12+

Михаил Тарасов

ЦИФРОВОЙ СЛЕД

путеводитель начинающего

КИБЕРДЕТЕКТИВА_

Михаил Тарасов

Цифровой след. Путеводитель начинающего кибердетектива

https://litres.ru/74504374
ISBN 9785007131421

Аннотация

Думаешь, кнопка Delete стирает файлы, а скрытый профиль делает тебя невидимым? «Цифровой след» — это боевой мануал по поиску улик в сети и на дисках. Внутри 72 практических задания: от настройки изолированной лаборатории и OSINT-разведки до чтения метаданных, восстановления стертых документов и анализа сетевых следов. Никакой воды — только реальный софт, соблюдение законов и пошаговые инструкции. Научись видеть то, что пытались скрыть, и стань цифровым охотником.

Содержание

Введение. Добро пожаловать в реальный мир 5
— Кто такой кибердетектив и чем он отличается от хакера (спойлер: один из них спит спокойно) 5
— Главное правило: Не навреди (себе и уликам) 12
— Дисклеймер: Разница между расследованием и ст. 272 УК РФ 19
Часть 1. Подготовка и менталитет (Setup) 26
Глава 1. Лаборатория параноика: готовим рабочее место 26
— Почему нельзя работать с основного компьютера 26
— Виртуальные машины (VM): твой цифровой презерватив 31
— OpSec (Operational Security): как самому не оставить следов, пока ищешь чужие 37
Конец ознакомительного фрагмента. 44

Цифровой след. Путеводитель начинающего кибердетектива

Михаил Тарасов

ISBN 978-5-0071-3142-1
Создано в интеллектуальной издательской системе Ridero

Введение. Добро пожаловать в реальный мир

— Кто такой кибердетектив и чем он отличается от хакера (спойлер: один из них спит спокойно)

Давай сразу расставим точки над «ё». Если ты открыл эту книгу в надежде, что я научу тебя взламывать банковские счета, красть переписки бывших или «наказывать обидчиков в интернете», то можешь закрывать её прямо сейчас. Серьезно. Иди лучше посмотри какой-нибудь боевик про гениального хакера, который за 30 секунд ломает Пентагон, попутно попивая Red Bull. Там красиво, эффектно и совершенно оторвано от реальности.

А мы здесь будем заниматься совсем другим делом. Мы будем учиться **находить правду**. И это, поверь мне, намного круче, чем просто ломать чужие пароли.

Кто же такой кибердетектив?

Кибердетектив (или специалист по цифровой криминалистике, если тебе нравятся длинные названия) — это человек, который занимается поиском, анализом и интерпрета-

цией цифровых следов. Проще говоря, это тот, кто разбирается в том, что осталось **после** события: взлома, утечки данных, мошенничества, кражи информации или даже обычного корпоративного инцидента, когда сотрудник слил коммерческую тайну конкурентам.

Представь себе классического детектива из книжек и фильмов: он приезжает на место преступления, собирает улики — отпечатки пальцев, волокна ткани, свидетельства очевидцев. Он восстанавливает картину произошедшего по кусочкам. Кибердетектив делает абсолютно то же самое, только его «место преступления» — это жесткий диск, сервер, смартфон или облачное хранилище. Его «отпечатки пальцев» — это логи системы, метаданные файлов, история браузера, удаленные (но не до конца) документы.

Кибердетектив работает **после факта**. Он не атакует системы — он их исследует. Он не взламывает пароли (ну, иногда взламывает, но об этом позже) — он восстанавливает данные, которые кто-то пытался уничтожить. Он не крадет информацию — он **доказывает**, кто её украл, когда и как именно это произошло.

И самое главное отличие от хакера: кибердетектив работает **в рамках закона**. Всегда. Без исключений. Потому что если ты нарушил закон в процессе расследования, то все твои доказательства летят в мусорку, а сам ты рискуешь оказаться на скамье подсудимых рядом с тем самым преступником, которого пытался поймать.

А кто такой хакер? (И почему это не комплимент)

Термин «хакер» за последние 20 лет превратился в какое-то мифическое существо. В массовой культуре хакер — это парень в толстовке с капюшоном, который сидит в темной комнате перед тремя мониторами с бегущим зеленым кодом и взламывает NASA, пока ест лапшу быстрого приготовления. Романтика, да?

В реальности всё скучнее и одновременно страшнее. Хакеры делятся на несколько категорий:

White Hat («Белые шляпы) — это этичные хакеры. Они взламывают системы **с разрешения** владельцев, чтобы найти уязвимости и помочь их закрыть. По сути, они делают то же, что и кибердетективы, только с другого конца: не ищут следы взлома, а проверяют, можно ли вообще взломать. Многие из них работают в компаниях на должностях пентестеров (специалистов по тестированию на проникновение) или bug bounty hunters (охотников за багами за вознаграждение).

Black Hat («Черные шляпы) — классические злодеи. Они взламывают системы ради денег, шантажа, кражи данных или просто для собственного удовольствия. Шифровальщики-вымогатели, которые парализуют работу больниц? Чёрные шляпы. Те, кто сливает миллионы паролей на даркнет-форумы? Тоже они. Эти ребята не спят спокойно не потому, что их мучает совесть (её у них нет), а потому что за ними охотятся правоохранительные органы со всего мира.

Gray Hat («Серые шляпы) — пограничный случай. Они могут взломать систему без разрешения, но не с целью навредить, а чтобы, например, показать компании её уязвимость (иногда требуя за это вознаграждение). Формально это незаконно, но мотивы у них не всегда злонамеренные. Впрочем, перед законом это не оправдание.

Так вот, главное отличие кибердетектива от любого типа хакера: **кибердетектив не нападает, он расследует** . Он не ищет дыры в системе, чтобы пролезть внутрь — он анализирует то, что осталось после того, как кто-то уже пролез.

Почему один спит спокойно, а другой — нет?

Помнишь спойлер из заголовка? Так вот, кибердетектив спит спокойно. Он знает, что его работа законна, что он помогает людям и организациям защитить себя, наказать виновных и предотвратить будущие инциденты. Его навыки востребованы в полиции, корпоративной безопасности, частных детективных агентствах, IT-компаниях и даже в судебной системе в качестве эксперта.

Хакер (за исключением белых шляп) живет в постоянном напряжении. Его может вычислить конкурирующая группировка, он может попасться на ошибке в OpSec (операционной безопасности), его могут сдать сообщники или просто подставить более опытные коллеги. А уж если за ним всерьез возьмутся спецслужбы или Интерпол — вопрос времени, когда его найдут. История киберпреступности полна примеров «непобедимых гениев», которые в итоге получили реальные

сроки: создатель Silk Road (даркнет-маркетплейса) — пожизненное заключение, участники группы Lapsus$ — арестованы, операторы ботнета Emotet — ликвидированы международной операцией.

А теперь представь: ты потратил годы на оттачивание навыков, рисковал свободой, заработал деньги (возможно, немалые), но не можешь спокойно их потратить, потому что любая крупная покупка привлечет внимание. Ты не можешь похвастаться своими достижениями в резюме, не можешь рассказать о них друзьям. И всё это время тебя могут отследить по одной-единственной ошибке: забыл выключить сервис на три буквы, использовал старый никнейм, оставил метаданные в файле.

Кибердетектив же не только спит спокойно — он ещё и может официально гордиться своей работой. Раскрыл дело о взломе? Отлично, вот тебе премия и уважение коллег. Помог вернуть украденные данные компании? Вот рекомендательное письмо и повышение зарплаты. Ты на светлой стороне, и это чертовски приятно.

Что общего у кибердетектива и хакера?

Несмотря на разницу в целях и методах, у них есть общие черты. Обоим нужны:

Технические знания. Ты должен понимать, как работают операционные системы, сети, базы данных, криптография. Ты должен уметь читать логи, разбираться в структуре файловых систем, знать основы программирования.

Любопытство и настойчивость. Расследование — это не спринт, это марафон. Иногда приходится копаться в гигабайтах данных, чтобы найти одну-единственную зацепку. Ты должен быть готов потратить часы, дни, недели на поиск ответа.

Критическое мышление. Умение задавать правильные вопросы: «Почему этот файл был создан именно в это время?», «Откуда взялся этот IP-адрес?», «Кто мог иметь доступ к этой системе?». Ты как следователь в детективе: собираешь факты, строишь гипотезы, проверяешь их.

Но вот чем они **категорически** отличаются — это этикой и законностью. Хакер может использовать свои навыки для атаки. Кибердетектив использует их исключительно для защиты и расследования.

Зачем вообще становиться кибердетективом?

Хороший вопрос. Если ты дочитал до этого места и ещё не закрыл книгу, значит, тебя действительно интересует эта тема. Вот несколько причин, почему это крутая профессия:

Востребованность. Киберпреступность растёт экспоненциально. Каждый день происходят тысячи инцидентов: утечки данных, взломы корпоративных сетей, мошенничество, кибершпионаж. Компании и государства отчаянно нуждаются в специалистах, которые могут разобраться, что произошло, кто виноват и как это предотвратить в будущем.

Разнообразие задач. Никакой рутины. Сегодня ты расследуешь утечку базы клиентов интернет-магазина, завтра

— ищешь доказательства корпоративного саботажа, послезавтра — помогаешь полиции найти педофила по метаданным фотографий. Каждый кейс уникален.

Интеллектуальный вызов. Это работа для тех, кому нравится решать головоломки. Ты — цифровой Шерлок Холмс, и каждое расследование — это новая загадка.

Легальность и моральное удовлетворение. Ты на стороне добра. Ты помогаешь жертвам, наказываешь преступников, делаешь мир чуть безопаснее. И тебя за это ещё и платят.

Что дальше?

Эта книга — твой первый шаг в мир цифровой криминалистики. Я не обещаю, что будет легко. Ты столкнешься с техническими терминами, непонятными командами, ошибками и тупиками. Но если ты готов учиться, экспериментировать и не сдаваться — добро пожаловать в реальный мир. Мир, где логи не врут, удалённые файлы можно восстановить, а самое слабое звено в любой системе безопасности — это человек.

Готов начать? Тогда переворачивай страницу. У нас впереди много работы.

— Главное правило: Не навреди (себе и уликам)

Прежде чем ты наденешь метафорический плащ детектива и начнешь сканировать порты соседа или восстанавливать удалённую переписку своей девушки (кстати, не делай этого, если не хочешь получить статьей по лицу), нам нужно поговорить о фундаменте. О том, что отличает профессионала от обезьяны с гранатой.

В медицине есть принцип *Primum non nocere* — «Не навреди». В цифровой криминалистике этот принцип возведен в абсолют, умножен на паранойю и закреплен уголовным кодексом. И работает он в две стороны: ты не должен навредить **себе** (своей свободе, репутации, безопасности) и ты не должен навредить **уликам** (потому что испорченная улика — это подарок адвокату преступника).

Давай разберем оба аспекта, потому что ошибка в любом из них будет стоить тебе карьеры еще до того, как она начнется.

Часть 1. Не навреди уликам (Или почему нельзя просто включить компьютер)

Представь ситуацию: ты приходишь на место преступления в реальной жизни. На полу лежит пистолет. Что сделает дилетант? Поднимет его, покрутит в руках, может быть, даже нажмет на курок, чтобы проверить, заряжен ли он. Что сде-

лает профи? Оцепит территорию, наденет перчатки, сфотографирует всё с десяти ракурсов и только потом, специальным инструментом, поместит улику в пакет.

В цифровом мире всё то же самое, только хуже. Потому что «цифровой пистолет» (жесткий диск, флешка, смартфон) меняется просто от того, что ты на него *посмотрел*.

Почему включение компьютера — это преступление против форензики?

Новички часто думают: «Ну, я просто включу комп, посмотрю, что там на рабочем столе, и выключу».

НЕТ.

В тот момент, когда ты нажимаешь кнопку питания, операционная система начинает жить своей жизнью.

— Изменяются метаданные. Система обновляет время последнего доступа к тысячам файлов. Ты только что затоптал следы преступника своими грязными ботинками.

— Записываются логи. Windows (или macOS, или Linux) запишет событие включения, запуска служб, подключения устройств. Это новый «шум», который перекроет старые записи.

— Работают фоновые процессы. Антивирус может удалить вредоносный файл, который был главной уликой. Индексатор поиска может перезаписать удаленные сектора диска, где лежали стертые фото.

— Триггеры самоуничтожения. Продвинутые злодеи могут поставить скрипт: «Если компьютер включен не с то-

го USB-порта или без ввода пароля за 30 секунд — удалить ключи шифрования». Поздравляю, ты только что превратил доказательства в бесполезный цифровой мусор.

Золотое правило форензики: Работай с копией, никогда с оригиналом

Профессионал никогда не анализирует «живую» систему, если есть возможность сделать её копию.

Процесс выглядит так:

— Блокировка записи. Ты подключаешь диск подозреваемого через специальное устройство — блокиратор записи (Write Blocker). Это такая «железка», которая физически не дает твоему компьютеру записать на диск ни одного байта.

— Создание образа (Imaging). Ты делаешь побитовую копию диска. Не просто копируешь файлы Ctrl+C -> Ctrl+V, а снимаешь полный слепок, включая пустое пространство, удаленные файлы и служебные области.

— Хеширование. Ты считаешь контрольную сумму (цифровой отпечаток) оригинала и копии. Если они совпадают до последнего знака — поздравляю, копия верна.

— Анализ. И вот теперь, с копией, ты можешь делать что угодно. Хоть вирус запускать, хоть файлы восстанавливать. Оригинал лежит в сейфе, нетронутый и девственно чистый.

Если ты работаешь «по-живому» (например, система не выключена, и выключать её нельзя из-за шифрования), ты должен документировать каждый свой чих. Каждую введенную команду. Каждое движение мыши. Потому что в суде

(или в отчете заказчику) тебя спросят: «А этот файл изменил хакер или вы, когда искали улики?». И если ты не сможешь доказать, что это не ты — дело развалится.

Часть 2. Не навреди себе (Или как не сесть за любопытство)

Теперь поговорим о твоей шкуре. Цифровая криминалистика и OSINT (разведка по открытым источникам) — это минное поле. Граница между «я просто посмотрел» и «неправомерный доступ к компьютерной информации» (ст. 272 УК РФ) тоньше, чем кажется.

Синдром Бога и статья 138

Когда ты освоишь первые инструменты, у тебя появится чувство всемогущества. Ты узнаешь, как найти соцсети человека по почте, как вытащить метаданные из фото, как пробить IP. И велик соблазн применить это не там, где надо.

Запомни:

— **OSINT — это легально**, пока ты используешь *открытые* данные. Если профиль закрыт, а ты подбираешь пароль — это взлом.

— **Пробив — это незаконно.** Покупка данных из закрытых баз (банковских, операторов связи, государственных реестров) в даркнете или у «знакомого мента» — это уголовка. Если ты в своем отчете напишешь «Я пробил номер через Глаз Бога и узнал прописку», ты сам себе подписал приговор. Ты стал соучастником преступления (нарушение тайны переписки, частной жизни и т.д.).

— **Активный скан — это атака.** Если ты сканируешь порты чужого сервера без письменного разрешения владельца, это может быть расценено как подготовка к атаке или вредоносное воздействие.

Правило «Чистых рук»

Ты должен быть чище, чем те, кого ты ищешь.

— **Лицензионный софт.** Использовать пиратский софт для расследования киберпреступлений — это оксюморон и идиотизм. Твои инструменты должны быть легальными (или Open Source).

— **Разделение сред.** Никогда не веди расследования со своего личного, домашнего компьютера, где ты играешь в «Доту» и хранишь фотки кота. Заведи отдельную машину или, как минимум, виртуальную машину.

— *Почему?* Во-первых, ты можешь случайно подцепить малварь от исследуемого объекта. Во-вторых, если дело дойдет до суда, твой рабочий компьютер могут изъять как вещдок. Ты готов отдать свой личный ноут следователю на полгода? Нет? Тогда используй виртуалку.

— **OpSec (Операционная безопасность).** Если ты исследуешь деятельность хакерской группировки или наркокартеля в даркнете, не делай это с домашнего IP-адреса. Они тоже умеют вычислять людей. Используй сервис на три буквы, Tor, «чистые» сим-карты. Не пали свою личность. Героизм хорош в кино, в жизни лучше оставаться анонимным профессионалом.

Этическая ловушка

Иногда к тебе будут приходить с просьбами: «Взломай ВК моей жены, я заплачу», «Удали этот компромат на меня с сервера», «Узнай, кто пишет гадости, я поеду и разберусь с ним».

Ответ всегда один: **НЕТ**.

Ты — исследователь, а не наёмник и не каратель.

— Если ты взломаешь жену — ты преступник.

— Если ты удалишь данные — ты преступник.

— Если ты дашь адрес обидчика клиенту, и тот проломит ему голову — ты соучастник (или подстрекатель).

Твоя задача — собрать информацию, проанализировать её и предоставить отчет. Что клиент будет делать с этим отчетом — идти в полицию, в суд или к психотерапевту — это уже не твоя зона ответственности. Но ты не должен давать инструменты для совершения преступлений.

Резюме раздела

«Не навреди» в нашей профессии означает:

— **Сохраняй неизменность данных.** Используй блокираторы записи, делай образы, считай хеш-суммы.

— **Документируй каждое действие.** Твой отчет должен быть воспроизводимым: любой другой эксперт, повторив твои шаги, должен получить тот же результат.

— **Знай законы.** Грань между OSINT и пробивом, между анализом и взломом — это твоя линия жизни. Не пересекай её.

— **Соблюдай OpSec.** Защищай свою цифровую личность так же тщательно, как препарируешь чужую.

Если ты усвоил это правило — добро пожаловать дальше. Теперь мы можем начать говорить о том, как искать, а не как садиться. Если же тебе кажется, что «ай, да ладно, никто не узнает» — закрой книгу, удали Kali Linux и иди выращивать цветы. Там безопаснее.

— Дисклеймер: Разница между расследованием и ст. 272 УК РФ

Мы подошли к самой скучной, но, пожалуй, самой важной части этой книги. Если ты пропустишь этот раздел, то есть ненулевая вероятность, что твоя карьера «кибердетектива» закончится не в уютном офисе службы безопасности, а в комнате с решетками на окнах.

Я серьезно.

В мире IT-расследований существует огромная пропасть между тем, что **технически возможно**, и тем, что **юридически допустимо**. Твой компьютер может позволить тебе подобрать пароль к Wi-Fi соседа за пять минут. Твой мозг может подсказать, как зайти на сервер конкурента через забытый открытый порт. Но Уголовный кодекс Российской Федерации (или любой другой страны, где ты находишься) смотрит на это не как на «крутой скилл» или «расследование», а как на преступление.

Давай разберем «большую тройку» статей УК РФ, которые висят дамокловым мечом над любым безопасником, пентестером и кибердетективом.

Статья 272: Неправомерный доступ к компьютерной информации

Это «королева» киберпреступлений. Она гласит, что наказывается **неправомерный доступ**, если это повлекло

уничтожение, блокирование, модификацию либо копирование информации.

— Как это видит новичок: «Я просто зашел посмотреть! Я ничего не ломал, ничего не стирал. Я просто проверил, подходит ли пароль 'admin', увидел админку и вышел. Я же ничего плохого не сделал!»

— Как это видит следователь: Ты осуществил доступ? Да. У тебя было право на этот доступ (договор, разрешение владельца)? Нет, значит, он неправомерный. Ты скопировал информацию? Даже если ты просто открыл страницу в браузере, она подгрузилась в кэш — технически это копирование. Всё, состав преступления готов.

Где проходит граница?

Граница — в слове **«разрешение»**.

— Если у тебя есть подписанный договор на пентест (тестирование на проникновение) или аудит безопасности — ты исследователь.

— Если ты делаешь то же самое без бумажки — ты преступник.

Пример: Твой друг попросил проверить безопасность его сайта.

— *Вариант А (Правильный):* Друг пишет тебе письмо (хотя бы в мессенджере, но лучше на почту): «Прошу провести аудит моего ресурса example.com, разрешаю сканирование и попытки обхода защиты». Ты сохраняешь это письмо как зеницу ока.

— *Вариант Б (Тюремный):* Друг сказал это на шашлыках. Ты полез, уронил сайт (блокирование информации). Друг обиделся и написал заявление. Доказать, что он разрешил, ты не сможешь.

Статья 273: Создание, использование и распространение вредоносных компьютерных программ

Эта статья страшна тем, что под неё можно подвести не только вирусописателей, но и любопытных студентов, скачавших «хакерский софт».

— **Как это видит новичок:** «Я скачал этот скрипт с GitHub, чтобы проверить уязвимость. Это же инструмент для безопасности!»

— **Как это видит суд:** Программа предназначена для несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты? Да. Ты её использовал? Да. Статья 273.

Тонкий лед:

Многие инструменты двойного назначения (Dual-use tools) находятся в серой зоне. Тот же Metasploit, Nmap, Burp Suite — это легальные инструменты администраторов. Но если ты используешь модифицированную версию, специально заточенную под скрытый взлом, или самописный скрипт для брутфорса (подбора паролей) — это уже квалифицируется как вредоносное ПО.

Важно: Хранение само по себе редко наказывается (хотя вопросы будут), но **использование** и **распространение**

(скинул другу ссылку на вирус) — это статья.

Статья 274: Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации

Менее популярная, но коварная статья. Она часто применяется к инсайдерам — сотрудникам, которые имеют легальный доступ, но творят дичь.

— Ситуация: Ты работаешь сисадмином. Решил майнить крипту на серверах компании в нерабочее время. Или отключил логирование, чтобы никто не увидел, как ты качаешь фильмы. Вроде бы ничего не взламывал, доступ у тебя есть.

— Реальность: Ты нарушил правила эксплуатации, что повлекло вред (износ оборудования, тормоза сети). Добро пожаловать под следствие.

Статья 138: Нарушение тайны переписки

Это бич всех мамкиных OSINT-еров, которые решили поиграть в шпионов.

— OSINT (Законно): Найти человека в VK, проанализировать его открытые посты, увидеть, что он лайкает порно-паблики, найти его ник на форуме любителей аниме. Это всё открытые данные. Человек сам выложил их в публичный доступ.

— Статья 138 (Незаконно): Подобрать пароль к его почте. Купить за 500 рублей выписку его звонков или СМС в Telegram-боте. Поставить кейлоггер (перехватчик нажатий

клавиш) на компьютер жены.

— Любое проникновение в *закрытую* переписку, к которой у тебя нет законного доступа — это уголовное преступление. Даже если ты просто прочитал и никому не рассказал.

Манифест легального кибердетектива

Чтобы эта книга стала для тебя учебником, а не протоколом допроса, запомни три аксиомы:

— Активный поиск — только с письменного согласия.

— Ты не имеешь права сканировать, брутфорсить или пытаться «прощупать» чужие сервера, сайты и Wi-Fi сети, если владелец не дал тебе прямого разрешения. Точка. Никаких «я только спросить».

— OSINT ограничивается публичными данными.

— Если для получения информации тебе нужно ввести чужой логин/пароль, обойти защиту, заплатить «пробивщику» или использовать уязвимость — это больше не разведка. Это взлом. Мы работаем с тем, что лежит на поверхности или что можно достать легальными запросами.

— Не знание закона не освобождает от ответственности.

— Фраза банальная, но в IT она критична. Судье плевать, что ты «учился по книге» или «хотел помочь найти уязвимость». Есть факт доступа, есть отсутствие полномочий — будет приговор.

«Но как же багхантеры?»

Ты спросишь: «А как же ребята, которые ищут баги за деньги на Bug Bounty платформах? Они же взламывают!»

Они работают в рамках **оферты**. Регистрируясь на платформе (HackerOne, Bugcrowd, Standoff365 и т.д.), они подписывают соглашение. Там четко прописано: «Можно ломать вот этот домен, вот этим способом. Нельзя трогать вот этот сервер. Нельзя смотреть данные пользователей». Пока они внутри этих рамок — они защищены юридически. Шаг влево, шаг вправо — и статус «белого хакера» превращается в статус «обвиняемого».

Итого

В этой книге я буду учить тебя методам. Но каждый раз, применяя метод, ты должен включать внутреннего юриста.

— Мы будем учиться восстанавливать данные? Да, но тренируйся на **своих** флешках или на образах, предоставленных в рамках учебных задач (CTF).

— Мы будем учиться искать информацию о людях? Да, но только ту, которую они **сами** о себе рассказали.

— Мы будем разбирать, как работают атаки? Да, чтобы знать, как их **находить** в логах, а не чтобы их проводить.

Если ты ищешь руководство «Как стать неуловимым хакером», закрой эту книгу и сожги её. Если ты хочешь стать специалистом, который знает правила игры и умеет выигрывать, не нарушая их, — читай дальше.

С юридической духотой покончено. Теперь, когда ты предупрежден (и значит, вооружен), давай перейдем к настрой-

ке твоей лаборатории. Надевай белый халат, мы начинаем.

Часть 1. Подготовка и менталитет (Setup)

Глава 1. Лаборатория параноика: готовим рабочее место

— Почему нельзя работать с основного компьютера

Знаешь, какая самая частая ошибка новичка, который только что посмотрел сериал «Мистер Робот» и решил стать кибердетективом? Он открывает свой любимый домашний ноутбук — тот самый, на котором залогинен в «ВК», где хранятся фотки с прошлогоднего отпуска в Турции и где браузер услужливо помнит пароль от «СберБанк Онлайн» — и начинает качать хакерский софт или лезть на подозрительные форумы.

Если ты сейчас узнал себя, то у меня плохие новости: ты не детектив, ты — жертва. Причем добровольная.

Работать с основного компьютера (хоста) в нашей профессии — это всё равно что прийти в инфекционное отделение

больницы в трусах и шлепанцах, а потом вернуться домой и лечь в постель к жене, не помыв руки. Это нарушение главного принципа безопасности: **изоляции**.

Давай разберем по косточкам, почему твой домашний ПК — это худшее место для ведения расследований.

1. Перекрестное опыление (Cross-Contamination)

Представь, что ты расследуешь фишинговую атаку. У тебя есть файл invoice. pdf. exe, который прислали жертве. Твоя задача — узнать, что этот файл делает.

Ты кликаешь по нему на своем основном компьютере. Поздравляю! Теперь вирус не только у жертвы, но и у тебя. Он зашифровал твои семейные фото, украл твои куки (cookies) от почты и теперь рассылает спам твоим друзьям.

Но даже если ты не запускаешь вирусы, есть понятие «цифровой грязи».

Когда ты проводишь OSINT-расследование, ты ходишь по сайтам, которые могут быть нашпигованы трекерами, скриптами деанонимизации и эксплойтами. Если ты делаешь это из своего основного браузера:

— Скрипты видят, что ты залогинен в Google/Яндекс/VK. Они связывают твой интерес к расследованию с твоей реальной личностью.

— Ты оставляешь в истории браузера и кэше следы, которые могут быть использованы против тебя, если твой компьютер когда-нибудь попадет на экспертизу.

— Ты рискуешь случайно сохранить улики (например,

скачанный архив с данными) в папку «Загрузки», где они смешаются с твоими личными файлами. Потом попробуй докажи в суде, что этот архив с украденными кредитками — часть расследования, а не твоя личная коллекция.

2. Утечка твоей личности (OpSec Fail)

Твой основной компьютер знает о тебе слишком много.

— Имя пользователя: Часто папка пользователя называется C:\Users\IvanPupkin. Если какой-то скрипт или программа сольет путь к файлу, злоумышленники узнают твое имя.

— Региональные настройки: Часовой пояс, язык клавиатуры, установленные шрифты — всё это формирует уникальный цифровой отпечаток (fingerprint).

— MAC-адрес и железо: Твое «железо» уникально.

Когда ты работаешь «с хоста», ты выходишь в сеть со своим реальным IP (если забыл сервис на три буквы) и со своим реальным цифровым отпечатком. Для серьезных людей на той стороне провода это как бейдж с фотографией и адресом на твоей груди.

Профессионал всегда работает из «чистой» среды, которая не связана с его реальной жизнью. Если эту среду скомпрометируют — он просто удалит её и создаст новую. Если скомпрометируют твой основной ПК — тебе придется переустанавливать Windows, менять все пароли и молиться, чтобы кредиты на твое имя еще не оформили.

3. Юридическая чистота

Вспомни про главу о законах. Если ты случайно перейдешь грань (или тебя подставят), к тебе могут прийти с обыском.

Следователи изымают **всё**. Твой ноутбук, твой телефон, твои флешки.

Если ты вел расследование на основной машине, ты лишаешься своего личного инструмента на месяцы, а то и годы.

Более того, эксперты-криминалисты будут копаться в *твоих личных данных*. Твои переписки с девушкой, твои финансовые документы, твоя история поиска (да-да, *вся* история) — всё это будет просмотрено чужими дядями в погонах. Тебе оно надо?

Работая в изолированной среде (на отдельном ноутбуке или виртуальной машине), ты четко разделяешь: вот здесь — моя личная жизнь, она неприкосновенна. А вот здесь — работа. Если забирают рабочую машину — неприятно, но личное остается при тебе.

4. Риск случайных действий

Человеческий фактор — самая большая уязвимость.

На домашнем компе постоянно всплывают уведомления: «Пришло письмо», «Обновление Discord», «Мама звонит в Skype». Это отвлекает.

А когда ты отвлекаешься, ты совершаешь ошибки.

— Забыл включить сервис на три буквы перед сканированием.

— Случайно кликнул лайк под постом подозреваемого со

своего личного аккаунта (эпический провал, но случается чаще, чем ты думаешь).

— Скопировал опасную ссылку не в тот чат.

Рабочая среда должна быть стерильной. Там нет твоего личного Телеграма, нет игр, нет музыки. Только инструменты. Это помогает держать фокус и паранойю на нужном уровне.

5. Невозможность отката (Snapshotting)

Это чисто технический, но критически важный момент.

В процессе расследования ты часто устанавливаешь кучу специфического софта (Python-библиотеки, анализаторы трафика, утилиты с GitHub). Этот софт часто конфликтует друг с другом, засоряет реестр и ломает систему.

Если ты загадишь свой основной Windows, тебе придется тратить выходные на переустановку и настройку всего заново.

В правильной среде (на виртуальной машине) есть волшебная функция — **Снапшот (Snapshot)**. Это точка сохранения, как в играх.

Перед тем как запустить подозрительный файл или установить кривой софт, ты нажимаешь кнопку «Сделать снимок».

Если что-то пошло не так — система зависла, вирус всё сожрал или ты просто что-то сломал — ты нажимаешь «Вернуться к снимку» и через 5 секунд система снова девственно

чиста, как будто ничего не было.

На основном «железе» такой роскоши у тебя нет.

Итог: Правило двух стульев

Есть старая поговорка про два стула, но мы её переделаем.

На одном стуле — твоя цифровая жизнь (игры, банки, соцсети, котики).

На другом стуле — цифровая смерть, грязь, вирусы и расследования.

Никогда не сиди на обоих стульях одновременно одной задницей.

Твой основной компьютер — это твоя крепость. Не открывай ворота врагу добровольно.

Для войны у нас будет специальный танк — Виртуальная Машина. Именно её настройкой мы займемся в следующей главе. И поверь, когда ты поймешь всю мощь этой технологии, ты будешь смотреть на людей, работающих с «хоста», как на безумцев, жонглирующих гранатами без чеки.

— Виртуальные машины (VM): твой цифровой презерватив

Если в прошлой главе я тебя убедил (а я надеюсь, что убедил), что работать с основного компа — это путь камикадзе, то сейчас возникает вопрос: «А где тогда работать?»

Ответ прост: в Матрице. Точнее, внутри другой операционной системы, которая живет внутри твоего компьютера, но

ничего не знает о нем. Это называется **Виртуальная Машина (VM)**.

VM — это песочница. Это полигон. Это твой цифровой презерватив. Что бы ни случилось внутри виртуалки — вирус-шифровальщик, кривой драйвер или атака хакеров — это останется внутри виртуалки. Если что-то пошло не так, ты просто удаляешь файл виртуальной машины, и угроза исчезает. Твой основной компьютер (хост) при этом стоит чистенький и невредимый, попивая электронный сок.

Выбор гипервизора: Кто будет главным?

Чтобы запустить одну ОС внутри другой, тебе нужна программа-прослойка — гипервизор. На рынке два главных игрока для простых смертных:

— Oracle VirtualBox.

— *Плюсы:* Бесплатный, Open Source, работает везде (Windows, macOS, Linux).

— *Минусы:* Иногда тормозит, интерфейс выглядит как привет из 2005 года.

— *Вердикт:* Идеально для новичка. Мы будем использовать его.

— VMware Workstation (Pro/Player).

— *Плюсы:* Быстрее, стабильнее, лучше работа с USB-устройствами.

— *Минусы:* Pro-версия платная (хотя для личного использования Broadcom недавно сделал поблажки, но там черт ногу сломит с лицензиями).

— *Вердикт:* Если ты мажор или уже профи — бери. Но для старта VirtualBox хватит за глаза.

Выбор оружия: Какую ОС ставить?

Теперь самое вкусное. Нам нужна операционка, заточенная под расследования. Ставить «голую» Windows и накатывать туда софт вручную — это путь боли. Лучше взять готовый дистрибутив, где умные дядьки уже собрали все инструменты.

Вариант 1: Kali Linux (Классика жанра)

Это швейцарский нож. Вообще-то он создан для пентестеров (взломщиков), но там есть огромный раздел «Forensics».

— *За:* Тонны мануалов, огромное комьюнити, крутой логотип с драконом (важно для понтов).

— *Против:* Это Linux. Если ты всю жизнь сидел на Windows, первое время будешь плакать от консоли.

— *Кому:* Тем, кто хочет стать профи и не боится трудностей.

Вариант 2: CSI Linux (Специально для детективов)

Менее попсовый, но дико крутой дистрибутив. Он заточен именно под OSINT и Форензику. Там уже предустановлены инструменты для пробива никнеймов, анализа соцсетей и даркнета, которые в Kali надо ставить руками.

— *За:* Идеальный набор софта «из коробки» для наших задач. Встроенная анонимизация (Tor/сервис на три буквы шлюз).

— *Против:* Жрет много ресурсов, интерфейс перегружен.

Вариант 3: Flare VM (Windows для тех, кому страшно)

Если от слова sudo apt-get update у тебя начинается паническая атака, твой выбор — Flare VM. Это не отдельная ОС, а скрипт, который превращает обычную Windows 10/11 в боевую станцию аналитика.

— *За:* Привычный интерфейс «Винды».

— *Против:* Windows сама по себе «стучит» телеметрией, так что для анонимности придется попотеть с настройками.

Мой совет: Ставь **Kali Linux**. Рано или поздно тебе придется учить Linux. Лучше рано.

Практическое задание №1: Поднимаем VirtualBox

Хватит теории. Давай пачкать руки.

— Иди на официальный сайт virtualbox.org и качай последнюю версию под свою ОС.

— Не забудь скачать там же **Extension Pack** (это важно для поддержки USB 2.0/3.0).

— Установи VirtualBox. Там всё просто: «Далее — Далее — Согласен — Готово».

— Установи Extension Pack (просто кликни по скачанному файлу, VirtualBox сам подхватит).

Практическое задание №2: Установка Kali Linux

Сейчас ты почувствуешь себя хакером.

— Иди на kali.org/get-kali/.

— Ищи раздел **Virtual Machines**. Не «Installer Images», а

именно готовые образы для виртуалок!

— Качай файл для VirtualBox (он будет весить гигабайта 3—4, так что завари кофе).

— Распакуй скачанный архив (7-Zip тебе в помощь).

— В папке найди файл с синим кубиком (расширение. vbox или. vbox-prev) и кликни дважды.

— Магия! В списке VirtualBox появится новая машина.

Настройка перед запуском:

— Выдели машину в списке, жми **«Настроить» (Settings)**.

— **Система -> Материнская плата:** Выдели ей хотя бы 4 ГБ оперативки (лучше 8, если у тебя богатое железо).

— **Сеть:** Убедись, что стоит «NAT». Это значит, что виртуалка будет ходить в интернет через твой комп, но из интернета напрямую до неё не достучаться. Безопасненько.

Первый запуск:

— Жми зеленую стрелку **«Запустить»**.

— Жди, пока пробегут строки кода (не пугайся, так надо).

— Логин/пароль по умолчанию у готовых образов Kali:

— Login: kali

— Password: kali

— Если ты увидел рабочий стол с драконом — поздравляю, Нео. Ты в системе.

Практическое задание №3: Первая команда (и обновление)

Линукс живет обновлениями. Первое, что делает профи

на новой системе — обновляет репозитории.

— Найди значок терминала (черный квадрат) в левом верхнем углу. Жми.

— Напиши (ручками!):

— sudo apt update && sudo apt full-upgrade -y

— Нажми Enter.

— Введи пароль (kali). **Внимание:** когда вводишь пароль в Linux, звездочки НЕ появляются. Курсор стоит на месте. Это нормально, это паранойя безопасности. Просто введи и нажми Enter.

— Смотри, как бегут буквы. Ты обновляешь свой арсенал.

Практическое задание №4: Снапшот (Твоя страховка)

Ты только что настроил чистую, обновленную систему. Самое время сохраниться, прежде чем ты её сломаешь.

— В меню окна виртуальной машины (сверху) нажми **Машина -> Сделать снимок (Take Snapshot)**.

— Назови его: Clean Install Updated.

— Описание: Чистая система после обновления.

— Жми ОК.

Всё. Теперь, если ты случайно удалишь системную папку или подцепишь вирус, ты просто выключишь машину, нажмешь **«Восстановить»** на этом снимке, и через 30 секунд вернешься в этот момент времени.

Поздравляю. У тебя есть лаборатория. Теперь ты не просто юзер, ты оператор боевой единицы. В следующей главе

мы научимся не светить своим IP-адресом, потому что анонимность — это наше всё.

— OpSec (Operational Security): как самому не оставить следов, пока ищешь чужие

Итак, лабораторию мы собрали. У тебя есть Kali Linux, ты умеешь делать снапшоты и чувствуешь себя властелином мира. Придержи коней. Прямо сейчас твоя виртуальная машина — это бронированный танк, на котором большими неоновыми буквами написан твой домашний адрес, ФИО и номер паспорта.

Если ты выйдешь в Сеть «голым» (без средств анонимизации), любой админ сайта, на который ты зашел в поисках улик, увидит твой реальный IP-адрес. А IP-адрес — это ниточка, за которую товарищ майор (или злой хакер) вытянет тебя из уютного кресла в реальный мир проблем.

Добро пожаловать в **OpSec** — искусство оставаться невидимым. Это не про то, как взламывать, это про то, как не спалиться.

Три слоя защиты: Презерватив, Фольга и Чужое лицо

Нам нужно построить эшелонированную оборону. Она состоит из трех компонентов:

— Техническая маскировка (сервис на три буквы):

Скрываем *откуда* мы.

— Сетевая анонимность (Tor): Скрываем *кто* мы.

— Социальная маскировка (Sock Puppets): Притворяемся *кем-то другим*.

Слой 1. сервис на три буквы: Твой цифровой камуфляж

сервис на три буквы — это труба. Ты залезаешь в трубу у себя дома, а вылезаешь из нее где-нибудь в Амстердаме или Панаме. Весь мир думает, что ты сидишь в Амстердаме.

Главное правило сервиса на три буквы для детектива:

Никогда. Слышишь? НИКОГДА не используй бесплатные сервисы на три буквы.

Бесплатный сервис на три буквы — это мышеловка. Если ты не платишь за товар, значит, товар — это ты. Бесплатные сервисы продают твои логи рекламодателям или, что хуже, сливают их по первому запросу органов.

Критерии выбора сервиса на три буквы для работы:

— No Logs Policy: Провайдер клянется (желательно, пройдя независимый аудит), что не пишет логи.

— Юрисдикция: Оффшоры (Панама, БВО, Сейшелы) или страны со строгими законами о приватности (Швейцария). Избегай стран «14 глаз» (США, Британия, Канада и др.), они делятся разведданными.

— Kill Switch: Функция, которая намертво обрубает ин-

тернет, если сервис на три буквы отвалился. Без неё, если сервис на три буквы упадет на секунду, твой реальный IP засветится, как голый зад на нудистском пляже.

Слой 2. Tor: Луковая маршрутизация

Если сервис на три буквы — это просто маска, то Tor — это когда ты надеваешь маску, садишься в такси, меняешь три машины по пути, запутываешь следы в лесу и выходишь в другой стране.

Tor заворачивает твой трафик в три слоя шифрования и прогоняет через три случайных узла (ноды) по всему миру:

— **Входная нода:** Знает, что это ты, но не знает, куда ты идешь.

— **Средняя нода:** Не знает ничего, просто передает пакет.

— **Выходная нода:** Знает, куда ты идешь, но не знает, кто ты.

Связка сервис на три буквы + Tor (Tor over сервис на три буквы):

Сначала включаешь сервис на три буквы на хосте (или в виртуалке), потом запускаешь Tor Browser.

— Твой провайдер видит только зашифрованный туннель до сервиса на три буквы.

— Входная нода Tor видит IP твоего сервиса на три буквы, а не твой реальный.

— Сайт видит IP выходной ноды Tor.

— Это золотой стандарт для пассивной разведки.

Слой 3. Sock Puppets: Искусство быть никем

Техника тебя защитила, но тут ты заходишь на форум киберпреступников и регистрируешься как ivan.ivanov@mail.ru. Поздравляю, ты провалил миссию.

Тебе нужны **Sock Puppets** (сок-паппеты, «марионетки») — фейковые личности. Это не просто «левый аккаунт», это легенда.

У хорошего «сока» есть:

— Имя и фото (сгенерированное нейросетью, а не украденное у реального человека, чтобы не найтись поиском по картинке).

— История (аккаунт создан не вчера, у него есть подписки, лайки, репосты котиков).

— «Чистая» сим-карта или виртуальный номер (для регистрации).

Где брать номера?

— *Плохой вариант:* Твой личный номер. (Смерть карьере).

— *Средний вариант:* Сервисы приема СМС (sms-activate и прочие). Дешево, но аккаунты часто банят, так как номера «заезженные». Плюс, сервис знает, что ты регистрировал.

— *Хороший вариант:* Физическая «левая» симка, купленная в переходе без паспорта (в РФ незаконно, но мы обсуждаем методы) или оформленная на дропа.

— *Идеальный вариант:* Анонимные eSIM или номера, арендованные за крипту через сервисы вроде *Fragment* (для

Telegram).

Практическое задание №1: Проверка утечек (Do I Leak?)

Давай проверим, насколько дырявая твоя защита прямо сейчас.

— Запусти свою Kali Linux.

— Открой Firefox (он там по умолчанию).

— Зайди на сайт ipleak.net или whoer.net.

— **Смотри в раздел IP Address.** Если ты видишь там название своего домашнего провайдера (Ростелеком, МГТС, Билайн) — у тебя проблемы. Ты голый.

— **Смотри в раздел DNS.** Если IP другой, но в DNS виден сервер твоего провайдера — это **DNS Leak**. Ты в маске, но бейдж с именем все равно торчит. Провайдер видит, куда ты ходишь.

Задача:

— Установи сервис на три буквы (если нет платного, для теста поставь Proton Free — он хотя бы честный, хоть и медленный).

— Включи сервис на три буквы.

— Обнови страницу ipleak.net.

— Добейся того, чтобы и IP, и DNS показывали другую страну.

Практическое задание №2: Создаем лицо, которого не существует

Подготовим аватарку для твоего будущего рабочего аккаунта.

— Иди на сайт thispersondoesnotexist.com.

— Этот сайт генерирует фото несуществующего человека с помощью нейросети GAN.

— Обновляй страницу, пока не найдешь лицо, которое выглядит максимально обычно. Избегай:

— Артефактов на фоне (странные пятна, кривые уши).

— Слишком красивых (модельных) лиц — они привлекают внимание.

— Детей и стариков (неудобно для легенды).

— Сохрани фото.

— **Важно:** Теперь проверь его уникальность. Загрузи это фото в «Яндекс. Картинки» и Google Images. Если поисковики ничего не нашли — отлично. Если нашли похожих людей — генерируй заново. Мы не хотим, чтобы нашу марионетку спутали с реальным бухгалтером из Саратова.

Практическое задание №3: Установка и настройка Tor Browser в Kali

В Kali Linux Tor Browser не всегда стоит по умолчанию (или может быть устаревшим). Давай сделаем всё правильно. Не надо работать под root (администратором) в Tor, это опасно, но для учебных целей пока просто запустим.

— Открой терминал.

— Установи загрузчик Tor:

— sudo apt update && sudo apt install -y tor torbrowser-

launcher

— Запусти лаунчер (ищи в меню приложений иконку луковицы или напиши torbrowser-launcher в консоли).

— Он скачает свежую версию браузера и проверит подпись (PGP).

— Когда браузер откроется, зайди на любой сайт для проверки IP (например, 2ip.io).

Конец ознакомительного фрагмента.