меры политики включают внутренние и внешние нормы, законы и механизмы обеспечения соблюдения, например нормы о запрете отправки внутреннего продукта труда с рабочей электронной почты на личную электронную почту или запрет использования личных аккаунтов в социальных сетях на рабочем компьютере.

4. Угрозы

81. Угрозы — это то, от чего необходимо защищать активы. Угрозой является все, что может позволить использовать, умышленно или случайно, фактор уязвимости и получить, повредить или уничтожить тот или иной актив. Угрозы могут быть внутренними или внешними по отношению к организации или расследованию и могут реализовываться отдельными лицами, группами, учреждениями или сетями. Лицам, проводящим расследования с использованием открытых данных, следует знать, в частности, о перечисленных ниже угрозах.

a) Распределенная атака типа «отказ в обслуживании»

82. Распределенные атаки типа «отказ в обслуживании» — это кибератаки, направленные на нарушение возможности доступа объекта к машине или сети. Для активов, предназначенных для пользования общественности, таких как веб-сайты и другие порталы удаленного доступа, следует предусматривать систему смягчения последствий таких атак. Кроме того, следует создать систему регистрации инцидентов, которая будет использоваться в случае атаки для регистрации всех действий и соответствующих субъектов.

b) Фишинговые атаки

83. Фишинг — это мошенническая попытка получить конфиденциальную информацию, такую как имена пользователей, пароли и данные кредитных карт, посредством электронного

[107] См. Dart Center for Journalism and Trauma, "Working with traumatic imagery", 12 August 2014 (URL: https://dartcenter.org/content/working-with-traumatic-imagery); Sam Dubberley, Elizabeth Griffin and Haluk Mert Bal, *Making Secondary Trauma a Primary Issue: A Study of Eyewitness Media and Vicarious Trauma on the Digital Frontline* (Eyewitness Media Hub, 2015) (URL: http://eyewitnessmediahub.com/research/vicarious-trauma); Sam Dubberley and Michele Grant, "Journalism and vicarious trauma: a guide for journalists, editors and news organisations" (First Draft News, 2017) (URL: https://firstdraftnews.org/wp-content/uploads/2017/04/vicarioustrauma.pdf); Center for Human Rights and Global Justice, "Human rights resilience project launches new website", 21 May 2018 (URL: https://chrgj.org/2018/05/21/human-rights-resilience-project-launches-resources-for-resilience-website); Keramet Reiter and Alexa Koenig, "Reiter and Koenig on challenges and strategies for researching trauma", Palgrave MacMillan (URL: www.palgrave.com/gp/blogs/social-sciences/reiter-and-koenig-on-researching-trauma).

[108] Дополнительную информацию о самопомощи см. в главе V.D ниже.

сообщения от якобы надежного отправителя[109]. Фишинг или телефонное мошенничество используются для получения конфиденциальной информации или преследования лиц, проводящих расследования. Личные аккаунты обычно подвергаются большему риску, чем профессиональные, поэтому их использование может стать угрозой для расследования или создания продукта труда.

c) Атаки типа «человек посередине»

84. Атаки типа «человек посередине» — это вид кибератак, при которых злоумышленники внедряются в процесс связи между двумя сторонами, выдают себя за эти стороны и получают доступ к информации, которую обе стороны пытались передать друг другу[110]. Атака типа «человек посередине» позволяет злоумышленнику перехватывать, отправлять и получать данные, предназначенные для другого лица или вообще не предназначенные для отправки, а соответствующие стороны узнают об этом только тогда, когда уже слишком поздно[111].

d) Социальная инженерия

85. Социальная инженерия — это психологическое манипулирование людьми с целью принудить их к совершению потенциально вредоносных действий, например к разглашению конфиденциальной информации. Существует множество различных примеров социальной инженерии, в частности адресный фишинг[112]. Поскольку методы социальной инженерии продолжают адаптироваться и развиваться, ведущим расследования лицам следует постоянно повышать свою квалификацию по вопросам выявления и избегания выявленных методов социальной инженерии.

e) Вредоносное программное обеспечение

86. Вредоносное программное обеспечение обозначает компьютерные программы, предназначенные для проникновения в компьютеры без согласия пользователя и для их повреждения. Существует несколько типов вредоносных программ, включая шпионские программы и программы-вымогатели.

5. Субъект, умышленно нарушающий информационную безопасность

87. Субъект, умышленно нарушающий информационную безопасность, или злоумышленник, — это физическое или юридическое лицо, несущее ответственность за событие или инцидент, которые имеют или могут иметь последствия для безопасности другой организации или другого субъекта. В ходе международных уголовных расследований и расследований нарушений прав человека субъектами, умышленно нарушающими информационную безопасность, весьма вероятно, являются предполагаемые преступники, объекты расследования, включая правительства, или их сторонники. Лицам, проводящим расследования с использованием открытых данных, важно идентифицировать субъектов, которые могут умышленно нарушить информационную безопасность, понять их возможности и оценить вероятность атак с их стороны.

6. Факторы уязвимости

88. Уязвимость — это слабое место или пробел в защитных мерах, которые могут существовать как в цифровой, так и в физической среде. Когда речь идет о действиях в Интернете, факторы уязвимости могут включать в себя слабые места в защитных мерах по обеспечению безопасности, которые могут быть использованы для получения несанкционированного доступа к активу, недостатки программного обеспечения в области безопасности, небезопасный дизайн, а также пользователей и код с избыточными привилегиями. В офлайн-среде такие факторы также могут включать в себя слабые стороны людей, например наличие члена группы, который может стать объектом шантажа или принуждения или быть дестабилизирован в результате воздействия большого объема тяжелых для восприятия материалов или других сложных условий работы[113]. Новые факторы уязвимости могут быть созданы путем раскрытия объекту расследования информации о том, что ведется расследование, или о его масштабах. Наконец, факторы уязвимости системы безопасности могут являться резуль-

[109] См. Phishing.org, "What is phishing?". URL: www.phishing.org/what-is-phishing.

[110] См. Veracode, "Man in the middle (MITM) attack". URL: www.veracode.com/security/man-middle-attack.

[111] Ibid.

[112] Адресный фишинг — это мошенническая практика отправки электронных писем якобы от известного или надежного отправителя с целью побудить лиц, которым они адресуются, раскрыть конфиденциальную информацию.

[113] Дополнительную информацию о стрессоустойчивости и самопомощи см. в главе V.D ниже.

татом воздействия внешних угроз, таких как новые вредоносные программы и вирусы, о которых ведущим расследования лицам следует знать. При составлении карт рисков безопасности и оценке рисков эти виды уязвимостей следует учитывать.

89. Лицам, проводящим расследования с использованием открытых данных, следует знать также о перечисленных ниже факторах уязвимости в онлайн-среде.

a) Куки

90. Куки — это небольшой файл, во многих случаях отправляемый веб-сайтом и либо хранимый в памяти компьютера пользователя, либо записываемый на диск компьютера для использования браузером. Куки часто необходимы для правильного функционирования веб-сайта, например для сохранения предпочтений пользователя на сайте и его личных данных, чтобы избавить его от необходимости повторно вводить данные при последующих посещениях. Куки были разработаны так, что они могут собирать и хранить большой объем данных — часто конфиденциальных — о посетителях и их посещениях. Некоторые из них превратились в централизованные инструменты, которые можно использовать для сбора данных, позволяющих составить представление об интересах и привычках пользователя при просмотре веб-сайтов. Куки могут храниться в компьютере до тех пор, пока срок их действия не истечет или пока они не будут удалены пользователем.

b) Трекеры

91. Трекер — это тип куки, который использует возможности браузера по ведению учета посещенных веб-страниц, введенных критериев поиска и т. д. Речь идет о постоянных куки, которые регистрируют действия посетителя сайта. В своей простейшей форме трекеры присваивают уникальный идентификатор браузеру пользователя и затем привязывают этот идентификатор ко всем последующим действиям в браузере и поисковым действиям (критерии поиска, посещенные страницы, последовательность посещенных страниц и т. д.). Это дает владельцу трекера возможность увязать друг с другом предыдущие и последующие посещения веб-сайта (или нескольких связанных веб-сайтов), чтобы составить подробное представление о пользователях и типичных для них действиях при просмотре веб-страниц. Трекеры часто встраивают в рекламу, которая затем распространяется по нескольким веб-сайтам, что дает трекеру появляется гораздо больше возможностей для фиксации активности и действий пользователя. Даже посещение «надежного» сайта может привести к установке трекеров на компьютер пользователя и отслеживанию его последующих действий в Интернете.

c) Веб-маяки

92. Веб-маяк — это механизм для отслеживания активности и действий пользователя. Веб-маяки представляют собой небольшой и незаметный (зачастую невидимый) элемент на веб-странице (иногда столь же маленький, как один прозрачный пиксель), но при его отображении браузером данные об этом браузере и связанном с ним компьютере отсылаются третьей стороне. Веб-маяки могут использоваться наряду с куки для запуска процесса сбора и передачи данных, а также для уникальной идентификации пользователей и регистрации типичных для них действий при просмотре веб-страниц. Веб-маяки тесно связаны с сайтами социальных сетей, для которых выявление отношений и сетей является ключевым компонентом создания сайтов. Наконец, веб-маяки могут использоваться в электронном письме в формате HTML для сбора сведений и предоставления отчетов о личности пользователя, а также для доступа ко всем куки, которые ранее были сохранены на данном компьютере.

d) Другие коды и скрипты

93. Все большее число веб-сайтов используют небольшие фрагменты кода, загружаемые браузером посетителя и способные хранить информацию о посещении. Такой код может влиять на то, как выглядит веб-сайт, как веб-сайт реагирует на вводимые данные и как браузер реагирует на веб-сайт. Код способен также хранить конфиденциальные данные, связанные с учетными данными посетителей, их действиями и т. д. Сбор данных может быть постоянным, они могут передаваться третьей стороне.

C. Соображения, касающиеся инфраструктуры

94. Под инфраструктурой понимаются структуры, объекты и системы, включая как программное, так и аппаратное обеспечение, необходимые для проведения расследований с использованием открытых данных. Инфраструктура должна обеспечивать меры безопасности (и обеспечиваться такими мерами сама), достаточные для защиты и сохранения

активов и данных организации. Для обеспечения устойчивости инфраструктуры следует предусматривать меры по смягчению последствий, которые позволят гарантировать непрерывность процессов в случае любого из следующих событий:

a) перебои в подключении к Интернету или его исчезновение;

b) нарушение или потеря доступа к сохраненным данным;

c) утрата, повреждение или уничтожение данных;

d) нарушение предоставления услуг программного обеспечения или его прекращение;

e) повреждение или утрата аппаратного оборудования;

f) несанкционированный доступ к устройствам;

g) несанкционированный доступ к сети;

h) случайное удаление данных или манипулирование ими;

i) намеренное уничтожение данных или манипулирование ими;

j) утечка данных или их похищение в целях вымогательства.

95. Необходимая архитектура определяется масштабом онлайн-мероприятий, которые необходимо осуществить в рамках расследования, характером расследования и предметом интереса, а также имеющимися финансовыми средствами для создания, поддержания и модификации инфраструктуры по мере необходимости.

1. Инфраструктура

96. Инфраструктура для расследований с использованием открытых данных будет включать в себя как минимум компоненты, перечисленные ниже, а дополнительные функции вносятся в соответствии с нуждами конкретных стратегий расследования.

a) Устройства

97. Лица, проводящие расследования с использованием открытых данных, должны иметь оборудование для доступа к онлайн-контенту, например настольный компьютер, ноутбук, планшет или смартфон. Аппаратное и иное оборудование следует защищать паролем, активировать на нем полнодисковое шифрование и в идеале использовать многофакторную аутентификацию[114]. Для всего оборудования следует регулярно создавать резервные копии. Когда аппаратное оборудование не используется, его следует надежно хранить, чтобы доступ к нему имел только его непосредственный пользователь и имеющий разрешение персонал. Личное оборудование не следует использовать для действий профессионального характера. Аналогичным образом оборудование, связанное с расследованием, не следует использовать в личных целях из-за риска увязки личных социальных сетей с виртуальными личностями, созданными для целей расследования[115].

b) Интернет-соединение

98. В идеале ведущие расследование лица должны иметь надежное, стабильное и частное подключение к Интернету и избегать использования общественных сетей Wi-Fi. Хотя бесплатные общественные сети Wi-Fi (в том числе получастные сети, например те, которые предоставляют гостиницы или интернет-кафе) весьма удобны, этот вариант использования очень опасен и сопряжен с многочисленными угрозами, самой большой из которых является возможность хакеров внедриться между пользователем и точкой подключения. Использование личной мобильной точки доступа, защищенной паролем, требует финансовых вложений, но это необходимо для обеспечения безопасности действий по расследованию в Интернете. Кроме того, хотя проводящее расследование лицо не всегда может контролировать этот фактор, наличие надежного и стабильного подключения к

[114] Многофакторная аутентификация — это усовершенствованный механизм безопасности, при использовании которого для входа в учетную запись пользователь должен предъявить два типа учетных данных, например предоставить как пароль, так и биометрические данные (отпечаток пальца) или смарт-карту. См. United States, National Institute of Standards and Technology, "Back to basics: multi-factor authentication (MFA)". URL: www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication.

[115] Выполнение этой рекомендации может быть затруднено во время командировок, поскольку многие проводящие расследование лица берут с собой рабочее устройство, но в нерабочее время они могут пожелать или им может понадобиться использовать его в личных целях. Поэтому организациям, проводящим расследования с использованием открытых данных, следует разработать разумный порядок использования оборудования в ходе командировок.

Интернету предпочтительно с точки зрения как функционала, так и безопасности. При использовании виртуальной частной сети (VPN) на нестабильном соединении проводящим расследование лицам следует устанавливать механизм, обеспечивающий отказобезопасность, с тем чтобы в случае обрыва соединения их IP-адрес не был раскрыт.

c) Веб-браузеры

99. Одним из основных инструментов онлайн-расследований является веб-браузер, который используется для запросов, поиска и получения доступа к веб-сайтам, размещенным в Интернете. Веб-браузеры служат основным интерфейсом взаимодействия проводящих расследования лиц с Интернетом, но при этом их зачастую не учитывают как один из источников риска. Современные веб-браузеры постоянно модифицируются и наделяются широким спектром встроенного функционала для удовлетворения огромного множества требований. Веб-браузеры являются также одной из ключевых мишеней для лиц, намеревающихся вести слежку или совершать атаки на противника, поскольку существующий функционал может быть использован не по назначению, а дополнительные функции можно добавить относительно легко. Веб-браузер имеет одновременный доступ к Интернету и к компьютеру и, соответственно, к потенциально идентифицирующей пользователя информации. Посредством утечки данных через веб-браузер может быть раскрыт объем данных, позволяющий предупредить объект расследования. Современные веб-браузеры имеют ряд встроенных функций и могут наделяться множеством дополнительных функций, так называемыми расширениями к браузерам, которые по отдельности или в совокупности способны приводить к утечке данных, что, в свою очередь, приводит к выявлению факта расследования, идентификации проводящего его лица или определению его направления и связанной с этим поисковой деятельности. Веб-браузеры также по умолчанию могут загружать и выполнять компьютерный код, полученный с какого-либо веб-сайта. Наличие и/или функции компьютерного кода могут быть неочевидны для проводящих расследование лиц, однако код может оказаться способен изменять доставляемый им цифровой контент, получать доступ к функционалу и данным на их компьютерах и даже обеспечивать выполнение компьютерами действий, отличных от ожидаемых. Лицам, проводящим расследования с использованием открытых данных, следует стремиться минимизировать эти риски посредством использования безопасных, обновляемых, регулярно проверяемых веб-браузеров, а также пользования соответствующим программным обеспечением и установки плагинов, смягчающих некоторые из вышеописанных рисков[116].

2. Меры безопасности

100. Основные элементы инфраструктуры могут быть использованы для идентификации пользователей и их местоположения. Для соблюдения принципа анонимности и недопущения возможности идентификации своей личности ведущим расследование лицам следует использовать для маскировки своих интернет-соединений перечисленные ниже стратегии. Эти стратегии позволяют маскировать местоположение и IP-адрес, а также машину, скрывая ее идентификационные признаки, операционную систему и браузер.

a) Соединение с маскировкой

101. IP-адрес может становиться источником информации, которую можно использовать для атаки на инфраструктуру организации. Лицам, проводящим расследования с использованием открытых данных, следует прибегать к использованию VPN, прокси-серверов или другого программного обеспечения для маскировки IP-адресов своих компьютеров, что означает, что при раскрытии IP-адреса в Интернете он не будет увязан с проводящим расследование лицом или его организацией. VPN также создают зашифрованный канал связи между компьютером ведущего расследование лица и VPN-сервером, таким образом любые сети/узлы, через которые проходит соединение, будут видеть только зашифрованные данные, что обеспечивает дополнительный уровень защиты. Однако некоторые страны и веб-сайты блокируют отдельные VPN, а факт их использования может привлечь внимание третьих сторон к действиям в рамках расследования как к потенциально подозрительным. В идеале VPN должны позволять ведущим расследование лицам использовать несколько IP-адресов с возможностью быстрого переключения между ними

[116] Актуальные рекомендации в отношении веб-браузеров и других мер операционной безопасности размещены на платформе Ресурсного центра компьютерной безопасности Национального института стандартов и технологии США (https://csrc.nist.gov).

в случае такой необходимости. IP-адреса не должны быть привязаны к какой-то одной стране, а должны быть разделены таким образом, чтобы отражать несколько разных местоположений по всему миру.

b) Маскировка машины

102. Для маскировки некоторых параметров, которые могут быть использованы для идентификации пользователей, ведущие расследование лица могут использовать виртуальные машины, которые представляют собой программы или операционные системы, эмулирующие работу отдельного компьютера. Использование виртуальной машины, по сути, создает новый компьютер внутри компьютера — среду, полностью отделенную от остальной машины. Виртуальная машина способна также выполнять такие задачи, как запуск приложений и программ, как если бы она являлась отдельным компьютером[117], что позволяет использующему ее при расследовании лицу появляться в онлайн-среде как другой субъект. Использование виртуальной машины дает ведущим расследование лицам систему для смены браузера, агента пользователя, программного обеспечения, открытых портов, операционной системы и другой информации о машине, что позволяет казаться другим субъектом при каждом выходе в Интернет. В идеале инфраструктура должна позволять ведущему расследование лицу использовать виртуальную машину, которая маскирует реально используемую. Виртуальные машины могут быть уничтожены и воссозданы, восстановлены до предыдущей точки, по-разному настроены, реплицированы для дальнейшего использования или сохранены для будущих нужд. В качестве альтернативы ведущие расследование лица могут использовать более обременительный, но также относительно эффективный подход, а именно изменять свои внешние данные вручную, используя разные браузеры при каждом выходе в Интернет, изменяя настройки для ограничения уникальности следов своих машин и используя предотвращающие отслеживание плагины.

3. Прочая инфраструктура

103. Перед началом работы ведущим расследование лицам следует изучить другие объекты инфраструктуры на предмет защиты своих сетей и инфраструктуры, включая следующие системы:

a) резервные системы;

b) системы ведения журналов для аудита деятельности и отслеживания действий пользователей;

c) системы раздельного хранения и подходящие места хранения для сбора цифровых материалов, выявленных в ходе поиска. Для защиты данных от внешнего воздействия организациям следует иметь платформы (такие как хранилища доказательств, базы данных или другие системы управления информацией), хранимые отдельно от основных сетей. Платформы должны состоять из двух основных частей, одна из которых подключена к Интернету, а другая — отключена от него. В некоторых случаях может быть целесообразно как можно скорее переносить данные из инфраструктуры, подключенной к Интернету, в более безопасную сеть/хранилище для безопасного просмотра информации.

D. Соображения, касающиеся пользователей

104. Одним из самых слабых звеньев любой системы безопасности является пользователь. Даже при наличии совершенной инфраструктуры соблюдение принципов безопасности не будет обеспечено без адаптации поведения пользователей путем регулярного обучения и надзора. Безопасность — это ответственность каждого. Пользователям не следует осуществлять действия, которые могут подвергнуть рискам данные или людей, без надлежащего обучения тому, как смягчить эти риски. Ведущих расследование лиц следует обучать тому, как оценивать уместность того или иного поведения при осуществлении различных действий в Интернете.

105. Анонимность может помочь минимизировать ущерб в ситуациях, когда субъекты, которые могут умышленно нарушить информационную безопасность, пытаются отследить источник действия до конкретной сети или пользователя[118]. Любое действие в Интернете может быть отслежено третьими лицами, поэтому ведущим расследование лицам при совершении действий в Интернете следует всегда считаться с такой угрозой. Чаще всего

[117] См. Techopedia, "Virtual machine (VM)", 21 May 2020. URL: www.techopedia.com/definition/4805/virtual-machine-vm.

[118] Отследить — обнаружить исходную точку для кого-либо или чего-либо путем продвижения по следу информации или ряда событий в обратном направлении.

отслеживают IP-адреса, веб-браузеры и разрешение экрана (используется для идентификации оборудования), а также время навигации и активность на веб-сайте (например, введенные поисковые запросы или посещенные страницы). Субъекты, которые могут умышленно нарушить информационную безопасность, могут попытаться определить источник онлайн-активности. В случае если будет предпринята попытка отслеживания, то такого субъекта следует направить по следу, уводящему в сторону от истинного местонахождения или идентификационных данных лица или организации, проводящих расследование. Это можно сделать благодаря мерам, позволяющим представить свой доступ в Интернет как осуществляемый из другого места, например с помощью VPN, или иным лицом путем создания и использования виртуальных личностей[119].

106. Маскировка соединения и машины при проведении онлайн-расследования обеспечивает важную защиту, но она может быть ослаблена, если пользователи сами раскрывают себя, идентифицируясь на сайте или, например, используя личную информацию для регистрации или входа в платформу социальных сетей или в другой частный аккаунт. Ведущим расследование лицам никогда не следует использовать свои личные учетные записи для проведения расследований или входить в личные учетные записи в веб-браузере, через который они ведут расследования с использованием открытых данных. Для создания некоторых учетных записей могут быть затребованы фотографии, номер телефона или адрес электронной почты. Никогда не следует использовать фотографии, телефоны, электронную почту или данные, которые носят личный характер или могут позволить идентифицировать проводящее расследование или другое лицо.

Маскировка пользователя

107. Виртуальная личность[120] — это вымышленная личность или профиль в Интернете, которые могут быть использованы для безопасного осуществления в рамках расследования тех или иных действий на платформах социальных сетей и других открытых веб-платформах, если для получения доступа к их контенту пользователь должен войти в систему. Виртуальная личность также может включать в себя виртуальные учетную запись, адрес электронной почты или учетную запись в мессенджере, базу данных, продукт или приложение, которые используют в Интернете вымышленную, а не реальную личность человека. С точки зрения безопасности лицам, проводящим расследования с использованием открытых данных, следует создавать и использовать виртуальные личности для проведения онлайн-действий в рамках расследований с использованием материалов из открытых источников. Это делается для того, чтобы, если субъект, который может попытаться умышленно нарушить информационную безопасность, попробует отследить онлайн-действия соответствующего профиля, такой субъект получил последовательную и убедительную информацию, происходящую от виртуальной личности и не раскрывающую реальную информацию о проводящих расследование лице или организации или о содержании или направленности расследования. Это также является важной мерой безопасности для защиты тех, кто может поддерживать расследование. Виртуальные профили, учетные записи и осуществляемые с их использованием действия следует планировать[121], использованную для создания учетных записей информацию следует регистрировать, а осуществленные с использованием таких учетных записей действия — фиксировать, с тем чтобы при необходимости их можно было впоследствии объяснить, например в суде[122].

[119] Вопрос о виртуальных личностях рассматривается также в главе II.C, главе III.F и главе IV.A и C выше.

[120] При любом использовании виртуальных личностей следует находить оптимальное соотношение между необходимостью обеспечения безопасности и этическим принципом прозрачности. См. главу II.C выше об этических принципах.

[121] См. главу V.C ниже о плане онлайн-расследования.

[122] См. главу VI.D ниже о сохранении.

V

ПОДГОТОВКА

КРАТКОЕ СОДЕРЖАНИЕ ГЛАВЫ

- **Подготовка и стратегическое планирование являются ключевыми факторами тщательного и безопасного расследования.**
- **Подготовка включает в себя три процесса: a) оценку угроз и рисков и разработку плана смягчения этих угроз и рисков; b) оценку информационного ландшафта; c) разработку плана расследования. Эти процессы могут пересекаться друг с другом и/или повторяться на протяжении всего жизненного цикла расследования.**
- **Подготовка включает в себя разработку плана преодоления любых негативных психосоциальных аспектов расследования, например таких, которые могут стать следствием воздействия тяжелых для восприятия или других потенциально травмирующих материалов.**
- **Подготовка включает в себя разработку плана обращения с любой собранной информацией на протяжении всего ее жизненного цикла, включая момент и условия ее удаления, передачи и определение лиц, которые могут иметь к ней доступ.**
- **В рамках подготовки следует проводить оценку программного обеспечения и других инструментов, использование которых может быть целесообразным. Ведущим расследование лицам следует понимать, каковы положительные и отрицательные стороны использования коммерческих ресурсов, ресурсов, разработанных по специальному техническому заданию, и ресурсов с открытым исходным кодом.**

108. Лицам, проводящим расследования с использованием открытых данных, следует начинать действия в Интернете в рамках расследования только после принятия определенных подготовительных мер. В состав подготовительных шагов следует включать проведение оценки цифровых угроз и рисков, а также оценку цифрового ландшафта[123]. После этого ведущим расследование лицам следует разработать план онлайн-расследования с учетом результатов этих оценок. Каждый из этих трех процессов более подробно описан ниже.

109. На организационном уровне важно также внедрить до начала сбора и хранения информации политику в отношении сохранения данных, удаления данных, доступа к данным и обмена данными в соответствии с приводимым ниже описанием.

A. Оценка цифровых угроз и рисков

110. Анализ потенциальных угроз и принятие стратегии управления рисками (будь то физическими, цифровыми или психосоциальными) обеспечит соблюдение принципов безопасности и этических принципов. Уже в самом начале следует провести оценку цифровых угроз и рисков, определив общие и конкретные для данного случая угрозы, которые могут возникнуть в результате действий в Интернете, в частности посещения целевых веб-сайтов, постоянного онлайн-мониторинга конкретных источников или извлечения данных (веб-скрейпинга) из платформ социальных сетей. В оценку следует включать элементы традиционного анализа угроз, такие как выявление всех лиц, которые могут умышленно нарушить информационную безопасность, оценка интересов и возможностей таких лиц, а также вероятность атаки, анализ факторов уязвимости и принятие мер защиты для минимизации этих факторов уязвимости. В ходе такой оценки целесообразно проводить консультации с экспертами по безопасности или получать их отзывы, особенно это касается экспертов, компетентных в области кибербезопасности[124]. Оценку следует периодически пересматривать и при необходимости обновлять. Кроме того, могут потребоваться дополнительные оценки в отношении отдельных видов онлайн-действий или в случае появления новых лиц, которые могут умышленно нарушить информационную безопасность[125].

B. Оценка цифрового ландшафта

111. Лицам, проводящим расследования с использованием открытых данных, следует понимать цифровую среду расследуемой ситуации. Тип доступной и используемой технологии, в том числе кем она используется, будет влиять на типы доступных цифровых данных. Для этого необходимо выявить наиболее часто используемые онлайн-платформы, коммуникационные услуги, платформы социальных сетей, мобильные технологии и мобильные приложения, используемые в географическом регионе, которого касается расследование. Например, при расследовании военных преступлений проводящим расследование лицам будет необходимо знать, какие виды транспорта, ИКТ и цифровых медиа используют все стороны, участвующие в вооруженном конфликте, а также сторонние наблюдатели или другие свидетели, чтобы понимать, какие виды информации с наибольшей вероятностью могут быть зафиксированы и распространены в сети.

112. Проводящим расследование лицам следует проанализировать категории людей, которые используют каждую из этих технологий в данном географическом регионе или имеют к ней доступ. В этой связи проводящим расследование лицам следует осознавать, что созданный пользователями общедоступный цифровой контент, включая сообщения в социальных сетях и информацию, распространяемую через сетевые платформы, может не в равной степени отражать весь масштаб нарушений в отношении всех лиц и групп. Это объясняется тем, что использование цифровых технологий может быть неоднородным, в частности по признаку

[123] См. ниже Приложение II с шаблоном оценки цифровых угроз и рисков и Приложение III с шаблоном оценки цифрового ландшафта.

[124] Общую информацию об угрозах и рисках при проведении расследований с использованием открытых данных см. в главе IV выше, посвященной безопасности.

[125] См. Приложение II ниже с шаблоном оценки цифровых угроз и рисков.

гендера[126], этнической принадлежности, религии, убеждений, возраста, социально-экономического статуса, принадлежности к расовому, языковому[127], этническому или религиозному меньшинству, принадлежности к коренному народу, миграционного статуса и географического местоположения[128]. Такой дисбаланс может являться результатом отсутствия доступа к устройствам, средствам или ресурсам[129], в результате чего соответствующие лица не имеют возможности создавать или загружать онлайн-информацию о касающихся их проблемах или нарушениях. Еще один возможный фактор — у упомянутых, среди прочих, лиц могло не быть доступа к равному образованию и поэтому их технические навыки не столь развиты. В результате пересекающихся форм дискриминации некоторые слои общества могут становиться вдвойне невидимыми в Интернете. Например, информация о женщинах и девочках, принадлежащих к одной из упомянутых выше маргинализированных групп, может быть представлена в открытых источниках в еще меньшем объеме. В результате воздействия этих факторов такие лица не создают контент сами или оказываются не охвачены в нем, что искажает результаты любого онлайн-расследования.

113. Кроме того, неравенство доступа к технологиям среди всех слоев общества может также приводить не только к смещению акцентов в представленности тех или иных лиц в онлайн-контенте, но и к неточному отражению в Интернете распространенности различных типов нарушений, в частности в том, что касается пользовательского контента. Например, если женщины пользуются мобильными телефонами, принадлежащими мужчинам из их семьи, или используют учетную запись совместно с кем-то еще, то, возможно, они не станут обсуждать такие деликатные темы, как сексуальное и гендерное насилие или вопросы, связанные с сексуальным и репродуктивным здоровьем. Помимо этого, пользовательский контент в социальных сетях, включая фотографии и видео, может в большей степени отображать какие-то определенные нарушения. Например, сексуальное и гендерное насилие, возможно, совершаемое в частной обстановке, может оказаться сложнее представить с помощью графических материалов, чем, например, разместить фотографии выселений.

114. Хотя некоторые из этих факторов могут быть смягчены посредством обращения к онлайн-информации различного типа, а не только к пользовательскому контенту, эти же факторы необходимо учитывать при анализе других типов информации из открытых источников. Например, при получении доступа к государственным данным и статистике проводящим расследование лицам всегда следует задаваться вопросом о том, точно ли эти данные отражают все сегменты и аспекты общества[130]. В этой связи могут быть оценены ряд ключевых вопросов и технологий, в зависимости от того, что является актуальным для конкретного расследования исходя из его географического и временного охвата. Проводящим расследование лицам следует принимать во внимание пол, возраст, географию, социально-экономические различия и другую соответствующую демографическую информацию. Цель этой оценки — позволить проводящим расследование лицам лучше понять расследуемые ситуации с целью разработки эффективных стратегий онлайн-расследования, а также принудить их заранее проанализировать возможные искажения в данных, доступных в Интернете. Все эти категории не обязательно актуальны для каждого расследования, поэтому проводящим его лицам следует адаптировать оценку цифрового

[126] Например, женщины, девочки и лесбиянки, геи, бисексуальные, трансгендерные и интерсекс-люди могут не иметь мобильного телефона или иметь доступ только к телефону, принадлежащему всей семье. Более подробно вопрос о так называемом «межгендерном цифровом разрыве» рассмотрен в документе A/HRC/35/9. См. также резолюцию 32/13 Совета по правам человека и Araba Sey and Nancy Hafkin, eds., *Taking Stock: Data and Evidence on Gender Equality in Digital Access, Skills, and Leadership* (Macao, China, EQUALS Global Partnership and the United Nations University, 2019). URL: www.itu.int/en/action/gender-equality/Documents/EQUALS%20Research%20Report%202019.pdf.

[127] Лица, принадлежащие к языковым меньшинствам, например, могут столкнуться с барьерами в части доступа к онлайн-пространству, которое обычно работает на доминирующем языке. Однако некоторые языковые меньшинства могут также располагать собственным онлайн-пространством, работающем на их родном языке или использующем такой язык. Соответственно, проводящим расследование лицам может потребоваться осуществлять поиск на языках меньшинств (в том числе на языках коренных народов).

[128] Например, в сельской местности возможности подключения к Интернету могут быть менее широкими.

[129] Например, отсутствие физического доступа к быстрому интернет-соединению или невозможность приобрести устройства или оплатить абонентскую плату.

[130] См. в целом УВКПЧ, «Правозащитный подход к данным. Никого не оставить без внимания в Повестке дня в области устойчивого развития на период до 2030 года» (Женева, 2018). URL: www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData_RU.pdf.

ландшафта к требованиям их конкретного случая[131]. Полный перечень категорий информации, которые могут включаться в оценку цифрового ландшафта, приведен в Приложении III ниже.

C. План онлайн-расследования

115. Перед началом расследования с использованием открытых данных следует составить план онлайн-расследования[132], который охватывает: a) общую стратегию расследования; b) конкретные действия в Интернете в рамках расследования. Если онлайн-расследование является частью более широкого расследования с использованием традиционных методов, таких как получение показаний свидетелей или сбор вещественных доказательств, то план онлайн-расследования следует интегрировать в основной план расследования. Проводящим расследование лицам следует учесть в плане расследования гендерные аспекты, с тем чтобы обеспечить охват всех гендерно значимых проблем и учесть дифференцированный характер доступа к технологиям[133]. В плане онлайн-расследования следует охватить перечисленные ниже темы.

1. Цели и планируемая деятельность

116. В плане следует указать цели и приоритеты расследования с использованием открытых данных, предлагаемую стратегию достижения этих целей и сроки их реализации.

2. Стратегия управления рисками

117. В план следует включать ключевые выводы вышеупомянутой оценки цифровых угроз и рисков, такие как потенциальные киберугрозы, а также стратегию управления рисками, в том числе способы выявления брешей или атак, реагирования на них и последующего восстановления.

3. Составление карты участников и возможностей сотрудничества

118. Лица, проводящие расследования с использованием открытых данных, могут счесть целесообразным составление карты других субъектов, проводящих аналогичные или пересекающиеся расследования, чтобы оценить, как их деятельность может повлиять друг на друга, и изучить потенциал партнерств и возможности для сотрудничества. Это может включать в себя выявление цифровых архивистов, журналистов или других групп или отдельных лиц, сохраняющих онлайн-контент, который может иметь отношение к расследованию. При составлении такой карты следует также учитывать потенциальную предвзятость и ограничения других участников, в связи с которыми выводы третьих сторон будут не полностью отражать всю сложность конкретной ситуации или не будут охватывать определенные группы из-за присущей цифровой сфере предвзятости, на которую не делаются поправки, как описано выше. В случае создания партнерств может быть целесообразно заключать письменное соглашение об обмене информацией.

4. Ресурсы

119. В плане следует определить ресурсы, необходимые для проведения запланированных мероприятий, включая персонал, обучение, инструменты и оборудование. Оценка кадровых потребностей может включать количество членов группы, необходимых для выполнения задач, их компетенции, инклюзивность и многообразие членов группы, а также оценку дополнительных потребностей в обучении. Это может включать в себя оценку необходимой инфраструктуры, включая аппаратное и программное обеспечение, а также финансовые затраты на сохранение цифрового материала в долгосрочной перспективе. В таком плане следует также предусмотреть наличие специальных ре-

[131] Шаблон см. в Приложении III ниже.

[132] См. Приложение I ниже с шаблоном плана онлайн-расследования.

[133] Более подробные рекомендации в отношении учета гендерной проблематики см. в публикации *Integrating a Gender Perspective into Human Rights Investigations: Guidance and Practice* (United Nations publication, Sales No. 19.XIV.2).

сурсов для целей обеспечения психологического благополучия ведущих расследование лиц с учетом гендерных факторов, особенно в тех ситуациях, когда в ходе расследования используется тяжелый для восприятия контент из открытых источников или же проводящие расследование или причастные к нему третьи лица могут подвергнуться особому риску репрессий в случае раскрытия их личности или нарушения неприкосновенности их частной жизни[134].

5. Функции и обязанности

120. В случае работы в группе или с внешними партнерами следует четко определять функции и обязанности лиц, проводящих расследования с использованием открытых данных, учитывая при этом необходимость координации деятельности, в том числе необходимость не допускать дублирования при осуществлении действий и сборе данных. Кроме того, в этом разделе плана следует проанализировать возможные потребности в специальных областях знаний для конкретного расследования и возможную необходимость консультаций с экспертом или его привлечения в случае его отсутствия в сформированной группе. Специальные области знаний могут включать в себя цифровую криминалистику, анализ спутниковых снимков и науку о данных. В некоторых областях знаний могут потребоваться активные усилия по выявлению экспертов с учетом многообразия гендерных и других аспектов, с тем чтобы обеспечить инклюзивность и многообразие проводящей расследование группы и ее анализа.

6. Документация

121. Расследования с использованием открытых данных следует документировать так, чтобы обеспечить эффективное управление ими и соблюдение принципа ответственности. В случае судебного разбирательства эта документация должна позволить проводившим расследование лицам продемонстрировать, что собранные доказательства относимы и обладают доказательной силой, а также объяснить, какие шаги были предприняты или не предприняты в ходе онлайн-деятельности и почему. Независимо от того, ставятся задачи самостоятельно или руководителем, в системе следует предусмотреть механизм создания задач по конкретным действиям в рамках расследования, включая онлайн-действия, например запросы на поиск информации о конкретном лице или другие запросы. В результаты выполнения задач, включая отчеты, следует включать описание использованных методологий и методов. В отчетности следует разделять оперативную информацию, конфиденциальность которой может потребоваться сохранять в целях защиты источников и методов расследования, и полученную в рамках расследования информацию, которая должна быть раскрыта в ходе судебного разбирательства.

122. План онлайн-расследования следует регулярно пересматривать и при необходимости вносить в него изменения. См. шаблон плана онлайн-расследования в Приложении I ниже.

D. План повышения стрессоустойчивости и самопомощь

123. Хотя лица, проводящие расследования с использованием открытых данных, могут не проводить очные беседы и непосредственно не посещать места преступления, особенности цифровых исследований заключаются в том, что они могут столкнуться с просмотром, сбором и анализом значительного количества тяжелой для восприятия или иным образом травмирующей цифровой информации, что, среди прочего, может привести к вторичной травме. Поэтому им следует знать о принципах самопомощи[135], а руководителям расследований следует развивать организационную среду, в которой ценится самопомощь и учет гендерных и культурных особенностей. Это следует предусмотреть на подготовительном этапе расследования путем разработки плана повышения стрессоустойчивости и смягчения негативных психосоциальных последствий расследования, ко-

[134] Например, расследователи могут столкнуться с ненавистническими высказываниями или преследованием в Интернете, и эти нападки могут носить гендерный характер (например, женщины и лесбиянки, геи, бисексуальные, трансгендерные, квир- и интерсекс-люди могут столкнуться с повышенными рисками ненавистнических высказываний в Интернете, доксинга, угроз изнасилования и других угроз применения насилия сексуального или гендерного характера). См., например, Amnesty International, "Toxic Twitter — a toxic place for women". URL: www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/.

[135] Дополнительную информацию о важности самопомощи для лиц, работающих в сфере расследований нарушений прав человека, см. в документе УВКПЧ: OHCHR, *Manual on Human Rights Monitoring* (Geneva, 2011), chap. 12 on trauma and self-care, pp. 20–39. URL: www.ohchr.org/Documents/Publications/CoI_Guidance_and_Practice.pdf.

торые могут быть различными в зависимости от гендерной принадлежности, культуры и возраста. Такой план необходим по этическим соображениям как элемент поощрения и уважения прав человека каждого члена расследовательской группы. Это также необходимо для обеспечения максимальной физической и цифровой безопасности. Даже при надлежащей подготовке человек, находящийся в состоянии стресса, может стать фактором уязвимости для безопасности членов группы, защиты информации и качества работы. Для обеспечения надлежащего выполнения плана следует выделить специальное время и ресурсы, особенно если предполагается, что онлайн-расследование может включать просмотр большого количества тяжелых для восприятия изображений, в том числе материалов насильственного характера или иного шокирующего контента. Стратегии смягчения потенциальных негативных последствий просмотра тяжелого для восприятия контента разнообразны, но, как правило, они делятся на три категории: индивидуальная осведомленность, тактика минимизации воздействия и поддержка коллектива.

124. Во-первых, лицам, проводящим расследования, следует иметь осведомленность о своем исходном поведении, а также поведении своих коллег по группе, включая режим работы, отдыха, сна и питания, чтобы можно было выявить и устранить какие-либо отклонения. Политика, согласно которой расследователи работают в паре, может помочь в выявлении, поскольку люди сами по себе могут не осознавать или не хотеть признавать изменения в своем собственном поведении, которые могут быть легче замечены другими. Членам группы следует с пониманием и уважением относиться к различиям в реакции на тяжелые для восприятия и другие материалы, которые могут вызывать сильные эмоции, и учитывать, что такие различия могут варьироваться у разных людей, гендеров и культурных групп, а также со временем у конкретных людей из-за степени стресса, который они испытывают, и других ситуационных факторов. Расследователям следует также признать, что эмоциональная реакция на тяжелый для восприятия или шокирующий контент часто вполне нормальна и не является признаком слабости, а может быть признаком нормальности — и даже силы.

125. Во-вторых, следует принять тактику минимизации воздействия вредного контента. Общие стратегии в этой связи могут включать следующие меры: отключение звука при первом просмотре потенциально натуралистического контента или когда это не требуется для решения непосредственной аналитической задачи, поскольку так много вызывающего эмоции контента заложено в звуке; максимально возможное уменьшение размеров экранов; скрытие тяжелого для восприятия материала при анализе обстоятельств, в которых произошло конкретное действие, а не самого действия; маркировка любого тяжелого для восприятия контента, содержащегося в наборе данных, чтобы никто не просматривал этот контент, не зная заранее, что им предстоит увидеть; предупреждение друг друга при обмене натуралистическим контентом, чтобы уменьшить элемент неожиданности; работа в парах; недопущение работы в уединении или поздно ночью; и регулярные перерывы по мере необходимости.

126. В-третьих, лицам и организациям следует способствовать формированию чувства принадлежности к коллективу между членами группы, что может оказать защитное воздействие, по сути воспроизводя чувство товарищества, которое может возникнуть при проведении расследований в полевых условиях. Этого можно достичь с помощью регулярных разборов результатов, что может уменьшить степень изоляции и помочь расследователям лучше понять положительное влияние их работы; групповые выезды, включая празднование важных этапов расследования; и групповой тренинг по стратегиям повышения стрессоустойчивости. Попытки повысить стрессоустойчивость могут быть особенно эффективными, если они предпринимаются на индивидуальном, культурном и структурном уровнях, например путем расширения возможностей лиц критически осмысливать свои психосоциальные потребности при работе над расследованием и создания среды, в которой серьезно относятся к психосоциальным аспектам работы, явно и неявно поощряются поддерживающие практики и обеспечивается инклюзивность и разнообразие.

E. Политика и инструменты обработки данных

127. Следует разрабатывать, внедрять и соблюдать в ходе расследования политику обработки, сохранения и уничтожения данных. Организациям следует разработать политику сохранения информации (политика сохранения) и удаления информации (политика удаления), когда это необходимо, а также политику доступа к информации (внутри организации) и обмена информацией (с внеш-

ними сторонами). Кроме того, полезной может оказаться специальная политика по созданию и использованию виртуальных личностей, а также политика доступа к утвержденному программному обеспечению и используемым инструментам.

1. Политика обработки данных

a) Политика сохранения данных

128. Политика сохранения данных важна для обеспечения соблюдения многих законов о защите данных и правил сохранения данных. В некоторых случаях существуют минимальные требования к срокам сохранения данных, а в других — максимальные ограничения сроков их сохранения. В политике следует отразить подходы к хранению долговременных данных и ведению соответствующей документации с целью выполнения юридических и бизнес-требований к архивированию данных. В различных стратегиях сохранения данных сопоставляются юридические задачи и задачи обеспечения конфиденциальности с экономическими соображениями и соображениями служебной необходимости, чтобы определить сроки хранения, правила архивирования, форматы данных и допустимые средства хранения, доступа и шифрования[136]. Понимание действующих правил необходимо для разработки таких стратегий.

b) Политика удаления данных

129. Удаление части набора данных без четкой политики удаления и сохранения, а также без ведения журналов регистрации того, что, кем и когда было удалено — а также для каких целей, — может вызвать значительные проблемы, в частности когда информация может быть использована в суде. Лицам, проводящим расследования, следует соблюдать применимые нормативные акты, касающиеся удаления цифровых данных, и учитывать, что могут возникнуть юридические проблемы, связанные с использованием того или иного метода.

c) Политика доступа к данным

130. Организациям, собирающим и обрабатывающим данные, особенно конфиденциальные, следует иметь четкую политику в отношении того, кто может иметь доступ к различным типам данных. Любые настройки в базах данных или системах должны отражать эту политику.

d) Политика обмена данными

131. Возможно, организациям стоит подумать о разработке политики обмена данными с внешними субъектами. При работе с внешними партнерами следует заключить меморандумы о взаимопонимании или контракты, чтобы обеспечить соблюдение партнерами такой политики.

2. Управление информацией

132. Прежде чем приступить к расследованиям с использованием открытых данных, особенно к сбору и сохранению цифровых материалов, расследователям, группам и организациям следует создать систему управления информацией. Существует целый ряд вариантов такой системы, и в Протоколе не поддерживается какой-то конкретный вариант. Вместо этого ниже представлены основные функциональные возможности, которые могут быть полезны в процессе расследования и в некоторых обстоятельствах могут быть необходимы. Кроме того, как уже говорилось в главе IV, необходимо создать инфраструктуру и протоколы безопасности.

a) Система управления расследованием

133. Система управления расследованием — это система документирования деятельности, проводимой в рамках расследования. Не все организации, проводящие расследования, имеют такие системы, но они настоятельно рекомендуются, особенно для крупных организаций и расследовательских групп. Такие системы можно использовать для распределения задач и составления отчетов о

[136] Yvonne Ng, "How to preserve open source information effectively", in *Digital Witness, Using Open Source Information for Human Rights Investigation, Documentation and Accountability*, Sam Dubberley, Alexa Koenig and Daragh Murray, eds. (Oxford, Oxford University Press, 2020), pp. 143–164.

деятельности, чтобы процесс был структурированным и максимально эффективным, поскольку это может помочь сократить дублирование усилий.

b) Системы управления информацией и доказательствами

134. Системы управления информацией используются для хранения данных, собранных в ходе расследований. Такая система должна быть в состоянии выполнять две различные функции: a) отслеживание сбора и обработки материалов; и b) отбор материала, который может быть использован в качестве доказательства.

3. Инфраструктура — материально-технические соображения и соображения безопасности

135. При разработке инфраструктуры для организации, занимающейся расследованиями с использованием открытых данных, или при выборе инструментов для независимого расследователя необходимо учитывать ряд важных материально-технических соображений и соображений безопасности. В целом существует три подхода к разработке систем: a) создание систем и инструментов на заказ; b) использование находящихся в открытом доступе или бесплатных инструментов и программного обеспечения, доступных в Интернете; или c) приобретение коммерческих продуктов у третьих лиц. Каждый из этих подходов имеет свои преимущества и недостатки, и их успех зависит от конкретных обстоятельств и контекста работы лиц, проводящих расследование. И в этом случае в Протоколе также не пропагандируется ни один из подходов, а представлены преимущества и недостатки каждого из них, а также конкретные факторы, которые следует принимать во внимание при принятии решения о том, какие продукты использовать.

a) Коммерческие продукты

136. Преимущество коммерческих продуктов заключается в том, что частное предприятие может иметь более эффективную инфраструктуру безопасности и быть в состоянии обеспечить постоянную и последовательную техническую поддержку. Однако они имеют очевидный недостаток — стоимость. Кроме того, взаимодействие с третьими сторонами и опора на них может стать проблемой для организаций, старающихся сохранить конфиденциальность своих расследований. Многие коммерческие продукты имеют закрытый исходный код для защиты своей интеллектуальной собственности. Коммерческие продукты могут также вызывать озабоченность относительно права собственности в отношении данных, переносимости и возможности экспорта данных, а также совместимости с другими системами. Кроме того, компании могут реагировать на давление правительства, требующего доступа к частной информации. Основная проблема заключается в том, что, хотя в компаниях есть группы по обеспечению безопасности для защиты своих продуктов и пользователей, пользователи должны быть уверены в том, что компании разработали и будут поддерживать свои системы должным образом и что на более позднем этапе не возникнет скрытых расходов.

b) Созданные на заказ или адаптированные инструменты

137. Преимущество создания инструмента на заказ или адаптации уже существующего инструмента заключается в том, что лица или организации, проводящие расследование, сохраняют контроль над всей системой и своими данными и, как следствие, могут избежать взаимодействия с третьими сторонами. Системы, изготовленные на заказ, также легче интегрировать с другими системами, изготовленными на заказ. Недостатки включают время, стоимость и профессиональные знания и навыки, необходимые для создания и поддержки таких систем, что будет сложной задачей для большинства организаций. Кроме того, при использовании закрытой системы с ограниченным числом бета-тестировщиков и пользователей может быть затруднительно выявление уязвимостей или получение достаточного количества отзывов для максимального улучшения функциональности.

c) Находящиеся в открытом доступе и бесплатные инструменты

138. Находящиеся в открытом доступе инструменты — это инструменты, для которых разработчики открыто опубликовали исходные коды, чтобы любой желающий мог свободно использовать или изменять их. Существует ряд коммерческих продуктов с открытым исходным кодом, а также доступны некоторые бесплатные инструменты с закрытым исходным кодом, но это исключения. Чаще всего инструменты с открытым кодом являются бесплатными. Для небольших организаций с ограниченным бюджетом, а также для крупных организаций с обременительными процедурами закупок платных продуктов, бесплатные инструменты могут стать важной

альтернативой, которую следует рассмотреть. Однако бесплатные для пользователей инструменты могут приносить прибыль другими способами, например за счет продажи данных пользователей и аналитической информации, что поднимает вопросы безопасности и конфиденциальности. Кроме того, использование этих инструментов требует предварительного исследования, чтобы узнать, кто их создал, прошли ли они независимую проверку и являются ли они устойчивыми. Все три аспекта могут подорвать доверие к расследованию. В частности, инструменты могут создать проблемы в правовом контексте, если дело дойдет до суда и инструмент будет оспорен противной стороной. Кроме того, для таких систем и средств программного обеспечения необходим план резервного копирования, а также система миграции и резервного копирования данных в случае их устаревания или отсутствия доступа к разработчикам. Хотя инструменты с открытым исходным кодом могут быть привлекательными для организаций (отчасти из-за того, что другие группы со схожими взглядами используют их), лица и организации, проводящие расследования, должны провести полную, независимую оценку того, как они работают и какие последствия может иметь их использование в конкретном контексте.

139. При принятии решения о создании инструмента на заказ, использовании бесплатного пробного или находящегося в свободном доступе программного обеспечения или покупке продукта расследователям следует учесть рекомендации по соблюдению должной осмотрительности, представленные в приложении V ниже.

VI

ПРОЦЕСС РАССЛЕДОВАНИЯ

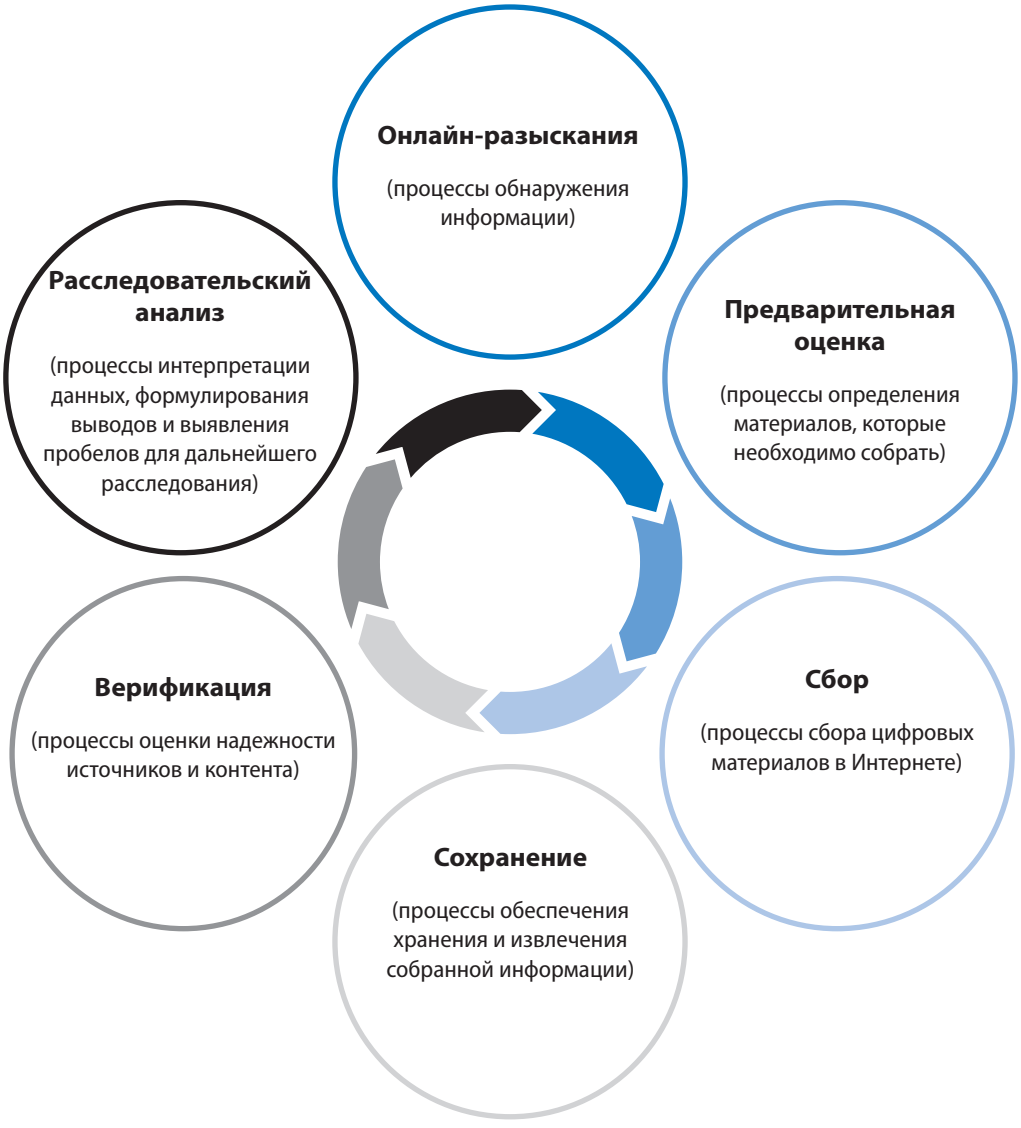
КРАТКОЕ СОДЕРЖАНИЕ ГЛАВЫ

- **Существует шесть основных этапов расследования. К ним относятся: a) онлайн-разыскания; b) предварительная оценка; c) сбор; d) сохранение; e) верификация; f) расследовательский анализ. В совокупности эти действия являются частью цикла, который может повторяться много раз в ходе расследования, поскольку вновь обнаруженная информация приводит к новым направлениям расследования.**

- **Лицам, проводящим расследование, следует документировать свои действия на каждом этапе. Это будет способствовать понятности и прозрачности их расследований, включая цепочки обеспечения сохранности, а также эффективности и результативности их расследований, включая полноту расследования и коммуникацию между членами группы.**

140. При проведении расследований с использованием открытых данных требуются тщательное наблюдение и систематические разыскания для установления фактов в сложной и динамичной цифровой среде. Лицам, проводящим расследования с использованием открытых данных, следует критически подходить к проверке онлайн-контента и уметь оценивать способы искажения цифрового материала или манипуляций с ним. Им следует также применять структурированный подход к онлайн-разысканиям, учитывая предвзятость, заложенную в алгоритмах, и неравенство в плане доступности открытых данных, касающихся конкретных групп, и динамичный характер онлайн-информации. Следует тщательно изучать все предполагаемые факты. В настоящей главе представлен структурированный подход к проведению расследований с использованием открытых данных. На рисунке ниже изображен цикл расследования с использованием открытых данных. Важно отметить, что расследования с использованием открытых данных редко бывают линейными, и часто требуется повторение этого процесса, учитывая циклический характер построения дела. Кроме того, могут быть веские причины для отклонения от этого порядка.

Цикл расследования с использованием открытых данных



A. Онлайн-разыскания

141. Существует два основных процесса онлайн-разысканий: a) поиск, то есть обнаружение информации и источников информации с помощью общей или расширенной методологии поиска; и b) мониторинг, то есть обнаружение новой информации путем последовательного и непрерывного изучения набора постоянных источников.

1. Поиск

142. Поиск в Интернете — это проблемно-ориентированная деятельность, направленная на обнаружение новой информации, имеющей отношение к определенной цели или исследовательскому вопросу. Поиск должен быть структурированным и систематизированным, в том числе начинаться с формулирования четкого вопроса исследования и параметров поиска, а также ключевых слов и операторов[137]. Различные поисковые системы, инструменты поиска, поисковые запросы и операторы поиска дадут разные результаты; поэтому лицам, проводящим расследования, следует проявлять определенную изобретательность и упорство, используя различные средства и каналы, чтобы найти необходимую информацию. Помимо поисковых систем, используемых для поиска информации на индексируемых веб-сайтах, структурированный поиск также может использоваться на платформах социальных сетей и в базах данных. В связи с необходимостью применения разнообразного, разностороннего и отдельного для каждого конкретного случая подхода расследователям следует тщательно документировать свои действия, чтобы их можно было объяснить в посвященных методологии разделах отчетов или в показаниях в ходе судебного разбирательства. Это может быть ретроспективный процесс, не обязательно идущий параллельно с самим исследованием. Однако документирование всегда следует проводить как можно более оперативно. При описании структурированного поиска необходимо зафиксировать следующую информацию:

a) цель и вопросы исследования: формулирование вопроса (вопросов), на нахождение ответа на который (которые) направлен поиск в Интернете, с учетом принципа объективности, изложенного выше;

b) факты, предположения и неизвестное: отправной точкой служат известные факты, если таковые были установлены. Также может быть полезно работать на основе вводной информации или логических предположений, даже если они еще не проверены. Однако важно фиксировать любые предположения. Наконец, может быть целесообразно сформулировать пробелы в знаниях или другие неизвестные моменты в самом начале расследования. Разграничение этих категорий информации поможет предотвратить необъективные или искаженные результаты путем уточнения поисковых запросов и их оснований;

c) поисковые запросы и ключевые слова: для проведения целенаправленного поиска расследователям следует составить списки ключевых слов в соответствии с принципом объективности на основе теории или нескольких теорий дела. В идеале лица, проводящие расследования, будут вводить в поиск ключевые слова на всех соответствующих языках и с использованием всех соответствующих систем письма и с осторожностью относиться к возможности получения чрезмерно инклюзивных или недостаточно инклюзивных результатов поиска. Несмотря на различия обстоятельств дел, существуют определенные общие темы, которые следует включить в списки ключевых слов, например значимые места, имена, организации, даты и соответствующие хештеги. Также может быть полезно определить, что может считаться инкриминирующей и оправдывающей информацией в контексте конкретного расследования;

d) поиск и поисковые системы: расследователям следует отслеживать свой поиск и фиксировать путь к соответствующему материалу, включая запросы, операторы и поисковые системы, которые привели к этому контенту. Им нет необходимости фиксировать все результаты поиска, поскольку это чрезмерно обременительно и не будет иметь большой доказательной силы.

[137] Булевые операторы — это простые слова, такие как «и», «или» и «не», которые можно использовать «для объединения или исключения ключевых слов в поисковом запросе, что позволяет получить более целенаправленные и продуктивные результаты». См. Alliant International University Library, "What is a Boolean operator?» URL: https://library.alliant.edu/screens/boolean.pdf.

2. Мониторинг

143. Мониторинг предполагает изучение установленного источника информации, например определенной темы, в течение определенного времени. Цель — отследить изменение контента, генерируемого постоянным источником. Онлайн-мониторинг должен быть структурированной деятельностью с использованием списков известных и ранее проверенных онлайн-источников, таких как веб-сайты или аккаунты в социальных сетях, а также поисковых разысканий, которые выполняются на постоянной основе с определенными целями. См., например, следующие источники:

a) веб-сайты и аккаунты в социальных сетях: расследователям следует вести рабочие списки веб-сайтов и профилей, подлежащих мониторингу, в которых должно быть указано обоснование причин, по которым они подвергаются мониторингу; лицо, ответственное за мониторинг; лицо, осуществляющее мониторинг; и периодичность мониторинга;

b) хештеги и ключевые слова: расследователям следует также вести и регулярно обновлять рабочий список хештегов и ключевых слов, в отношении которых ведется мониторинг;

c) автоматизация: мониторинг может включать использование автоматизированных инструментов, которые могут, например, периодически проводить поиск на определенных сайтах или с использованием определенных параметров. Всегда следует фиксировать использование таких инструментов, включая их названия и версии, а также вводимую в них информацию.

3. Предвзятость

144. При проведении структурированного поиска и мониторинга лицам, проводящим расследования с использованием открытых данных, следует всегда сохранять бдительность в отношении предвзятости — как собственной когнитивной предвзятости, так и предвзятости, присущей информации, доступной в Интернете. Например, если они ищут информацию об изнасиловании, большинство предоставленных данных или вопросов, обсуждаемых в Интернете, скорее всего, будут касаться изнасилований в отношении женщин репродуктивного возраста, совершенных вне брака. В результатах поиска могут быть недопредставлены данные о менее известных или реже регистрируемых видах изнасилования, таких как сексуальное насилие в отношении мужчин и мальчиков, лесбиянок, геев, бисексуальных, трансгендерных и интерсекс-людей, пожилых женщин, а также случаях изнасилования в браке.

145. Другой пример — расследование случаев насилия, спровоцированного ненавистническими высказываниями в Интернете, поскольку ненавистнические высказывания часто включают закодированный язык и символы, которые нелегко обнаружить лицам, проводящим расследования, и машинам, и зависят от них. Особенно когда расследователи не принадлежат к сообществам, в отношении которых направлены их действия, они могут не знать о культурной и контекстуальной специфике применения терминов и символов, используемых для разжигания ненависти или насилия. Ситуация осложняется тем, что ненавистнические высказывания в Интернете часто намеренно сформулированы таким образом, чтобы избежать обнаружения машинами и лицами, проводящими мониторинг, и их удаления с онлайн-платформ, хотя на самом деле они направлены на подстрекательство к насилию или дискриминации в отношении целевой группы населения. В целях преодоления трудностей, связанных с выявлением подстрекательства к дискриминации, вражде и насилию, расследователям следует применять тест, основанный на правах человека, как, например, предусмотрено в Рабатском плане действий по запрещению пропаганды национальной, расовой или религиозной ненависти, представляющей собой подстрекательство к дискриминации, вражде или насилию[138].

146. В конечном итоге лучший способ для лиц, проводящих расследование, противостоять «предвзятости машины» вместе со своей предвзятостью — это осознание возможности существования такой предвзятости, признание рисков и принятие активных мер, когда это возможно, чтобы нивелировать предвзятость путем изучения терминологии и символов, которые имеют отношение к определенному контексту или набору преступлений или инцидентов, а также расширения и диверсификации онлайн-разысканий. В слу-

[138] См. УВКПЧ, «Свобода выражения мнений и разжигание ненависти: УВКПЧ и Рабатский план действий». URL: www.ohchr.org/ru/freedom-of-expression.

чаях, связанных с сексуальным и гендерным насилием, а также любых других преступлений, в которых жертвы подвергаются стигматизации и используется закодированный язык, расследователям следует консультироваться с экспертами, которые могут определить и разъяснить закодированный язык и практику общения, которые такие жертвы и преступники часто используют при общении в онлайн-пространстве[139].

B. Предварительная оценка

147. Прежде чем приступить к сбору контента из Интернета, лицам, проводящим расследование с использованием открытых данных, следует провести предварительную оценку любого материала, который они выявляют, чтобы избежать сбора избыточной информации и соблюсти принципы минимизации данных и целенаправленного расследования, а также убедиться, что сбор материала не нарушает право на неприкосновенность частной жизни. Лицам, проводящим расследования с использованием открытых данных, следует учитывать следующие факторы, чтобы определить, следует ли осуществлять сбор того или иного цифрового материала из Интернета.

1. Актуальность

148. При проведении расследований с использованием открытых данных следует определить, является ли цифровой материал prima facie актуальным для конкретного расследования. Актуальность любого материала зависит от его содержания и источника, а также от целей расследования и того, что известно о ситуации. На ранних этапах расследования может быть трудно определить, что относится к делу, а что может вести расследователей в направлении сбора избыточной информации. Тем не менее лицам, проводящим расследования с использованием открытых данных, следует постараться сформулировать, почему они считают тот или иной материал потенциально актуальным, и такую оценку необходимо зафиксировать (например, с помощью простой и удобной для пользователя системы маркировки или хранения, которая связывает собранную информацию, например, с местом, датой, инцидентом, лицом или типом расследуемого нарушения).

2. Надежность

149. Лицам, проводящим расследования с использованием открытых данных, следует определить, является ли информация или утверждения, содержащиеся в цифровом контенте, надежными prima facie, путем анализа и оценки контента, а также контекстуальной информации, содержащейся в файле. Это может включать проверку встроенных метаданных, связанной информации и источника[140]. В рамках этого процесса следует пытаться определить первоисточник материала, что может потребовать отслеживания происхождения данных в Интернете, лица, загрузившего их, или автора.

3. Удаление

150. Лицам, проводящим расследования с использованием открытых данных, следует оценить вероятность удаления цифрового материала из Интернета или его изъятия из публичного доступа. Когда есть вероятность удаления контента, следует отбирать наиболее надежную известную версию контента, даже если продолжается проверка и расследование относительно более ранних или лучшего качества версий. Вероятность удаления контента может быть оценена на основе ряда факторов, включая предполагаемую личность источника, местонахождение контента и совместимость контента с условиями оказания услуг их поставщиком. Например, натуралистический или оскорбительный контент, который может иметь большую доказательную силу для установления преступлений или нарушений, является одним из примеров контента, который будет удален с наибольшей вероятностью.

4. Безопасность

151. Лицам, проводящим расследования с использованием открытых данных, следует определить, является ли цифровой материал безопасным для сбора или можно и нужно принять дополнительные меры предосто-

[139] См., например, Koenig and Egan, "Hiding in plain site: using online open source information to investigate sexual violence and gender-based crimes".

[140] См. ниже в главе VI.E о верификации.

рожности. Опасения могут возникнуть, если сбор осуществляется с веб-сайта, который может содержать поврежденные элементы, способные нанести ущерб внутренней системе.

5. Последующие обязанности

152. Лицам, проводящим расследования с использованием открытых данных, следует определить, какие обязанности могут возникнуть в случае принятия на хранение цифрового материала, например обязанность хранить его безопасным образом в соответствии с законами о защите данных[141].

C. Сбор

153. Сбор — это действия по получению онлайн-информации посредством скриншота, конвертирования в PDF, криминалистического скачивания или другой формы фиксации. После того, как цифровой контент идентифицирован и признан имеющим отношение к расследованию и prima facie актуальным и надежным для его цели, расследователю следует определить надлежащий метод сбора данных. Методы сбора могут варьироваться в зависимости от того, имеет ли онлайн-контент потенциальную доказательную силу в судебных процессах, будет ли он использоваться или можно ли полагаться на него в целях принятия решений, или же он будет способствовать только внутренним результатам работы. В случаях, когда речь идет просто о результате работы, может быть достаточно скриншота экрана или конвертации в PDF, в то время как в отношении контента, имеющего потенциальную доказательную силу, может потребоваться более тщательный и надежный метод фиксации (например, путем присвоения хеш-значения — см. ниже).

154. Сбор онлайн-контента может осуществляться вручную, в соответствии со стандартной операционной процедурой, или может быть автоматизирован с использованием различных инструментов или сценариев. Независимо от процесса, перечисленные ниже данные в идеале должны быть получены в момент сбора. Такая информация может быть полезна для установления подлинности цифрового материала. Это может быть особенно важно в случае судебного разбирательства, в котором материал предлагается в качестве доказательства, особенно если автор или создатель не установлен, не найден или не может дать показания. Лицам, проводящим расследования с использованием открытых данных, следует собирать онлайн-контент в исходном формате или в состоянии, наиболее близком к первоначальному формату. Следует документировать любые изменения, преобразования или конвертации в связи с процессом сбора.

155. Ниже приводятся руководящие указания относительно того, что и как собирать. Существует ряд инструментов, которые помогают собрать указанную ниже информацию, или это можно сделать вручную. В то время как сбор всей следующей информации считается лучшей практикой, первые три пункта (унифицированный указатель ресурса (URL), исходный код на языке разметки гипертекста (HTML-код) и снимок всей страницы) служат минимальным стандартом для представления доказательств в суде. Конечно, такие стандарты будут отличаться в разных обстоятельствах, но фиксирование всех перечисленных ниже элементов обеспечит прочную основу в любом контексте:

a) целевой веб-адрес: необходимо записать веб-адрес собранного контента, также известный как унифицированный указатель (URL) или идентификатор (URI) ресурса;

b) исходный код: расследователям следует сохранить HTML-код веб-страницы, если это применимо. HTML-код содержит гораздо больше информации, чем видимая часть сайта. Он поможет проверить подлинность собранного материала;

c) снимок всей страницы: расследователям следует сначала сделать снимок экрана целевой веб-страницы с указанием даты и времени. Причина этого процесса заключается в том, чтобы получить наилучшее возможное представление о том, что было видно во время сбора материала;

d) встроенные медиафайлы: при загрузке веб-страницы с видео или изображениями, например, следует также извлечь и

[141] См. ниже в главе VI.D о сохранении.

собрать с веб-страницы эти конкретные элементы;

e) встроенные метаданные: расследователям следует собирать дополнительные метаданные цифрового материала, если они доступны и применимы. Метаданные могут варьироваться в зависимости от источников, но общие метаданные включают идентификатор пользователя, загрузившего материал; идентификатор публикации, изображения или видео; дату и время загрузки; геотег; хештег; комментарии; и аннотацию;

f) контекстные данные: также необходимо проводить сбор контекстного контента, если он имеет отношение к пониманию цифрового объекта. Это могут быть комментарии к видео, изображениям или публикациям; информация о загрузке; и/или информация о загрузившем ее лице/пользователе, например имя пользователя, настоящее имя или биографические данные. Вопрос о том, следует ли собирать сопровождающую информацию, следует решать исходя из специфики дела и цифрового материала;

g) данные о сборе: лицам, проводящим расследования с использованием открытых данных, следует фиксировать все соответствующие данные, относящиеся к сбору, такие как имя лица, собравшего информацию, IP-адрес машины, используемой для сбора информации, используемая виртуальная личность, в случае наличия таковой, и временная отметка. Расследователям следует убедиться в точности системных часов, желательно синхронизировав их с сервером сетевого протокола синхронизации (сервером NTP). Этот шаг необходим для того, чтобы метаданные, связанные со временем, были точно представлены в собранных файлах. Если для доступа к собранной информации используется виртуальная личность, это следует указать;

h) хеш-значение: хеш-значения — это уникальная форма цифровой идентификации, которая подтверждает с помощью криптографии, что собранный контент уникален и не был изменен с момента сбора. В момент сбора лицам, проводящим расследования с использованием открытых данных, следует вручную добавить — или инструмент сбора должен автоматически добавить — хеш-значение. Существует множество различных типов хешей, из которых можно выбирать, и стандарты меняются с течением времени. Расследователям следует определить, какой хеш использовать, исходя из принятого в настоящее время стандарта[142].

156. В случаях автоматизированного сбора некоторые из описанных процессов могут быть выполнены инструментами, предназначенными для сбора соответствующего контента и метаданных. По каждому собранному материалу должен быть составлен технический отчет, включающий вышеуказанную информацию для последующего установления подлинности материала. Контекстную информацию и все типы метаданных всегда следует хранить и сохранять вместе с цифровым материалом, как объясняется в следующем разделе.

D. Сохранение

157. Долговечность и доступность информации в Интернете зачастую зависят от непредвиденных обстоятельств. Платформы социальных сетей могут удалять контент со своих платформ в соответствии со своими условиями использования, или пользователи могут решить удалить или отредактировать свой собственный загруженный контент. Кроме того, информация в Интернете может быть легко деконтекстуализирована, потеряна, стерта или повреждена[143]. Для того чтобы цифровые материалы оставались доступными и пригодными для использования в целях обеспечения юридической ответственности, их необходимо сохранять как в краткосрочной, так и в долгосрочной перспективе[144]. Как правило, целью сохранения цифровых материалов является поддержание их доступности[145]. Однако когда речь идет о сохранении цифровых материалов для обеспечения юридической ответственности, целью является управление цифровыми материалами и их сохранение с учетом

[142] Национальный институт стандартов и технологии США является одной из организаций, к которой можно обратиться за руководством относительно действующего стандарта. См. www.nist.gov.

[143] Ng, "How to preserve open source information effectively".

[144] Ibid. p. 143. См. United Nations Educational, Scientific and Cultural Organization, "Concept of digital preservation". URL: https://en.unesco.org/themes/information-preservation/digital-heritage/concept-digital-preservation.

[145] Ng, "How to preserve open source information effectively".

обеспечения их доступности, подлинности и возможности использования механизмами привлечения к ответственности, включая их допустимость в ходе судебного разбирательства. Таким образом, сохранение цифровых данных в контексте расследования предполагает сохранение информации в течение длительного времени таким образом, чтобы собранный материал оставался понятным для предполагаемых пользователей независимо от контекста и имел достаточный уровень подтверждения его подлинности.

158. Для долгосрочного сохранения может потребоваться обновление оборудования и форматов хранения, чтобы обеспечить доступность материалов при использовании современных устройств.

1. Свойства цифрового материала, которые должны защищаться и сохраняться в течение длительного времени

159. По мнению архивистов, свойства цифрового материала, защита и сохранность которых должна обеспечиваться в течение длительного времени, включают его подлинность, доступность, идентифицируемость, сохраняемость, отображаемость и понятность, как кратко описано ниже.

a) Подлинность

160. Подлинность означает способность продемонстрировать, что цифровой материал остается неизменным с момента его сбора. Требуется, чтобы цифровой материал оставался неизменным, находясь в архиве, или чтобы любые вносимые изменения были задокументированы[146].

b) Доступность

161. Доступность означает наличие цифрового материала в простом смысле постоянного существования и возможности извлечения, а также в юридическом смысле обеспечения соответствующих прав интеллектуальной собственности для доступа и использования материала[147].

c) Идентифицируемость

162. Идентифицируемость означает возможность нахождения цифрового материала по ссылке. Цифровой материал должен быть идентифицируемым и отличимым от других цифровых материалов, например путем регистрации с помощью идентификатора, такого как уникальный идентификационный номер[148].

d) Сохраняемость

163. С технической точки зрения под сохраняемостью понимается целостность и устойчивость цифрового материала. Битовые последовательности цифрового материала должны быть неповрежденными, доступными для обработки и извлечения[149].

e) Отображаемость

164. Отображаемость означает способность людей или машин использовать цифровой материал или производить с ним какие-либо действия с помощью соответствующего оборудования и программного обеспечения[150].

f) Понятность

165. Понятность означает способность предполагаемых пользователей интерпретировать и понимать цифровой материал[151].

2. Вопросы, связанные с конкретным расследованием

166. Лицам, проводящим расследование, следует рассмотреть связанные с конкретным расследованием вопросы, которые могут или будут возникать в процессе сохранения, и подготовиться к их решению.

a) Цепочка обеспечения сохранности

167. Цепочка обеспечения сохранности означает хронологическое документирование последовательности хранителей информации или доказательств, а также документирование контроля, даты и времени, передачи, анализа и распоряжения любыми такими доказательствами. После сбора цифровых материалов необходимо обеспечить их сохранность

146 Ibid. Обратите внимание, что использование термина «подлинность» в данном контексте отличается от его использования в юридическом контексте.

147 Ibid.

148 Ibid.

149 Ibid.

150 Ibid.

151 Ibid.

путем создания надлежащей системы цифрового хранения.

b) Экземпляр, служащий доказательством

168. Экземпляр, служащий доказательством, — это цифровой материал, собранный лицом, проводившим расследование, в его оригинальной форме, без искажений и изменений. Цифровые материалы должны храниться в первоначальной форме. Это означает сохранение чистого оригинала собранного цифрового материала во всех форматах, в которых он был собран.

c) Рабочие копии

169. Копия или копии цифрового материала должны быть созданы для целей анализа и храниться отдельно, чтобы лица, проводящие расследование, могли работать с копией, а не с оригиналом. Это позволяет минимально взаимодействовать с оригиналом и снизить риск его повреждения или изменения. Все изменения, вносимые в материал, включая создание копий, следует документировать. По возможности следует использовать отдельные системы хранения для экземпляров, служащих доказательством, и рабочих копий.

d) Хранение

170. Хранение помогает обеспечить сохранность цифровых материалов и возможность их поиска и извлечения. Хранение следует рассматривать не в пассивном ключе, а как активный процесс, включающий постоянные, управляемые задачи и обязанности. Оно включает постоянное хранение, в котором важную роль играют носители информации, а также управление иерархией хранения, замену носителей информации, проверку ошибок, проверку неизменяемости (проверка того, что материал не был изменен), аварийное восстановление, а также поиск и возврат хранящихся материалов[152]. Цифровая информация может храниться на рабочем месте (онлайн или офлайн) или за его пределами (онлайн или офлайн)[153]. Варианты хранения цифрового контента включают локальный жесткий диск или локальный съемный носитель; либо сетевой накопитель, являющийся частью локальной сети или удаленного сервера или облачной системы хранения данных. При выборе хранилища следует учитывать следующие факторы: емкость хранилища (свободное место); доступ и контроль; резервные копии; соответствующее законодательство; и информационную безопасность и защиту данных. При выборе системы хранения следует также учитывать скорость, доступность, стоимость, устойчивость, управление хранением и системы извлечения[154].

i) Резервное копирование

171. Если произойдет потеря данных или возникнут ошибки, архивист или технический специалист может попытаться восстановить данные. В идеале предварительно должна быть создана резервная копия данных или они должны быть продублированы в отдельном месте. Эксперты в области информационных технологий рекомендуют иметь не менее трех копий данных по крайней мере в двух различных типах хранилищ, причем как минимум одна копия должна быть географически отделена от других копий.

ii) Разрушение носителей

172. Одна из проблем хранения заключается в том, что носители со временем разрушаются. Архивисты могут снизить риск выхода из строя хранилища, используя особо долговечные типы носителей; однако любое устройство хранения данных рано или поздно приобретет повреждения, износится или случайно выйдет из строя. Даже без полного отказа ошибки данных или повреждение файлов могут возникать по мере разрушения носителя. Поэтому важно иметь резервные копии и регулярно контролировать инфраструктуру хранения и неизменность хранимых файлов, например регулярно проверяя хеш-значения случайных образцов, чтобы убедиться, что не произошло ухудшения состояния.

iii) Моральное устаревание

173. Цифровые файлы устаревают, когда оборудование, необходимое для доступа к данным, перестает быть реально доступным или его невозможно поддерживать в надлежащем состоянии. Независимо от того, насколько долговечным может быть любой носитель информации, он также подвержен риску устаревания, что затрудняет или делает невозможным извлечение сохраненных данных. Поэтому в рамках расследования следует обеспечить обслуживание и при необходимости обновление носителей информации

[152] Ibid., p. 154.

[153] Shira Scheindlin and Daniel J. Capra, *Electronic Discovery and Digital Evidence in a Nutshell* (Saint Paul, West Academic Publishing, 2009), pp. 21–22.

[154] Ng, "How to preserve open source information effectively", p. 156.

для поддержания отображаемости и доступности данных.

iv) Восстановление

174. Цифровые файлы могут быть случайно или намеренно удалены. Когда пользователь «удаляет» файл на компьютере, содержимое удаленного файла остается на носителе информации до тех пор, пока оно не будет перезаписано другим файлом[155]. Поэтому чем больше действий на компьютере или другом носителе информации, тем быстрее он будет перезаписан и станет невосстановимым. Большинство компьютеров имеют встроенные в операционную систему утилиты, позволяющие восстанавливать удаленные файлы. Кроме того, можно приобрести программное обеспечение для восстановления данных, которое иногда используется для отмены удаления файлов. Для получения доступа к удаленным данным лицам, проводящим расследования с использованием открытых данных, может потребоваться помощь специалистов по информационным технологиям.

v) Обновление

175. Обновление подразумевает копирование содержимого с одного носителя на другой. Оно направлено только на предупреждение устаревания носителей и не является комплексной стратегией сохранения. Однако обновление следует рассматривать как неотъемлемую часть более широкой стратегии сохранения[156].

E. Верификация

176. Верификация — это процесс установления точности или правдивости информации, собранной в Интернете. Верификация открытых данных может быть проведена как часть анализа всех источников — включая информацию из закрытых и конфиденциальных источников — или исключительно на основе открытых источников. Верификация охватывает три отдельных аспекта: источник, цифровой материал или файл и контент, — которые должны рассматриваться в совокупности и сравниваться на предмет соответствия.

1. Анализ источника

177. Анализ источника — это процесс оценки достоверности и надежности источника. Онлайн-среда создает трудности для анализа источников, поскольку многие источники анонимны или используют псевдонимы. Для того чтобы правильно проанализировать источники информации, лицам, проводящим расследования с использованием открытых данных, следует сначала определить правильный источник или источники для анализа, что означает атрибутирование информации к ее первоисточнику. Анализ с целью атрибуции означает определение источника цифровой информации, которым может быть конкретный сайт, абонент или пользователь определенной учетной записи или платформы, или личности тех, кто является авторами определенного контента, создали или загрузили его. Анализ с целью атрибуции не всегда возможен и может потребовать дополнительных онлайн- и офлайн-действий в рамках расследования или применения передовых методов поиска и анализа. Хотя определение авторства полезно, отсутствие информации об авторе, как правило, не имеет решающего значения для установления подлинности онлайн-материала, поскольку существуют другие способы проверки подлинности открытых данных.

a) Происхождение

178. Происхождение означает первоисточник или самое раннее известное существование чего-либо. Когда речь идет об онлайн-контенте, происхождение может означать самое раннее появление в сети или оригинальный материал до того, как он был загружен в Интернет. В случае онлайн-контента предпочтительнее ссылаться на «первую копию, найденную в сети», а не на «первую копию в сети», поскольку оригинал мог быть удален. Даже когда лица, проводящие расследования, убеждены, что нашли первую версию, например, видео или других открытых данных, они не могут быть уверены в ее происхождении из-за существования закрытых каналов, таких как электронная почта и группы личных сообщений, которые могли использоваться для обмена информацией до ее публичного появления в сети[157].

[155] Scheindlin and Capra, *Electronic Discovery and Digital Evidence in a Nutshell*, p. 24.

[156] Cornell University Library, "Digital imaging tutorial". URL: http://preservationtutorial.library.cornell.edu/tutorial/preservation/preservation-03.html.

[157] Например, один пользователь может отправить фотографию по электронной почте другому пользователю, который затем загружает ее в социальные сети. Таким образом, фотография принадлежит автору письма, а не тому, кто ее опубликовал.

b) Достоверность

179. История публикаций, онлайн-активность и присутствие источника в Интернете могут содержать соответствующую информацию, которая свидетельствует против или в пользу доверия к источнику. Лицам, проводящим расследования с использованием открытых данных, следует изучить присутствие источника в сети и историю его публикаций, что может даже помочь выявить умышленную попытку обмана. Например, при публикации информации о событиях в конкретной стране говорят ли окружающие публикации источника о том, что он или она действительно находится в этой стране?

c) Независимость и беспристрастность

180. В ходе расследования необходимо проверить беспристрастность источника. Это можно сделать, изучив любые группы, организации или объединения, с которыми лица связаны, а также то, как они зарабатывают деньги и от кого они получают финансирование. Имеются ли связи или отношения с любой из сторон, вовлеченных в дело или в расследуемый инцидент? При определении независимости источников необходимо изучить, могут ли они быть связаны с соответствующими организациями (например, сторонами конфликта). Идеология источника и принадлежность к какой-либо группе также могут иметь значение. В отношении всех источников расследователям следует изучить и выявить их скрытые мотивы, интересы или планы, а также степень, в которой они могут повлиять на их истинность.

d) Конкретика

181. Чем точнее информация и утверждения, тем легче их доказать или опровергнуть. Широкие и расплывчатые утверждения, как правило, труднее поддаются критической оценке.

e) Снижение надежности

182. Тексты, составленные во время событий, о которых в них идет речь, обычно считаются более надежными, чем те, которые были созданы спустя долгое время после того, как эти события произошли[158]. Этот фактор может создавать проблему для лиц, проводящих расследования с использованием открытых данных, когда неясно, когда был создан цифровой текст.

2. Технический анализ

183. Технический анализ означает анализ самого цифрового материала, будь то документ, изображение или видео. Чтобы проверить целостность файла, то есть был ли он изменен, модифицирован или с ним проводились какие-либо манипуляции в цифровом формате, лица, проводящие расследования с использованием открытых данных, могут посчитать целесообразным подвергнуть его цифровой криминалистической экспертизе, иногда называемой цифровым расследовательским анализом. Ниже перечислены компоненты такого анализа.

a) Метаданные

184. Метаданные — это данные, которые описывают другие данные и предоставляют о них информацию. Они могут быть созданы пользователем — автором материала, другими пользователями, поставщиком услуг связи или любым устройством, на котором создаются, передаются, принимаются или просматриваются данные. Метаданные имеют значение для описания материала и обстоятельств его создания, распространения или изменения. Они могут включать создателя файла, дату создания, данные о загрузке, модификации, размер файла и геоданные. Метаданные могут быть встроены в файл, отражены на веб-странице или присутствовать в исходном коде. Некоторые метаданные могут быть удалены до или во время загрузки или в результате использования приложений социальных сетей, но если они доступны, их следует просмотреть на случай, если они могут помочь установить подлинность. Оригинальные метаданные могут быть утрачены, поскольку платформы часто перекодируют загруженные медиафайлы, чтобы оптимизировать их для просмотра, обмена или воспроизведения в режиме онлайн. В таких случаях метаданные будут отражать новый файл, а не оригинал. Если они были удалены, лицам, проводящим расследования с использованием открытых данных, следует искать другие способы проверки материала.

b) Данные о формате файлов изображений с возможностью обмена (EXIF)

185. Данные о формате файлов изображений с возможностью обмена — это тип метаданных, определяющий форматы изображений, звука и вспомогательных тегов, используемых

[158] Institute for International Criminal Investigations, *Investigators Manual*, 5th ed. (The Hague, 2012), p. 88.

цифровыми камерами, сканерами и другими системами, работающими с файлами изображений и звука, записанными цифровыми камерами.

c) Исходный код

186. Исходный код — это программа, лежащая в основе любой веб-страницы или программного обеспечения. В случае с веб-сайтами этот код может просмотреть любой человек, используя различные инструменты, даже сам веб-браузер. Исходный код сайта легко просмотреть с помощью ряда инструментов, находящихся в свободном доступе. Он может содержать мета-контент, скрытый или измененный контент, а также показывать структуру ссылок и неработающие ссылки.

3. Анализ контента

187. Анализ контента — это процесс, в ходе которого информация, содержащаяся в видео, изображении, документе или заявлении, оценивается на предмет ее подлинности и истинности. Анализ контента также многогранен и включает анализ визуальных символов или, например, подтверждение изображения метаданными. Особенности онлайн-среды порождают множество проблем, которые могут повлиять на фактическую или воспринимаемую правдивость или истинность открытых данных. К ним относятся круговой вброс недостоверной информации, деконтекстуализация информации и неправильная интерпретация. Данные контента — это данные, содержащиеся в цифровом материале, таком как видео, изображение, аудиозапись, документ или неструктурированный текст.

a) Уникальные идентификаторы

188. При проверке визуального контента расследователям следует начать с поиска уникальных или идентифицирующих характеристик. К ним могут относиться здания, флора и фауна, люди, символы и знаки различия. Особую осторожность следует проявлять при анализе характеристик человека с целью идентификации конкретного лица[159]. Практика идентификации обычно требует специальных навыков, приобретаемых со временем и в результате специальной подготовки эксперта-криминалиста. Дилетантский анализ, проводимый неподготовленными специалистами, может быть неточным, предвзятым и/или иным образом проблематичным.

b) Объективно верифицируемая информация

189. Часто бывает полезно начать с определения того, что может быть квалифицировано как «объективно верифицируемая информация». Например, погода в определенный день, имя и звание командира или местоположение здания — все это может быть объективно проверено. Оценка открытых данных должна включать изучение их содержания на основе такой объективно верифицируемой информации.

c) Геолокация

190. Геолокация — это идентификация или оценка местоположения объекта, действия или места, в котором был создан материал. Например, с помощью методов геолокации можно определить место, откуда было снято видео или фотография, загруженные из Интернета. Такие методы могут включать, например, идентификацию уникальных географических объектов на фотографии с их фактическим местоположением на карте.

d) Хронолокация

191. Хронолокация — это подтверждение дат и времени событий, изображенных в каком-либо фрагменте информации, обычно визуальном образе. Например, можно определить время суток, когда была сделана фотография, изучив длину теней, создаваемых солнечным светом, наряду с другими показателями.

[159] Криминалистический анализ и идентификация характеристик человека с помощью инструментов или анализа с участием специалистов (например, распознавание лиц, анализ походки и др.) требуют участия эксперта-криминалиста. См. Nina M. van Mastrigt and others, "Critical review of the use and scientific basis of forensic gait analysis", *Forensic Sciences Research*, vol. 3, No. 3 (2018), pp. 183–193 (URL: www.tandfonline.com/doi/full/10.1080/20961790.2018.1503579); Royal Society and Royal Society of Edinburgh, "Forensic gait analysis: a primer for courts" (London, 2017) (URL: https://royalsociety.org/-/media/about-us/programmes/science-and-law/royal-society-forensic-gait-analysis-primer-for-courts.pdf). См. также European Network of Forensic Science, *Best Practice Manual for Facial Image Comparison* (2018) (URL: http://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf); National Center for Audio and Video Forensics, "Height analysis of surveillance video" (URL: https://ncavf.com/what-we-do/forensic-height-analysis).

e) Полнота

192. Неполный документ или видеозапись, тем не менее, может иметь доказательную силу, однако пробелы могут повлиять на весомость, которая может быть придана материалу. Поэтому при сборе открытых данных важно зафиксировать целевой файл полностью и, когда это уместно, окружающий контекст.

f) Внутренняя согласованность

193. Оценка внутренней согласованности может быть проведена в отношении отдельного блока информации из открытого онлайн-источника или в отношении совокупности информации из конкретного источника (и/или источников с одинаковым происхождением или авторством). Оценка внутренней согласованности отдельного блока онлайн-информации направлена на установление того, является ли информация последовательной и согласованной сама по себе. Внутренне согласованный блок информации или вся информация в совокупности не должны противоречить сами себе.

g) Внешнее подтверждение

194. Внешнее подтверждение обеспечивается информацией, которая находится вне самого цифрового материала, но совпадает с его содержанием и тем самым подтверждает его истинность.

F. Расследовательский анализ

195. Расследовательский анализ — это практика рассмотрения и интерпретации фактической информации для формулирования предметных выводов, имеющих значение для принятия решений или построения дела. В связи с объемом и различным качеством открытых данных требуется хорошо структурированный подход к анализу.

196. Перед проведением определенных видов анализа открытые данные, возможно, придется сначала обработать. Обработка может включать перевод с иностранных языков или агрегирование различных наборов данных для помощи в анализе действий отдельных лиц, мест и объектов, а также отношений или сетей, перемещений, деятельности или транзакций. Кроме того, она может включать изменение характера или формата цифрового материала для обеспечения его совместимости с определенным программным обеспечением. Общие виды обработки данных включают:

a) перевод: если данные представлены на языке, на котором не говорят лица, проводящие расследование, или не обрабатываются программным обеспечением, необходимым для просмотра материала, данные, возможно, придется перевести, прежде чем предпринимать дальнейшие шаги;

b) агрегирование: лицам, проводящим расследование, может понадобиться объединить различные наборы данных в один более крупный блок данных, чтобы проанализировать его;

c) переформатирование: чтобы сделать данные более удобными для поиска или извлечения, лицам, проводящим расследование, может понадобиться изменить формат цифрового материала.

197. Рекомендуется обрабатывать только рабочие копии цифрового материала, а не оригинал или экземпляр, служащий доказательством. Любую обработку цифрового материала следует документировать. Если лица, проводящие расследование, используют цифровые технологии для обработки данных, например анализируют данные с помощью алгоритмов, включая обработку материалов на естественном языке и глубокое обучение, они должны знать о риске предвзятости при обработке таких данных.

198. После обработки информация может быть проанализирована. Продукты аналитической работы с открытыми данными будут различаться в зависимости от цели, типа и объема информации первоисточника, сроков их создания и аудитории. Они будут подготовлены в соответствии с потребностями расследования и могут включать диаграммы, резюме, глоссарии, словари и наглядные пособия, в том числе карты и составление схем[160].

199. Лицам, проводящим расследования, следует применять строгие стандарты для обеспечения объективности, своевременности, актуальности и точности данных и выводов, содержащихся в аналитических материалах, а также для защиты конфиденциальности и исходя из других соображений, связанных с правами человека, особенно при работе с информацией, позволяющей установить личность. Такую информацию следует включать только в те отчеты, в отношении которых

[160] См. ниже в главе VII об отчете о результатах.

лица, проводящие расследования, получили согласие вовлеченных лиц и только когда она служит непосредственной цели расследования. Ее следует также рассмотреть в свете правовых и этических ограничений, связанных с ее использованием[161].

200. В следующих разделах приведены распространенные виды анализа, которые могут быть использованы для достижения целей расследования с использованием открытых данных.

1. Сравнительный анализ изображений/видео

201. Сравнительный анализ или научное сравнение — это процесс сравнения характеристик объектов, лиц и/или мест с другими неизвестными и/или известными материалами, когда хотя бы один из рассматриваемых материалов является изображением. Это анализ содержания изображений и видео, включая элементы сравнения различных элементов и характеристик, а также качества их изображения и визуальных параметров (свет, перспектива и др.). Хотя многие неспециалисты сегодня знают основы сравнительного анализа изображений, помощь квалифицированного и дипломированного эксперта в области криминалистического видеоанализа и/или цифровой криминалистики может оказать содействие в проведении научного анализа, включая экспертное заключение. Такая экспертиза может быть полезна также с точки зрения придания дополнительного веса выводам в рамках расследований нарушений прав человека и других видов расследований.

2. Интерпретационный анализ изображений/видео

202. Со сравнением изображений/видео связан интерпретационный анализ изображений/видео, который предполагает анализ цифрового материала для понимания его визуального содержания. Например, анализ выстрелов, ран, крови, транспортных средств, оружия и военных объектов или анализ скорости движущегося транспортного средства или возраста человека — все это является частью интерпретационного анализа изображений/видео. Он может быть проведен аналитиками в целях расследования либо криминалистами или специалистами в определенной области в случае установления фактов в ходе судебного разбирательства или подготовки выводов о нарушении прав человека.

3. Пространственный анализ

203. Пространственный или геопространственный анализ может включать анализ визуального контента и анализ метаданных материалов, содержащих географические координаты или географические названия. Пространственный анализ предполагает изучение различных объектов и особенностей ландшафта в подходящем разрешении и сверку со спутниковыми или другими изображениями, геоданными и картами, информацией о соответствующем деле и контексте, а также инструментами географической информационной системы[162].

4. Составление карты действующих лиц

204. Составление карты действующих лиц — это техника, необходимая для понимания ключевых действующих лиц и выявления властных отношений и каналов влияния[163]. Таким образом, все начинается с определения основных действующих лиц и последующего составления схемы отношений между ними.

5. Анализ социальных сетей

205. Подобно составлению карты действующих лиц, анализ социальных сетей — это составление схемы и оценка отношений между людьми, группами, организациями, компьютерами, URL-адресами и другими связанными объектами информации/знаний[164]. Люди и группы часто называются узлами, а связи показывают отношения между узлами. Анализ социальных сетей использует связи в социальных сетях и на других мобильных или веб-платформах для установления и понимания взаимоотношений между лицами. Анализ данных о связях может быть выполнен вручную лицом, проводящим расследование, или с помощью аналитического программного обеспечения.

---

[161] См. выше в главе III о правовой основе.

[162] Географическая информационная система — это компьютеризированная база данных для управления пространственными данными и их анализа.

[163] OHCHR, *Manual on Human Rights Monitoring*, chap. 8 on analysis, p. 24.

[164] Orgnet, "Social network analysis: an introduction". URL: www.orgnet.com/sna.html.

6. Составление карты инцидента

206. Составление карты инцидента — это аналитический метод, используемый для установления временных и географических связей между различными инцидентами, что в контексте международных уголовных преступлений и нарушений прав человека может означать место совершения таких нарушений или преступлений, включая предшествующие и последующие события. Оно также может включать составление карты других значимых событий, например где и когда были сделаны заявления предполагаемыми преступниками.

7. Анализ почерка совершения преступления/нарушения

207. В контексте национальной правоохранительной деятельности почерк совершения преступления — это наличие набора из двух или более преступлений, о которых было сообщено правоохранительным органам или которые были выявлены правоохранительными органами и которые являются уникальными, поскольку имеют по крайней мере одну общую черту: тип преступления; действия правонарушителей или пострадавших; характеристики преступника (преступников), пострадавших или целей; забранное имущество; или место их совершения[165]. Аналогичным образом почерк совершения преступлений и нарушений может быть установлен в международных уголовных делах и делах о нарушениях прав человека на основе открытых данных.

[165] International Association of Crime Analysts, "Crime pattern definitions for tactical analysis", Standards, Methods and Technology Committee White Paper 2011-01, p. 1.

VII

ОТЧЕТ О РЕЗУЛЬТАТАХ

КРАТКОЕ СОДЕРЖАНИЕ ГЛАВЫ

- **Результаты расследования с использованием открытых данных, касающиеся либо собранных данных, либо выводов, сделанных на их основе, могут быть представлены в устной, визуальной или письменной форме.**
- **При принятии решения о том: a) какой формат использовать и b) какие данные включать, — лицам, проводящим расследование, следует изучить, какие форматы наиболее уместны в соответствии с их мандатами и подходят для предполагаемой аудитории с учетом таких факторов, как технологическая грамотность аудитории и доступность, объективность, прозрачность и безопасность.**

208. В настоящей главе описаны способы представления или сообщения результатов расследований с использованием открытых данных, включая методологии, исходные данные и аналитические выводы. Во многих случаях открытые данные будут представлены в тандеме с другой информацией, собранной с помощью других методов расследования. Презентации могут принимать различные формы, включая письменные, устные или визуальные отчеты, или любую комбинацию этих форм. Отчеты могут быть предназначены для внутреннего пользования или для внешней публикации и могут рассматриваться как экспертные или неэкспертные в зависимости от ряда факторов. При составлении отчетов следует учитывать следующие аспекты:

a) точность: в отчетах следует точно представлять собранные данные[166]. В них следует включить оправдательную информацию, а также объяснение любых сокращений или пробелов;

b) атрибуция: в отчетах следует четко разграничить контент, который находится в открытом доступе и является несекретной информацией общего характера, информацию, которая является секретной или по иным причинам закрытой, и контент, отражающий суждение или мнение лиц, проводящих расследование, и/или других специалистов. Лицам, проводящим расследование, или другим лицам, сообщающим об открытых данных, следует также проявлять должную осмотрительность и получать соответствующие разрешения на использование контента, который может принадлежать другим лицам, например путем обеспечения всех необходимых прав интеллектуальной собственности;

c) полнота: в выводах следует дать указание на полноту исходных данных, особенно если данные намеренно исключены;

d) конфиденциальность: несмотря на то, что они найдены в открытых источниках, следует рассмотреть, какие материалы следует опустить или отредактировать для защиты конфиденциальности или минимизации иных рисков, в частности потенциальных рисков для источников, свидетелей, пострадавших и членов сообществ, имеющих отношение к открытым данным;

e) язык: в отчетах следует использовать нейтральный язык и избегать эмоциональных высказываний. В них следует четко излагать факты, без злоупотребления эпитетами и выразительными средствами. При написании отчетов следует использовать гендерно-нейтральные формулировки. В идеале публичные отчеты должны быть доступны на языках пострадавших сообществ в дополнение к любым официальным языкам, используемым лицами или органами, проводящими расследование;

f) прозрачность: в отчетах следует четко указать, как расследователи выполняли свою работу, каковы их цели, действия и методы. Обычно это включается в раздел отчета, посвященный методологии, но также должно служить ориентиром для описаний по всему тексту. Описания должны быть максимально прозрачными и не создавать при этом рисков для безопасности, например при раскрытии конфиденциальной информации.

A. Письменный отчет

209. Расследование с использованием открытых данных может быть представлено в письменной форме, что может включать внутренние отчеты и отчеты для заказчиков, а также публичные отчеты. Одним из методов представления аналитических выводов является письменный отчет, который может включать, в частности, отчеты НПО, комиссий по расследованию, миссий по установлению фактов и Организации Объединенных Наций, отчеты экспертов для суда или трибунала[167]. Открытые цифровые данные часто интегрируются с другими формами открытых и закрытых данных и анализа. В письменных отчетах следует представить анализ собранной информации, с тем чтобы сделать логические выводы, оценки и прогнозы. В них следует отразить надежную методологию и объяснить ее целевой аудитории. Истинность и честность информации, лежащей в основе отчета,

[166] См. выше в главе II.B о методологических принципах.

[167] В качестве примера письменного отчета о расследовании с использованием открытых цифровых данных см., например, Human Rights Investigations Lab, "Chemical strikes on Al-Lataminah: March 25 & 30, 2017 - a student-led open source investigation" (Berkeley, Human Rights Center, University of California, Berkeley, School of Law, 2018).

имеют решающее значение. Неправильные данные приведут к неправильным выводам[168].

210. В письменные отчеты следует включать следующие разделы, за исключением случаев, когда есть обоснованная и сформулированная причина не делать этого, например необходимость сохранения в тайне некоторых методов, способов и источников онлайн-расследования:

a) цели расследования: в отчетах следует указать цели расследования и лежащие в их основе мандаты или инструкции заказчика, в том числе четко сформулированные, понятные вопросы исследования;

b) методология: в отчетах следует указать методы исследования, чтобы обеспечить возможность их воспроизведения и чтобы аудитория могла понять информацию и результаты расследований, включая их сферу охвата, и оценить их достоверность;

c) выполненные действия: в отчеты следует включать краткое описание выполненных действий, имеющих существенное значение для выводов или оценки качества анализа, включая действия по определению исходных данных, того, что было собрано и что было проанализировано;

d) исходные данные и источники: в отчеты следует включать описание исходных данных, в том числе их источники и качество;

e) пробелы или неясности: в отчетах следует указывать любые пробелы или неясности в исходных данных или анализе, которые могут быть существенными для выводов;

f) результаты и рекомендации: в отчеты следует включать интерпретацию расследователями данных или выводов на основе анализа данных с указанием оговорок и новых версий.

B. Устный отчет

211. Если результаты расследования с использованием открытых данных дойдут до суда, лицам, проводившим расследование, возможно, придется давать показания в качестве свидетелей; таким образом, представить свои расследования в виде устных показаний. Другие формы устных отчетов могут включать презентации перед комиссиями по установлению истины, форумами НПО, народными трибуналами или на мероприятиях СМИ.

212. Любое лицо, которому необходимо устно представить результаты своего расследования с использованием открытых данных, должно быть в состоянии четко и точно объяснить проведенную им работу, включая примененную методологию и использованные инструменты. Это придаст должную весомость устным показаниям и выводам.

213. В случае судебного разбирательства часто именно руководителям расследований приходится давать показания, и они должны быть в состоянии рассказать о работе своих групп. Для этого, конечно, необходимо, чтобы они знали, что делали их сотрудники, и могли ответить на вопросы о выполняемых функциях и обосновании любых решений, касающихся рамок расследования, его методов, используемых инструментов и др. Лица, проводившие расследование, могут выступить как в качестве свидетелей-экспертов, так и обычных свидетелей. Свидетели-эксперты, считающиеся экспертами благодаря своему опыту, знаниям, навыкам, подготовке, образованию или соответствующим полномочиям, могут давать показания о выводах, к которым они пришли, и других результатах аналитической работы. Обычные свидетели, как правило, ограничиваются дачей показаний о фактах, в частности о тех, которые они наблюдали лично.

C. Визуальный отчет

214. Визуализация данных — это графическое представление информации в виде, например, диаграмм, графиков, таблиц, карт и инфографики, которые обеспечивают доступный способ увидеть и понять тенденции, отклонения и закономерности в данных[169]. Сюда относятся: диаграммы и другие графические представления данных в простран-

[168] С учетом обстоятельств и требований конфиденциальности рекомендуется проводить экспертную оценку для обеспечения точности и качества данных, а также анализа и выводов, сделанных на основе этих данных.

[169] Примеры визуального отчета в различных контекстах включают цифровые платформы, использованные в качестве демонстрационных доказательств в деле *Прокурор против Ахмада аль-Факи аль-Махди* в Международном уголовном суде и *Прокурор против Салима Джамиля Айяша и др.* в Специальном трибунале по Ливану; доклад с подробными выводами независимой международной комиссии по расследованию протестов на оккупированной палестинской территории (URL: www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session40/Documents/A_HRC_40_74_CRP2.pdf); BBC Africa Eye, "Cameroon atrocity: what happened after Africa Eye found who killed this woman", BBC News, 30 May 2019 (URL: www.bbc.com/news/av/world-africa-48432122/cameroon-atrocity-what-happened-after-africa-eye-found-who-killed-this-woman). См. также в целом работу организаций Forensic Architecture и SITU Research.

стве и времени; графики (включая те, которые демонстрируют математические связи, тенденции или отношения); сетевые графики, которые демонстрируют взаимоотношения между различными лицами; и статистические графики и диаграммы. Двухмерные и трехмерные карты для визуализации объектов в пространстве и времени, а также трехмерные реконструкции различных объектов, включая места преступлений, также являются примерами визуализации данных[170]. Эти инструменты могут быть полезны для понимания больших объемов данных, что часто бывает в расследованиях с использованием открытых данных, или для лучшего понимания сложных фактических обстоятельств.

215. Другие виды визуализации данных включают:

a) интеллект-карты: интеллект-карта — это графический способ представления идей и концепций и их взаимосвязи. Интеллект-карты структурируют информацию таким образом, что ее легче анализировать, обобщать и понимать. Они часто включают объяснение того, как были обнаружены исходные данные;

b) схемы: схема — это графическое представление последовательности событий, таких как шаги, заложенные в алгоритм, рабочий процесс или аналогичные процессы;

c) инфографика: инфографика — это иллюстрированное представление идеи или концепции; она может быть использована для представления статистической информации.

216. Открытые данные могут быть представлены различными способами, начиная с аудиовизуального показа одной видеозаписи или вебсайта и заканчивая интерактивными, цифровыми и обобщёнными мультимедийными презентациями[171]. Визуальная демонстрация и иллюстрации или цифровые платформы могут быть использованы для представления информации таким образом, чтобы целевой аудитории было легче понять основные факты. Примерами могут служить временные шкалы, составные фотографии (например, 360-градусный обзор места преступления) и отредактированные видеозаписи.

217. В случае представления визуализации данных и мультимедийных доказательств в зале суда или другой публике лицам, проводившим расследование, необходимо понимать, какие технические вопросы могут возникнуть, в том числе какие платформы могут понадобиться адвокатам, чтобы сделать их презентации максимально полезными для лиц, устанавливающих факты. При выборе оптимальной формы представления исходных данных следует учитывать целый ряд факторов. К таким факторам относятся целевая аудитория и уровень удобства для нее потенциальных форматов, а также ее способность понимать сообщаемую информацию[172]. В конечном итоге все презентации должны способствовать достижению цели освещения фактов, относящихся к делу, таким образом, чтобы они имели доказательную силу и не были пристрастными, и должны соответствовать юридическим и этическим требованиям юрисдикции, в которой представлена информация.

[170] См., например, платформу International Criminal Court Digital Platform: Timbuktu, Mali (разработана SITU Research в качестве ресурса для дела *Аль-Махди* в Международном уголовном суде). URL: http://icc-mali.situplatform.com. См. также разнообразные онлайн-расследования с использованием открытых данных и визуальные отчеты о них на сайте Forensic Architecture. URL: https://forensic-architecture.org/methodology/osint.

[171] Группа визуальных расследований «Нью-Йорк Таймс» подготовила ряд визуальных объяснений, предназначенных для обобщения открытых онлайн-данных, содействия анализу сложных инцидентов и составления отчетов о результатах, хотя они не предусмотрены для использования в суде. См., например, Nicholas Casey, Christoph Koettl and Deborah Acosta, "Footage contradicts U.S. claim that Nicolás Maduro burned aid convoy", *New York Times*, 10 March 2019 (URL: www.nytimes.com/2019/03/10/world/americas/venezuela-aid-fire-video.html); Malachy Browne and others, "10 minutes. 12 gunfire bursts. 30 videos. Mapping the Las Vegas massacre", *New York Times*, 21 October 2017 (URL: www.nytimes.com/video/us/100000005473328/las-vegas-shooting-timeline-12-bursts.html).

[172] См. Alexa Koenig, "Open source evidence and human rights cases: a modern social history", in *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation and Accountability*, Sam Dubberley, Alexa Koenig and Daragh Murray, eds. (Oxford, Oxford University Press, 2020), pp. 38–40.

VIII

ГЛОССАРИЙ

КРАТКОЕ СОДЕРЖАНИЕ

- **Термины и определения, которые применяются в рамках расследований с использованием открытых данных или которые могут встречаться в имеющих отношение к расследованию или связанных с ним ресурсах.**

218. В настоящей главе содержатся термины и определения, которые могут быть полезны лицам, проводящим расследования с использованием открытых данных. Не все термины используются в Протоколе, но они включены, поскольку могут встречаться в имеющих отношение к расследованию или связанных с ним ресурсах.

Администрация адресного пространства Интернета (IANA): организация, контролирующая присвоение IP-адресов, номеров автономных систем и систем доменных имен по всему миру.

Адрес интернет-протокола (IP-адрес): любое цифровое устройство, подключающееся к Интернету, имеет IP-адрес. Существует два типа IP-адресов: IPv4 (32-битное число) и IPv6 (128-битное число). IP-адрес может использоваться для идентификации компьютеров и других устройств в Интернете.

Алгоритм: четко определенная процедура или набор инструкций, которые позволяют компьютеру решить задачу или отреагировать на заранее определенный сценарий.

Анонимизация: процесс, делающий невозможной идентификацию конкретного лица.

Блокчейн: технология, основанная на криптографии, с помощью которой открытый распределенный реестр, состоящий из «блоков», может использоваться для эффективной, верифицируемой и постоянной записи операций между двумя сторонами или организациями.

Большие данные: большие массивы данных, которые могут быть проанализированы для обнаружения корреляций между единицами данных и выявления закономерностей, которые могут помочь в прогнозировании. Основными характеристиками больших данных являются объем и сложность.

Булевый поиск: метод поиска в Интернете, который позволяет пользователям комбинировать ключевые слова с операторами или модификаторами (например, И, НЕ, ИЛИ) для сужения результатов поиска и, таким образом, предоставления более релевантных и конкретных результатов поиска.

Веб-маяк: механизм для отслеживания активности и действий пользователя. Веб-маяки представляют собой небольшой и незаметный (зачастую невидимый) элемент на веб-странице (столько же маленький, как один прозрачный пиксель), но при его отображении браузером данные об этом браузере и используемом компьютере отсылаются третьей стороне.

Веб-скрейпинг: метод извлечения большого количества данных с веб-сайтов.

Виртуальная машина: программное обеспечение, имитирующее работу компьютерной системы.

Виртуальная частная сеть (VPN): защищенная сеть или система защищенных узлов, использующих шифрование и другие процессы безопасности для обеспечения доступа к сети только авторизованных пользователей. Сети VPN маскируют IP-адрес и предотвращают перехват данных.

Владелец доменного имени: лицо, компания или иной субъект, которые владеют доменным именем или используют его.

Воздушный зазор (физическая изоляция): когда цифровое устройство не подключено напрямую к Интернету или какой-либо сети, что обеспечивает безопасность информации, хранящейся на этом устройстве.

Вредоносная программа: вредоносное программное обеспечение, предназначенное для нанесения вреда цифровому устройству, сети, серверу или пользователю. Существует множество различных видов вредоносных программ, включая вирусы, троянские программы, программы-вымогатели, рекламное и шпионское ПО.

Всемирная паутина (WWW): информационное пространство, в котором документы и другие веб-ресурсы обозначаются URL-адресами, которые могут быть связаны между собой гипертекстом и доступны через Интернет. Доступ к ресурсам Всемирной паутины может осуществляться пользователями с помощью программного приложения, называемого веб-браузером.

Встроенные данные: данные, хранящиеся в исходном файле или на веб-странице.

Данные о трафике: любые данные, обрабатываемые с целью передачи информации в сети электронных коммуникаций или для выставления счетов за эти коммуникации. Такие данные включают данные, относящиеся к маршрутизации, времени или продолжительности сеанса связи.

Даркнет: часть Интернета, доступ к которой возможен только с помощью специального программного обеспечения, что позволяет пользователям и операторам сайтов сохранять анонимность и оставаться не отслеживаемыми.

Доменное имя: метка, идентифицирующая сетевой домен. В Интернете доменные имена формируются в соответствии с правилами и процедурами системы доменных имен (DNS). Как

правило, доменное имя представляет ресурс интернет-протокола (IP), например персональный компьютер, используемый для доступа в Интернет, сервер, на котором размещен веб-сайт, сам веб-сайт или любой другой сервис, передаваемый через Интернет.

Драгнет: в сетевом контексте широкая автоматизированная система сбора или наблюдения.

Изъятие метаданных: технологический процесс удаления метаданных из файла без преобразования его в другие форматы.

Интеллектуальный анализ данных: практика изучения и извлечения данных из баз данных с целью получения сведений или новой информации.

Интернет-корпорация по присвоению имен и номеров (ICANN): организация, отвечающая за обеспечение стабильной и безопасной работы Интернета путем координации ведения нескольких баз данных, связанных с именами и числовыми пространствами Интернета, и их процедур.

Интернет-провайдер (ИП): организация, предоставляющая пользователям Интернета услуги по доступу к Интернету и его использованию.

Интернет-форум (также известный как доска обсуждений): веб-сайт, на котором пользователи могут размещать сообщения и вести беседы. На форумах обычно более длинные сообщения, чем в чатах, и контент чаще всего архивируется.

Интерфейс программирования приложений (API): код, позволяющий компьютерным программам взаимодействовать друг с другом.

Интранет: частная компьютерная сеть, использующая Интернет-протоколы и сетевое подключение для создания внутренней версии Интернета.

Искусственный интеллект (ИИ): отрасль информатики, посвященная разработке программ для машин, которые учатся реагировать на неизвестные переменные и адаптироваться к новым условиям.

Исходный файл: файл в исходном формате.

Капча: сокращение для полностью автоматического публичного теста Тьюринга для различения компьютеров и людей (CAPTCHA — Completely Automated Public Turing test to tell Computers and Humans Apart). Это тип теста «запрос–ответ», используемый в вычислительной технике для определения того, является ли пользователь человеком.

Криптографическая подпись: математический процесс проверки подлинности цифрового материала. Используя алгоритм, можно сгенерировать два математически связанных ключа: закрытый и открытый. Для формирования цифровой подписи используется программное обеспечение для создания хеша электронных данных. Затем закрытый ключ используется для шифрования хеша.

Криптография: практика цифрового кодирования или декодирования информации.

Куки: небольшой фрагмент данных, отправляемый веб-сайтом и либо хранимый в памяти компьютера пользователя, либо записываемый на диск компьютера для использования браузером. Куки часто необходимы для эффективного функционирования веб-сайта — для сохранения предпочтений пользователя на сайте и его личных данных, избавления его от необходимости постоянно вводить данные при последующих посещениях.

Локальная сеть (LAN): совокупность цифровых устройств, подключенных к одной сети в определенном физическом месте.

Машинное обучение: вид искусственного интеллекта, который использует статистические методы, чтобы создать для компьютеров возможность «учиться» на основе данных, не будучи специально запрограммированными.

Метаданные: данные о данных. Они содержат информацию об электронном файле, которая либо встроена в файл, либо связана с ним. Метаданные часто включают характеристики и историю файла, такие как его имя, размер, даты создания и изменения. Они могут описывать, как, когда и кем был собран, создан, использовался, был изменен и отформатирован цифровой файл.

Неструктурированные данные: данные и информация в различных формах, не организованные в строгий формат, в связи с чем их нелегко обрабатывать и анализировать. Как правило, это текст, но они также могут включать изображения, аудио- и видеофайлы.

Облачные вычисления: операционная модель, позволяющая хранить, обрабатывать и анализировать данные через интранет или Интернет. Существует три типа облаков: частные, публичные и гибридные.

Поверхностная сеть: часть Интернета, которая доступна через любой браузер и поиск в которой осуществляется с помощью традиционных поисковых систем.

Поисковый робот (также называемый пауком или краулером): программа, которая систематически просматривает сайты в Интернете в соответствии с автоматизированным скриптом для загрузки и индексации посещенных сайтов.

Поставщик веб-услуг: организация, предоставляющая услуги и продукты в Интернете, например социальная сеть.

Прогнозно-аналитическое программное обеспечение: программное обеспечение, использующее алгоритмы прогнозирования и машинное обучение для анализа данных с целью составления прогнозов относительно будущего или неизвестных событий и действий.

Протокол передачи гипертекста (HTTP): протокол, лежащий в основе Интернета и определяющий порядок передачи и получения данных.

Псевдонимизация: обработка персональных данных таким образом, что информация больше не может быть соотнесена с конкретным субъектом данных без использования дополнительной информации.

Система доменных имен (DNS): система, с помощью которой регулируется присвоение доменных имен.

Социальная инженерия: психологическое манипулирование человеком с целью получения несанкционированного доступа к информации. Сходно с хакерством, но предполагает использование уязвимости человека, а не техники. Существует множество различных видов социальной инженерии, включая фишинг и адресный фишинг.

Структурированные данные: данные или информация, которые соответствуют строгому формату в хранилище (обычно это база данных, но может быть и набор заполненных форм), с тем чтобы их элементы были доступны для обработки и анализа.

Трекер: тип куки, который использует возможности браузера по ведению учета посещенных веб-страниц, введенных критериев поиска и т. д. Как правило, трекеры — это постоянные куки, которые ведут журнал действий конкретного посетителя.

Унифицированный указатель ресурса (URL): местоположение веб-страницы в Интернете. Это то же самое, что и веб-адрес.

Формат переносимых документов (PDF): формат файлов с фиксированным макетом, который сохраняет формат документа (включая шрифты, интервалы и изображения) независимо от программного обеспечения, оборудования и операционных систем, используемых для открытия и просмотра этого документа. Преобразование файла из исходного формата в PDF лишает его метаданных, предоставляя статичное изображение документа.

Хеш или хеш-значение: вычисления, которые можно выполнить для любого типа цифрового файла для создания буквенно-цифровой строки фиксированной длины, которая может быть использована в качестве доказательства того, что цифровой файл не был изменен. Эта строка будет оставаться неизменной при каждом запуске вычисления до тех пор, пока файл не изменится.

Цифровое сохранение: политика и стратегии, необходимые для управления цифровой информацией с непреходящей ценностью и ее хранения в течение длительного времени, чтобы цифровая информация была доступна и пригодна для использования предполагаемыми пользователями в будущем.

Цифровой архив: коллекция документов, веб-страниц или электронных записей. Этот термин также может означать официальную или неофициальную организацию, которая берет на себя ответственность за сохранение информации и обеспечение ее доступности для авторизованных пользователей.

Чат: веб-сайт в Интернете, позволяющий пользователям вести онлайн-беседы в режиме реального времени.

Шифрование: процесс, делающий данные недоступными без ключа для расшифровки.

Язык разметки гипертекста (HTML): язык программирования, который используется для разработки веб-страниц, доступных с помощью браузера.

WHOIS: протокол, позволяющий определить, кто является владельцем конкретного доменного имени на основе организации, которая его зарегистрировала. Лица, проводящие расследования с использованием открытых данных, могут использовать инструмент поиска WHOIS как часть процесса анализа и проверки источника.

ПРИЛОЖЕНИЯ

КРАТКОЕ СОДЕРЖАНИЕ

- **Шаблон плана онлайн-расследования**
- **Шаблон оценки цифровых угроз и рисков**
- **Шаблон оценки цифрового ландшафта**
- **Форма для сбора онлайн-данных**
- **Критерии для проверки новых инструментов**

Приложение I

Шаблон плана онлайн-расследования

Номер расследования:	
Дата оценки:	
Краткое описание расследования: *предмет, территориальные и временные рамки расследования*	

1. Цели и планируемая деятельность

Цели и стратегия онлайн-расследования, а также конкретные действия с указанием сроков их выполнения.

2. Резюме оценки цифрового ландшафта

Оценка цифрового ландшафта на исследуемой географической территории, например популярных социальных сетей, мобильных приложений и других технологий, а также лиц, имеющих доступ к этим технологиям и использующих их.

3. Стратегия снижения рисков и меры защиты

Основные результаты оценки цифровых угроз и рисков, а также стратегия выявления таких угроз, управления ими и реагирования на них.

4. Составление списка соответствующих действующих лиц

Список субъектов, первыми отреагировавших на инцидент, которые могли собрать потенциально релевантный, но затем исчезнуший онлайн-контент; цифровых архивов и поставщиков интернет- и веб-услуг, которые могут иметь оригинальные версии или дополнительные метаданные онлайн-контента и передать их по запросу о предоставлении помощи. Хотя неофициальные лица, проводящие расследование, могут не иметь юридических полномочий запрашивать закрытые данные, контакты в среде интернет-провайдеров, тем не менее, могут быть полезны для получения ответов на вопросы и помощи пользователям в навигации по их платформам.

5. Функции и обязанности

Определение функций и обязанностей членов группы; кроме того, следует указать координатора, который будет координировать действия в сети. Можно также включить оценку того, кто потенциально может нести ответственность в случае вызова для дачи показаний в суде.

6. Ресурсы

Оценка кадровых потребностей (количество лиц, проводящих расследование, разнообразие и инклюзивность персонала), а также любая специальная подготовка и оборудование, необходимые для проведения онлайн-расследований.

7. Документация

Конкретные указания о том, как и где членам группы следует документировать свои онлайн-действия по расследованию.

Приложение II

Шаблон оценки цифровых угроз и рисков

Номер расследования:	
Дата оценки:	
Краткое описание расследования: *предмет, территориальные и временные рамки расследования*	
Цели расследования:	

1. Каковы ваши активы?

Люди (в разбивке по гендеру):
Материальное имущество:
Нематериальное имущество (например, данные):

2. Каковы ваши факторы уязвимости?

3. Какие типы угроз могут включать использование этих факторов уязвимости и нанести ущерб вашим активам?

4. Какие субъекты могут умышленно нарушить информационную безопасность?

A. Каковы их интересы?
B. Каковы их возможности?
C. Какова вероятность атаки?

5. Какие меры по снижению риска возможны/целесообразны? Есть ли необходимость реагировать на различные риски, с которыми сталкиваются представители разных гендеров?

Необходимо учитывать следующее:

- Физический ущерб
- Цифровой ущерб
- Психосоциальный ущерб

Приложение III

Шаблон оценки цифрового ландшафта

Номер расследования:	
Дата оценки:	
Краткое описание расследования: *предмет, территориальные и временные рамки расследования*	
Цели расследования:	

Звездочка (*) означает, что лицам, проводящим расследование, следует принимать во внимание различные факторы, в частности возраст, гендерную принадлежность, местонахождение и другую соответствующую демографическую информацию.

1.	Соответствующие стороны (т. е. конкретные сообщества, вооруженные группы и др.). Укажите, существуют ли между сторонами различия в использовании технологий или в их представленности в Интернете в разбивке по гендеру, возрасту или инвалидности.
2.	Соответствующие языки (включая сленг и другие инсайдерские языки)*.
3.	Часто используемые поисковые системы*
4.	Популярные платформы социальных сетей*
5.	Популярные веб-сайты*
6.	Использование/распространение Интернета (в разбивке по гендеру, возрасту и др.)
7.	Предпочтения в отношении мобильных телефонов/операционных систем (в разбивке по гендеру, возрасту и др.)
8.	Популярные мобильные приложения (в разбивке по гендеру, возрасту и др.)
9.	Поставщики телекоммуникационных услуг
10.	Связь: расположение Wi-Fi/вышек сотовой связи
11.	Соответствующие законы (свобода слова, доступ к информации, неприкосновенность частной жизни)
12.	СМИ и репортеры (присутствие в сети)
13.	Открытые базы данных (например, правительственных данных, данных НПО/исследователей)
14.	Платные базы данных (например, правительственных данных, данных частных компаний/ исследователей)
15.	Репрезентативность онлайн-контента (включенные и исключенные группы)

Приложение IV

Форма для сбора онлайн-данных

1.	**Информация о лице, проводящем сбор**
	Расследование:
	Лицо, проводящее сбор:
	IP-адрес лица, проводящего сбор:
	Начало сбора (отметка даты/времени):
	Конец сбора (отметка даты/времени):
2.	**Целевая информация**
	Веб-адрес (URL):
	Исходный код HTML:
	Скриншот:
	Полученные данные:
	IP-адрес (адреса):
3.	**Информация о пакете сбора данных**
	Имя файла пакета сбора данных:
	Список хешей пакета сбора данных:
	Хеш файла списка хешей пакета сбора данных:
4.	**Используемые сервисы**
	Программный продукт (продукты):
	Сервис времени:
	IP-сервис:
	WHOIS-сервис:

Приложение V

Критерии для проверки новых инструментов

Характеристики
Открытый или закрытый исходный код
Платный или бесплатный продукт
Сведения о владельце (физическом лице или компании), его связи или интересы
Финансирование (как и насколько хорошо финансируется инструмент? Каков вероятный срок службы продукта?
Вопросы безопасности
Кто владеет инструментом или исходным кодом?
Является ли исходный код открытым или закрытым?
Осуществляется ли независимая проверка инструмента?
Где будут храниться все собранные данные?
У кого будет доступ к собранным данным?
Какова инфраструктура безопасности инструмента?
Какие юридические обязательства могут повлиять на безопасность использования инструмента?
Если имеет место нарушение закона, существует ли право на средство правовой защиты?
Операционные вопросы
Каковы функциональные возможности инструмента?
Насколько инструмент удобен в использовании?
Каковы возможности поддержки пользователей со стороны владельца, поставщика или инструмента?
Как часто осуществляется обновление инструмента?
Насколько инструмент совместим с другими системами?

HUMAN RIGHTS CENTER
UC Berkeley School of Law

Калифорнийский университет
Центр по правам человека (ЦПЧ)
2224 Piedmont Avenue
Berkeley, CA 94720
Эл. почта: hrc@berkeley.edu
Веб-сайт: https://humanrights.berkeley.edu/

ОБЪЕДИНЕННЫЕ НАЦИИ
ПРАВА ЧЕЛОВЕКА
УПРАВЛЕНИЕ ВЕРХОВНОГО КОМИССАРА

Управление Верховного комиссара по правам человека
Организации Объединенных Наций
Дворец Наций
CH 1211 Geneva 10, Switzerland
Эл. почта: ohchr-infodesk@un.org
Веб-сайт: www.ohchr.org/ru

Опубликовано совместно Организацией Объединенных Наций — от имени Управления Верховного комиссара Организации Объединенных Наций по правам человека — и Центром по правам человека при Школе права Калифорнийского университета в Беркли.

ISBN: 978-92-1-154249-3

Printed at United Nations, Geneva – 2012695 **(R)** – December 2022 – 1,138 – **HR/PUB/20/2**