АДРИАН НОРТВЕЙЛ

НЕ ВЕРЬ ПЕРВОЙ ССЫЛКЕ

Как находить факты,
а не чужие ошибки

Адриан Нортвейл

Не верь первой ссылке. Как находить факты, а не чужие ошибки

https://litres.ru/74253623
SelfPub; 2026

Аннотация

В открытых источниках много шума, и он отлично маскируется под правду.

Вы узнаете, как искать людей, компании, домены, фото, видео, документы и утечки так, чтобы не ловить себя на красивой ошибке. Начнёте отличать факт от догадки, сможете проверять связи, не путать однофамильцев, не писать лишнее в отчёте. Сэкономите часы на бесполезных поисках, перестанете тонуть в вкладках и начнёте собирать цепочку, которую можно спокойно показать другому человеку. Эта книга для тех, кто хочет видеть больше, но не хочет врать себе ради вывода.

Содержание

Адриан Нортвейл
Не верь первой ссылке. Как находить факты, а не чужие ошибки

Введение

Разведка по открытым источникам редко начинается с красивого рабочего стола, специальных программ и уверенного человека в темной комнате. Чаще все проще. Перед вами вопрос, вокруг него слишком много шума, а времени мало. Кто-то прислал ссылку. В новостях появился странный заголовок. На сайте компании лежит документ, который никто не заметил. В социальной сети человек сам оставил след, но этот след надо еще увидеть, отделить от случайности и не принять чужую фантазию за факт.

Открытые источники удобны тем, что они рядом. В этом и ловушка. Кажется, раз информация лежит в поиске, в профиле, в реестре или в старой копии страницы, то ее можно просто взять и сразу сделать вывод. На практике открытая информация ведет себя как базарная площадь. Там кричат, спорят, продают, скрывают, хвастаются, путают даты, повто-

ряют слухи и иногда говорят правду. Работа начинается не с добычи, а с умения не потерять голову среди этого шума.

Эта книга написана для человека, которому нужна не коллекция модных инструментов, а рабочий способ думать. Инструменты меняются. Одни сервисы закрывают бесплатный доступ, другие ломают поиск, третьи становятся популярными на сезон и исчезают. Принцип остается. Найди источник. Проверь, откуда он взялся. Пойми, кто заинтересован в том, чтобы ты поверил именно этой версии. Сохрани след. Свяжи факты между собой. Остановись там, где любопытство уже не помогает делу.

В открытой разведке приятно чувствовать себя умнее остальных. Это опасное чувство. Оно толкает к лишним поискам, к поспешным версиям, к желанию собрать про человека все, хотя для задачи хватило бы двух проверенных фактов. Я не считаю такую работу игрой. Даже когда источники открыты, последствия бывают настоящими. Чужая репутация, безопасность, деньги, свобода, доверие внутри компании - все это может зависеть от того, насколько аккуратно вы обращаетесь с найденным.

Поэтому я буду говорить не только о том, где искать. Куда важнее другое: как не обмануться, как вести записи, как не смешивать факт с предположением, как отличать полезную зацепку от бесполезного любопытства. Хороший поиск не выглядит как бесконечное открывание вкладок. Он больше похож на спокойную работу следователя, бухгалтера и

редактора сразу. Следователь ищет связь. Бухгалтер требует подтверждения. Редактор вычеркивает лишнее.

Источник, на котором основана эта книга, выстроен как практическое руководство по OSINT: от определения и истории до областей применения, законов, этики и рабочих записей. Я беру эту логику как основу, но пишу новый русский текст, без копирования страниц и без попытки превратить живую тему в сухой конспект. Здесь будут не только названия методов, но и разговор о привычках, без которых метод быстро превращается в хаос.

Открытая разведка полезна в кибербезопасности, корпоративных проверках, журналистике, правовой работе, поиске людей, проверке слухов и анализе публичных событий. Но во всех этих областях один и тот же вопрос возвращается снова: что именно мы знаем, откуда мы это знаем и насколько этому можно доверять. Пока вы не ответили на эти три вопроса, у вас нет разведки. У вас есть набор находок.

В книге не будет обещания, что после чтения вы станете всевидящим наблюдателем. Такие обещания продают курсы, а не помогают работать. Я хочу дать другое: порядок. Как начинать поиск. Как сужать круг. Как не забывать о законе. Как уважать границы, даже когда технически можно пройти дальше. Как оформлять заметки так, чтобы через неделю вы сами поняли, почему поверили одному источнику и отвергли другой.

Начнем с фундамента. Что такое OSINT на самом деле,

почему он появился задолго до интернета, чем отличается от других видов разведки и где применяется сегодня. Без этого легко спутать OSINT с обычным поиском в сети. Поиск дает ответы. Разведка требует проверки, контекста и решения, которое можно объяснить другому человеку. Разница кажется небольшой только до первой серьезной ошибки.

Глава 1. Разведка из открытых источников: с чего всё начинается

Если говорить просто, OSINT - это работа с открытой информацией, из которой нужно получить полезный вывод. Не просто собрать ссылки, не просто найти чужую фотографию, не просто выписать имя из реестра. Полезный вывод появляется тогда, когда разрозненные данные проходят через проверку, сравнение и здравый смысл. До этого момента перед нами лежит сырье. Иногда ценное, иногда мусорное, часто перемешанное.

Открытым источником может быть новостная заметка, профиль в социальной сети, запись в государственном реестре, судебный документ, научная статья, карта, доменное имя, старый форум, архивная копия страницы, метаданные файла, публичный отчет компании или комментарий под видео. Все это доступно без взлома, подкупа, тайного проникновения и других способов, после которых разговор быстро переходит из профессиональной плоскости в юридическую.

Но доступность не делает источник честным. Человек может придумать биографию. Компания может красиво описать слабый продукт. Новость может повторить чужую ошибку. Реестр может устареть. Фотография может быть сделана в одном месте, а выложена с подписью про другое. Поэтому

первый навык в OSINT не технический. Это недоверие без паранойи. Нужно сомневаться, но не превращать каждую находку в заговор.

Представьте, что вы проверяете небольшую фирму перед сделкой. На сайте все выглядит прилично: адрес, команда, отзывы, история успеха. Дальше вы находите домен и смотрите, когда он зарегистрирован. Потом проверяете юридическое лицо. Потом ищете судебные споры. Потом смотрите, кто именно пишет отзывы и не повторяются ли одни и те же фразы на разных площадках. Отдельно каждая находка может ничего не значить. Вместе они дают картину.

Вот здесь и появляется слово intelligence, которое часто переводят слишком торжественно. Речь не о шпионской романтике. Речь о сведениях, пригодных для решения. Если после вашей работы человек может сказать: мы идем в сделку, мы не идем в сделку, мы усиливаем защиту, мы передаем материалы юристу, мы проверяем еще один источник - значит, разведка состоялась. Если после вашей работы стало только больше вкладок и тревоги, значит, порядок еще не наведен.

Граница OSINT проходит там, где заканчивается открытый доступ и начинается нарушение. Зайти на публичную страницу можно. Обойти защиту нельзя. Прочитать опубликованный судебный документ можно. Выдавать себя за другого человека, чтобы получить закрытые сведения, нельзя. Использовать поисковые операторы можно. Ломать чужой

сервер нельзя. Эти правила звучат скучно, но именно они отделяют профессиональную работу от самодеятельности с плохим финалом.

Сфера открытых источников широка потому, что люди и организации давно живут публично. Они оставляют следы в документах, публикациях, объявлениях, изображениях, доменах, утечках, тендерах, презентациях, интервью и списках участников конференций. Даже когда человек старается молчать, за него говорят окружение, инфраструктура, старые записи и случайные совпадения. Задача не в том, чтобы вытащить из мира все. Задача в том, чтобы найти достаточно надежное для конкретного вопроса.

У начинающих есть привычка искать сразу везде. Это понятно. Кажется, чем больше источников, тем выше шанс. Но без плана широкий поиск быстро превращается в прогулку. Вы начали с проверки домена, через десять минут читаете старый спор на форуме, еще через пятнадцать смотрите чужой профиль, а исходный вопрос уже забыт. Поэтому перед поиском надо записать цель одной фразой. Не красиво, не официально, а точно: узнать владельца ресурса, проверить дату события, связать человека с компанией, подтвердить факт публикации.

После цели полезно записать ограничения. Какие источники допустимы? На каком языке искать? Какой период интересует? Нужно ли сохранять доказательства для отчета? Есть ли риск задеть частную жизнь? Какие данные нельзя

собирать без отдельного основания? Такие вопросы не тормозят работу. Они спасают ее от расползания.

В OSINT много направлений. Есть социальная разведка по открытым публикациям, где смотрят связи, интересы, маршруты и публичные высказывания. Есть работа с государственными и корпоративными реестрами. Есть техническая разведка: домены, DNS, IP-адреса, сертификаты, открытые сервисы. Есть геолокация по изображениям и картам. Есть анализ документов и метаданных. Есть мониторинг новостей, форумов, тендеров, архивов. Каждое направление требует своих инструментов, но логика проверки остается общей.

Плохая OSINT-работа обычно видна по двум признакам. Первый: много уверенности при слабых источниках. Второй: много найденного, но непонятно, что из этого следует. Человек приносит десятки ссылок, скриншотов, имен, никнеймов, адресов, а потом сам не может объяснить, какие факты подтверждены, какие вероятны, а какие просто похожи на правду. В серьезной работе такое не проходит.

Я советую с самого начала разделять три категории: факт, предположение и вопрос. Факт: документ опубликован по такому адресу, дата такая-то, имя указано так-то. Предположение: этот аккаунт может принадлежать тому же человеку, потому что совпадают ник, город и фотография. Вопрос: почему у компании два разных адреса в разных источниках? Такая простая разметка дисциплинирует лучше мно-

гих сложных программ.

История OSINT началась не с поисковых систем. Государства давно читали чужие газеты, слушали радио, переводили речи, изучали научные журналы и отчеты. Во время больших войн публичные сообщения давали сведения о настроениях, снабжении, пропаганде и планах. В холодную войну открытые публикации помогали оценивать технологии, экономику и военные возможности. Интернет не создал открытую разведку. Он сделал ее быстрой, массовой и более беспорядочной.

С появлением интернета изменилась скорость. Раньше аналитик ждал газету, перевод, бюллетень или радиоперехват. Теперь он получает поток. Сайты, блоги, базы данных, социальные сети, форумы, видео, карты, объявления, архивы. Каждую минуту появляется новое. Старое исчезает, редактируется, переезжает. Поэтому современный OSINT требует не только поиска, но и фиксации. Если вы нашли важную страницу, сохраните ее адрес, время доступа, копию или скриншот, иначе завтра вы можете доказывать самому себе, что она точно существовала.

Социальные сети изменили работу еще сильнее. Люди начали добровольно публиковать то, что раньше приходилось узнавать через знакомых: места работы, фотографии, поездки, круг общения, взгляды, привычки. Но социальные сети не являются исповедью. Там люди играют роли, скрывают часть жизни, преувеличивают успех, удаляют неудобное, по-

вторяют чужие мнения. Аналитик должен видеть не только содержание поста, но и обстоятельства: когда он опубликован, кем, для кого, с какой реакцией, как связан с другими источниками.

В кибербезопасности OSINT помогает увидеть собственную поверхность атаки. Какие домены принадлежат организации, какие сервисы торчат наружу, какие сотрудники публикуют лишнее, какие учетные данные могли попасть в утечки, какие обсуждения угроз идут на форумах. Здесь открытая разведка работает как фонарь. Она показывает то, что уже видно миру, но внутри компании на это часто не смотрят.

В корпоративных проверках OSINT нужен для другой задачи: понять, с кем имеешь дело. Партнер, подрядчик, конкурент, кандидат на должность, объект сделки - все они оставляют публичные следы. Можно смотреть судебные дела, финансовые отчеты, связи руководителей, историю доменов, отзывы, патенты, тендеры, новости, санкционные списки, публичные выступления. Но и здесь нельзя превращать проверку в охоту за личными деталями. Если факт не связан с деловой задачей, он чаще мешает, чем помогает.

В правоохранительной работе открытые источники помогают строить линии времени, искать свидетелей, отслеживать публичные заявления, проверять изображения, сопоставлять места и связи. Но цена ошибки там особенно высока. Неверно связанный аккаунт, неправильно понятая шут-

ка, случайное совпадение имени могут испортить человеку жизнь. Поэтому в таких задачах требуется железная привычка подтверждать выводы разными путями и ясно показывать степень уверенности.

Журналистика тоже давно использует OSINT, хотя не всегда называет это так. Проверить видео с места событий, найти первоисточник фотографии, сопоставить тень на снимке с временем дня, найти компанию в реестре, проверить владельца сайта, поднять старую версию страницы - все это открытая разведка. Хороший журналист не просто сообщает, что нашел в сети. Он показывает, почему этому можно верить.

Отдельный разговор - закон и этика. Закон отвечает на вопрос, что вам разрешено. Этика спрашивает, что вам стоит делать, даже если формально можно. Эти вопросы иногда совпадают, иногда нет. Публичный пост можно сохранить. Но нужно ли включать в отчет личную деталь, не связанную с расследованием? Старую фотографию можно найти в архиве. Но нужно ли ее распространять, если она не имеет отношения к делу? Взрослая работа начинается там, где человек способен остановиться.

Самый надежный ограничитель - цель исследования. Если цель достигнута, дальнейший сбор данных должен быть обоснован отдельно. Любопытство не основание. Желание узнать еще немного не основание. Особенно когда речь идет о персональных данных, семье, здоровье, адресах, привыч-

ках и частной жизни. OSINT не должен превращаться в доносительство под видом анализа.

Международные правила добавляют сложности. Персональные данные в Европе, Калифорнии, Канаде и других юрисдикциях защищаются по-разному, но общий смысл ясен: публичность не отменяет ответственности. Имя, адрес электронной почты, IP-адрес, фотография, сведения о работе или местоположении могут быть персональными данными. Если вы собираете, храните и передаете такие сведения, вам придется объяснить, зачем и на каком основании вы это делаете.

Скрапинг тоже не так прост, как кажется. Страница открыта, но сайт может запрещать автоматический сбор в правилах. Где-то это гражданский спор, где-то риск блокировки, где-то вопрос доступа к системе. Профессионал не запускает массовый сбор только потому, что нашел готовый скрипт. Он сначала понимает цель, объем, правовую рамку и последствия.

Есть еще одна частая ошибка: путать анонимность с безнаказанностью. VPN, Tor, отдельная виртуальная машина, чистый браузер, новые учетные записи - все это может защищать исследователя и не раскрывать его раньше времени. Но эти средства не дают права нарушать границы. Они нужны для безопасности работы, а не для того, чтобы делать то, за что потом стыдно или страшно отвечать.

Ведение записей кажется скучной частью OSINT, пока вы

не столкнетесь с длинной проверкой. Через несколько дней вы уже не помните, почему открыли именно этот сайт, откуда взялась версия с другим ником, какая ссылка была первичной, а какая повторяла чужой материал. Память ненадежна. Записи нужны не для красоты отчета, а чтобы не обмануть самого себя.

Хорошая заметка должна отвечать на несколько простых вопросов: что найдено, где найдено, когда найдено, почему это относится к задаче, как это проверено, что остается неизвестным. Если есть скриншот, нужен адрес и время. Если есть документ, нужна версия или дата доступа. Если есть вывод, нужно отделить его от исходных данных. Эта дисциплина экономит часы и спасает от ложной уверенности.

Я люблю простую структуру рабочего файла. Вверху цель. Ниже короткая хронология действий. Потом таблица источников: ссылка, тип источника, дата, что подтверждает, надежность, комментарий. Отдельно список вопросов. Отдельно список гипотез. В конце черновой вывод, который постоянно переписывается по мере проверки. Не обязательно использовать именно такую форму, но какая-то форма должна быть. Иначе исследование расползется.

Инструменты для заметок можно выбирать по задаче. Кому-то достаточно текстового файла и папки со скриншотами. Кому-то удобнее OneNote, Obsidian, Joplin, Hunchly или другая система, где можно сохранять страницы, метаданные и связи. Название программы не делает работу качествен-

ной. Качественной ее делает привычка фиксировать путь от источника к выводу.

Полезно хранить не только найденное, но и отвергнутое. Например: аккаунт с похожим ником не подходит, потому что город другой и фотография появилась позже. Новость не подходит, потому что ссылается на тот же неподтвержденный пост. Документ не подходит, потому что относится к другой компании с похожим названием. Такие записи кажутся лишними, пока кто-то не спросит, почему вы не учли этот источник. Тогда они становятся защитой вашей логики.

Проверка источника начинается с происхождения. Кто это опубликовал? Когда? Был ли он очевидцем? Ссылается ли он на документы? Повторяют ли его другие независимые источники? Не является ли это перепечаткой? Не изменялась ли страница? Есть ли финансовый, политический или личный интерес? Эти вопросы не требуют особой техники, но без них даже дорогой инструмент выдаст мусор с красивой визуализацией.

В OSINT часто приходится работать с вероятностями. Не всегда можно сказать: это точно тот человек. Иногда честный вывод звучит скромнее: с высокой вероятностью, потому что совпадают три независимых признака; вероятно, но требуется подтверждение; связь не подтверждена. Такая осторожность не слабость. Это профессиональная чистота. Лучше написать менее эффектный вывод, чем уверенно ошибиться.

Нужно привыкнуть к тому, что отсутствие данных тоже

является результатом, но не доказательством. Если вы не нашли судебных дел, это не значит, что их нет. Если в поиске нет упоминаний, это не значит, что события не было. Возможно, вы искали не на том языке, не в той юрисдикции, не в том периоде, по неправильному написанию имени. Поэтому отрицательный вывод требует особой осторожности: где искали, как искали, что именно не найдено.

Работа с именами особенно коварна. Один человек может использовать разные написания, транслитерации, сокращения, прежние фамилии, никнеймы. Два разных человека могут иметь одинаковое имя и город. Компания может иметь бренд, юридическое лицо и несколько дочерних структур. Домен может быть зарегистрирован на посредника. Любой совпадающий признак надо воспринимать как зацепку, а не как доказательство.

Технические источники выглядят точными, но тоже требуют контекста. WHOIS может быть закрыт приватной регистрацией. IP-адрес может принадлежать хостингу, а не владельцу сайта. Открытый порт может быть тестовым, забытым или специально оставленным. Сертификат может показать связь доменов, но не всегда доказывает общую собственность. Техника дает сильные сигналы, если понимать, что именно она показывает.

Геолокация по изображениям кажется почти магией, когда видишь готовый разбор. На деле это терпеливая работа с деталями: вывески, дорожная разметка, тени, горы на го-

ризонте, форма окон, язык объявлений, погода, растительность, номера, отражения. Один признак может обмануть. Несколько независимых признаков начинают держать вывод. И опять нужны записи, иначе через час вы сами не вспомните, почему решили, что это именно тот перекресток.

Документы тоже говорят больше, чем кажется. Имя автора файла, дата создания, версия программы, скрытые свойства, стиль оформления, путь к шаблону, совпадающие формулировки - все это может дать направление. Но метаданные легко меняются и иногда появляются случайно. Их нельзя воспринимать как окончательный ответ. Это повод проверить дальше.

Когда данных становится много, появляется соблазн нарисовать большую карту связей. Визуализация полезна, если за ней стоят проверенные факты. Но красивая схема может создать ложное ощущение доказанности. Две линии на графе выглядят убедительно, хотя одна может означать подтвержденную деловую связь, а другая - случайное упоминание в одном списке. Поэтому связи нужно подписывать: источник, дата, тип связи, степень уверенности.

Отчет по OSINT должен быть понятен человеку, который не сидел рядом с вами во время поиска. Он должен видеть исходный вопрос, краткий ответ, главные подтверждения, ограничения и дальнейшие шаги. Не надо превращать отчет в свалку скриншотов. Скриншоты нужны как доказательная база, но вывод должен быть написан человеческим языком.

Что это значит для решения? Что известно точно? Что требует проверки? Где риск ошибки?

Хороший отчет честен насчет слабых мест. Если источник один, так и пишите. Если дата не подтверждена, не прячьте это в примечании. Если найденная связь косвенная, не называйте ее прямой. Руководитель, юрист, редактор или специалист по безопасности должны понимать, на чем стоит вывод. Иначе они примут решение на основании вашей уверенности, а не на основании фактов.

В начале пути полезно тренироваться на безопасных задачах. Проверить историю домена собственного проекта. Найти первоисточник изображения из новости. Составить хронологию публичного события по независимым источникам. Проверить компанию по открытым реестрам. Собрать карту публичных активов своей организации. Такие упражнения учат не хуже громких расследований, зато не толкают к лишнему риску.

Еще полезно время от времени проверять самого себя. Какие данные обо мне открыты? Какие аккаунты связаны одним ником? Какие старые документы лежат в сети? Какие фотографии содержат лишние детали? Такая проверка быстро отрезвляет. После нее легче уважать чужую приватность, потому что понимаешь, насколько легко собрать неприятно точный портрет из мелочей.

OSINT требует трезвости. Не верить первому найденному. Не радоваться слишком рано совпадению. Не стыдиться

писать 'не подтверждено'. Не собирать лишнее. Не нарушать закон ради красивой находки. Не подменять анализ набором инструментов. Если держать эти правила в голове, открытые источники становятся мощным рабочим материалом, а не бесконечным шумом.

В этой первой главе нам нужен один главный вывод: OSINT - это не про то, чтобы знать секреты. Это про то, чтобы аккуратно работать с тем, что уже открыто, и получать из этого проверяемый смысл. Иногда этот смысл помогает предотвратить атаку. Иногда - не подписать плохой договор. Иногда - исправить ошибочную публикацию. Иногда - понять, что данных недостаточно и лучше остановиться. Последний вариант тоже бывает правильным результатом.

Дальше можно говорить об инструментах, рабочих средах, виртуальных машинах, поисковых операторах, социальных сетях, доменах, утечках и отчетах. Но все это будет держаться на фундаменте из этой главы. Цель, источник, проверка, запись, граница. Без них любое расследование быстро превращается в беспорядочное любопытство. С ними даже простой поиск начинает работать как настоящая разведка.

Перед тем как перейти к инструментам, стоит закрепить практическую привычку. Открывая новый источник, не спрашивайте сначала: что я могу отсюда вытащить? Спросите иначе: какой вопрос этот источник способен честно подтвердить? Новостная статья подтверждает факт публикации и позицию автора, но не всегда факт события. Реестр под-

тверждает запись в реестре, но не всю реальную деятельность. Социальный профиль подтверждает публичное поведение аккаунта, но не всегда личность владельца. Такая разница кажется мелкой, пока на ней не строят решение.

И еще одно. В OSINT не нужно выглядеть таинственным специалистом. Нужно быть аккуратным человеком, который умеет читать, сравнивать, сохранять и признавать ограничения. Это звучит проще, чем модные описания профессии, зато ближе к реальной работе. Большая часть сильных находок рождается не из секретного инструмента, а из внимательного чтения того, что другие пролистали слишком быстро.

Есть еще практическая сторона, о которой редко говорят в начале. OSINT утомляет. Не физически, а вниманием. После часа поиска человек начинает видеть связи там, где есть только похожие слова. После трех часов он уже хочет закрыть задачу и выбирает версию, которая удобнее. Поэтому рабочий режим так же важен, как набор источников. Делайте паузы, возвращайтесь к исходному вопросу, перечитывайте свои заметки холодно. Если вывод выглядит слишком красивым, проверьте его особенно жестко.

Полезно работать слоями. Первый слой - быстрый обзор, чтобы понять, какие источники вообще существуют. Второй - проверка надежных мест: реестры, официальные страницы, первичные документы, архивы. Третий - сопоставление косвенных признаков: даты, имена, адреса, технические сле-

ды, повторяющиеся формулировки. Четвертый - оформление вывода. Если перепутать эти слои, человек начинает писать отчет еще до того, как проверил основу, или наоборот собирает бесконечные мелочи и боится сделать ясный вывод.

В любой проверке я стараюсь отдельно отмечать первичные и вторичные источники. Первичный источник ближе к событию: документ, запись в реестре, исходная публикация, оригинальное видео, страница организации. Вторичный источник пересказывает, объясняет или оценивает. Он может быть полезен, но его нельзя ставить на то же место. Если пять сайтов повторили одну ошибку из шестого, у вас не пять подтверждений. У вас одна ошибка в пяти копиях.

Архивы заслуживают отдельной привычки. Страница, которая сегодня выглядит безобидно, вчера могла содержать другие имена, адреса, цены, партнеров или обещания. Старые версии сайтов часто показывают не тайну, а историю изменений. Но и здесь нельзя делать поспешный вывод. Компания могла переехать, сменить подрядчика, исправить ошибку, убрать устаревшее. Архив помогает задать правильный вопрос, а не всегда дает окончательный ответ.

Надежность источника не равна официальности. Официальный пресс-релиз может умолчать о важном. А маленький форум иногда первым показывает проблему, которую потом подтвердят документы. Разница в том, как вы используете находку. Форум может дать направление. Документ может подтвердить факт. Свидетельство очевидца может дать де-

таль. Сводный отчет может дать контекст. Когда каждый источник стоит на своем месте, картина становится крепче.

Нельзя забывать о языке. Один и тот же объект может называться по-разному на русском, английском, местном языке, в транслитерации, в сокращении, в старом написании. Иногда весь поиск ломается из-за одной буквы. Поэтому в начале проверки стоит выписать варианты имен, доменов, адресов, брендов, юридических форм. Это не бюрократия. Это способ не пройти мимо нужного документа только потому, что он написан иначе.

Еще одна рабочая привычка - не доверять интерфейсу. Поиск в социальной сети, выдача поисковика, фильтры на сайте реестра, подсказки платформы - все это не нейтральные окна в реальность. Они сортируют, скрывают, персонализируют, ошибаются, зависят от языка и региона. Если результат важен, проверьте его другим путем: другим поиском, другой датой, другим языком, прямым запросом к источнику, архивной копией.

В конце каждой стадии полезно писать короткий промежуточный вывод, даже если он кажется очевидным. Например: 'На этом этапе подтверждено только существование компании и домена, связь с указанным человеком не доказана'. Такая фраза удерживает от незаметного скачка. Через час вы можете уже говорить так, будто связь установлена, хотя она была только гипотезой. Промежуточные выводы возвращают на землю.

OSINT часто привлекает людей возможностью найти скрытое в открытом. Но зрелая работа часто заключается в обратном: не брать лишнее, не делать лишний шаг, не превращать случайную личную деталь в аргумент. Сильный специалист отличается не тем, что умеет открыть сто источников. Он умеет закрыть девяносто из них и объяснить, почему оставил десять.

Поэтому первая глава заканчивается не техникой, а настроем. Работайте спокойно. Не соревнуйтесь с источником. Не пытайтесь победить интернет. Сформулируйте вопрос, проверьте путь, сохраните след, отделите факт от версии, уважайте границы. Тогда открытые данные перестают быть шумом и становятся материалом, с которым можно принимать решения без лишнего драматизма и без самообмана.

Есть простой тест качества. Попробуйте пересказать свой вывод человеку, который не видел ваших материалов. Если вы начинаете говорить: 'ну там много всего' и не можете назвать три главных основания, значит, вывод еще сырой. Если можете спокойно назвать источник, подтверждение и слабое место, работа уже похожа на работу. OSINT ценен не объемом найденного, а ясностью, которую он приносит после проверки.

Другой тест касается вреда. Перед тем как включить персональную деталь в заметки или отчет, спросите себя: без этого задача развалится? Если нет, лучше не включать. Адрес, родственники, личные фотографии, старые обиды, слу-

чайные высказывания часто создают ощущение глубины, но на деле засоряют анализ и повышают риск. Чем меньше лишнего вы храните, тем легче защищать результат и себя.

Наконец, не стоит стыдиться простых источников. Иногда лучший ответ лежит не в темном форуме и не в сложной базе, а в старом пресс-релизе, странице закупки, PDF-файле на сайте ведомства или подписи к фотографии. Новички часто перескакивают через очевидное, потому что оно кажется недостаточно эффектным. Опытный человек сначала проверяет очевидное. Там часто и находится то, что нужно.

Такой подход может показаться медленным. На самом деле он быстрее. Ошибка, сделанная в начале, потом тянет за собой десятки лишних проверок. Неподписанный скриншот приходится искать заново. Непроверенная связь попадает в отчет и возвращается вопросами. Нечеткая цель раздувает задачу. Аккуратность в первые полчаса экономит день работы, а иногда и избавляет от неприятного разговора с теми, кто будет принимать решение по вашим материалам.

Главное правило остается прежним: источник, проверка, запись, граница. Повторите этот круг столько раз, сколько требует задача, и не добавляйте ничего ради впечатления. Тогда работа с открытыми данными остается трезвой, полезной и безопасной.

Главное правило остается прежним: источник, проверка, запись, граница. Повторите этот круг столько раз, сколько требует задача, и не добавляйте ничего ради впечатления.

Тогда работа с открытыми данными остается трезвой, полезной и безопасной.

Главное правило остается прежним: источник, проверка, запись, граница. Повторите этот круг столько раз, сколько требует задача, и не добавляйте ничего ради впечатления. Тогда работа с открытыми данными остается трезвой, полезной и безопасной.

Главное правило остается прежним: источник, проверка, запись, граница. Повторите этот круг столько раз, сколько требует задача, и не добавляйте ничего ради впечатления. Тогда работа с открытыми данными остается трезвой, полезной и безопасной.

Главное правило остается прежним: источник, проверка, запись, граница. Повторите этот круг столько раз, сколько требует задача, и не добавляйте ничего ради впечатления. Тогда работа с открытыми данными остается трезвой, полезной и безопасной.

Главное правило остается прежним: источник, проверка, запись, граница. Повторите этот круг столько раз, сколько требует задача, и не добавляйте ничего ради впечатления. Тогда работа с открытыми данными остается трезвой, полезной и безопасной.

Глава 2. Мастерская для разведки из открытых источников

У многих людей первое знакомство с OSINT начинается с красивой картинки. На ней обычно десятки сервисов, стрелки, карты связей, поисковые панели, какие-то темные интерфейсы. Смотришь на это и думаешь: вот оно, настоящая работа. Надо поставить побольше инструментов, завести десять аккаунтов, открыть пять браузеров и сразу станешь человеком, который умеет находить скрытое.

На практике всё проще и неприятнее. Инструменты сами по себе почти ничего не решают. Они похожи на ящики в гараже. Можно купить отличный набор ключей, но если человек не понимает, что именно он пытается открутить, он будет только шуметь железом. В OSINT такая ошибка встречается постоянно. Новичок собирает программы, расширения, ссылки на сайты, списки операторов поиска, а потом тонет в собственном наборе. Вроде всё есть, но работа не идёт.

Я отношусь к рабочей среде как к мастерской. В ней должно быть достаточно всего, чтобы не бегать за каждой мелочью, но не настолько много, чтобы спотыкаться о вещи. Стол нужен чистый. Инструменты должны лежать там, где рука их помнит. Бумаги должны быть подписаны. Опасные предметы должны быть отдельно. И если на столе появился неиз-

вестный файл, его не надо сразу открывать на основной машине, как будто это открытка от старого друга.

Вторая глава этой книги как раз об этом. Не о магии программ и не о списке модных названий. О том, как подготовить место, где можно спокойно собирать данные, проверять версии, хранить заметки, не подставлять себя и не превращать расследование в беспорядок.

Начинать приходится с операционной системы. Это звучит скучно, но от этого зависит слишком многое. Рабочая среда задаёт привычки. Она решает, насколько легко установить нужный инструмент, насколько удобно разделять проекты, насколько быстро можно восстановиться после ошибки. В обычной жизни человек может работать на чём угодно. Для переписки, документов и браузера хватит любой современной системы. Но расследование из открытых источников требует чуть больше контроля.

Linux поэтому так часто появляется в разговорах про OSINT. Не потому, что он делает человека умнее. Не потому, что черное окно терминала само по себе прибавляет опыта. Просто Linux даёт больше свободы и меньше лишних слоёв между человеком и системой. Он позволяет собрать окружение под конкретную задачу, поставить нужные пакеты, быстро автоматизировать повторяющиеся действия, посмотреть, что происходит в сети, и не зависеть от чужого интерфейса там, где нужно точное действие.

Есть ещё одна причина. Большая часть открытых инстру-

ментов для разведки, сетевого анализа, проверки доменов, работы с метаданными и автоматизации исторически хорошо живёт именно в Linux. Многие программы можно запустить и на Windows, и на macOS, но инструкции, зависимости, примеры и советы чаще пишутся с расчётом на Linux. Когда инструмент ломается, это заметно. В Windows человек иногда тратит вечер не на расследование, а на борьбу с путями, библиотеками и странными ошибками установки.

Но отсюда не следует, что Windows плоха, а macOS бесполезна. Такой подход только мешает. Windows удобна тем, что знакома большинству людей и поддерживает массу коммерческих программ. Многие корпоративные расследования ведутся именно там, потому что в компании уже есть политики безопасности, офисные приложения, доступы, почта и согласованные средства защиты. Если следователь работает внутри организации, ему не всегда можно просто поставить любимый дистрибутив и делать вид, что политика отдела безопасности его не касается.

macOS тоже может быть хорошей рабочей площадкой. Внутри у неё Unix-подобная основа, многие инструменты ставятся через пакетные менеджеры, терминал нормальный, стабильность высокая. Ограничения есть, но для человека, который умеет разделять задачи и не пытается всё делать на одной машине, macOS вполне подходит.

Поэтому вопрос не в том, какая система самая правильная. Вопрос в том, где вы можете контролировать работу.

Контроль в OSINT важнее вкуса. Если система удобна, но вы не понимаете, где хранятся файлы, как отключить синхронизацию, какие расширения видят ваши страницы и что уходит в облако, среда уже не ваша. Она просто кажется вашей.

Я бы начинал с простой схемы. Основная машина остаётся для обычной жизни: почта, документы, рабочие дела, личные аккаунты. Для расследований создаётся отдельная среда. Чаще всего это виртуальная машина. В ней можно поставить Linux, настроить браузеры, VPN, инструменты для сбора данных, папки проектов и правила хранения. Если что-то пошло не так, виртуальную машину можно выключить, откатить к снимку или удалить. Это не абсолютная защита, но она убирает массу глупых рисков.

Виртуальная машина хороша тем, что приучает думать границами. Вот здесь личная жизнь. Вот здесь рабочий поиск. Вот здесь тестовый браузер. Вот здесь папка с файлами конкретного проекта. Пока границы видны, меньше шансов случайно войти в личный аккаунт, открыть подозрительный сайт с основного профиля или перемешать данные разных расследований.

Для виртуализации обычно хватает VirtualBox или VMware. Не надо делать из выбора религию. Важнее настроить среду так, чтобы она была удобной и безопасной. Выделить достаточно памяти, но не отдавать всё железо. Создать отдельный диск для данных. Настроить сеть так, чтобы понимать, через что идёт трафик. Отключить лишний общий

буфер обмена и общие папки, если они не нужны. Эти мелочи кажутся занудством ровно до первого случая, когда вредный файл или случайная ссылка прыгает из гостевой системы в основную.

Снимки состояния виртуальной машины заслуживают отдельного разговора. Это одна из тех функций, которые люди недооценивают, пока не потеряют день. Перед установкой нового инструмента сделали снимок. Перед заходом на сомнительный ресурс сделали снимок. Перед экспериментом с настройками сети сделали снимок. Потом сломали систему, посмотрели на результат, откатились. Никакой драмы. В расследовании и так хватает неопределённости, не надо добавлять её там, где можно нажать одну кнопку заранее.

Но виртуальная машина не отменяет здравый смысл. Если внутри неё вы храните важные материалы без шифрования, работаете под одним и тем же аккаунтом на всех сервисах, скачиваете файлы из непонятных мест и открываете их как обычные документы, изоляция быстро превращается в декорацию. Среда должна помогать дисциплине, а не заменять её.

Следующий слой мастерской - сеть. OSINT связан с посещением сайтов, поиском по публичным базам, просмотром профилей, чтением форумов, проверкой доменов, иногда с мониторингом неприятных площадок. В каждом таком действии остаются следы. IP-адрес, cookies, отпечаток браузера, время запросов, язык системы, расширения, разрешение

экрана, история переходов. Часть следов видит сайт, часть провайдер, часть сервисы аналитики. Не всегда это опасно, но всегда лучше знать, что именно вы раскрываете.

VPN часто называют первым средством защиты. С этим можно согласиться, если не делать из VPN волшебный плащ. Он шифрует трафик до своего сервера и скрывает ваш реальный IP от посещаемых сайтов. Это полезно. Но провайдер VPN сам становится участником цепочки. Он может видеть многое, если сервис устроен плохо или ведёт журналы. Поэтому бесплатные VPN для серьёзной работы годятся плохо. Они часто зарабатывают на данных пользователей или экономят на безопасности. Экономия здесь странная: человек прячет следы с помощью сервиса, который сам может торговать этими следами.

Платный VPN тоже надо выбирать не по рекламе. Нужны понятная политика журналов, нормальная репутация, поддержка нужных протоколов, возможность быстро менять серверы, защита от утечек DNS, аварийное отключение соединения при обрыве. И всё равно полезно проверять, какой IP виден наружу, не утекает ли DNS, не раскрывается ли WebRTC в браузере. Такие проверки занимают минуты, но экономят много неприятных объяснений.

Tor нужен для другой задачи. Он проводит соединение через цепочку узлов и усложняет привязку активности к исходному адресу. Для доступа к onion-ресурсам он незаменим. Для обычного веба его тоже можно использовать, но надо

помнить про ограничения. Tor может быть медленным, часть сайтов его блокирует, а вход в личные аккаунты через Tor способен сам по себе привлечь внимание систем безопасности. Плюс Tor не спасает от ошибок человека. Если вы зашли в личную почту, написали со своего аккаунта или скачали файл и открыли его вне защищённой среды, цепочка узлов уже не поможет.

Прокси решают более узкие задачи. Они могут менять видимый адрес, помогать проверять региональную выдачу, снижать риск блокировки при аккуратном сборе публичных данных. Но прокси бывают разными, и слепо доверять им нельзя. Плохой прокси легко превращается в лишнего свидетеля ваших действий. А массовый сбор через прокси может нарушить правила площадки и закон. Если расследование требует автоматизации, сначала надо понять правовые границы и только потом писать скрипт.

Вообще автоматизация в OSINT опасна именно тем, что кажется нейтральной. Один запрос руками выглядит безобидно. Тысяча запросов за минуту уже похожа на атаку или незаконный сбор. Скрипт не думает о последствиях. Он делает то, что вы ему сказали. Поэтому автоматизацию надо начинать не с кода, а с вопроса: зачем мне эти данные, имею ли я право их собирать, как я буду хранить результат, что произойдёт, если там окажутся персональные сведения, которые мне не нужны.

Теперь об инструментах. Вокруг OSINT их столько, что

можно составить каталог толщиной с отдельную книгу. Но рабочий набор обычно скромнее. Нужны средства для поиска людей, доменов, адресов, документов, утечек, связей, изображений, социальных сетей, карт, метаданных и заметок. Всё сразу не освоить. И не надо.

Хороший инструмент отвечает на конкретный вопрос. Maltego помогает увидеть связи между сущностями: доменами, адресами, компаниями, людьми, аккаунтами. TheHarvester собирает почтовые адреса, домены и другие открытые сведения вокруг организации. SpiderFoot автоматизирует разведку по цели и подтягивает данные из разных источников. Recon-ng удобен как модульная среда для веб-разведки. Shodan и Censys показывают устройства и сервисы, доступные из интернета. FOCA полезна при работе с документами и метаданными. У каждого из этих инструментов есть место, но ни один не обязан быть включён в каждое расследование.

Самая частая ошибка - открыть автоматический сканер слишком рано. Человек ещё не сформулировал цель, не записал исходные данные, не понял контекст, но уже запускает сбор. На выходе получает длинный отчёт. В нём много строк, ссылок, адресов, технических деталей. Часть правдива, часть устарела, часть относится к однофамильцам или чужим доменам. Потом начинается имитация анализа: человек читает результат и пытается придумать, что он значит.

Работать лучше наоборот. Сначала вопрос. Потом гипо-

теза. Потом источник. Потом инструмент. Например: нужно понять, какие домены связаны с компанией. Тогда уместны WHOIS, DNS, сертификаты, архивы, корпоративные сайты, поисковая выдача, Shodan или Censys. Нужно проверить публичный образ руководителя. Тогда важнее новости, судебные базы, соцсети, выступления, корпоративные реестры. Нужны следы утечки. Тогда смотрим публичные индексы, форумы, упоминания домена, мониторинг даркнета, но без покупки украденных данных и без участия в преступной среде.

Инструмент должен входить в работу как ответ на потребность. Тогда он помогает. Если он входит как игрушка, он создаёт шум.

Отдельно стоит сказать о социальных сетях. Многие думают, что OSINT там сводится к поиску профиля. Нашёл страницу, посмотрел фотографии, записал пару фактов. На деле социальная сеть ценна связями, временем, реакциями, языком, повторяющимися привычками. Кто кого отмечает. Кто появляется рядом на фотографиях. Какие места повторяются. Какие публикации исчезли. Какие темы вызывают активность. Но социальные сети быстро меняются, закрывают старые функции, режут поиск, прячут данные, требуют входа. Поэтому платформа для мониторинга не заменяет наблюдательность.

TweetDeck, аналоги мониторинга упоминаний, сервисы для отслеживания хэштегов и публичных обсуждений могут

быть полезны. Но они показывают только то, что могут достать. Не надо принимать их выдачу за полную картину. Если сервис не нашёл упоминаний, это не значит, что их нет. Если показал всплеск активности, это не значит, что всплеск естественный. Нужно смотреть источники, проверять время, сравнивать площадки, искать первичный пост, отделять живых людей от сетки аккаунтов.

Для работы с сетями связей полезны графовые инструменты. Они красиво рисуют узлы и линии. Но здесь есть ловушка. Красивая схема убеждает сильнее, чем заслуживает. На экране видно плотное облако, крупные узлы, цветные группы, и мозг сам начинает верить, что перед ним доказательство. На самом деле граф - это только способ посмотреть на данные. Если данные плохие, граф будет красивым мусором. Если связи не проверены, линии ничего не доказывают. Если критерии построения непонятны, схема может обмануть даже автора.

Поэтому я люблю простое правило: любой визуальный вывод должен быть возвращаем к исходнику. Увидели связь между двумя аккаунтами - покажите, на чём она держится. Совместная фотография? Взаимные комментарии? Один номер телефона? Один домен? Один адрес регистрации? Одно совпадение может быть случайностью. Два уже интереснее. Три и больше дают повод продолжать, но всё равно требуют проверки.

Метаданные - ещё один участок, где инструменты дают

сильный результат, если пользоваться ими аккуратно. Документы, изображения, презентации, таблицы иногда несут в себе больше, чем видно на странице. Имя автора файла, путь на компьютере, версия программы, дата создания, дата изменения, координаты снимка, модель устройства. В корпоративной проверке такой след может показать, кто готовил документ. В расследовании фотографии - где и когда она могла быть сделана. В анализе утечки - из какой среды файл вышел наружу.

Но метаданные легко потерять. Достаточно переслать файл через мессенджер, скачать копию с сайта, открыть и сохранить заново. Поэтому исходники надо хранить отдельно. Любые копии для анализа должны быть копиями. Хорошая привычка: получил файл, сохранил оригинал в папку с исходниками, посчитал контрольную сумму, сделал рабочую копию и уже с ней экспериментируешь. Это звучит как работа криминалиста, но на самом деле это обычная аккуратность. Когда через неделю вас спросят, откуда взялась дата в отчёте, будет неприятно отвечать: кажется, она была в файле, но я его уже пересохранил.

Заметки в OSINT важнее, чем набор программ. Без заметок расследование превращается в прогулку по ссылкам. Сегодня вы нашли интересный профиль. Завтра не помните, почему он показался интересным. Послезавтра у вас двадцать вкладок, три скриншота, пять одинаковых имён и раздражение. Нормальная запись должна отвечать на простые

вопросы: что найдено, где найдено, когда найдено, почему это имеет значение, насколько источник надёжен, что надо проверить дальше.

Можно использовать Evernote, OneNote, Obsidian, Joplin, Hunchly, простые Markdown-файлы или корпоративную систему заметок. Не название решает дело. Решает дисциплина. Запись должна быть понятна человеку, который откроет её через месяц. Ссылка без пояснения почти бесполезна. Скриншот без даты слаб. Вывод без источника опасен. Хорошая заметка не обязана быть красивой, но должна быть проверяемой.

Hunchly полезен тем, что автоматически сохраняет посещённые страницы и создаёт след просмотра. Это удобно, когда материалы могут исчезнуть или измениться. Obsidian хорош для связей между заметками: один профиль связан с доменом, домен с компанией, компания с судебным делом, судебное дело с адресом. Joplin привлекает тех, кому нужны локальное хранение и шифрование. OneNote удобен в командах, где все и так работают в экосистеме Microsoft. Но любой инструмент надо настроить под процесс, иначе он станет ещё одной папкой, где всё потерялось.

Я предпочитаю начинать проект с простой структуры. Папка проекта. Внутри исходные данные, рабочие копии, заметки, скриншоты, экспорт инструментов, черновики отчёта. Имена файлов должны быть скучными и понятными: дата, источник, краткое описание. Никаких финал, финал2,

новый_финал, точно_финал. Такая комедия смешна только до момента, когда нужно поднять цепочку доказательств.

Для скриншотов важны дата и контекст. Сам скриншот страницы без адреса и времени слабее, чем кажется. Лучше сохранять URL, время доступа, локальную копию страницы, если это допустимо, и краткую заметку, почему снимок сделан. Если материал может быть использован в юридическом или корпоративном процессе, требования к фиксации становятся жёстче. Тут уже нужно согласовывать метод с юристами или внутренними правилами.

Ещё одна часть мастерской - браузеры и профили. Для OSINT нельзя жить в одном браузере со всеми личными расширениями, сохранёнными паролями, историей и cookies. Это как идти на встречу под прикрытием в куртке с бейджем своей компании. Нужны отдельные профили. Один для обычного поиска. Один для работы с социальными сетями. Один для тестовых задач. В каждом минимум расширений. Чем больше расширений, тем шире поверхность утечки и тем уникальнее отпечаток браузера.

Расширения стоит ставить только тогда, когда понятно, зачем они нужны. Менеджер скриншотов, инструмент для проверки ссылок, просмотр метаданных, переводчик, контейнеры профилей, блокировщик трекеров. Всё это может пригодиться. Но каждое расширение получает доступ к части вашей активности. Некоторые видят все посещаемые страницы. Некоторые могут читать и менять содержимое

сайтов. В обычной жизни люди нажимают установить, не читая разрешений. В OSINT это плохая привычка.

Пароли и учётные записи тоже надо отделять. Для рабочих задач нужен менеджер паролей. KeePassXC, Bitwarden или другой надёжный вариант. Главное - уникальные пароли, двухфакторная защита, резервные коды в безопасном месте. Если используются служебные аккаунты для мониторинга публичных источников, они должны быть оформлены по правилам организации. Самодельные легенды, поддельные личности и заходы в закрытые сообщества без разрешения быстро выводят работу из открытых источников туда, где начинаются юридические проблемы.

Во многих расследованиях достаточно вообще не взаимодействовать с объектом. Смотреть открытые материалы, сохранять ссылки, проверять архивы, читать публичные документы. Как только вы пишете человеку, добавляетесь в друзья, вступаете в закрытую группу, соглашаетесь с правилами площадки от имени вымышленного лица, ситуация меняется. Иногда такие действия допустимы в рамках закона и полномочий. Иногда нет. В частной работе без юриста и понятного основания лучше не изображать из себя оперативника.

Безопасность данных не заканчивается на сборе. Собранная информация может содержать персональные сведения, коммерческие тайны, адреса, телефоны, семейные связи, данные о здоровье, политические взгляды, следы личной жизни. Если всё это хранится в обычной папке, синхронизи-

руется в личное облако и лежит рядом с отпускными фотографиями, проблема уже создана. Даже если расследование велось честно.

Нужно шифрование. Для дисков, архивов, внешних носителей. VeraCrypt, BitLocker, FileVault, LUKS - вариантов хватает. Нужно понимать, где лежат ключи и резервные копии. Нужно удалять лишнее, когда проект закрыт, если правила хранения не требуют обратного. Нужно ограничивать доступ: не каждый участник команды должен видеть всё. Чем меньше людей имеют доступ к чувствительным данным, тем меньше риск утечки и случайного вреда.

Резервные копии тоже должны быть шифрованными. Обычная копия на внешний диск без защиты - не резерв, а второй источник риска. Облако удобно, но перед загрузкой туда материалов надо понять, разрешено ли это правилами проекта и законом. Особенно если в данных есть сведения о людях из других юрисдикций. GDPR, CCPA и похожие режимы не исчезают только потому, что файл лежит у вас на ноутбуке.

В рабочей среде полезно иметь чек-лист начала проекта. Он не должен быть длинным. Цель расследования. Правовое основание. Разрешённые источники. Запрещённые действия. Папка проекта создана. Виртуальная машина подготовлена. VPN проверен. Браузерный профиль очищен. Заметки заведены. Метод фиксации источников выбран. Резервное копирование настроено. Такой список кажется бю-

рократией, но он защищает от хаоса.

Чек-лист окончания проекта не менее важен. Данные сохранены в нужном формате. Источники проверены. Лишние копии удалены. Отчёт отделён от черновиков. Доступы закрыты. Снимки виртуальной машины, которые больше не нужны, удалены или заархивированы по правилам. Пароли временных аккаунтов сменены или аккаунты закрыты, если это предусмотрено. Если проект был чувствительным, проводится короткий разбор: что сработало, что мешало, где был риск, что нужно поправить в мастерской до следующего раза.

Хорошая OSINT-среда со временем становится спокойной. В ней нет ощущения, что вы каждый раз начинаете с нуля. Вы открываете проект, знаете, где заметки, где источники, где инструменты, как проверить соединение, как сохранить страницу, как зафиксировать изображение, как вернуться к чистому состоянию. Это не делает расследование лёгким. Оно убирает лишнюю нервную работу.

Именно к этому стоит стремиться. Не к коллекции программ. Не к впечатляющему рабочему столу. Не к списку из сотни ссылок, который приятно показать новичку. Нужна среда, в которой вы меньше ошибаетесь, быстрее проверяете факты и лучше помните, почему сделали тот или иной вывод.

Открытые источники редко дают аккуратную картину сразу. Они дают обрывки. Один домен, одно фото, старую

публикацию, странный комментарий, совпавший адрес, архивную копию страницы, документ с метаданными, профиль с неправильной датой. Мастерская нужна для того, чтобы эти обрывки не рассыпались. Чтобы каждый кусок лежал на своём месте. Чтобы сомнение было записано рядом с находкой. Чтобы вывод можно было разобрать обратно до источников.

Инструменты меняются. Платформы закрывают доступы. Поисковые операторы перестают работать как раньше. Сервисы покупают друг друга, вводят платные тарифы, режут API, удаляют функции, меняют правила. Человек, который привязан только к конкретной программе, каждый раз начинает паниковать. Человек, который понимает процесс, просто ищет новый инструмент под старую задачу.

Поэтому во второй главе я бы оставил одну мысль, без торжественного финала. Соберите себе рабочее место так, чтобы оно выдерживало вашу невнимательность. Потому что ошибки будут. Вы забудете закрыть вкладку, скачаете не тот файл, перепутаете однофамильцев, устанете, поверите красивому графу, потеряете ссылку, зайдёте не с того профиля. Хорошая среда не сделает вас безошибочным. Она хотя бы не даст одной мелкой ошибке испортить всё расследование.

Глава 3. Защита следов

Человек, который впервые берётся за открытые источники, часто думает о поиске. Где найти профиль, как выйти на старую публикацию, каким запросом вытащить забытый документ, как не пропустить связь между доменом и почтовым адресом. Это понятное желание. Поиск даёт быстрый азарт. Вбил имя, увидел результат, пошёл дальше. Кажется, что работа началась.

На практике она началась раньше. В тот момент, когда ты открыл браузер.

Любая разведка по открытым источникам оставляет следы. Иногда грубые и заметные: IP адрес, аккаунт, cookies, история переходов, отпечаток браузера. Иногда мелкие, которые вспоминают только после ошибки: язык системы, часовой пояс, размер окна, привычная раскладка клавиатуры, имя в пути к скачанному файлу, старый логин в автозаполнении. Всё это не выглядит опасным, пока не попадает в чужие руки. А потом выясняется, что расследователь сам стал частью расследования.

Операционная безопасность не делает человека невидимым. Это первое, что надо принять. Невидимость продают рекламные тексты про VPN и приватные браузеры. В реальной работе задача скромнее и полезнее: не давать лишнего, разделять рабочее и личное, заранее понимать, где можно

ошибиться, и не строить расследование на надежде, что никто не заметит.

Я отношусь к OPSEC как к ремню безопасности. Он не гарантирует, что аварии не будет. Он нужен потому, что аварии иногда случаются именно тогда, когда водитель уверен в себе. В OSINT это особенно неприятно, потому что ошибки часто выглядят не как громкий взлом, а как маленькая бытовая небрежность. Открыл ссылку из личного профиля. Скачал файл в основную систему. Ответил с почты, которую когда-то использовал на форуме. Зашёл на сайт без изоляции, а там аналитика, пиксели, сбор отпечатков. Ничего драматичного. Просто через неделю кто-то понимает, кто интересовался темой.

Если говорить честно, большинство провалов начинается не с технической сложности. Они начинаются с лени. Человек знает, что надо работать в отдельной среде, но ему быстрее открыть всё в обычном браузере. Знает, что аккаунты должны быть разделены, но оставляет синхронизацию. Знает, что нельзя смешивать личные файлы и материалы дела, но кладёт всё в одну папку на рабочем столе. Потом приходится объяснять, почему в отчёте оказался путь с фамилией пользователя или почему целевой сайт видел один и тот же браузер в разных контекстах.

Поэтому я начинаю не с инструментов. Инструменты будут потом. Сначала нужна привычка задавать себе простой вопрос: что я сейчас раскрываю?

Когда ты открываешь сайт, ты раскрываешь больше, чем адрес подключения. Сервер может увидеть технические параметры браузера, операционную систему, язык, разрешение экрана, шрифты, заголовки запросов, время обращения, последовательность переходов. Рекламные сети и аналитические скрипты могут связать визит с прежними сессиями. Платформа может заметить, что новый аккаунт ведёт себя странно: только что создан, сразу ищет конкретных людей, быстро переходит по однотипным страницам, не имеет обычной истории поведения. Иногда этого достаточно, чтобы аккаунт заблокировали. Иногда хуже: достаточно, чтобы объект понял, что им интересуются.

В обычной жизни человек не думает об этом. И правильно делает. Нельзя каждый день жить как специалист по следам. Но в расследовании обычные привычки становятся слабым местом. Если задача чувствительная, работа должна идти в отдельной среде. Не в отдельной вкладке, не в режиме инкогнито, а именно в отдельной среде, где нет личных cookies, личных аккаунтов, рабочих переписок, сохранённых паролей и случайных подсказок.

Режим инкогнито любят переоценивать. Он не сохраняет часть локальной истории и после закрытия чистит сессию. На этом его чудеса заканчиваются. Он не скрывает адрес от сайта, не делает браузер одинаковым для всех, не защищает от ошибок человека, не превращает личный компьютер в стерильную лабораторию. Использовать его можно, но пола-

гаться на него как на защиту нельзя.

Более правильный подход состоит в разделении. Есть личная жизнь. Есть рабочие документы. Есть расследовательская среда. Между ними должны быть стены. Не символические, а настоящие: отдельный браузер, отдельный профиль, отдельная виртуальная машина, отдельные учётные записи, отдельная папка для материалов. Чем выше риск, тем толще стены.

Виртуальная машина хороша тем, что она приучает к дисциплине. Ты запускаешь отдельную систему и уже психологически входишь в другой режим. Внутри нет привычных закладок, нет личной почты, нет семейных фотографий, нет банковских вкладок. Там только задача. Закончил этап, сделал снимок состояния или откатился к чистой версии. Если сайт оказался грязным, если файл был подозрительным, если инструмент повёл себя странно, ущерб не расползается по основной машине.

Но виртуальная машина не спасает от глупости. Если в ней войти в личный аккаунт, она перестаёт быть отдельной средой. Если включить общий буфер обмена и таскать туда-сюда куски текста с личными данными, граница дырявая. Если подключить общую папку и складывать туда всё подряд, изоляция становится декоративной. Я видел, как люди аккуратно ставят VM, настраивают VPN, а потом загружают туда документ с именем автора в свойствах файла. Техника была нормальная. Процесс подвёл.

Хороший OPSEC держится на процессе.

Перед началом работы надо понять уровень риска. Не всякая задача требует одинаковой защиты. Проверить публичные реквизиты небольшой компании и исследовать активность преступной группы в закрытых сообществах - разные вещи. Смотреть архив новостей и заходить на сомнительные сайты с вредоносной рекламой - тоже разные вещи. Ошибка многих новичков в том, что они либо защищаются от всего сразу и быстро устают, либо не защищаются вообще. Оба варианта плохие.

Риск надо назвать. Кто может обратить внимание на твою активность? Что он способен увидеть? Что будет, если он поймёт, кто ты? Какие данные нельзя потерять? Какие действия могут нарушить закон, правила платформы или внутренние требования организации? Эти вопросы скучные. Но именно они экономят больше всего сил.

Если расследование простое, достаточно базовой гигиены: отдельный профиль браузера, отключённая синхронизация, аккуратные заметки, проверенные источники, сохранение копий важных страниц, отсутствие личных логинов. Если работа чувствительная, добавляется виртуальная машина, VPN, Tor там, где он уместен, отдельные почтовые ящики, строгая работа с файлами, шифрование, журнал действий. Если риск высокий, нужен отдельный компьютер, одноразовые среды, заранее прописанные правила контакта с источниками и консультация с юристом или ответственным

за безопасность.

Мне не нравится слово «паранойя». Его часто используют, чтобы высмеять осторожность. Но в OSINT осторожность обычно дешевле исправления ошибки. Паранойя начинается там, где человек не может объяснить, от чего защищается. Нормальная OPSEC работа всегда объяснима. Я использую отдельный браузер, потому что не хочу смешивать cookies. Я выключаю общий буфер обмена, потому что не хочу случайно перенести личный текст. Я шифрую архив, потому что в нём есть персональные данные. Я не захожу в личную почту из рабочей VM, потому что это свяжет контексты. Всё просто.

Теперь о VPN.

VPN полезен. Он шифрует трафик до сервера провайдера VPN и показывает внешним сайтам не твой обычный IP адрес, а адрес выбранного сервера. Это снижает прямую привязку к месту и сети, из которой ты работаешь. Для базового уровня это хороший слой защиты.

Но VPN не волшебная шапка. Сайт всё равно видит браузер. Аккаунт всё равно может выдать тебя поведением. Платёж за VPN может быть связан с тобой. Сам провайдер VPN может вести логи, ошибаться, получать запросы от властей, менять правила. Бесплатные VPN особенно неприятны: если сервис не берёт деньги с пользователя, он часто зарабатывает на данных, рекламе или сомнительных партнёрствах. Для расследовательской работы это плохая сделка.

Выбор VPN должен быть спокойным, без веры в красивые обещания. Нужна понятная политика логов, репутация, нормальная юрисдикция, поддержка kill switch, отсутствие утечек DNS, стабильная работа. Перед использованием надо проверить, какой IP виден снаружи, какой DNS используется, не протекает ли WebRTC. Это занимает несколько минут. Лучше потратить их до работы, чем потом гадать, что именно видел сайт.

Иногда VPN мешает. Некоторые платформы подозрительно относятся к известным VPN адресам, чаще требуют проверки, режут функциональность, блокируют регистрацию. В таких случаях приходится выбирать: либо сохранять защиту и мириться с ограничениями, либо менять подход. Плохой вариант - в раздражении выключить VPN посреди сессии и продолжить тем же аккаунтом. Так контекст связывается мгновенно. Если слой защиты меняется, сессия должна начинаться заново, в чистой среде, с пониманием последствий.

Tor нужен для других задач. Он хорошо скрывает источник подключения, пропуская трафик через цепочку узлов. Он незаменим для доступа к onion ресурсам и полезен там, где важно не раскрывать реальный адрес. Но Tor тоже не отменяет дисциплину. Вход в личный аккаунт через Tor всё равно сообщает сервису, кто ты. Скачивание документов и открытие их вне Tor может раскрыть внешний адрес через встроенные обращения. Изменение настроек браузера, установка расширений, нестандартный размер окна делают от-

печаток менее обычным. Чем больше ты «улучшаешь» Tor Browser под себя, тем хуже можешь слиться с общей массой пользователей.

Самая частая ошибка с Tor - относиться к нему как к броне. Человек запускает Tor и начинает делать всё, что раньше боялся. Заходит куда попало, скачивает файлы, открывает документы, регистрирует аккаунты, пишет сообщения. А потом удивляется, что проблема возникла не в сети, а в поведении. Tor защищает маршрут. Он не защищает от самораскрытия.

Прокси тоже надо понимать трезво. Прокси может помочь сменить видимый адрес, обойти географическое ограничение, разделить потоки запросов. Но дешёвые и случайные прокси часто грязные: ими пользовались спамеры, боты, мошенники, и платформы уже относятся к ним как к мусору. Для массового сбора данных прокси могут быть технически удобны, но юридически и этически опасны, особенно если сбор нарушает правила сайта или затрагивает персональные данные. Прокси не делает плохую идею хорошей.

Есть ещё одна тема, о которой редко говорят в красивых инструкциях: правдоподобие поведения.

Платформы видят не только адрес. Они видят ритм. Обычный пользователь не открывает за пять минут сорок профилей подряд, не копирует однотипные блоки, не ищет только сотрудников одной компании, не создаёт аккаунт и сразу идёт в глубину чужой сети. Даже если техническая за-

щита настроена нормально, поведение может кричать: это не обычный человек, это сборщик.

Конец ознакомительного фрагмента.