


**КЕВИН МИТНИК**

ВИЛЬЯМ Л. САЙМОН

ПРИЗРАК В СЕТИ

**МЕМОУАРЫ  
ВЕЛИЧАЙШЕГО  
ХАКЕРА**

3-е издание

 **БОМБОРА**  
ИЗДАТЕЛЬСТВО  
Москва

# Оглавление

<b>Предисловие</b> .....	8
<b>Пролог</b> .....	10
<b>Часть I. Рождение хакера</b> .....	15
Глава 1. Жесткий старт .....	15
Глава 2. Просто посмотреть .....	22
Глава 3. Первородный грех .....	40
Глава 4. Мастер выпутываться .....	59
Глава 5. Все ваши телефонные линии теперь мои ...	73
Глава 6. Взлом во имя любви .....	86
Глава 7. Поспешная свадьба .....	99
Глава 8. Лекс Лютор .....	112
Глава 9. Льготный тарифный план для Кевина Митника .....	142
Глава 10. Таинственный хакер .....	153
<b>Часть II. Эрик</b> .....	161
Глава 11. Подозрительная смерть .....	161
Глава 12. Тебе не скрыться .....	168
Глава 13. Перехватчик .....	182
Глава 14. Вы следите за мной, я слежу за вами ...	190
Глава 15. «Как, черт возьми, вы это достали?» ...	206
Глава 16. Непрошенный визит на личную вечеринку Эрика .....	215
Глава 17. Приоткрывая занавес .....	220
Глава 18. Анализ трафика .....	233
Глава 19. Разоблачения .....	241
Глава 20. Обратное жало .....	248
Глава 21. Кошки-мышки .....	255

Глава 22. Расследование .....	265
Глава 23. Обыск .....	280
Глава 24. Исчезновение .....	290
<b>Часть III. В бегах .....</b>	<b>303</b>
Глава 25. Гарри Гудини .....	303
Глава 26. Частный детектив .....	314
Глава 27. Когда дело дошло до Sun .....	328
Глава 28. Охотник за трофеями .....	344
Глава 29. Отъезд .....	364
Глава 30. Удар исподтишка .....	385
Глава 31. Глаза в небе .....	397
Глава 32. Неспящие в Сиэтле .....	419
<b>Часть IV. Конец и начало .....</b>	<b>439</b>
Глава 33. Хакер против самурая .....	439
Глава 34. Скрываясь в Библейском поясе .....	450
Глава 35. Игра окончена .....	472
Глава 36. Валентинка от ФБР .....	481
Глава 37. Как выиграть, поставив на козла отпущения .....	490
<b>Послесловие. Что было после того, как судьба сменила гнев на милость .....</b>	<b>521</b>
<b>Благодарности .....</b>	<b>534</b>
От Кевина Митника .....	534
От Билла Саймона .....	541
<b>Биография автора .....</b>	<b>543</b>

*Моей маме и бабушке*  
*К. Д. М.*

*Аринн, Виктории и Дэвиду, Шелдону, Винсенду*  
*и Елене Роуз и в особенности Шарлотте*  
*У. Л. С.*

# 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 устройство, 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 похождениях. 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 авантюры Кевина Митника.

*Стив Возняк,  
соучредитель Apple Inc.*

# Пролог

**Ф**изический 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 пропуски. 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 ходил 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 сотрудников 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 звукопроницаемыми 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 поделщик залезает на стол.

Я хватаю его за ноги и поднимаю достаточно высоко. Ему удастся приподнять звуконепроницаемую пластину. Я нагибаюсь, 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, вошедшего 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 «радужные 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 проблема. 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 проскальзывал 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, Куамамото, 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 pcog qh vjg uauvgo wugf da jco qrgtcvqtu  
vq ocmg htgg rjqpg ecnnu?*<sup>1</sup>

**М**ой 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 начинался 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.

---

<sup>1</sup> 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](http://fabiensanglard.net/Ghost_in_the_Wires/index.php)) — *Здесь и далее примечания переводчика.*

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 лиге<sup>1</sup>, 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

---

<sup>1</sup> Лига для мальчиков и девочек 8–12 лет.

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 покупать на фокусы. Это ошеломляющее открытие изменило всю мою жизнь.

Лавка волшебника, расположенная от нас на расстоянии 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»<sup>1</sup>. 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

---

<sup>1</sup> «CBers» — это пользователи радиосвязи «гражданского диапазона». Сам диапазон называется «Citizen's Band» или сокращено «CB» (Си Би). СВ доступен по дешевой (а часто бесплатной) лицензии. Надпись на футболке в шуточной форме сообщала о заинтересованности человека любительской радиосвязью.

письменный экзамен. Освоил и азбуку Морзе, по крайней мере столько, чтобы соответствовать требованиям. Вскоре почтальон принес конверт из Федеральной комиссии 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 разбираться 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 пригодились 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.

---

---

Несколько недель я ходил в вечернюю школу. Там вдумчиво изучал схемы и нормы любительского радио, чтобы сдать письменный экзамен.

---

---

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*