

КЕВИН МИТНИК

ВИЛЬЯМ Л. САЙМОН

18+



3-е издание

ПРИЗРАК В СЕТИ

МЕМОУАРЫ ВЕЛИЧАЙШЕГО ХАКЕРА

 **БОМБОРА**
ИЗДАТЕЛЬСТВО

Уильям Л. Саймон
Кевин Митник
Призрак в Сети. Мемуары
величайшего хакера
Серия «КиберБез. Лучшие
книги о безопасности в сети»

Текст предоставлен правообладателем

http://www.litres.ru/pages/biblio_book/?art=73883617

*Призрак в Сети. Мемуары величайшего хакера / Кевин Митник, Вильям Л. Саймон ; [перевод с английского].: Эксмо; Москва; 2026
ISBN 978-5-04-246337-2*

Аннотация

НЕЗАКОННОЕ ПОТРЕБЛЕНИЕ НАРКОТИЧЕСКИХ СРЕДСТВ, ПСИХОТРОПНЫХ ВЕЩЕСТВ, ИХ АНАЛОГОВ ПРИЧИНЯЕТ ВРЕД ЗДОРОВЬЮ, ИХ НЕЗАКОННЫЙ ОБОРОТ ЗАПРЕЩЕН И ВЛЕЧЕТ УСТАНОВЛЕННУЮ ЗАКОНОДАТЕЛЬСТВОМ ОТВЕТСТВЕННОСТЬ.

Кевин Митник по праву считается самым неуловимым мастером компьютерного взлома в истории. Он проникал в сети крупнейших мировых компаний, – и, как бы оперативно ни спохватывались власти, Митник был быстрее, вихрем проносясь

через телефонные коммутаторы, компьютерные системы и сотовые сети.

Он долгие годы рыскал по киберпространству, всегда опережая преследователей не на шаг, а на три шага, и заслужил славу человека, которого невозможно остановить. Но для Митника хакерство не сводилось только к технологическим эпизодам – он плел хитроумные сети обмана, проявляя редкое коварство и выпытывая у ничего не подозревающего собеседника ценную информацию.

Он обходил системы безопасности и проникал в такие корпорации, как Motorola, Pacific Bell и Sun Microsystems. Но когда ФБР начало брать хакера в кольцо, он пустился в бега – и началась сложнейшая игра в «кошки-мышки». В ходе этой облавы Митник сменил несколько личностей, городов, не раз чудом уходил от ареста – до последней неравной схватки с агентами, которые во что бы то ни стало стремились его арестовать.

«Призрак в Сети» – это портрет провидца, обладающего такой изобретательностью, хваткой и настойчивостью, что властям пришлось полностью переосмыслить стратегию погони за ним. Отголоски этой эпической схватки чувствуются в сфере компьютерной безопасности и сегодня.

В формате PDF А4 сохранен издательский макет книги.

Содержание

Предисловие	7
Пролог	10
Часть I	17
Глава 1	17
Глава 2	26
Конец ознакомительного фрагмента.	32

**Кевин Митник,
Вильям Саймон**
**Призрак в Сети. Мемуары
величайшего хакера**

*Моей маме и бабушке
К. Д. М.*

*Арини, Виктории и Дэвиду, Шелдону, Винсенту и
Елене Роуз и в особенности Шарлотте
У. Л. С.*

Серия «КиберБез. Лучшие книги о безопасности в Сети»

Перевод с английского
3-е издание

GHOST IN THE WIRES:

My Adventures as the World's Most Wanted Hacker

© 2011 by Kevin Mitnick with William L. Simon

This edition published by arrangement with Little, Brown and
Company,
New York, New York, USA. All rights reserved.

Редакция никоим образом не поощряет и не оправдывает использование методов хакинга в целях незаконного проникновения, кражи данных или иных противоправных действий. Книга представляет собой автобиографический рассказ Кевина Митника о его опыте в области компьютерной безопасности и социальной инженерии.

Мы настоятельно подчеркиваем, что информация предназначена исключительно для понимания принципов работы систем безопасности. Использование описанных методов для совершения противоправных действий является незаконным и может повлечь за собой серьезные юридические последствия.



БОМБОРА
ИЗДАТЕЛЬСТВО

Предисловие

Впервые я встретил Кевина Митника в 2001 году, во время съемок документального фильма «История хакинга» для канала Discovery. На этом наше общение не закончилось. Через два года я прилетел в Питтсбург, чтобы прочитать вступительную речь к его выступлению в Университете Карнеги – Меллона, где изумился его хакерской биографии. Он взламывал корпоративные компьютеры, но не портил файлы, не использовал и не продавал те номера кредитных карточек, к которым имел доступ. Он брал программы, но никогда не торговал ими, так как делал это для удовольствия и самоутверждения.

В лекции Кевин подробно рассказал невероятную историю о том, как раскусил идущую против него операцию ФБР. Митник раскрыл все детали и обнаружил, что его новый приятель-хакер – шпион. Кевин узнал имена, домашние адреса всех агентов ФБР, которые занимались его делом, даже прослушал телефонные звонки и голосовую почту сыщиков, пытавшихся собрать против него улики. Специально устроенная система сигнализации предупреждала Кевина о том, когда именно ФБР готовило на него облаву.

Как-то продюсеры телешоу *Screen Savers* пригласили меня и Кевина выступить в роли ведущих на один выпуск. Они попросили продемонстрировать новое электронное устрой-

ство, которое тогда только появилось на потребительском рынке, – GPS. Я должен был колесить на автомобиле, который они отслеживали по навигатору. В эфире показали мой, казалось бы, случайный маршрут на карте. Линии пути складывались в два слова:

СВОБОДУ КЕВИНУ.

С Кевином нам довелось выступать и в 2006 году, когда Митник подменял Арта Белла на его ток-шоу. Он предложил мне стать его собеседником в эфире. К тому времени я многое о нем знал и в тот вечер рассказал, через что прошел сам, мы много смеялись – нам всегда было весело вдвоем.

Кевин изменил мою жизнь. Однажды я осознал, что он не раз звонил мне, когда был за тридевять земель: Митник ездил в Россию, где читал лекцию, в Испанию, где консультировал одну компанию по вопросам безопасности, в Чили, где помогал банку справиться с недавним компьютерным взломом. Все это звучало потрясающе. Я почти десять лет не пользовался загранпаспортом, пока эти звонки не пробудили во мне жажду странствий. Кевин познакомил меня со своим агентом, который организовывал его лекции. Эта дама как-то сказала: «Могу и вам организовать выступления». Так, благодаря Кевину, я принялся путешествовать по миру.

Кевин стал одним из моих лучших друзей. Мне нравится проводить с ним время, слушать о его курьезах и походе-

ниях. Жизнь его не менее яркая и увлекательная, чем лучшие фильмы про ограбления.

Теперь и вы сможете узнать все те истории, которые я слышал одну за другой на протяжении многих лет. В известном смысле я немного завидую, ведь перед вами только открывается необычное путешествие. Вам предстоит узнать удивительную, даже невероятную биографию и хронику авантюр Кевина Митника.

*Стив Возняк,
соучредитель Apple Inc.*

Пролог

Физический доступ – это проникновение в здание интересующей вас компании. Мне это никогда не нравилось. Слишком рискованно. Пишу об этом – и меня уже пробивает холодный пот.

Однако вот он я, теплым летним вечером прячусь на темной парковке компании, которая ворочает миллиардами долларов, и подгадываю нужный момент. За неделю до этого я посетил здание среди бела дня. Пришел под предлогом того, что нужно оставить письмо для одного сотрудника. На самом же деле я хотел как следует – в деталях – разглядеть местные пропуска. Итак, фото сотрудника в анфас в левом верхнем углу. Прямо под ним – фамилия и имя большими печатными буквами. В нижней части карточки – название компании, крупным красным шрифтом.

Я сходил в интернет-клуб и посмотрел сайт компании. На нем можно было скачать и скопировать изображение логотипа этой фирмы. Проработав около 20 минут в Photoshop с логотипом и сканом своей фотографии, я сделал вполне убедительное факсимиле идентификационной карточки. Результат творения я аккуратно вставил в копеечный бейджик. Еще один фальшивый пропуск смастерил для друга, который согласился подсобить, если понадобится его помощь.

Раскрою секрет: пропуску вполне хватит и отдаленного

сходства. В 99% случаев на него смотрят мельком. Если основные элементы бейджа расположены правильно и выглядят похоже, то вас пропустят. Однако какой-нибудь чересчур ретивый охранник или сотрудник, решивший поиграть в цербера, может попросить вас поднести бейджик ближе. И если вы живете, как я, то такую опасность никогда нельзя списывать со счетов.

На парковке меня не видно. Я смотрю на огоньки сигарет той череды людей, которые выходят на улицу покурить. Наконец, замечаю группу из пяти-шести человек, возвращающихся в здание. Дверь черного хода – одна из тех, что открываются только тогда, когда кто-то из сотрудников подносит ключ-карту к считывающему устройству. Я пользуюсь моментом и последним пристраиваюсь к этой группе. Парень передо мной переступает порог, замечает, что за ним кто-то идет, мельком меня оглядывает, видит бейдж, как и у всех сотрудников, и придерживает дверь, чтобы я вошел. Я благодарно киваю.

Такой прием называется «паровозик».

Внутри я сразу замечаю плакат, расположенный так, что его обязательно увидит каждый посетитель. Он предупреждает, что в целях безопасности заходить в здание нужно по одному, не придерживая дверь для того, кто идет после вас. Было важно, чтобы каждый подносил свою ключ-карту к считывающему устройству. Однако обычная вежливость, бытовая любезность к «коллеге-товарищу», заставляет со-

трудников с завидным постоянством игнорировать предупреждающий плакат.

Итак, я внутри. Иду вперед по длинным коридорам широким шагом человека со срочным делом. По правде же я мчусь в поисках офиса отдела информационных технологий (ИТ). Нахожу его минут через десять в западной части здания. Я хорошо подготовился к визиту и знаю имя одного системного администратора этой компании. Полагаю, у него самые широкие права доступа в корпоративную сеть.

Черт возьми! Когда я нахожу его рабочее место, оказывается, что это не обычная отгороженная кабинка типа «заходи кто хочет», а отдельный офис, где дверь закрыта на ключ. Однако я вижу решение. Подвесной потолок выстлан белыми звуконепроницаемыми квадратами. Выше него часто оставляют технический этаж для труб, электропроводки, вентиляции и т. п.

Я звоню товарищу, говорю, что нужна его помощь, и возвращаюсь к черному ходу, чтобы впустить соучастника. Он, худой и высокий, должен выполнить то, что не под силу мне. Возвращаемся в ИТ-отдел, и мой подельник залезает на стол. Я хватаю его за ноги и поднимаю достаточно высоко. Ему удается приподнять звуконепроницаемую пластину. Я напрягаюсь, поднимаю его еще выше – он хватается за трубу и подтягивается. Не проходит и минуты, и я слышу, как он приземляется в офисе. Ручка двери поворачивается – товарищ стоит весь в пыли, но с улыбкой до самых ушей.

Я захожу и тихо закрываю дверь. Теперь нас с меньшей вероятностью заметят. В офисе темно. Включать свет опасно, но он и не нужен: мне хватает света монитора, чтобы увидеть все необходимое. Так риск гораздо меньше. Я быстро рассматриваю стол, проверяю, что лежит в верхнем ящике и под клавиатурой – вдруг администратор оставил шпаргалку, на которой записал пароль к компьютеру. Не нашел. Жаль, но это совсем не проблема.

Достаю из сумки загрузочный компакт-диск с операционной системой Linux с инструментарием хакера, вставляю в дисковод и перезапускаю компьютер. Один из инструментов позволяет изменить пароль локального администратора. Я меняю его на собственный, чтобы можно было войти в систему. Затем убираю диск и вновь перезагружаю компьютер. На этот раз уже вхожу в систему через учетную запись локального администратора.

Я работаю как можно быстрее. Устанавливаю троян удаленного доступа – особый вирус, который дает мне полный доступ к системе, – и теперь могу вести учет всех нажатий клавиш, собирать зашифрованные значения (хеши) паролей и даже приказывать веб-камере фотографировать пользователя. Тот троян, что я установил на машине, каждые несколько минут будет подключаться через Интернет к другой моей системе, предоставляя полный контроль над зараженной машиной. Делаю последнюю операцию: захожу в реестр компьютера и указываю в качестве последнего пользователя, во-

шедшего в систему (last logged in user), логин ничего не подозревающего инженера. Так я стираю все следы того, что проникал в систему через локальную учетную запись администратора. Утром инженер придет на работу и заметит, что он зачем-то вышел из системы. Ничего страшного: как только он снова в нее войдет, все будет выглядеть именно так, как нужно.

Пора идти обратно. Мой товарищ уже заменил звукопроницаемую плитку.

Уходя, я закрываю дверь на замок.

На следующий день в 08:30 системный администратор включает компьютер и устанавливает соединение с моим ноутбуком. Поскольку троян работает под его учетной записью, у меня есть все права администратора в этом домене. Всего за несколько секунд я нахожу контроллер, который содержит пароли от всех учетных записей сотрудников этой компании. Хакерский инструмент fgdump позволяет мне собрать в отдельном файле хешированные, то есть зашифрованные пароли каждого пользователя.

За несколько часов я прогоняю список хешей через «радушные таблицы» – огромную базу данных, содержащую заранее расшифрованные хеши паролей, – и восстанавливаю пароли большинства сотрудников этой компании. В конце концов я нахожу внутренний сервер, который обрабатывает пользовательские транзакции, но понимаю, что номера кредитных карточек зашифрованы. Однако это совсем не про-

блема. Оказывается, ключ, используемый для шифрования номеров, спрятан в хранимой процедуре внутри базы данных на компьютере так называемого «SQL-сервера», доступ к которому открыт для любого администратора базы данных.

Несколько миллионов номеров кредитных карточек. Я могу покупать все, что захочу, каждый раз пользоваться другой карточкой, а главное – они никогда не закончатся.

Но я ничего не купил. Эта правдивая история не очередная попытка хакинга, из-за которого я нажил себе уйму неприятностей. Меня наняли для того, чтобы я совершил это проникновение.

Мы сокращенно называем такую операцию пен-тестом. «Пен» означает пенетрацию, то есть проникновение. Это значительная часть той жизни, которой я теперь живу. Я проskalывал в здания крупнейших мировых компаний, взламывал самые неприступные компьютерные системы, которые когда-либо разрабатывались. Все это происходило по поручению самих этих компаний. Такие тесты помогали им совершенствовать меры безопасности, чтобы компания не стала жертвой настоящего хакера. Я во многом самоучка и потратил немало лет на изучение методов, тактики и стратегии, позволяющих преодолевать компьютерную защиту и лучше понимать принципы работы компьютерных и телекоммуникационных систем.

Страсть к технике и увлеченность ею толкнули меня на скользкую дорожку. Хакерские проделки стоили мне более

пяти лет за решеткой, а моим близким и любимым людям – невероятной душевной боли.

В этой книге – моя история. Настолько подробная и точная, насколько я могу ее припомнить. С оглядкой на мои личные записи, протоколы судебных заседаний, документы, полученные по закону о свободном доступе к информации, перехваченные ФБР телефонные разговоры, скрытые записи, многочасовые показания и беседы с двумя правительственными информаторами.

Это история о том, как я стал самым разыскиваемым и востребованным хакером в мире.

Имена Бетти, Дэвид Биллингсли, Джерри Коверт, Кумамото, Скотт Лайонз, Мими, Джон Нортон, Сара и Эд Уолш вымышлены. Под ними выступают реальные люди, с которыми мне доводилось сталкиваться. Я воспользовался этими псевдонимами, потому что хоть и умею хорошо запоминать числа и ситуации, но настоящие имена иногда забываю.

Часть I

Рождение хакера

Глава 1

Жесткий старт

*Yjcv ku vjg pcoq qh vjg uauvgo wugf da jco qrgtcvqtu
vq ocmg htgg rjqpg ecnnu?¹*

Мой инстинкт, который помогал обходить преграды и охрану, проявился очень рано. Когда мне было полтора года, я сумел выбраться из кровати, доползти до детских ворот в дверном проеме и отпереть их. Для моей мамы это был первый звоночек, предвещавший будущие невероятные события.

Я рос единственным ребенком в семье. После того как от нас ушел отец (мне было три года), мама Шелли и я жили в симпатичных недорогих квартирках в спокойных районах долины Сан-Фернандо, а прямо за близлежащим холмом на-

¹ Как называется система, используемая операторами любительского радио для бесплатных звонков по телефону? Здесь и далее – расшифровки эпитафий по сайту http://fabiensanglard.net/Ghost_in_the_Wires/index.php – *Здесь и далее примечания переводчика.*

чинался Лос-Анджелес. Мама зарабатывала на хлеб, работая официанткой то в одной, то в другой забегаловке, которые были разбросаны вдоль бульвара Вентура, что протянулся с востока на запад по всей долине. Отец жил в другом штате. Пусть он и заботился обо мне, но появлялся в жизни лишь изредка, пока не перебрался в Лос-Анджелес, когда мне было уже тринадцать.

Мы с мамой переезжали слишком часто, поэтому мне было сложно заводить друзей. Почти все раннее детство у меня был уединенный и сидячий образ жизни. Когда я пошел в школу, учителя часто говорили маме, что у меня удивительные способности к математике и правописанию, и я на несколько лет опережаю свой возраст. Однако я был неугомонным мальчишкой, и мне было сложно сидеть на месте.

Пока я рос, мама трижды выходила замуж и сменила еще несколько мужчин. Один из них меня обижал, другой, работавший в какой-то правоохранительной организации, пытался совратить. Мама, в отличие от других матерей, о которых мне доводилось читать, никогда не закрывала на это глаза. Как только она узнавала, что меня обижают или даже грубо разговаривают, любовники собирали манатки и исчезали. Оправдываться не буду, но могли ли эти жестокие мужчины оказать какое-то влияние на мою взрослую жизнь, через которую красной нитью прошло неповиновение авторитетам?

Моей любимой порой года было лето, особенно когда у мамы был перерыв между сменами в середине дня. Мне

очень нравилось ходить с ней на чудесный пляж Санта-Моника. Мама любила лежать на песке, загорать, расслабляться и смотреть, как я плескался в прибое: волна сшибала меня, а я выныривал с хохотом из воды. Плавать я научился в лагере YMCA (Христианской ассоциации молодых людей), где несколько лет отдыхал летом. На самом деле меня раздражало там абсолютно все, кроме прогулок на пляж.

В детстве у меня не было проблем с физкультурой, я с удовольствием играл в Малой бейсбольной лиге², нередко проводя свободное время за тренировками с битой. Однако страсть, которая определила ход моей жизни, началась лет в десять. У наших соседей была дочка примерно моего возраста. Она мне очень нравилась и отвечала взаимностью. Признаюсь, она даже танцевала передо мной голышом. Однако в те годы меня интересовала не ее прелесть, а то, что мог мне дать ее отец, – волшебство.

Этот дядя был успешным фокусником. Его трюки с картами, монетками и масштабные иллюзии страшно занимали меня. Но что гораздо важнее, я увидел, как его зрители – то один, то трое, то целый зал – получали удовольствие от того, что их обманывают. Тогда эта мысль не была осознанной. Однако позже я понял, насколько людям нравится покупаться на фокусы. Это ошеломляющее открытие изменило всю мою жизнь.

Лавка волшебника, расположенная от нас на расстоянии

² Лига для мальчиков и девочек 8–12 лет.

всего лишь краткой велосипедной прогулки, стала моим прибежищем, где я проводил все свободное время. Именно магия научила меня обманывать людей.

Иногда я ездил туда не на велосипеде, а на автобусе. Прошло пару лет и однажды Боб Аркоу, водитель автобуса, заметил, что я надел футболку с надписью «CBers Do It on the Air»³. Он рассказал мне, что недавно нашел полицейскую рацию фирмы Motorola.

Я предположил, что через нее Боб теперь может прослушивать переговоры на закрытых полицейских частотах, а это, конечно же, было очень круто. Оказалось, водитель просто пошутил. Однако он был заядлым радиолюбителем и своим энтузиазмом заразил меня. Боб научил, как, используя радиочастоты, бесплатно звонить по телефону с помощью службы, которая называлась «автопатч». Поддерживали ее такие же любители, как он сам. Бесплатные телефонные звонки! Невозможно передать, как это меня впечатлило. Я просто подсел на радиосвязь.

Несколько недель я ходил в вечернюю школу. Там вдумчиво изучал схемы и нормы любительского радио, чтобы сдать письменный экзамен. Освоил и азбуку Морзе, по крайней мере столько, чтобы соответствовать требованиям. Вскоре почтальон принес конверт из Федеральной комиссии

³ «CBers» – это пользователи радиосвязи «гражданского диапазона». Сам диапазон называется «Citizen's Band» или сокращенно «CB» (Си Би). СВ доступен по дешевой (а часто бесплатной) лицензии. Надпись на футболке в шуточной форме сообщала о заинтересованности человека любительской радиосвязью.

по связи. Там лежала моя лицензия на любительские занятия радиосвязью. Немногие дети в 12 лет могли похвастаться таким документом. Меня охватило чувство огромного удовлетворения.

Обманывать людей фокусами было клево. Однако разобраться в том, как работают телефонные системы, оказалось гораздо круче. Я хотел досконально знать всю внутреннюю кухню телефонных операторов. В начальной и средней школе, где-то до седьмого класса, я учился очень хорошо. Примерно в восьмом или девятом классе начал прогуливать уроки и зависать в Henry Radio – любительском радиомагазине на западе Лос-Анджелеса. Я часами читал книги по теории радиосвязи. Наведаться туда для меня было, как съездить в Диснейленд. Кроме того, мои навыки пригождались людям. Какое-то время я подрабатывал по выходным и осуществлял техническую поддержку радиосвязи в местном отделении Красного Креста. Однажды летом я целую неделю занимался подобной работой на олимпиаде для спортсменов с особенностями развития.

Катаясь на автобусах, я словно был туристом на каникулах – наслаждался красотами города, хотя многие из них видел не раз. Это было в Южной Калифорнии. Погода там практически всегда великолепная, если, конечно, не висит смог. В те годы ситуация со смогом была гораздо хуже, чем сейчас. Билет на автобус стоил 25 центов, еще 10 центов приходилось платить за пересадку. На летних каникулах, пока мама

работала, я иногда катался на автобусе целыми днями. Мне тогда было 12, но я уже любил замышлять неладное. В один прекрасный день я осознал, что *если бы мог сам компостировать пересадочные талоны, то поездки на автобусе стали бы бесплатными*⁴.

Мой отец и дяди по профессии занимались продажами и у них всех был подвешен язык. Думаю, я унаследовал это качество от них. С самого раннего детства я мог убедить людей оказать мне услугу. Вот и в тот день я прошел в начало автобуса и сел поближе к водителю. Когда он остановился на светофоре, я сказал: «Знаете, мне тут в школе дали творческое задание. Мне нужен дырокол, чтобы пробивать им на картоне разные узоры. Вот бы мне такой дырокол, как тот, которым вы пробиваете пересадочные талоны. Не подскажете, его можно где-нибудь купить?»

Я и не думал, что водитель поверит в такую чушь. Полагаю, у него просто не возникло мысли о том, что такой па-

⁴ Эта мысль будет понятнее, если представлять себе принцип использования пересадочных билетов, которые применялись в то время. Вот что рассказывает об этих билетах сам Митник в первой главе книги «Искусство обмана»: «Пересадочный талон позволял сменить маршрут и доехать на другом автобусе. Но я придумал, как с их помощью кататься куда хочу задаром. Добывать пустые талоны было раз плюнуть: в мусорках у автовокзалов всегда валялись не до конца заполненные книжки с пересадочными талонами. Водители просто выбрасывали их в конце смены. С талонной книжкой и дыроколом я мог сам пробивать пересадки и кататься по всем маршрутам Лос-Анджелеса. Вскоре я почти наизубок выучил расписание всех автобусов. Это ранний пример моей удивительной памяти на определенные типы информации, и даже сейчас я могу вспомнить телефонные номера, пароли и прочую, казалось бы, мелочь аж с детских лет».

дан, как я, может им манипулировать. Он сказал мне название магазина, я позвонил туда и узнал, что они действительно продают дыроколы по 15 долларов за штуку. Могли ли вы в 12 лет убедительно выпросить у матери 15 долларов? Уже на следующий день я купил в магазине дырокол. Однако это был только Первый Шаг. Где мне раздобыть непробитые талоны?

Хорошо, а где моют автобусы? Я пошел в ближайший автопарк, нашел недалеко большой мусорный ящик, заглянул внутрь...

Джекпот!

Я набил карманы талонными книжками, в которых была масса непробитых билетов. Это был мой первый, и далеко, далеко не последний опыт в том, что позднее назовут «дампстер-дайвингом» – копанием по мусоркам в поисках чего-нибудь ценного.

Память у меня всегда была отличной. Мне удалось запомнить расписание большинства автобусов долины Сан-Фернандо. Я стал ездить на них повсюду, куда только можно было доехать: округ Лос-Анджелес, округ Риверсайд, округ Сан-Бернардино. Я наслаждался видами этих разнообразных мест, осматривая окружающий мир⁵.

В своих странствиях я познакомился с мальчишкой

⁵ В оригинале – игра слов. Take in на американском английском означает «осматривать достопримечательности», а на литературном английском – «обманывать».

Ричардом Уильямсом. Он делал то же, что и я, но с двумя существенными отличиями. Во-первых, Ричард мог ездить бесплатно на вполне законных основаниях: его катал отец, который был водителем автобуса. Второе, что нас отличало (по крайней мере, поначалу) – разница в весе. Ричард был очень грузным. По пять-шесть раз в день он хотел заглянуть в фастфудную Jack in the Box⁶ и слопать там Супер Тако. Я почти сразу перенял его привычку неправильно питаться и стал толстеть.

Вскоре и какая-то блондиночка с косичками, с которой мы вместе ездили на автобусе в школу, сказала: «Ты так-то милый, но жирок мешает. Тебе бы похудеть.»

Думаете, я последовал ее грубому, но, бесспорно, дельному совету? Нет, конечно!

Не возникло ли у меня проблем из-за лазанья по мусоркам, махинаций с пересадочными талонами и бесплатным катанием? Ни малейших. Мама хвалила мою находчивость, отец видел в этом проявление инициативности, а водители автобусов, знавшие, что я сам пробиваю себе билеты, находили это очень забавным. Будто все вокруг только и говорили: «Какой молодец!»

Но я и без чужих восхищений моими шалостями шел бы по скользкой дорожке. Мог ли кто-нибудь подумать, что простой поход за покупками преподаст мне урок и заставит сде-

⁶ Популярная американская сеть фастфуда с похожим на McDonalds ассортиментом.

лать на жизненном пути серьезный поворот, который вел в
нерадужное будущее.

Глава 2

Просто посмотреть

*Wbth lal voe htat oy voe wxbirtn vfzbqt wagye C poh
aeovsn vojgav?*⁷

Многие еврейские семьи, которые не отличаются религиозностью, все равно хотят, чтобы сын прошел обряд бар-мицвы⁸. Я был как раз таким сыном. Во время обряда мальчик стоит перед членами общины и читает отрывок из свитка Торы на иврите. Как известно, в иврите используется особый алфавит, с такими символами, как ם , ן , ך и т. п. этому на то, чтобы выучить фрагмент из Торы, может уйти несколько месяцев.

Я был зачислен в еврейскую религиозную школу в Шерман-Оукс, но меня выгнали за то, что я валял дурака на уроках. Тогда мама устроила мне индивидуальные занятия с кантором, и я больше не мог читать техническую литературу под столом. Мне удалось выучить отрывок достаточно хорошо и выполнить свой долг. Я вслух прочитал этот фрагмент перед общиной, запинаясь не более, чем обычно, и не

⁷ Как называлась та центральная телефонная станция, где меня почти поймали?

⁸ Бар-мицва – церемония, которую проходит еврейский мальчик, достигший 13 лет. С этого момента он считается взрослым и обязан исполнять все заповеди Торы.

оконфузился.

Позже родители ругали меня за то, что я пытался передразнивать акцент и жестикуляцию раввина. Однако я это делал подсознательно. Потом узнал, что такая техника очень эффективна, поскольку человека привлекают люди, похожие на него. Так в юном возрасте совершенно неосознанно я уже занимался тем, что позже стало называться социальной инженерией. Эта ненамеренная или намеренная манипуляция заставляла людей делать вещи, которые они не сделали бы сами по себе. Убеждать их, что так и надо, не вызывая подозрений.

Потом на приеме в ресторане «Одиссей» на меня пролился целый дождь подарков от родственников и других свидетелей бар-мицвы. Среди этих подарков я получил и несколько долгосрочных облигаций банка США, которые составили в денежном выражении удивительно кругленькую сумму.

Будучи жаждущим читателем с особыми вкусами, я набрел на книжный магазин Survival в Северном Голливуде – небольшую лавку в бедноватом районе. Заведовала ею молодая приветливая дама-блондинка, она разрешила обращаться к ней по имени. Там я словно обнаружил пиратский клад. В те годы моими кумирами были Брюс Ли, Гарри Гудини и Джим Рокфорд – крутой сыщик, которого блестяще сыграл Джеймс Гарнер в сериале «Досье детектива Рокфорда». Рокфорд умел взламывать замки, манипулировать людьми и выдавать себя за другого человека в считанные секунды. Я

очень хотел научиться всем этим классным трюкам.

В магазине Survival нашлись книги о том, как овладеть всеми приемами Рокфорда, и не только. С 13 лет я проводил здесь многие выходные, читая целыми днями одну книгу за другой. Например, книгу Барри Рейда «Путешествие с бумажкой». В ней рассказывалось, как создать себе новую личность при помощи свидетельства о рождении уже умершего человека.

В книге «Игра в Большого брата» за авторством Скотта Френча были инструкции, как завладеть личным делом водителя, выписками из имущественного реестра, кредитными историями, данными о банковском счете, засекреченными телефонными номерами и даже про то, как выуживать информацию из полицейских участков. Позже, когда Френч писал второй том, он позвонил мне и поинтересовался, не хочу ли я написать главу о социальной инженерии при манипулировании телекоммуникационными компаниями. В то время мы с соавтором как раз писали нашу вторую книгу «Искусство проникновения». Я был слишком занят, чтобы поучаствовать в проекте Френча, но меня позабавило такое совпадение, а сама просьба льстила.

Как вы уже поняли, магазин ломился от подпольной литературы – книг, которые учили запретным вещам. Мне это очень нравилось, так как всегда страшно хотелось сорвать такой запретный плод с дерева. Я впитывал знания, которые оказались просто бесценными через 20 лет, когда я был в

бегах.

Помимо книг меня привлекли и другие их товары – наборы отмычек. Я купил несколько разных видов.

Есть известный американский анекдот: «Как же попасть в Карнеги-Холл?» (Престижнейший Нью-Йоркский концертный зал)

Ответ: «Практика, практика, практика!»⁹

Именно на практике я постигал искусство вскрытия замков. Находил время и спускался в общий гараж нашего дома, где было множество ячеек для временного хранения вещей. Все они запирались на всякие замки. Там я их вскрывал, менял местами и снова закрывал. Тогда эти проделки казались мне веселыми розыгрышами, но теперь я понимаю, что вызвал у многих людей праведный гнев и доставил им немало хлопот, не говоря уже о тратах на новый замок после снятия старого. Все это кажется смешным только подростку.

Однажды, когда мне было около 14, мы гуляли с дядей Митчеллом, который тогда являлся для меня примером для подражания. Мы отправились в службу регистрации транспортных средств, внутри было полным-полно народу. Дядя велел мне подождать, а сам пошел регистрироваться (да, так и пошел мимо длинной очереди).

Скучающая дама в окошке с удивлением взглянула на

⁹ Игра слов: Спрашивающий хочет просто пройти к зданию, а собеседник дает ответ, что нужно делать, чтобы попасть туда как исполнитель – оттачивать свое мастерство.

него. Дядя не дал ей закончить работу с мужчиной перед ним и просто начал говорить. Стоило ему сказать всего несколько слов, как женщина кивнула, попросила мужчину пропустить дядю и зарегистрировала его. Мой дядя умел находить подход к людям.

Кажется, и у меня был такой талант. Это оказался первый на моей памяти практический пример социальной инженерии.

Как ко мне относились люди в средней школе Монро? Учителя сказали бы, что я всегда вытворял какие-то неожиданные вещи. Пока другие ребята относили телевизоры для починки в ремонтные мастерские, я шел по стопам Стива Джобса и Стива Возняка и стал сам делать синюю коробку, помогающую мне манипулировать телефонной сетью и даже бесплатно звонить. Я всегда брал с собой в школу портативную рацию и говорил по ней во время обеда и на переменах.

Однако один из однокашников задал моей жизни новый курс. Стивен Шалита был высокомерным парнем и воображал себя полицейским под прикрытием. Его машину просто окутывали радиоантенны. Стивену нравилось демонстрировать фокусы, которые он умел проделывать с телефоном. Честно говоря, умел он немало. Шалита показывал, как принимать звонки, не раскрывая свой настоящий номер, используя «петлю» – тестовый канал телекоммуникационной компании. Он звонил на один номер, присвоенный этой петле, а собеседник звонил на второй. Между двумя абонентами на

линии как по волшебству возникало соединение. Стивен мог узнать имя и адрес обладателя любого телефонного номера, как общедоступного, так и секретного. Для этого нужно было позвонить в Службу имен и адресов (CNA) телефонной компании. Так после одного-единственного звонка он узнал номер моей мамы, а его не было в справочнике. Вот это фокус! Стивен мог узнать любой телефонный номер и адрес, даже кинозвезды. Казалось, весь штат телефонной компании только и ждет, чтобы ему помочь.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.