СОДЕРЖАНИЕ

К РУССКОМУ ИЗДАНИЮ

О чем эта книга, кратко можно сформулировать так: она об аналитической силе простых средств. Информация доступна, и с ее помощью можно сделать все что угодно. Доступность информации в сочетании с несложными манипулятивными приемами открывает любые двери.

В 1947 году, когда начиналась холодная война, основатель аналитической разведки Шерман Кент заявил, что в мирное время 80% данных для политических решений можно добыть в открытых источниках*. Уже выйдя на пенсию, бывший директор Разведуправления Министерства обороны США скорректировал эту оценку: 90% открытых источников и лишь 10% — агентурных операций**. Раньше пользовались газетами, журналами, ведомственными брошюрами, проспектами с выставок и телефонными справочниками. Сейчас все стало еще легче: к перечисленному добавились корпоративные сайты и социальные сети; смартфоны сопровождают фотографии геотегами, а для сбора данных о контактах любого человека достаточно просмотреть список его друзей.

Открытые источники дают огромную власть и одновременно делают вас крайне уязвимым. Информации из открытых источников достаточно, чтобы узнать об актив-

---

* Allen W. Dulles. Memorandum Respecting Section 202 (Central Intelligence Agency) of the Bill to Provide for a National Defense Establishment, April 25, 1947, p. 525.

** Donna O'Harren, "Opportunity Knocking: Open Source Intelligence For the War on Terrorism," Thesis, Naval Postgraduate School, December 2006, p. 9.

ном человеке почти все. Как? Однажды я потерял контакт с коллегой, с которым долго сотрудничал. Он удалил свою почту, профиль в Facebook и даже счет на PayPal. Но, когда потребовалось, я нашел его… по списку любимых книг. Можно сменить фамилию, переехать в другую страну и устроиться в международную организацию, но нельзя отказать себе в удовольствии отметиться под книгой, над которой работал. Сочетание русских и английских книг выдавало переводчика, а потом обнаружилось подтверждение — комментарий, в котором проскользнуло настоящее имя владельца аккаунта. Мы снова сотрудничаем, но мой коллега заволновался: только ли я смог проследить его связи со старой жизнью? Информация под руками, и все вполне законно — нужно лишь комбинировать данные.

В другом случае открытые данные пришлось сочетать с импровизацией. Моего приятеля, пожилого уже человека, обманули при покупке в интернете. Он перевел деньги по номеру телефона, после чего продавец попросту перестал отвечать на звонки. Мы перевели один рубль по тому же телефону, и через интерфейс онлайн-банка узнали его имя, отчество и первую букву фамилии. Затем я позвонил на тот же телефон через Skype:

— Иван Иванович, здравствуйте. Вас выбрали присяжным на процесс по делу о коррупции. Вы сможете явиться в Тверской городской суд послезавтра? Повестку мы пришлем.

— Но я живу в Туле.

— Вы ведь Иванов?

— Нет, я Петров.

— Простите, вечно у нас всё путают.

Мы нашли «Петрова» в соцсети, со всеми родственниками. Приятель по-стариковски обратился к его отцу. Тот оказался человеком понимающим, извинился, а через 15 минут извинялся сам незадачливый обманщик. Да, мы имели дело с неопытным мелким мошенником, который не умел прятаться, но,

во-первых, большинство из нас и не думает скрывать информацию о себе, а во-вторых, нельзя не пожалеть воришку — он показался мне таким беззащитным и в общем неплохим человеком.

Ну а вот дело посерьезнее. Работая с бухгалтерскими системами десять лет назад, мы не спрашивали пароли у владельцев рабочих мест: они были одинаковыми. Сегодня изощренные программы заставляют менять пароли и требуют фраз потруднее. Их трудно запомнить, но творческие бухгалтеры находят выход — они записывают пароли на обратной стороне клавиатуры. Злоумышленнику ничего не стоило проникнуть в нужный офис, устроившись на работу в клининговую компанию. Минимальная зарплата, текучка, уборщики меняются чуть ли не каждый день, да и кто замечает столь незначительного человека? А уж сфотографировать с экрана компьютера список крупных дебиторов — дело нескольких секунд. Простейшая разведка, дерзкая афера и банальная беспечность привели к невосполнимой потере рыночных позиций.

Читая «Искусство обмана», я переживал моральную коллизию. С одной стороны, автор учит использовать добро как слабость, тем самым обесценивая его. С другой — знание защищает. Описанные Кристофером Хэднеги методики сильны, но в то же время они и шаблонны. Как в фокусах иллюзиониста, их сила развеивается перед тем, кто знает секрет. Отрадно, что мошенники не умнее своих жертв, у них просто другие цели. Ввиду этого книга воспринимается совсем иначе. Она дает свободу совершать осознанные поступки, а не следовать манипуляциям, свободу ограничивать доступ к информации о себе, свободу частной жизни.

При редактирования перевода нам приходилось принимать решения о выборе слов для обозначения часто встречающихся терминов. В конечном счете он сводился к тому, предназначать ли книгу для узкого круга людей, тесно связанных

с социальной инженерией, или делать ее понятной для всех. Мы выбрали второе. Надеемся на понимание читателей, для которых профессиональный жаргон стал родным — за «сбором данных из открытых источников» они узнают OSINT, за «легендой» — претекст и т. д.

Денис Букин,
психолог, психотерапевт,
автор книги «Развитие памяти по методикам спецслужб»

ОБ АВТОРЕ

Кристофер Хэднеги — генеральный директор компании Social-Engineer, LLC. Он ведущий разработчик и создатель первого систематизированного поискового интернет-ресурса, посвященного социальной инженерии, http://www.social-engineer.org. Хэднеги — основатель так называемой Деревни социальной инженерии (Social Engineering Village, или SEVillage) на конференциях DEF CON и DerbyCon* и разработчик популярной игры «Захват флага»**, предназначенной для социальных инженеров (Social Engineering Capture The Flag — SECTF). Кристофер — востребованный во всем мире спикер и тренер: он выступал на таких мероприятиях, как RSA, Black Hat, DEF CON, и даже получал приглашение проводить консультации в Пентагоне. В Twitter он пишет под ником @humanhacker.

---

* Крупные конференции хакеров и специалистов по информационной безопасности. DEF CON проводится в Лас-Вегасе с 1993 года, DerbyCon — с 2011 года в Луисвилле. — *Прим. науч. ред.*

** «Захват флага» (Capture the Flag) — командная игра, участники которой стремятся захватить «флаг» соперника. В разных вариантах игры «флагом» может быть что угодно: настоящий флаг, предмет или информация. В книге речь идет об игре для специалистов по информационной безопасности, в которой игроки либо выполняют задания по взлому защиты, либо охраняют свои серверы, атакуя при этом серверы противников. «Флагом» здесь становится информация, которую надо выкрасть у других и защитить у себя. Сайт игры в России: https://ctfnews.ru. — *Прим. науч. ред.*

О ТЕХНИЧЕСКОМ КОНСУЛЬТАНТЕ

Мишель Финчер — глава отдела информационной безопасности в химической компании. Уже больше 20 лет она занимается изучением человеческого поведения, а также является специалистом по информационной безопасности. Мишель специализируется на изучении психологических основ принятия решений, связанных с безопасностью, особенно в контексте социальной инженерии.

В роли тренера и спикера по различным техническим и поведенческим аспектам она выступала перед специалистами правоохранительных органов и разведки, а также в частном секторе, в том числе на таких мероприятиях, как Black Hat Briefings, RSA, SourceCon, SC Congress, Interop и Techno Security.

Мишель получила степень бакалавра в области проектирования с учетом человеческого фактора в Академии ВВС США, а также степень магистра в сфере консультирования в Обернском университете. Она является сертифицированным специалистом в сфере информационной безопасности (CISSP).

БЛАГОДАРНОСТИ

«Всего несколько лет назад мы с моим другом и учителем Мати Ахарони решили запустить сайт http://www.social-engineer.com» — такими словами начиналось первое издание книги «Искусство обмана: Социальная инженерия в мошеннических схемах». Сегодня, когда я перечитываю эти строки, мне кажется, что я сплю, вот-вот проснусь — и смутное воспоминание о том времени растворится. Я часто размышляю над тем, что случилось со мной за 12 лет, прошедших с выпуска того издания, и особенно о событиях последних восьми лет, которые нашли отражение в этой книге.

За восемь лет мне довелось поработать с Полом Экманом, Робином Дрейке, Нилом Феллоном и прочими прекрасными людьми. Мне выпала честь брать интервью у Роберта Чалдини, Эми Кадди, Дова Бэрона, Эллен Лангер, Дэна Ариели и многих других выдающихся личностей. Мне посчастливилось выступать с Аполло Роббинсом и встретиться с Уиллом Смитом. Меня приглашали в Великобританию тренировать агентов MI5 и MI6. С точки зрения социальной инженерии я анализировал работу 35 генералов в Пентагоне, а также глав государств и других людей, обладающих властью.

Последние восемь лет были похожи на американские горки. Но, как говорится, один в поле не воин, так что этот опыт, удивительные знакомства и вся моя жизнь сложились именно так, а не иначе, благодаря людям, которые помогали мне. Моя жена Ариса — одна из самых терпеливых и прекрасных женщин, которых мне довелось встретить в жизни. И хотя ей

чужд мир социальной инженерии, который стал для меня уже родным, она меня любит и всегда поддерживает. Благодаря Арисе моя жизнь полна смеха, приключений и счастливых воспоминаний.

Когда мой сын Колин был маленьким, он собирался стать врачом, потом писателем, а потом волонтером. Удивительно, он действительно попробовал себя в писательском деле и уходе за нуждающимися, а волонтерством занимается и сейчас. Его позитивный настрой и доброжелательность всегда были для меня примером.

Помню, как клялся: никогда близко не подпущу свою дочь Амайю к социальной инженерии: уж она-то будет жить в полной безопасности. Но Амайя ясно показала мне, что обеспечить ее безопасность я могу, только обучая своему делу и вовлекая в свою работу. Впрочем, она научила меня намного большему, чем я ее.

Хотя Пол Экман напрямую не участвовал в создании этой книги, его доброта, энтузиазм и щедрость меня очень вдохновили. Благодарю его за это.

Я также хочу поблагодарить всех людей, которые сопровождали меня на моем пути:

Пинг Лук — он всегда готов бескорыстно поддержать и помочь советом.

Дружба Дейва Кеннеди и его поддержка дали мне очень многое.

Хочу также поблагодарить членов фонда «Невинные жизни» (ILF) — они были неотъемлемой частью процесса.

Никогда бы не подумал, что мы с Нилом Фэллоном станем друзьями (ущипните меня). Но теперь он помогает мне, направляет и поддерживает меня. И главное — напоминает, что значит быть человеком.

ILF возник во многом благодаря поддержке и защите Тима Мэлони. Невозможно найти слова, чтобы выразить степень моей благодарности за его дружбу, веру и поддержку.

Энтузиазм Кейси Холл и ее стремление во что бы то ни стало найти решение, надо признать, очень заразительны.

Я благодарю Эй Джей Кук за помощь фонду и за то, как легко оказалось с ней работать. Ее преданность нашей общей цели спасения детей можно ставить в пример.

Профессиональная этика, доброта и способность сосредоточиться Аиши Тайлер делают ее примером для всех нас (даже ее имя кажется каким-то нереальным).

У меня в Social-Engineer, LLC, работает отличная команда. Колин, Майк, Кэт, Райан, Аманда, Каз, Джен и Карен — каждый из вас помог мне стать лучше и поддерживал меня. Спасибо!

Мне очень повезло с редактором этой книги, Шарлоттой. Иногда вообще казалось, что она может написать ее за меня — так легко Шарлотта понимала мои мысли и так умно помогала их выразить (вот уж работка, не позавидуешь!).

Читатели моих книг, ценители проекта Social-Engineer Podcast, посетители нашей Деревни SEVillage на конференциях и других мероприятиях, посвященных социальной инженерии! Благодаря вам моя планка поднялась очень высоко. Вы не боялись указывать мне на глупые ошибки и тем самым мотивировали меня постоянно развиваться. Благодарю!

ПРЕДИСЛОВИЕ

Когда в 1976 году мы со Стивом Джобсом основали Apple Computers, я и представить себе не мог, насколько это событие изменит мир. Тогда меня увлекла фантастическая идея: создать персональный компьютер, с которым мог бы самостоятельно работать отдельный пользователь. Прошло всего-то 40 с небольшим лет, а замысел уже давно воплотился в жизнь. По всему миру работают миллиарды ПК, смартфонов и других умных устройств, технологии проникли в самые разные аспекты нашей жизни. Теперь пришло время сделать шаг назад и подумать, как сохранить безопасность, не убивая при этом дух инноваций, продолжая развиваться и взаимодействовать с новыми поколениями.

Мне нравится работать с молодежью, вдохновлять ее на инновации и рост. Нравится смотреть, как загораются глаза молодых, когда у них появляются новые идеи и творческие решения по использованию технологий. Я просто обожаю следить за тем, как эти технологии улучшают нашу жизнь.

При этом я понимаю: для того чтобы будущее, которое мы строим, было безопасным, нужно потрудиться. В своей вступительной речи на конференции HOPE в 2004 году я говорил, что часто за компьютерными взломами стоит манипулирование: людей заставляют совершать весьма странные поступки. За годы работы в сфере безопасности мой друг Кевин Митник освоил искусство, которое принято называть социальной инженерией.

В книге Криса раскрыта суть социальной инженерии: это явление описано и разложено по полочкам в доступной форме. В новом издании также отражены принципы принятия решений и особенности манипулирования этим процессом.

Взломом компьютерных систем уже давно никого не удивишь, а манипуляции и вовсе существуют столько же, сколько и человечество. Эта книга научит вас обороняться от них, а также понимать и предотвращать связанные с социальной инженерией риски.

Стив Возняк

ВВЕДЕНИЕ

Я помню времена, когда в интернете по запросу «социальная инженерия» выпадали ссылки на видео о том, как получать бесплатно бургеры или заманить девушку на свидание. Сегодня же этот термин вошел в обиход и для краткости обозначается аббревиатурой СИ. Буквально на днях подруга нашей семьи (человек, бесконечно далекий от темы информационной безопасности) рассказывала о схеме мошенничества с использованием электронной почты. И резюмировала: «Согласитесь, отличный пример социальной инженерии!»

Я на секунду опешил. Но чему удивляться: восемь лет назад, когда я открыл компанию, сосредоточенную исключительно на социальной инженерии, это было в новинку, но сегодня СИ превратилась в полноценную отрасль.

Возможно, название этой книги могло сформировать у вас неправильное представление о моих намерениях: будто я собираюсь научить «плохих парней» воплощать в жизнь их дурные намерения. Но нет, это диаметрально противоположно истине.

Когда я взялся писать свою первую книгу, многие не одобряли эту затею: переживали, что я сослужу добрую службу недобрым людям. Но и тогда (как и сейчас) я понимал, что, прежде чем защищаться от социальной инженерии, надо разобраться во всех ее проявлениях. Ведь она как молоток, лопата, нож или пистолет. Каждый из этих предметов можно использовать для того, чтобы создавать, спасать, кормить, выживать. Но ими же можно калечить, убивать, разрушать. Чтобы понять,

как использовать социальную инженерию в благих целях, нужно разобраться и с ее деструктивным применением. Это особенно актуально для тех, чья задача — защищать. Чтобы уберечь себя и других от применения социальной инженерии во вред людям, нужно сначала заглянуть «на темную сторону».

Недавно я расспрашивал актрису Эй Джей Кук о ее работе в сериале «Мыслить как преступник». Она сказала, что в процессе подготовки к роли Джей-Джей не раз встречалась с реальными агентами ФБР, которые расследовали преступления серийных убийц. Так вот, моя книга написана по такому же принципу.

Читая ее, отбросьте предвзятость: я изложил все знания, опыт и практические наблюдения, которые собрал за последние десять лет работы в СИ. Конечно, здесь, как и в любой книге, могут обнаружиться ошибки. Возможно, какая-то информация вам не понравится или окажется не до конца понятной. Я всегда готов к дискуссии, только дайте знать! Найти меня можно на Twitter под ником @humanhacker. Или же пишите мне на электронные адреса, указанные на сайте http://www.social-engineer.org или http://www.social-engineer.com.

Когда я провожу пятидневный курс обучения СИ, то всегда прошу посетителей ни в коем случае не думать, будто я никогда не допускаю ошибок. Я только рад обсуждению, когда выясняется, что знания и соображения слушателей противоречат моим утверждениям, или если кому-то просто кажется, что я говорю не то. Я обожаю учиться, расширять и углублять понимание темы. Поэтому и вас прошу относиться к изложенной в книге информации критически.

Наконец, я хочу сказать вам спасибо. За то, что потратили свое бесценное время на прочтение этой книги. За то, что за последние годы вы помогли мне стать намного лучше. За обратную связь, идеи, критику и советы.

Надеюсь, книга вам понравится.

Кристофер Хэднеги

1 Заглянем в *новый* мир социальной инженерии

Пожалуй, успех — это залог безопасности,
а хороший вкус — залог успеха.

Гордон Рамзи

Я отчетливо помню, как на экране моего компьютера появился первый абзац книги «Искусство обмана: Социальная инженерия в мошеннических схемах». Это было в *далеком* 2010 году. Так и хочется сказать, что в те древние времена рукописи набирались на печатной машинке, но так и быть, не стану драматизировать.

В те годы, введя в поисковую строку запрос «социальная инженерия», вы могли найти лишь пару страниц о самом известном специалисте в этой области, Кевине Митнике, да еще пару видео о том, как соблазнить девушку или получить бесплатные бургеры в McDonald's. Прошло восемь лет — и термин вовсю используется в повседневной жизни. В последние три-четыре года я неоднократно подмечал, как приемы из социальной инженерии используются в сфере безопасности, управления, образования, психологии, в военных организациях — словом, везде, где только можно представить.

Волей-неволей захочешь разобраться в причинах таких масштабных изменений. Один коллега сказал мне: «Так ты сам в этом виноват, Крис». Похоже, он говорил с укором, но я ощутил гордость. Впрочем, не один я несу ответствен-

ность за то, что сегодня повсеместно используется термин *социальная инженерия*. Полагаю, он вошел в обиход не только потому, что это самый простой способ атаки на системы безопасности различных компаний (как считалось семь лет назад), но и потому что сейчас атакующие получают самые большие прибыли. Себестоимость такой прибыльной атаки мала, риски — и того меньше. Окупаемость получается *огромной*. Моя команда собирает новости об атаках, проведенных с применением социальной инженерии, и связанную с ними статистику. И я с уверенностью могу сказать, что в 2017 году более 80% случаев взлома систем безопасности включали в себя тот или иной элемент СИ.

Согласно исследованию «Стоимости утечки данных», опубликованному IBM в 2017 году, из-за одной подобной утечки компании теряли порядка $3,62 млн. Понятно, почему мошенники с удовольствием используют СИ: ставки слишком высоки.

СОВЕТ ПРОФИ **К 2017 году IBM выпускали такие исследования уже 12 лет подряд. Скачать последнее из них можно по ссылке https://www-03.ibm.com/security/data-breach/. Или же просто ввести в строку поисковика запрос: «IBM, стоимость утечки данных».**

Помню первое интервью, которое я дал после публикации предыдущего издания этой книги в 2010 году. Меня спросили: «Не боитесь ли вы, что ваши советы возьмут на вооружение “плохие парни”?» Нет, не боюсь. Потому что отношусь к СИ как любому новому типу вооружения: все зависит от того, как его использовать.

В связи с этим мне вспоминается история, как в 1960-х Брюс Ли оказался в Америке. Тогда были сильны расовые предрассудки, а он взялся за дело, которым до него не занимался никто: обучал представителей всех рас, с любым цветом кожи,

и национальностей древнему китайскому боевому искусству джиткундо. Он часто участвовал в турнирах со студентами своего университета. Те думали, что знают толк в драках, но Брюс, ко всеобщему удивлению, клал на обе лопатки одного соперника за другим. Многие из них потом стали его друзьями или учениками.

Для чего я привожу этот пример? Чтобы показать: людям пришлось адаптироваться к новому типу ведения борьбы, в противном случае они были обречены на поражение. Мог ли кто-то из учеников Брюса Ли использовать полученные навыки, чтобы навредить другим людям? Конечно. Тем не менее Брюс передавал свои знания, потому что понимал: он должен учить людей защищаться.

Поэтому на вопрос, не боюсь ли я, что такая важная информация окажется на вооружении у «плохих парней», я отвечаю так же, как и восемь лет назад. Я не могу управлять тем, как читатели будут использовать полученные знания. Кто-то прочтет эту книгу и бросится применять описанные методы, чтобы красть деньги. А кто-то использует эти знания, чтобы защититься и для достижения благих целей. Ведь и «хороших парней» кто-то должен обучать. Одним словом, выбор за вами.

Чтобы противостоять противнику, владеющему новым стилем борьбы, недостаточно наловчиться принимать удары. Как и осваивая джиткундо, вам нужно будет разобраться в искусстве нападения и защиты, понимать, когда уместно одно, а когда — другое. Обучаясь социальной инженерии, придется научиться думать, как «плохие парни» (помня при этом, что вы к ним не относитесь). Раз уж я начал приводить аналогии, вот еще одна: нужно уметь использовать силу, но не переходить на темную сторону.

А сейчас вы, наверное, думаете: «Раз его мнение не изменилось, зачем он издает новую версию книги?». Сейчас расскажу.