

КАРМАННЫЕ ТЕХНОЛОГИИ ВЛИЯНИЯ

ПОИСК ЛЮДЕЙ, ПРОВЕРКА ФАКТОВ
И ДРУГИЕ ПРИЕМЫ ЦИФРОВОГО
РАССЛЕДОВАНИЯ



В-01 [ИНФОРМАЦИЯ
РЕШАЕТ]



БОМБОРА
ИЗДАТЕЛЬСТВО

Москва

УДК 004.9
ББК 32.973.202
О-47

О-47 **OSINT.** Поиск людей, проверка фактов и другие приемы цифрового расследования. — Москва : Эксмо, 2026. — 192 с. — (Карманные технологии влияния).

ISBN 978-5-04-250087-9

Вам не нужно быть хакером, чтобы найти информацию о ком угодно!

OSINT (разведка по открытым источникам) — это не взлом серверов и не зеленые цифры на черном фоне из фильмов про хакеров. Это набор простых и легальных приемов, которые превращают информационный шум в четкую картину мира. И этому может научиться любой, кто умеет пользоваться браузером.

УДК 004.9
ББК 32.973.202

© Бортник В.О., обложка, 2026
© Оформление. ООО «Издательство
«Эксмо», 2026

ISBN 978-5-04-250087-9

Оглавление

Введение	7
----------------	---

Часть I. Точка входа

Глава 1. Что такое OSINT и почему это не просто погуглить	19
--	----

Глава 2. Зачем вам это: как решать рабочие и бытовые задачи с помощью OSINT	31
--	----

Глава 3. Где проходит красная линия: закон и этика.	41
---	----

Часть II. Следы из хлебных крошек

Глава 4. Основы работы с информацией и обзор инструментов OSINT	53
--	----

Глава 5. Социальные сети как золотая жила: что можно узнать из профиля.	64
---	----

Глава 6. Государственные реестры и открытые базы данных.	75
--	----

Глава 7. Архивы интернета: как читать удаленные страницы	87
---	----

Глава 8. Извлечение информации из изображений: метаданные, обратный поиск, геолокация.	99
---	----

Глава 9. Продвинутый поиск: дорки и никнеймы	111
---	-----

Глава 10. Комплексные платформы и автоматизация	123
--	-----

Часть III. Правила следопыта

Глава 11. Критическое мышление и типичные ошибки	135
---	-----

Глава 12. От фактов к выводам: триангуляция и систематизация	145
---	-----

Глава 13. Приватность других людей и цифровая гигиена	157
--	-----

Глава 14. От вопроса до готового отчета: пример мини-расследования	167
---	-----

Глава 15. Что дальше: как развивать навык OSINT самостоятельно	180
---	-----

Введение

«Срочный сбор ребенку на операцию!», «Посмотри это видео до конца!» — как часто вам приходят подобные сообщения? Готов поспорить, минимум пару раз в день. Вы их пролистываете, жмете «переслать» или просто закрываете.

На всякий случай вы никому не доверяете, но иногда все же не можете отделаться от мысли: а вдруг человеку действительно нужно помочь? Но давайте честно: в девяти случаях из десяти у вас нет ни навыков, ни инструментов, чтобы разобраться, что

перед вами — реальная просьба о помощи или чья-то циничная манипуляция.

И это еще цветочки. Где-то в интернете спокойно гуляют ваши старые селфи, которые вы предпочли бы больше никогда не видеть, e-mail десятилетней давности, номер телефона и куча другой информации, о которой вы вспоминаете только, когда звонят «из службы безопасности банка».

Один российский фотограф однажды провел эксперимент: фотографировал случайных людей в метро, а затем за несколько секунд находил их настоящие профили в соцсети — просто по одному снимку и бесплатному приложению. Ни взлома, ни секретных баз данных — только то, что люди сами, добровольно выложили в открытый доступ. Через несколько лет похожий принцип сработал уже в обратную сторону: утечка данных сервиса доставки еды превратилась в интерактивную карту, где любой мог увидеть имя, телефон и точный адрес конкретного человека,

в том числе и адреса реальных знаменитостей. Это не сюжет фильма про хакеров. Это то, что происходит с обычными людьми — то есть с вами — прямо сейчас, пока вы читаете эти строки.

**Мы живем в мире, где
каждый может опубликовать
практически что угодно
и с любыми намерениями:
от искреннего желания
помочь до попытки
выманить у другого человека
последние деньги.**

Информации стало больше, а вот ориентироваться в ней — сложнее: новости противоречат друг другу, мошенники убедительнее настоящих волонтеров, личные данные оказываются в публичном доступе, а мы узнаем об этом порой из мемов. И дело не в том, что пострадавший «сам виноват, потому что не проверил». Нас просто никогда не учили разбираться

в информации и проверять ее. Пора это исправить.

Если вы впервые слышите слово «OSINT» (Open Source Intelligence — разведка по открытым источникам) и представляете хакеров в худи, что-то очень загадочное и не совсем законное, сразу хочу вас успокоить: это не так. И спойлер: в этой книге мы ничего не будем взламывать. Даже холодильник.

OSINT для обычного человека — это прежде всего набор вполне практических навыков, которые можно освоить самостоятельно, даже без специального образования в сфере программирования. В том числе с помощью этой книги. В ваших руках — практическое руководство для обычного человека, который умеет пользоваться интернетом и мессенджерами, чувствует, что «что-то тут не так», когда ему в третий раз за неделю присылают «шокирующее видео», и хочет навести порядок в своей цифровой жизни, перестав быть легкой добычей для фейков и мошенников.

Зачем вам все это?

Во-первых, ради элементарной цифровой гигиены. Чтобы понимать, какие следы вы уже оставили в сети и кто их может увидеть, вовремя закрывать самые очевидные «дыры» — например, открытый профиль с личными данными — и замечать, если кто-то использует ваши фото, имя или e-mail в своих мутных делах. В этом смысле OSINT похож на лампу в темном подвале: он не меняет то, что там происходит, но помогает увидеть, где давно течет труба.

Во-вторых, чтобы вас нельзя было обмануть, играя на эмоциях: вызвать жалость с помощью фальшивого сбора, напугать сенсационной новостью или заманить обещанием «идеальных инвестиций без риска». Когда у вас есть набор простых приемов и привычка сомневаться, вы по-прежнему можете помогать, сопереживать и донатить — только уже осознанно, а не вслепую.

А в-третьих, если вам это интересно, чтобы участвовать в расследованиях и волонтерских проектах. Делать это законно, уважать чужую приватность и не выдавать догадки за факты.

Возможно, сейчас вы лишь смутно представляете, что такое OSINT. Но к последней странице этой книги вы поймете, что это за метод, как им пользоваться, и, главное, будете готовы провести свое собственное первое расследование. Не откладывая его на неопределенное «когда-нибудь»: закроете последнюю страницу — и сможете сразу применить полученные знания на практике.

Чтобы этот путь не превратился в хаотичное блуждание, книга построена как маршрут настоящего следопыта — от первых шагов до самостоятельной охоты за фактами. И, конечно же, здесь будет много практических упражнений.

В первой части мы разберемся, что такое OSINT и чем он отличается от простого

погуглить. Посмотрим, как этот метод помогает решать вполне бытовые (а не только шпионские) и рабочие задачи, и сразу проведем главную границу — что законно и этично, а что уже нет. Это ваша точка отсчета. Без базовых понятий и четких рамок двигаться дальше небезопасно.

Любой человек и любая организация оставляют в интернете цифровой след — множество отдельных фрагментов информации, разбросанных по разным сайтам и сервисам.

Во второй части мы разберемся, где искать эти следы и как связывать их между собой: от профилей в соцсетях и государственных реестров до архивов удаленных страниц, скрытых данных внутри фотографий и продвинутых поисковых приемов. Научимся работать с никнеймами

и использовать инструменты автоматизации, которые ускоряют сбор информации.

Найти информацию — лишь половина задачи. Не менее важно правильно оценить найденное, не потерять нить расследования и не нарушить чужие границы.

В третьей части мы разберем типичные ошибки мышления, которые сбивают с толку даже опытных исследователей, научимся проверять разрозненные находки и превращать их в обоснованные выводы, поговорим о приватности других людей и цифровой гигиене. А затем вместе пройдем через полное мини-расследование — от постановки первого вопроса до составления готового отчета. Последняя глава станет не финалом, а стартовой площадкой: вы узнаете, как дальше развивать навык OSINT самостоятельно, когда книга уже закончится.

От вас не требуется «раскрывать международные заговоры» и доказывать все до последней запятой — пусть этим занимаются профессионалы. Ваша задача как любителя проще: научиться быть внимательнее, осторожнее и чуть лучше защищать себя в мире, где каждый день на нас обрушиваются потоки информации, а оставленный в сети цифровой след продолжает жить собственной жизнью, часто без нашего ведома.

И еще один совет перед тем, как мы начнем: держите под рукой ноутбук или телефон и сразу выполняйте упражнения, которые встретятся по ходу книги. Не откладывайте их на потом — именно практика превращает прочитанное в навык. Иначе книга рискует остаться еще одной «умной книжкой на полке», а вы — по-прежнему жить в мире, где любой «срочный сбор» кажется правдой просто потому, что кому-то не захотелось потратить три минуты на проверку.