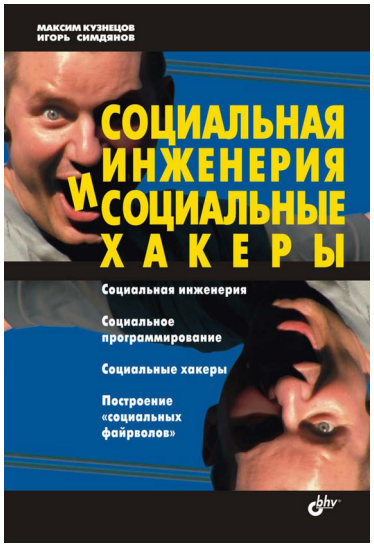
МАКСИМ КУЗНЕЦОВ
ИГОРЬ СИМДЯНОВ
СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ И СОЦИАЛЬНЫЕ ХАКЕРЫ
Социальная инженерия
Социальное программирование
Социальные хакеры
Построение «социальных файрволов»
bhv

**Игорь Вячеславович Симдянов**
**Максим Валерьевич Кузнецов**

# Социальная инженерия и социальные хакеры

*http://www.litres.ru/pages/biblio_book/?art=6657922*
*Максим Кузнецов, Игорь Симдянов. Социальная инженерия и социальные хакеры: БХВ-Петербург; Санкт-Петербург; 2007*
*ISBN 5-94157-929-2*

## Аннотация

Прием, когда хакер атакует не компьютер, а человека, работающего с компьютером, называется социальной инженерией. Социальные хакеры – это люди, которые знают, как можно "взломать человека", запрограммировав его на совершение нужных действий.

В книге описан арсенал основных средств современного социального хакера (трансактный анализ, нейролингвистическое программирование), рассмотрены и подробно разобраны многочисленные примеры социального программирования (науки, изучающей программирование поведения человека) и способы защиты от социального хакерства. Книга будет полезна IT-специалистам, сотрудникам служб безопасности предприятий, психологам, изучающим социальную инженерию и социальное программирование, а также пользователям ПК, поскольку именно они часто выбираются социальными хакерами в качестве наиболее удобных мишеней.

Для широкого круга читателей.

# Содержание

Введение 4
Для кого и о чем эта книга 4
Благодарности 7
Часть I 8
Глава 1 9
Основная схема воздействия в социальной инженерии 12
Основные отличия социальной инженерии от социального программирования 17
Глава 2 21
Об истории социальной инженерии 21
Основные области применения социальной инженерии 21
Финансовые махинации 22
Информация о маркетинговых планах организации 28
Воровство клиентских баз данных 36
Фишинг 39
Фарминг 42
Рейдерские атаки 42
Глава 3 49
"Пожар" в кинотеатре 49
Как сделать "соляной кризис" методами социального программирования 51
Венки на трассе 53
Конец ознакомительного фрагмента. 55

# Максим Кузнецов, Игорь Симдянов Социальная инженерия и социальные хакеры

## Введение

## Для кого и о чем эта книга

Предметом книги является рассмотрение основных методов социальной инженерии – по мнению многих исследователей одного из основных инструментов хакеров XXI века. По своей сути, это книга о роли человеческого фактора в защите информации. О человеческом факторе в программировании выходило несколько хороших книг, одна из них, книга Ларри Константина, так и называется "Человеческий фактор в программировании". Это, пожалуй, единственная книга на данную тему, переведенная на русский язык. Вот что пишет автор в предисловии к этой книге: "Хорошее программное обеспечение создается людьми. Так же как и плохое. Именно поэтому основная тема этой книги – не аппаратное и не программное обеспечение, а человеческий фактор в программировании (peopleware)". Несмотря на то, что книга Л. Константина скорее по психологии, чем по программированию, первое издание книги было признано классическим трудом в области информационных технологий.

Информация тоже защищается людьми, и основные носители информации – тоже люди, со своим обычным набором комплексов, слабостей и предрассудков, на которых можно играть и на которых играют. Тому, как это делают и как от этого защититься, и посвящена данная книга. Исторически так сложилось, что хакерство с использованием человеческого фактора называют *"социальной инженерией"*, поэтому наша книга так и называется "Социальная инженерия и социальные хакеры".

Защититься от социальных хакеров можно только зная их методы работы. Наша цель, как авторов книги, – ознакомить читателей с этими методами, чтобы лишить социальных хакеров их главного козыря: неискушенности их жертв в вопросах мошенничества и методах скрытого управления человеком. Мы также надеемся, что изучение материала книги будет полезным для читателей не только в профессиональном, но и в жизненном плане. Ведь изучение тех разделов психологии, о которых мы будем говорить в этой книге, позволит вам взглянуть на окружающую действительность глазами психолога. Поверьте, это большое удовольствие и большая экономия нервов, сил и времени.

Авторы предлагаемой книги пришли к социальному программированию и основным его концепциям, с одной стороны (и большей частью), через программирование, связанное с защитой информации, а с другой – через одно из направлений нашей профессиональной деятельности, связанное с проектированием и установкой средств защиты информации от несанкционированного доступа, систем охранной сигнализации, систем контроля доступа и т. д. Анализируя причины и методы взлома ПО или каналы утечки информации из различных структур, мы пришли к очень интересному выводу о том, что примерно в восьмидесяти (!) процентах причина этого – человеческий фактор сам по себе или умелое манипулирование оным. Хотя это наше открытие, безусловно, не ново. Потрясающий эксперимент провели английские исследователи. Не мудрствуя лукаво, они разослали сотрудникам одной крупной корпорации письма якобы от системного администратора их компании с просьбой предоставить свои пароли, поскольку намечается плановая проверка оборудования. На это письмо

ответило 75% сотрудников компании, вложив в письмо свой пароль. Как говорится, комментарии излишни. Не нужно думать, что это просто люди такие глупые попались. Вовсе нет. Как мы увидим дальше, человеческие поступки тоже вполне неплохо программируются. И дело здесь не в умственном развитии людей, которые попадаются на подобные удочки. Просто есть другие люди, которые очень неплохо владеют языком программирования человеческих поступков. Сейчас интерес к социальной инженерии очень высок. Это можно заметить по многим признакам. К примеру, пару лет назад по запросу "социальная инженерия" в поисковой системе Google было только 2 ссылки. Теперь же их сотни… Известный хакер К. Митник, использующий для взломов методы социальной инженерии, выступает с лекциями в гостинице "Редиссон-Славянская" для топ-менеджеров крупных IT-компаний и специалистов служб безопасности корпораций… По социальной инженерии стали устраивать конференции, в ряде университетов собираются вводить курсы лекций на эту тему…

Однако у многих лекций и опубликованных статей, с которыми ознакомились авторы, есть несколько серьезных недостатков. Во-первых, не объясняется психологическая подоплека применяемых приемов. Авторы статей просто говорят: "Это делается так-то". А почему именно так – никто не объясняет. В лучшем случае приводятся фразы: "в основе этого приема лежат принципы нейролингвистического программирования", что, правда, запутывает еще больше. Иногда еще говорят, что "для того, чтобы не стать жертвой социальных хакеров, нужно развивать в себе психологическое чутье". О том, куда за этим самым чутьем сходить и где его приобрести, тоже ничего не говорится. И, наконец, третий и, пожалуй, самый серьезный недостаток публикуемых в настоящее время статей по социальной инженерии состоит в том, что большинство примеров, которые в них приводятся – надуманные ("киношные"), которые в реальной жизни не сработают. Читатель, изучая этот пример, понимает, что если к нему заявится такой хакер, он его непременно раскусит. Что правда: такого, – раскусит. Но когда к нему приходит настоящий, – он выкладывает ему самые сокровенные секреты. Предлагаемая книга призвана, с одной стороны, устранить эти недостатки и дать читателю реальный психологический минимум, который лежит в основе "социального хакерства". С другой стороны, в книге много реальных, а не выдуманных примеров, что тоже поможет читателю в освоении материала, и покажет основные приемы, которыми действуют социальные хакеры. Прочитав эту книгу, читатели будут в немалой степени защищены от подобных манипуляций. И еще одно небольшое замечание. Во многих местах книга написана в стиле учебника по социальной инженерии. Таким образом, мы нередко писали так, как если бы обучали читателей методам социальной инженерии. Это не из-за того, что нам хотелось научить читателей методам мошенничества, а потому, что очень часто, для того чтобы распознать манипулятора, нужно знать, как он действует, вжиться в эту роль… Не для того, чтобы кого-то "охмурить", а только для того, чтобы суметь предвидеть опасность и предсказать дальнейшие действия.

Книга будет в одинаковой степени полезна представителям трех видов профессий: IT-специалистам, сотрудникам служб безопасности предприятий и психологам, изучающих социальную инженерию. В первую очередь, книга будет интересна IT-специалистам, причем самого широкого круга профессий: программистам, системным и сетевым администраторам, специалистам по компьютерной безопасности и т. д. Хотя бы потому, что за кражу ценной информации из "недр компьютера" спрашивают именно с IT-специалистов. И именно им в первую очередь приходится "расхлебывать" последствия такой кражи. Нередко на плечи IT-специалистов ложится и выяснение причин утечки информации. В силу этого многие зарубежные университеты уже вводят для специалистов по компьютерной безопасности курс лекций по основам социальной психологии. Книга будет интересна также и "рядовым" пользователям ПК, поскольку именно они наиболее часто выбираются социальными хакерами в качестве наиболее удобных мишеней.

Психологам книга будет интересна по причине того, что в ней впервые изложены основные принципы социальной инженерии и показано, на каких психологических концепциях она базируется. Сотрудникам служб безопасности она полезна по причине того, что за несанкционированное проникновение на объект отвечают именно они, а такие проникновения очень часто строятся на использовании "человеческого фактора".

Читатели книги смогут задать любой вопрос, посвященный методам социального программирования, на специальном форуме на сайте авторов.

# Благодарности

Авторы выражают признательность сотрудникам издательства "БХВ-Петербург", благодаря которым наша рукопись увидела свет.

# Часть I
# Что такое социальная инженерия и кто такие социальные хакеры

В первой части обсуждаются основные концепции социальной инженерии и социального хакерства. Первая глава, как обычно, – это введение в обсуждаемый вопрос, а во второй главе приведены различные примеры использования методов социальной инженерии.

**Глава 1.** Социальная инженерия – один из основных инструментов хакеров XXI века

**Глава 2.** Примеры взломов с помощью методов социальной инженерии

**Глава 3.** Примеры социального программирования

**Глава 4.** Построение социальных файрволов

**Глава 5.** Психологические аспекты подготовки социальных хакеров

# Глава 1
# Социальная инженерия – один из основных инструментов хакеров XXI века

…В начале февраля 2005 года многие специалисты по информационной безопасности нашей страны ждали выступления К. Митника, известного хакера, который должен был рассказать о том, какую опасность представляет собой социальная инженерия, и какими методами пользуются социальные инженеры (которых мы в дальнейшем будем называть социальными хакерами). Увы, ожидания не очень-то оправдались: Митник рассказал лишь об основных положениях социальной инженерии. И много говорил о том, что методы социальной инженерии используют преступники всего мира для получения самой различной засекреченной информации. По мнению многих участников встречи, слушать было интересно, т. к. человек действительно очень обаятельный, но никаких особых тайн раскрыто не было.

> ***Примечание***
>
> Кевин Митник – известный хакер, которому противостояли лучшие эксперты по защите информации из ФБР, и осужденный в 90-х годах правосудием США за проникновение во многие правительственные и корпоративные секретные базы. По мнению многих экспертов, Митник не обладал ни значительной технической базой, ни большими познаниями в программировании. Зато он обладал искусством общения по телефону в целях получения нужной информации и того, что сейчас называют "социальной инженерией".

То же самое можно сказать и о его книгах – никаких особенных откровений там нет. Мы совершенно не исключаем, что Митник это все прекрасно знает, более того, мы даже в этом почти уверены, только, к сожалению, он ничего из того, что действительно знает, не рассказывает. Ни в своих выступлениях, ни в книгах.

> ***Примечание***
>
> Что, наверное, в общем-то, и неудивительно, т. к. ФБР взялось тогда за него очень плотно, показав, кто в доме хозяин, и нервы ему подергали изрядно. Было и множество объяснений, и запрет на работу с ЭВМ в течение нескольких лет, и тюремное заключение. Не стоит удивляться тому, что после таких перипетий он стал весьма законопослушным человеком, и не будет

не то какие-то секретные базы похищать, но даже и о не секретных вещах станет говорить с большой осторожностью.

В результате таких недоговорок социальная инженерия представляется этаким шаманством для избранных, что не так. Более того, есть еще один важный момент. Во многих описаниях атак пропускаются целые абзацы, если не страницы. Это мы вот к чему. Если взять конкретно схемы некоторых, наиболее интересных атак, и попытаться их воспроизвести согласно написанному, то, скорее всего, ничего не выйдет. Потому что многие схемы К. Митника напоминают примерно такой диалог.

– Вася, дай пароль, пожалуйста!

– Да на! Жалко мне, что ли для хорошего человека.

Разбор же этой "атаки" напоминает примерно следующее: "Вася дал социальному хакеру, потому что он с рождения не умел говорить "Нет!" незнакомым людям. Поэтому основной метод противодействия социальным инженерам – это научиться говорить "Нет"". …Может быть, эта рекомендация и подходит для Америки, но, боюсь, что не для России, где большинство скорее не умеют говорить "Да", а "Нет" у всех получается весьма неплохо. Действительно, есть тип людей, которые органически не могут отказать другому человеку, но, во-первых, таких людей немного, а всех остальных нужно к такому состоянию подводить. А о том, как подводить, не сказано ни слова.

***Примечание***

О психологической типологии и о том, как эти знания использовать в социальной инженерии, мы подробно поговорим в приложении 2.

Вот примерно это и имеется в виду, когда мы говорим, что у Митника нередко пропускаются целые абзацы. Можно допустить, что первая фраза могла иметь место в начале, а вторая – в конце разговора. Но между ними было еще очень многое и самое интересное. Потому что, чтобы все было так просто, нужно человека погрузить либо в глубокий гипноз, либо вколоть ему "сыворотку правды". Но даже если это так и было, то об этом тоже нужно писать.

В жизни же происходит, как правило, по-другому. И пароли говорят, и базы выносят, не потому что не просто "нет" ответить не могут, а потому что "нет" отвечать бывает, … очень не хочется. А для того, чтобы человеку, который владеет какой-то серьезной информацией, очень сложно было ответить "нет", нужно его подвести к такому состоянию. Проследив за ним, скажем, в течение недельки. Вдруг что интересное обнаружиться? Может он сам "засланный казачок" или по вечерам на конкурентов подрабатывает, а может дело то вообще серьезнее обстоит: по вечерам он подрабатывает не на конкурентов, а ходит в публичный дом …для людей с нетрадиционной сексуальной ориентацией, и, будучи для всех прочих примерным семьянином, очень не хочет, чтобы об этом кто-то узнал. Вот имея примерно такую информацию, к нему же можно смело подходить и говорить:

– Вася, а ну скажи-ка мне все пароли, которые знаешь. И доступ мне в свою сеть открой, чтобы я время попусту не терял.

И вот в этом случае уже очень многие Васи ответят:

– Да на, пожалуйста. И пароли дам и доступ открою. Жалко мне, что ли для хорошего человека…

На языке разведчиков это называется "вербовка". И если вдруг в вашей организации все куда-то исчезает, все пароли кому-то известны, подумайте о том, не сел ли кто "на хвост" кому-то из ваших сотрудников. Вычислить того, на кого сели, и тех, кто сел, обычно бывает не сложно. Умные сотрудники служб безопасности, кстати, прежде чем доверять людям ключевые посты, обычно очень сильно его проверяют на предмет, скажем так, слабых сторон

кандидата на должность. И следят за ним, и тесты всякие умные устраивают, чтобы знать, что за человек работать пришел.

…Это вступление написано не для того, чтобы покритиковать К. Митника – каждого из нас есть за что покритиковать – а для того, чтобы показать, что в социальной инженерии не все так просто, как это иногда преподносится, и относиться к этому вопросу нужно серьезно и вдумчиво. Теперь, после этого вступления, как говорится, давайте начнем.

Компьютерная система, которую взламывает хакер, не существует сама по себе. Она всегда содержит в себе еще одну составляющую: человека. Образно выражаясь, компьютерную систему можно представить следующей простой схемой (рис. 1.1).

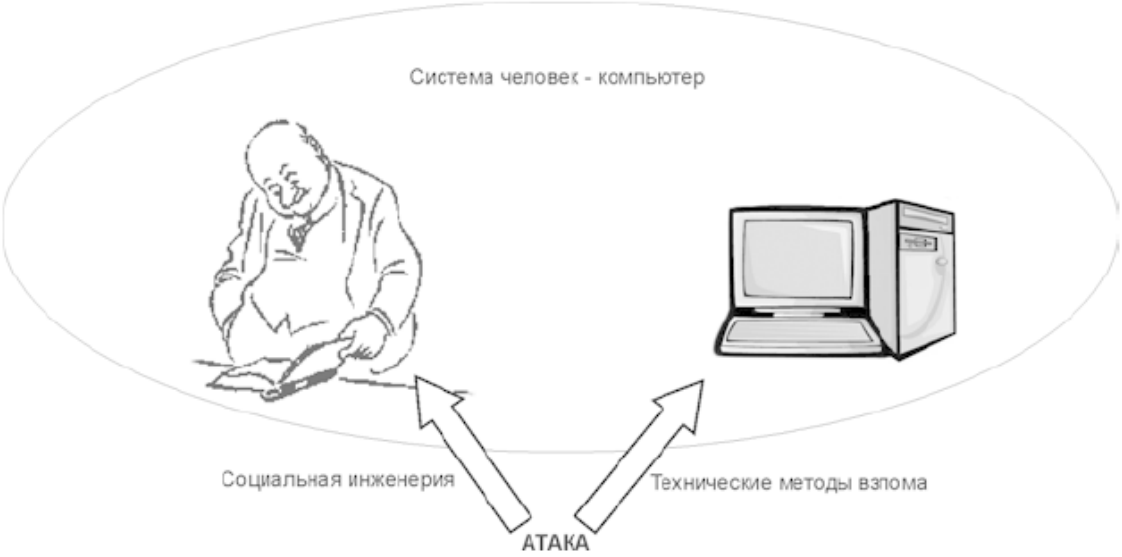


**Рис. 1.1.** Основные варианты взлома компьютерной системы (человек – с карикатуры Х. Бидструпа)

Задача хакера состоит в том, чтобы взломать компьютерную систему. Поскольку, как мы видим, у этой системы две составляющие, то и основных путей ее взлома соответственно два. Первый путь, когда "взламывается компьютер", мы назовем техническим. А *социальной инженерией* называется то, когда, взламывая компьютерную систему, вы идете по второму пути и атакуете человека, который работает с компьютером. Простой пример. Допустим, вам нужно украсть пароль. Вы можете взломать компьютер жертвы и узнать пароль. Это первый путь. А пойдя по второму пути, вы этот же самый пароль можете узнать, попросту спросив пароль у человека. Многие говорят, если правильно спросить.

По мнению многих специалистов, самую большую угрозу информационной безопасности, как крупных компаний, так и обычных пользователей, в следующие десятилетия будут представлять все более совершенствующиеся методы социальной инженерии, применяемые для взлома существующих средств защиты. Хотя бы потому, что применение социальной инженерии не требует значительных финансовых вложений и досконального знания компьютерных технологий. Так, к примеру, Рич Могулл, глава отдела информационной безопасности корпорации Gartner, говорит о том, что "социальная инженерия представляет из себя более серьезную угрозу, чем обычный взлом сетей. Исследования показывают, что людям присущи некоторые поведенческие наклонности, которые можно использовать для осторожного манипулирования. Многие из самых вредоносных взломов систем безопасности происходят и будут происходить благодаря социальной инженерии, а не электронному взлому. Следующее десятилетие социальная инженерия сама по себе будет представлять самую высокую угрозу информационной безопасности". Солидарен с ним и Роб Форсайт, управляющий директор одного из региональных подразделений антивирусной компании

Sophos, который привел пример "о новом циничном виде мошенничества, направленного на безработных жителей Австралии. Потенциальная жертва получает по электронной почте письмо, якобы отправленное банком Credit Suisse, в котором говорится о свободной вакансии. Получателя просят зайти на сайт, представляющий собой почти точную копию настоящего корпоративного сайта Credit Suisse, но в поддельной версии представлена форма для заполнения заявления о приеме на работу. А за то, чтобы рассмотрели заявление, "банк" просил пусть символические, но деньги, которые требовалось перевести на такой-то счет. Когда же деньги перевели весьма много человек, сумма получилась уже не столь символическая. Фальшивый сайт сделан столь мастерски, что экспертам потребовалось время, чтобы убедиться, что это подделка. Стоит признать, что злоумышленники применили довольно хитрую комбинацию технологий. Их цель – самые нуждающиеся члены общества, т. е. те, кто ищет работу. Это как раз те люди, которые могут поддаться на такого рода провокацию", – говорится в словах Форсайта. Энрике Салем, вице-президента компании Symantec, вообще считает, что такие традиционные угрозы, как вирусы и спам, – это "проблемы вчерашнего дня", хотя компании обязательно должны защищаться и от них. Проблемой сегодняшнего дня Салем называет фишинг с использованием методов социальной инженерии.

***Примечание***

Подробно о фишинге – в *главе 2*.

Почему же многие исследователи считают, что социальная инженерия станет одним из основных инструментов хакеров XXI века? Ответ прост. Потому что технические системы защиты будут все больше и больше совершенствоваться, а люди так и будут оставаться людьми со своими слабостями, предрассудками, стереотипами, и будут самым слабым звеном в цепочке безопасности. Вы можете поставить самые совершенные системы защиты, и все равно бдительность нельзя терять ни на минуту, потому что в вашей схеме обеспечения безопасности есть одно очень ненадежное звено – человек. Настроить человеческий брандмауэр, иначе говоря *файрвол* (firewall), – это самое сложное и неблагодарное дело. К хорошо настроенной технике вы можете не подходить месяцами. Человеческий брандмауэр нужно подстраивать постоянно. Здесь как никогда актуально звучит главный девиз всех экспертов по безопасности: "Безопасность – это процесс, а не результат". Очень простой и часто встречающийся пример. Пусть вы директор, и у вас очень хороший сотрудник, который, по вашему мнению, ну уж никогда ничего никому не продаст и никого не продаст. В следующем месяце вы понизили ему зарплату, скажем, по тем или иным причинам. Пусть даже эти причины весьма объективны. И ситуация резко изменилась: теперь за ним глаз да глаз, потому что он места себе не находит от обиды, он уже вас убить готов, что уж тут говорить о каких-то внутрикорпоративных секретах.

Замечу также, что для того, чтобы заниматься обеспечением безопасности, особенно в части настройки "человеческих файрволов", нужно обладать устойчивой нервной и психической системой. Почему, вы поймете из следующей прекрасной фразы А. Эйнштейна, которую мы, вслед за Кевином Митником, не можем не повторить: "Можно быть уверенным только в двух вещах: существовании вселенной и человеческой глупости, и я не совсем уверен насчет первой".

## Основная схема воздействия в социальной инженерии

Все атаки социальных хакеров укладываются в одну достаточно простую схему (рис. 1.2).

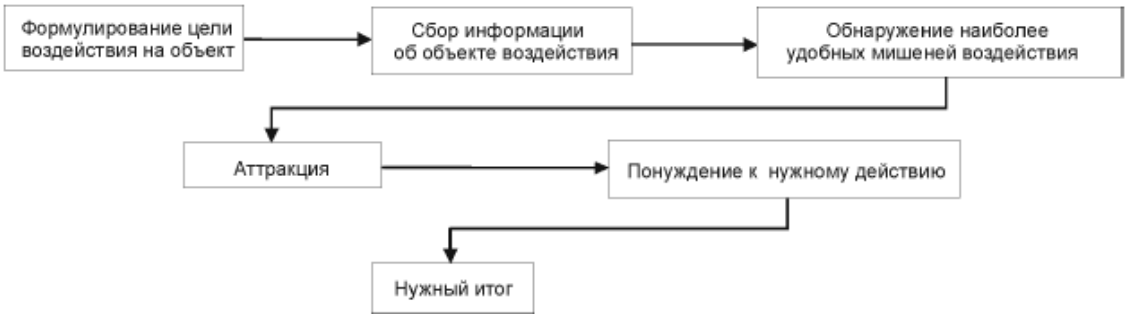


**Рис. 1.2.** Основная схема воздействия в социальной инженерии

***Примечание***

Эта схема носит название *схема Шейнова*. В общем виде она приведена в книге белорусского психолога и социолога В.П. Шейнова, долгое время занимавшегося психологией мошенничества. В немного измененном нами виде эта схема подходит и для социальной инженерии.

Итак, сначала всегда формулируется цель воздействия на тот или иной объект.

***Примечание***

Под "объектом" здесь и далее мы будем иметь в виду жертву, на которую нацелена социоинженерная атака.

Затем собирается информация об объекте, с целью обнаружения наиболее удобных *мишеней воздействия*. После этого наступает этап, который психологи называют *аттракцией*. Аттракция (от лат. *attrahere* – привлекать, притягивать) – это создание нужных условий для воздействия социоинженера на объект. Принуждение к нужному для социального хакера действию обычно достигается выполнением предыдущих этапов, т. е. после того, как достигнута аттракция, жертва сама делает нужные социоинженеру действия. Однако в ряде случаев этот этап приобретает самостоятельную значимость, к примеру, тогда, когда принуждение к действию выполняется путем введения в транс, психологического давления и т. д.

Вслед за В.П. Шейновым, проиллюстрируем данную схему на примере рыбной ловли. Мишень воздействия в данном случае – потребность рыбы в пище. Приманкой служит червяк, кусок хлеба, блесна и т. д. А аттракция – это создание условий, необходимых для успешной рыбной ловли: выбор нужного места ловли, создание тишины, выбор нужной насадки, прикорм рыбы. Принуждение к действию, это, допустим, рывки удилищем, благодаря которым червяк или другая насадка дергается и рыба понимает, что пища может и уйти и надо действовать активнее. Ну а с итогом все понятно.

Другой пример: подкуп сотрудника. Здесь мишень – потребность сотрудника предприятия в деньгах. О том, что он в них нуждается и что с большой вероятностью "примет предложение", узнается на этапе сбора информации. Аттракцией может быть, к примеру, создание таких условий, при которых сотрудник будет в деньгах очень нуждаться.

***Примечание***

Эти условия часто создаются умышленно. Банальный пример – ехал сотрудник на машине и "слегка попал в аварию", после которой и машину надо ремонтировать, и тому джипу, в который он врезался, деньги заплатить. Количество таких "дорожных подстав" сейчас выросло неимоверно, и исполнителей найти не сложно.

Теперь кратко остановимся на таком популярном виде преступлений, как *кража баз данных.*

> ***Примечание***
>
> Кража баз данных – это одна из основных областей применения социальной инженерии. Разговор о кражах баз данных мы продолжим также и в *главе 2.*

Каких только баз сейчас не найдешь: и базы МГТС, и базы Центробанка, и базы Пенсионного фонда, и базы БТИ, и базы МВД с ГИБДД, и базы по прописке… В настоящий момент эксперты спорят о том, к какому виду преступлений относить кражу клиентских баз данных. С одной стороны, данный вид преступлений, вроде бы, по мнению многих экспертов, относится к преступлениям в области IT. Те, кто так считают, исходят из того простого положения, что базы данных хранятся на жестких дисках серверов, и, значит, если их украли, то это преступление в IT. Но с другой стороны, это не совсем так, потому что большинство краж совершаются с использованием методов социальной инженерии.

**Кто и каким способом ворует базы данных?** Если в ответ на этот вопрос вы услышите, что их воруют хакеры, взламывая корпоративные серверы государственных органов и крупных компаний – не верьте этому. Это не так. Все гораздо проще и прозаичнее. Воруют их обыкновенные люди, не пользуясь, в большинстве случаев, никакими сложными приборами, если таковым не считать обыкновенный накопитель Flash Drive, подключаемый к порту USB.

Как мы уже говорили, примерно в 80 случаях из 100 информацию воруют не по техническому каналу, а по социальному. Таким образом, это не хакеры сидят ночи напролет и взламывают серверы, а, скажем, обидевшийся системный администратор уволился. Но не один, а вместе со всеми базами данных и всей информацией о предприятии. Или за умеренную плату сотрудник компании сам "сливает" на сторону информацию о компании. Или просто пришел человек со стороны, представился лучшим другом системного администратора, и сел налаживать "глючную" базу данных, потому что лучший друг нынче болен. После его ухода эта база действительно стала работать лучше, но – в другом месте. Если вы считаете, что это очень тривиально и проходит только в маленьких и совсем уж беспечных компаниях, то вы зря так считаете. Совершенно недавно именно так похитили ценную информацию в одной из весьма крупных питерских компаний, работающих в области энергетики. И таких примеров очень много. Тот факт, что основной канал утечки информации – социальный, задачу защиты информации крайне сильно усложняет. Потому что вероятность утечки по техническому каналу в принципе можно свести к нулю. Можно сделать сеть очень защищенной, что никакая атака извне ее "не прошибет". Можно вообще сделать так, что внутренняя сеть учреждения не будет пересекаться с внешней, как это сделано в российских силовых ведомствах, к примеру, где внутренние сети не имеют выхода в Интернет. Кабинеты руководства и все кабинеты, в которых проводятся важные совещания, следует оборудовать средствами защиты от утечки информации. Никто ничего на диктофон не запишет – мы поставили подавители диктофонов. По радиоканалу и каналу побочных электромагнитных излучений никто ничего не прослушает – поставили генератор радиошума. Виброакустический канал тоже перекрыли, невозможен и лазерный съем информации по колебаниям оконного стекла, через вентиляционные шахты тоже никто ничего не услышит. Телефонные линии защитили. … Итак, все сделали. А информация все равно "сделала ноги". Как, почему? А люди унесли. Без всяких сложных технических манипуляций. В очередной раз сработал тот самый пресловутый и навязший в зубах человеческий фактор, о котором все вроде бы и знают, и о котором все стараются забыть, живя по принципу "пока гром не грянет…". Заметьте: похитить информацию из сетей государственных органов по техническому каналу практически невоз-

можно. А она, тем не менее, похищается. И это является еще одним доказательством того, что, в основном, информацию похищают с использованием людей, а не технических средств. Причем похищают иногда до смешного просто. Мы проводили аудит одного крупного предприятия нефтехимической отрасли на предмет организации в нем защиты информации. И выяснили интересную штуку: доступ к столу секретаря генерального директора могла иметь любая ночная уборщица. И имела, судя по всему. Вот такая демократия царила на этом предприятии. А бумаг на этом столе столько было разбросано, что по ним можно было составить представление почти обо всей нынешней деятельности предприятия и о планах его развития на ближайшие 5 лет. Оговоримся еще раз, что это действительно крупное предприятие, с солидной репутацией и миллионными оборотами. В долларовом эквиваленте, конечно. А защита информации была поставлена… Впрочем, никак она не была поставлена. Еще один интересный социоинженерный канал утечки информации – это различные выставки, презентации и т. д. Представитель компании, который стоит у стенда, из самых лучших побуждений, ради того, чтобы всем понравиться, нередко выдает самые сокровенные секреты компании, которые ему известны, и отвечает на любые вопросы. Я не раз это говорил многим своим знакомым директорам, и один из них в шутку предложил мне подойти к представителю его компании на ближайшей выставке и попытаться таким образом что-нибудь этакое у него выведать. Когда я принес ему диктофонную запись, он, можно, сказать, плакал, потому что одна из фраз звучала примерно так: "А вот недавно наш директор еще ездил в Иран…". Этот способ добычи информации, кстати, используется немалым количеством фирм.

***Примечание***

Подробнее о том, как выведывается информация на презентациях – в *главе 2.*

…К сожалению, многие люди крайне беспечны, и не хотят заботиться о сохранности информации. Причем часто даже в очень крупных организациях это "не хотение" простирается от самых рядовых сотрудников до генерального директора. И при таком раскладе один системный администратор или начальник службы безопасности, будь они даже полными параноиками, помешанными на защите информации, ситуацию не спасут. Потому что на данный момент, увы, даже те из руководителей, которые понимают, что информацию защищать надо, не всегда осознают еще одну вещь: что защита информации должна быть системной, т. е. проводится по всем возможным каналам утечки. Вы можете сколько угодно защищать компьютерную сеть, но если люди получают низкую зарплату и ненавидят предприятие, на котором они работают, хлеще, чем советский народ гитлеровских оккупантов, то на эту защиту можно даже не тратить денег. Другой пример несистемности можно нередко наблюдать, ожидая приема у дверей какого-нибудь директора. Очень нередки случаи, когда те, кто конструирует систему безопасности, не учитывают такую вещь: директора имеют свойство говорить громко, иногда срываясь на крик. Двери же в кабинет генерального директора часто настолько звукопроницаемы, что совещающихся в "генеральском" кабинете можно слушать, совершенно не напрягаясь, даже если они говорят шепотом. Как-то я[1] приехал в Москву к одному "близкому к телу" директору проконсультироваться с ним на предмет, что же ожидает дальше нашу отрасль. А у него как раз случилось важное незапланированное совещание, и меня попросили подождать. Посидев 15 минут у его кабинета, я понял, что узнал гораздо больше того, что хотел узнать, и в принципе можно уезжать. Остался только из приличия. Пикантность ситуации в том, что когда дошла очередь до меня, на мои вопросы директор почти не ответил, говоря, что, мол, сам понимаешь, очень конфиденциально, я и

[1] Здесь и далее, когда повествование ведется от первого лица, это означает, что либо приводимые примеры из коллекции одного из авторов, либо излагается личный опыт одного из авторов. – *Прим. авт.*

сам пока не очень-то в курсе… И так далее. Тем не менее, я его очень горячо и любезно поблагодарил.

…Возвращаясь к базам данных, содержащих конфиденциальные сведения, следует отметить, что после вышенаписанного полностью понятно, кто и как их крадет. Обыкновенные люди их крадут. Очень часто – сами же сотрудники предприятий. Недавно вот осудили таможенника в чине подполковника, который снабжал рынок таможенными базами данных. В соседнем регионе поймали за руку начальника отдела налоговой инспекции, который за умеренную плату сливал данные местным криминальным браткам. И так далее.

**Для чего их воруют и кому это нужно?** Нужно это многим. От млада до велика. Нужно как рядовым гражданам, так и "финансовым акулам". Если начать с граждан, то не вдаваясь в глубинные рассуждения об особенностях русского менталитета, скажем лишь, что пока в справочных службах наших "телекомов" сидят крикливые и всем недовольные барышни, то даже самому законопослушному и честному человеку гораздо проще для своих нервов пойти и купить эту базу номеров телефонов организаций на рынке пиратского ПО, чем позвонить на справочную службу.

Это по понятным причинам нужно всем тем, кто занимается конкурентной разведкой.

Это нужно криминалитету. К примеру, каждый уважающий себя угонщик автомобилей имеет базу ГИБДД. Криминалу также немаловажно знать, не обделяют ли его те, кого он "крышует". Домушники находят себе жертв с помощью баз данных.

Это нужно финансовым гигантам, практикующим практику рейдерских наездов.

> ***Примечание***
>
> *Рейдерские наезды* – это такая практика в новой российской истории, при которой, грубо говоря, большая компания прибирает к рукам те компании, которые меньше с помощью так называемых рейдеров. Допустим, некая большая компания захотела купить какую-то другую компанию, которая поменьше. Для этого она делает заказ рейдерам, – людям, которые построят план захвата компании и его исполнят. Подробно о рейдерах рассказано в *главе 2*.

…Продолжать можно долго. В общем, рынок обширен и спрос на продукцию есть. А спрос всегда рождает предложение. Это один из основных законов экономики. Если есть спрос, обязательно, рано или поздно, дорогое или дешевое, но предложение будет. Каким бы этот спрос не был. Даже если этот спрос очень кощунственный, к примеру, спрос на детские органы. Страшнее спрос сложно придумать. А все равно предложение есть. Что уж тут говорить про какие-то базы данных.

> ***Примечание***
>
> В настоящее время цена вопроса на воровство одной базы данных крупного предприятия составляет около $2000.

**Можно ли вообще прекратить воровство баз данных?** На государственном уровне это можно сделать, наверное, только ужесточив наказание за данное преступление. Хотелось бы посмотреть на того, кто осмелился бы своровать какую-то базу в советские времена. Правда, "ужесточив", это не совсем тот термин: дело в том, что сейчас базы данных можно красть практически безнаказанно. Ну чего стоит любому сотруднику практически любой структуры вынести эту самую базу? Правильно – ничего не стоит. В худшем случае уволят. Но это еще надо умудриться попасться. Дошло до того, что согласно публикации в "Комсомольской правде" от 03.03.06 базами данных приторговывает даже Московский центр экономической безопасности, который, судя из названия, должен эти самые базы охранять. Поэтому, как всегда, на государство, конечно, стоит уповать, но рассчитывать на него не стоит. И некоторые компании сами, не дожидаясь государства, пошли другими путями. К

примеру, по пути дискредитации этого рынка и тех, кто на нем работает. Проще говоря, сливают обыкновенную "дезу", действуя по принципу, если государство не может нас защитить, то приходится самим учиться играть в шпионские игры. И многие неплохо учатся. Я знаю случай, когда одна компания, узнав, что ее "заказали", сама подготовила всю необходимую информацию, которую и украл злоумышленник. Когда "заказчик" понял, в чем дело, он, говорят, был вне себя. А цена вопроса была высока. История умалчивает, что было с теми, кто эту информацию добывал, но, по слухам, после этого случая количество желающих, в том числе и сотрудников, добывать конфиденциальную информацию о деятельности этой компании резко уменьшилось.

Кстати, хотя и говорят, что нет подзаконных актов, направленных на то, чтобы прекратить воровство баз данных, дело, зачастую, совсем не в них. Да, с подзаконными актами действительно проблема. Но в большинстве краж, как мы уже говорили ранее, виноваты сами организации. Кстати, в судах практически нет обращений от организаций, у которых крадут информацию. Что объясняется одной простой вещью: никто не хочет выносить сор из избы. Что, в общем-то, понятно, но, с другой стороны, очень сильно упрощает дело злоумышленникам. Дело еще и в том, что даже в том случае, когда фирме точно известно, что ее сотрудник похитил информацию, и она желает подать на этого сотрудника в суд, вероятность того, что фирма выиграет дело очень мала. По причине все той же беспечности: очень минимальное количество фирм оформляет договоры с сотрудниками должным образом, т. е. так, чтобы в нем было прописано, что сотрудник ознакомлен с тем, что имеет дело с конфиденциальной информацией и что ему будет за то, если он эту информацию разгласит.

## Основные отличия социальной инженерии от социального программирования

Кроме социальной инженерии, мы будем еще употреблять термин *"социальное программирование",* которое, хотя и кажется на первый взгляд похожим на социальную инженерию, на самом деле от нее очень отличается. Тому, чтобы прекратить эту путаницу в терминах, и посвящен этот раздел.

*Социальную инженерию* можно определить ***как манипулирование человеком или группой людей с целью взлома систем безопасности и похищения важной информации.*** *Социальное программирование* же может применяться безотносительно от какого-либо взлома, а для чего угодно, к примеру, для обуздания агрессивной толпы или обеспечения победы какого-либо кандидата на очередных выборах, или наоборот, для очернения кандидата и для того, чтобы миролюбивую толпу сделать агрессивной. Важно то, что здесь уже речи о той или иной ЭВМ нет и в помине. Таким образом, термин социальная инженерия мы будем употреблять тогда, когда речь идет об атаке на человека, который является ***частью компьютерной системы,*** как это показано на рис. 1.1.

> ***Примечание***
>
> Иногда кроме термина социальная инженерия употребляется также термин *обратная социальная инженерия.* Суть в том, что при обратной социальной инженерии вы человека напрямую ни к чему не принуждаете, а создаете такие условия, что он сам к вам обращается. К примеру, если вам нужно прийти в организацию под видом телефонного мастера, вы можете просто прийти и начать проверять телефонные коробки. Это в данной терминологии – социальная инженерия. А можно поступить и по-другому. Вы создаете такую ситуацию, при которой в какой-то конкретной организации вас знают как телефонного мастера. После этого вы ждете, когда что-то случиться с телефонами, или сами делаете с ними что-то, и

спокойно ждете, когда вам позвонят и попросят прийти. Это и есть обратная социальная инженерия. Таким образом, не вы сами куда-то ни с того ни с сего приходите, а вас просят прийти. Конечно, второй случай намного предпочтительнее, т. к. снимает с вас вообще все подозрения. Грамотные социоинженерные подходы именно так и строятся, поэтому этот термин мы считаем излишним, и его употреблять не будем.

Социальное программирование можно назвать наукой, которая изучает методы целенаправленного воздействия на человека или группу лиц с целью изменения или удержания их поведения в нужном направлении. Таким образом, по сути, социальный программист ставит перед собой целью овладение искусством управления людьми. Основная концепция социального программирования состоит в том, что *многие поступки людей и их реакции на то или иное внешнее воздействие во многих случаях предсказуемы.* Вещь, вообще говоря, очень интересная. Но в большинстве своем это действительно так. Общая схема методов работы социальных программистов представлена на рис. 1.3.

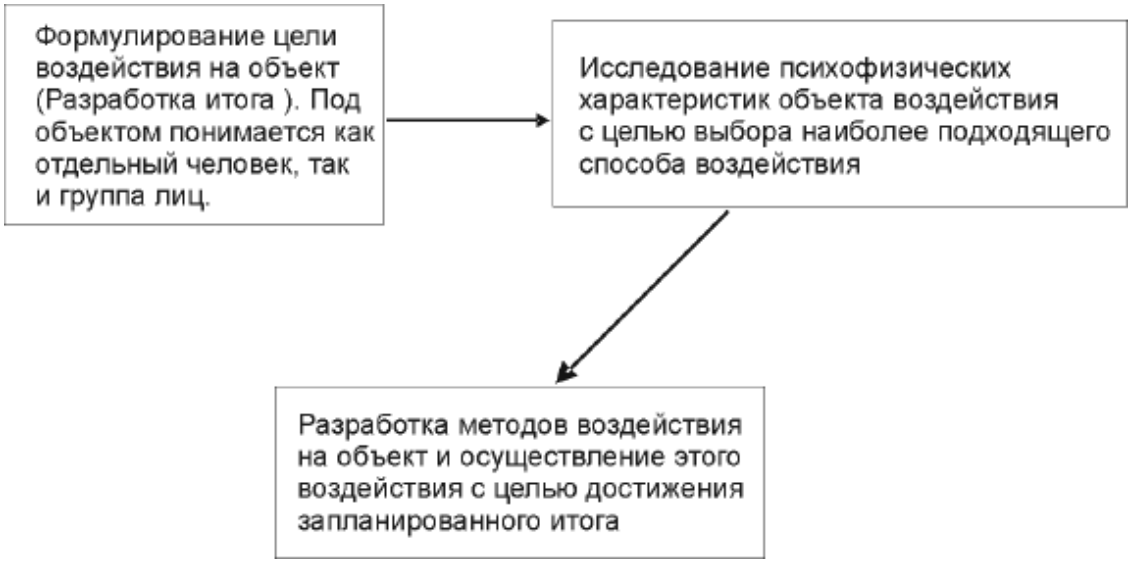


**Рис. 1.3.** Общая схема методов работы социальных программистов

В социальном программировании разработка схемы воздействия идет с конца, т. е. от нужного итога. Приведу один очень простой и очень нехороший пример. Пускай есть некто, к примеру, заместитель, которому ну очень мешает начальник. Допустим, этот заместитель знает, что у его начальника больное сердце и слабые сосуды, и тот, у которого больное сердце, очень любит "приложиться к рюмочке". Родственники, конечно, чуть не по пятам ходят и эту рюмочку отбирают, и это даже действует. А наш зам. начальника теми или иными способами начинает того, у которого больное сердце, целенаправленно спаивать. В конце концов, сосуды не выдерживают. Геморрагический инсульт. Зам. начальника стал начальником. На похоронах рыдал больше всех, да и потом остался самым близким другом семьи. Несмотря на то, что фактически убил главу семейства.

Чем методы социального программирования прекрасны для преступников, что о них либо вообще никто никогда не узнает, как в вышеописанном примере, либо даже если кто-то о чем-то догадывается, привлечь к ответственности такого деятеля очень сложно. Ну нет у нас в уголовном кодексе статьи "Доведение до инсульта". А если б и была – пойди, докажи, что все так и было, ведь "доведенный" все делал сугубо добровольно, будучи дееспособным, в гипноз его никто не вводил, электромагнитными лучами никакими не облучал…

Это мы рассмотрели достаточно классическую и очень простую схему отрицательного применения социального программирования. В разных вариациях эта схема действует с глубокой древности, если вспомнить историю. В данном случае нужный итог – физическое устранение соперника. Итак, цель сформулирована. Дальше проработаны психофизические характеристики, в результате которой выяснена склонность к выпивке и наличие хронических сердечно-сосудистых заболеваний. Затем разрабатывается мера воздействия (чрезмерное употребление алкоголя), которая при правильном применении и дает запланированный результат. Очень важно то, что поведение человека естественно для него самого. Что и интересно. Для этого и производится расчет психофизических характеристик. Потому что иначе это было бы не социальное программирование. Ведь, когда маньяк-убийца, к примеру, уже выбрал себе жертву и собирается ее убить, он тоже знает о будущем поведении жертвы того, что она еще сама о себе не знает (что ее скоро не будет на этом свете). Но, согласитесь, поведение жертвы в этом случае вряд ли можно называть естественным: сложно представить, что встречи с маньяками это ее естественное времяпрепровождение. Таким образом, социальное программирование, это когда вы искусственно моделируете ситуацию под конкретного человека, в которой вы знаете, как этот человек поступит, исходя из знания психотипа этого человека. То же самое относится и к группе людей.

> ***Примечание***
>
> В *главе 3* мы рассмотрим еще несколько примеров именно социального программирования, например, проанализируем, какими способами можно усмирить агрессивную толпу, а также подумаем о том, каким образом с помощью методов социального программирования можно было учинить скандально известный недавний "соляной кризис".

Социальное программирование базируется на следующих психологических концепциях:

- трансактном анализе *(см. главу 6);*
- социологии (науке о поведении людей в группах) *(см. главу 8);*
- нейролингвистическом программировании *(см. главу 7);*
- сценарном программировании *(см. главу 6);*
- психологической типологии *(см. приложение 2).*

Социальное программирование, в отличие от социальной инженерии, имеет более обширную область применения, т. к. работает со всеми категориями людей, независимо от того, частью какой системы они являются. Социальная же инженерия всегда работает только с человеком, который является частью компьютерной системы, хотя методы в том и другом случае используются аналогичные.

Другое важное различие состоит в том, что социальная инженерия – это почти всегда отрицательная область применения, социальное программирование же, как и любая область знания, имеет и положительную и отрицательную область применения. Одним из примеров отрицательной области применения социального программирования является как раз социальная инженерия.

Поэтому, когда мы будем говорить о манипулировании человеком в том случае, когда он является частью компьютерной системы, или просто носителем секретной информации, которую требуется похитить, мы будем говорить о социальной инженерии, а в том случае, когда будет идти речь об управлении людьми вообще, мы будем говорить о социальном программировании. Наша книга – о социальной инженерии, но иногда, чтобы лучше была понятна суть многих методов, мы будем делать набеги в социальное программирование.

В заключение разговора о социальном программировании приведем известный пример о том, как искусно можно манипулировать людьми.

Однажды один гроссмейстер получил по почте письмо, в котором неизвестный ему человек, представившись молодым начинающим шахматистом, предложил сыграть дистанционную партию в шахматы. Дистанционную, потому что ходы отправлялись по почте. За выигрыш гроссмейстеру была обещана очень большая сумма денег, а если будет ничья, или, упаси бог, гроссмейстер проиграет, то деньги платит он. Правда, в два раза меньшую сумму, чем ту, которую получит он сам, если проиграет молодой шахматист. Гроссмейстер, не долго думая, согласился. Заключили пари, и стали играть. Уже с первых ходов знаменитый гроссмейстер понял, что "на халяву" заработать денежку не удастся, потому что уже первые ходы выдавали в молодом шахматисте перспективного мастера. В середине мачта гроссмейстер потерял покой и сон, постоянно просчитывая следующие ходы противника, который оказался не просто перспективным мастером, а очень большим мастером. В конце концов, через немалое время, гроссмейстеру едва удалось свести партию вничью, после чего он обрушил на молодого человека кучу комплиментов и предложил ему не деньги, а свою поддержку, сказав, что с такими талантами сделает его чемпионом мира. Но молодой шахматист сказал, что всемирная слава ему не нужна, и что просит всего лишь выполнить условия пари, т. е. выслать выигранные им деньги. Что гроссмейстер и сделал, скрепя сердце. А где же здесь манипулирование, спросите вы? А манипуляция здесь в том, что против гроссмейстера играл не молодой человек, а …другой великий гроссмейстер, который получил от молодого человека точно такое же письмо и точно так же согласился "быстренько подзаработать". На точно таких же условиях: за выигрыш ему платит большую сумму молодой человек, а за проигрыш или ничью платит гроссмейстер молодому человеку. В результате два великих шахматиста около полугода сражались между собой, а молодой "талантливый шахматист", выражаясь современным языком, работал почтовым ретранслятором, т. е. лишь пересылал их письма друг другу. А потом, в результате ничьи, оба гроссмейстера отправили деньги … этому молодому человеку.

# Глава 2
# Примеры взломов с помощью методов социальной инженерии

В этой главе мы немного поговорим об истории социальной инженерии, а потом продолжим проводить примеры того, как действуют социальные инженеры.

## Об истории социальной инженерии

Очень часто "отцом социальной инженерии" называют известного хакера К. Митника, что не совсем верно. Митник одним из первых стал применять искусство манипулирования человеком применительно к компьютерной системе, взламывая не "программное обеспечение", а человека, который работает за компьютером. И с его легкой руки все, что связано с кражей информации посредством манипулирования человеком, стали называть социальной инженерией. Мы в этой книге, вслед за Митником, тоже придерживаемся подобной терминологии.

На самом же деле, все методы манипулирования человеком известны достаточно давно, и в основном эти методы пришли в социальную инженерию, большей частью, из арсенала различных спецслужб.

> ***Историческое примечание***
>
> Первый известный случай конкурентной разведки относится к VI веку до нашей эры, и произошел в Китае, когда китайцы лишились тайны изготовления шелка, которую обманным путем выкрали римские шпионы.

## Основные области применения социальной инженерии

Авторы многих статей на тему социальной инженерии обычно сводят ее применение к звонкам по телефону с целью получения какой-либо конфиденциальной информации (как правило, паролей) посредством выдачи себя за другое лицо. Однако области применения социальной инженерии гораздо шире.

Основные области применения социальной инженерии показаны на рис. 2.1.

Рассмотрим подробнее на примерах каждую из этих областей.

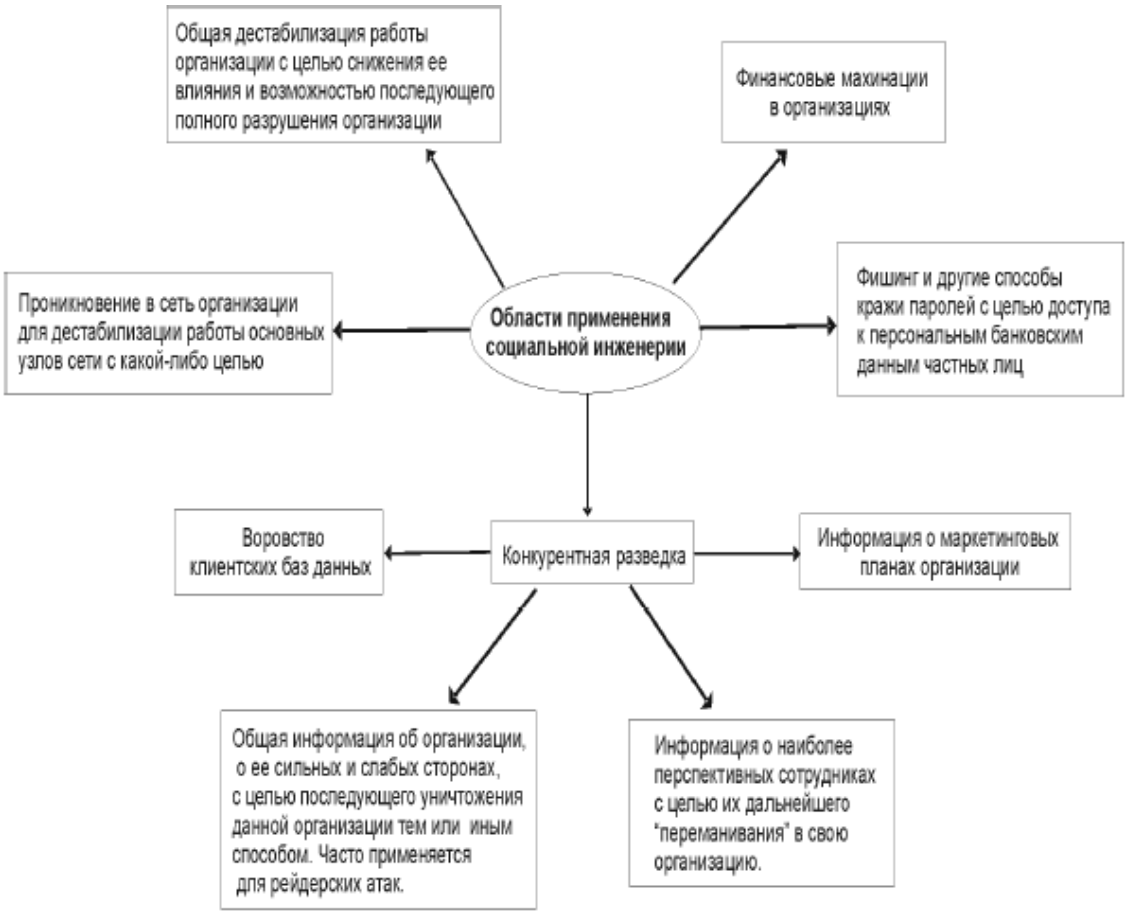


**Рис. 2.1.** Основные области применения социальной инженерии

## Финансовые махинации

…Была весна, была любовь. Бухгалтер фирмы средней руки Наташа была беззаветно влюблена в юношу Илью. Такого прекрасного, такого милого, такого обаятельного. Они с ним случайно встретились в ночном клубе, и там она узнала, что Илья недавно приехал в их город получать образование на вечернем отделении финансового факультета. Бывший слесарь, руки золотые. "Ну и что, что слесарь", – рассуждала Наташа, – "выучится скоро и будет финансистом". Коллега, можно сказать. В общем, затевалась большая свадьба, а впереди была только любовь и много всего приятного, что с этим связано. А при чем же здесь финансовые махинации, спросите вы? А при том, что в планы Наташи жестко вмешалась реальная жизнь, в которой кроме любви бывает еще и жестокий обман. И однажды она узнала, что с ее компьютера был осуществлен перевод на счет некоей фирмы немалой суммы денег. Она точно помнила, что ничего такого не делала, да и вообще девушка это была старательная и без вредных привычек. В общем, шок. Который усугублялся тем, что ее любимый Илья вдруг куда-то исчез. Между прочим, о том, что эту аферу провернул именно Илья, догадались не сразу, потому что никому в голову не могло прийти, что такой обаятельный, такой милый, такой отзывчивый вот так вот может.

Что же произошло? А произошел классический сюжет. Обаятельный Илья влюбил в себя Наташу для того, чтобы воспользоваться ее служебным положением. История очень часто происходящая, только цели разные. В данном случае целью было воровство денег.

***Примечание***

Мишень воздействия в данном случае – потребность Наташи в любви. Аттракция, естественно, любовные ухаживания Ильи за Наташей. Кроме того, аттракцией здесь также является и показ серьезности своих намерений (как помним, готовилась свадьба).

И вот, дождавшись удобного момента, когда он был один в рабочий день в кабинете Наташи, он перевел деньги туда, куда хотел. О том, как это делается, она сама ему рассказала, потому что он спрашивал, мотивируя свои вопросы тем, что ему это интересно для образования (он же, как помним, на финансовом факультете учился, да и вообще, все, что связано с легендированием, в данном случае сделано очень грамотно). Во время же этих бесед Илья выяснил, где лежат дискеты с ЭЦП (Электронно-цифровая подпись) главбуха и директора. Была ли Наташа дурочкой? Нет, не была. Хотя бы потому, что в Илью за те несколько месяцев, что он был рядом с Наташей, влюбились почти все сотрудники фирмы, включая директора, который лично благословил их быструю свадьбу и готов был в скором будущем взять Илью в штат своей фирмы. И потому, что она, по большому счету не виновата в том, что деньги во многих наших фирмах переводятся по упрощенной процедуре. Как по правилам должен происходить перевод денег? Нужно, к примеру, перевести какую-то сумму. Приходит главный бухгалтер, вставляет дискетку со своей ЭЦП, потом вставляет свою дискету директор. И только после этого деньги переводятся, так как наличие ЭЦП и директора и главбуха – необходимое условие для перевода денег. И если бы все делать по правилам, то такая атака, конечно же, немыслима. Но… даже самая мелкая фирма может делать в день до десяти переводов. А теперь представьте, что директор каждый раз будет бегать и вставлять свою дискету. А если фирма не мелкая? Да он фирму скорее закроет, чем таким самоистязанием будет заниматься. Поэтому очень нередко, когда обе дискетки с ЭЦП просто лежат в столе у того бухгалтера, который переводит деньги. Как было и в описанном случае.

А что было Илье? А ничего не было. Потому что он после того, как все сделал, сразу куда-то уехал. То ли в другой город, то ли в другую страну. Паспорт, естественно, был подделным, у него вообще этих паспортов было больше, чем в паспортном столе.

***Примечание***

Оставим за скобками дальнейшее развитие или возможное развитие этой ситуации, так как нам оно, в принципе, не важно. Деньги могли быть и переведены, а потом обналичены, а могли и не успеть их обналичить, потому что сотрудники фирмы оперативно "откатили ситуацию". История финансовых махинаций знает примеры и того и другого вариантов развития событий. Для нас важен сам факт доступа к компьютеру, с которого осуществлялись банковские переводы, и факт осуществления этого перевода, т. е. тот этап работы, который связан с социальным хакерством был сделан, и сделан успешно. Разговор же о том, какими способами можно успеть обналичить деньги до того, как фирма (И/ИЛИ компетентные органы, если им сообщили об инциденте) начнет принимать меры, как можно сделать так, чтобы успеть обналичить деньги и т. д., выходит за рамки данной книги.

Честно сказать, универсальных рекомендаций, позволяющих защититься от данного вида атак, не существует. Эта история с точностью до небольших вариаций не раз происходила и наверняка еще не раз произойдет. Многие авторы в похожих случаях говорят мол, нужно быть внимательнее, нужно четко следовать инструкциям и подобные вещи просто будут невозможны. Мы с этими словами, конечно же, полностью согласны, но, увы, это только слова. Не имеющие никакого отношения к реальной жизни слова. А если дело поставлено серьезно, и им занимаются серьезные люди, знающие, как такие дела делаются, можно гарантировать, что на эту удочку попадутся процентов 90 населения. А многие – еще и не один раз. Поэтому не будем опускаться до банальностей и честно скажем: гарантированных способов защиты нет. А теперь представьте на секунду, что влюбили не девушку Наташу,

а директора. И представьте последствия. Причем сделать все это не очень сложно: определяется психотип человека, на основании чего выясняется, какие девушки (или юноши) ему (ей) нравятся – и через некоторое время жертва находит "ту единственную и неповторимую любовь, о которой всю жизнь мечтала". Излюбленный метод мошенников всех времен и народов. И очень действенный метод, потому что является атакой, основанной на физиологических потребностях человека. О физиологических потребностях мы здесь говорим более шире, чем принято, и понимаем под этими потребностями не только, скажем, потребность в еде, сексе и прочее, а также потребность в любви, потребность в деньгах, потребность в комфорте и т. д. и т. п. И вот, когда мишенью является одна из таких потребностей, дело плохо. В том смысле, что очень сложно. А умные социальные инженеры в качестве мишеней выбирают именно такие потребности. Рассмотренная нами атака – как раз из этой категории, когда в качестве мишени воздействия была выбрана потребность в любви.

Давно известно, что в крупных городах России существуют целые агентства, которые содержат обольстительниц самого разного вида на самый разный, в том числе и изощренный, вкус. Цель их существования – получение прибыли путем "развода" богачей мужского пола. Действительно, зачем строить достаточно сложную комбинацию, как в только что приведенном примере, когда можно сделать все легче: влюбить в себя до беспамятства богатого человека, который сам по своей доброй воле будет переводить денежки на твой счет. Незачем нанимать орду хакеров, проворачивать финансовые аферы, балансировать на грани закона, – все можно сделать так, что человек сам отдаст деньги и отдаст их добровольно. Схема работы такая. На первом этапе сотрудники агентства выясняют все, что только можно о "клиенте": какую пищу предпочитает, какие книги, каких девушек, какие машины, какую музыку, – в общем все. Здесь действуют по принципу, что информация лишней быть не может. Это делается для того, чтобы в соответствии со вкусами жертвы, подобрать для него ту единственную и неповторимую, от которой он просто физиологически не сможет отказаться. Действительно, ну какой мужчина откажется от женщины, которая мало того что в его вкусе и красоты неписанной, но и страстная поклонница футбола (как и он сам, естественно), да еще и болеет за ту же самую команду. И, – о ужас, когда он как-то раз подвез ее на машине, она с сожалением и с некоторым кокетством констатировала:

– Володя, вот если бы не одно, но, я могла бы сказать, что ты мужчина моей мечты.

– Какое НО? – слегка насторожившись, но, придав тону игривость, спрашивает банкир Володя.

– Ты не любишь классику…

– Почему? Почему ты так решила, – слегка запнувшись, и уже без всякой игривости в голосе спросил он.

– А ты вечно крутишь какую-то попсу в машине, а классику ни разу не включил, а я попсу терпеть не могу.

– Что же ты раньше не сказала, ведь я тоже люблю классику, просто боялся тебе в этом признаться, думал, что сочтешь меня не современным.

– Какая, к чертям, современность, все эти "Муси-пуси, трали-вали, поцелуй меня же Люся, пока нас не разорвали", – с ехидством пропела она, – от этой нынешней классики жить не хочется. То ли дело Бетховен… Все эти трали-вали в сравнении с ним…

"Мой любимый композитор", – подумал он, а вслух спросил:

– А что тебе больше всего у Бетховена нравится?

– Соната до-минор, наверное, – ответила она, на мгновенье задумавшись.

"Моя любимая соната, – думает он, – о, ужас… Нет, таких совпадений не может быть. Я первый раз встретил красивую и современную девушку, от которой я и так почти без ума, и которой еще вдобавок нравится классика, и, более того, даже в классике наши вкусы совпали. А, впрочем, почему я так думаю? Разве я не заслужил того, чтобы мне господь послал

ту единственную и неповторимую? Разве мало я детям помогал, деньги в детдом № 5 перечислял? Может это и есть та награда за добрые дела, о которой говорят умные авторы в умных книжках, над которыми мои друзья только цинично посмеиваются. Может на фиг все? Может рискнуть? Ну что жена… С ней никогда и раньше то общего не было, а сейчас, ошалев от моих денег, вообще перестала всем интересоваться, сидит только дома, обрюзгла вся… Тьфу, смотреть неприятно. Да еще служба безопасности докладывает, что вроде она с кем-то на стороне, с каким-то программистом молодым, которому женщины "в соку" нравятся. Черта с два, женщины ему нравятся. Видать жить не на что, вот и выманивает у моей дуры мои деньги. А может и эта, которая рядом, тоже из-за денег? А ну-ка мы ее сейчас спросим…"

– Марин, извиняюсь за нескромный вопрос, а ты чем занимаешься?

– Володь, я директор модельного агентства. Володь, если ты подозреваешь, что я специально подсела к тебе в машину для того, чтобы тебя соблазнить, то это решается просто. Останови машину, пожалуйста. Вот здесь, если не сложно.

– Да, что ты, Марина! Я просто ради интереса…

"Бог мой, она словно читает мои мысли", – подумал он. "Идиот. Тебе, Володя, уже не банком надо заведовать, а в Кащенку идти добровольно сдаваться, чтобы вылечили тебя там от твоей подозрительности. Я не могу ее просто так высадить. Чтобы она вот так просто ушла в никуда, и, возможно, мы больше никогда не увидимся. Нет, нельзя упускать такое счастье", – продолжал он думать, перестраиваясь в крайне правый ряд. "А как же дети?" – спросил строгий внутренний голос. – "Что ты скажешь детям, когда разрушишь семью?". "Дети уже выросли и вполне самостоятельны", – ответил он внутреннему голосу, – "детям уже тех денег, которые я им даю, не хватает для того, чтобы бегать за всеми "юбками", и они не должны быть на меня в обиде, я тоже имею право на любовь, а ведь для них я сделал не так уж и мало. Дети учатся в престижных вузах, три раза в год отдыхают за границей, я спонсирую их любовные похождения, наконец. А дети, к слову, ни разу не поинтересовались, как у папы дела".

– Марин, – наконец решился он, – а ты не против, если мы сегодня посидим в каком-нибудь уютном ресторанчике?

– Володь, если честно, то против.

– Почему?

– Нет, я не прочь провести с тобой вечер, мне первый раз встретился мужчина, который совмещает богатство с любовью к сонате до-минор. А я много общалась с людьми, которые намного богаче, чем я, и что-то от всех от них оставалось какое-то никудышное впечатление. А ты какой-то другой… И мне хочется, если честно, побыть с тобой хоть на чуть-чуть, но дольше, даже врать не буду. Но просто я не люблю рестораны…

– Марин, да если честно, я тоже их ненавижу! Давай тогда в мою вторую квартиру, в которой я люблю иногда наедине с самим собой побыть. А? Сейчас позвоню, привезут еды, вина, посидим вечерочек…

– Нет, давай я лучше чего-нибудь на скорую руку сама сготовлю. Я очень люблю готовить, но, увы, теперь не часто получается самой это делать, а тут такой случай.

– Я согласен, если ты, конечно, этого сама хочешь. А что ты будешь готовить, если не секрет?

– Секрет. Увидишь. Я сготовлю свое любимое блюдо. Сверим наши вкусы, как говорится.

"Терпеть не могу таких сюрпризов, сейчас сготовит что-то, что есть не сможешь, и придется себя пересиливать, лучше бы пригласить мою кухарку, чтобы она сготовила то, что я лю…"…

– Мариночка, это что же за блюдо такое, – закричал он, не додумав до конца свою мысль, когда Марина вошла в гостиную со свежеприготовленным "коронным блюдом".

– Володь, незачем так кричать. Это всего лишь лосось в икорном соусе.

– Откуда… Откуда ты узнала?

– Что узнала?

– Что это мое любимое блюдо?

– Да?! Если честно, даже не подозревала. Володя, как, оказывается, у нас с тобой много общего… А это, заметь, и мое любимое блюдо, меня научил готовить папа, он офицером служил на тихоокеанском флоте, и иногда по праздникам баловал нас этим деликатесом.

…Вот примерно так, все и происходит с некоторыми вариациями. Не буду дальше рассказывать о том, как развивались отношения Володи и Марины. Скажем лишь о том, что потом Володя добровольно перечислял огромные суммы на счет Марины, чтобы она себе ни в чем не отказывала, бросил семью, и даже уговорил Марину оставить свое модельное агентство, чтобы она как можно чаще была с ним. Его счастье бы очень омрачилось, узнай он о том, что сорок процентов с перечисленных им сумм Марина переводила держательнице агентства, "шахине", как они ее между собой называли. И ту машину, которую подарил ей Володя, она тоже должна была продать, после разрыва с ним, или найти сорок процентов ее стоимости в денежном эквиваленте, чтобы отдать их "шахине". Не знал Володя и того, что встреча его с Мариной была подстроена по всем правилам разведки. Что неполадка в ее авто была сымитирована, и то, что он в этот момент оказался рядом с ней, тоже было подстроено. Не знал он и того, что вариантов таких случайных встреч – масса. Не знал он и того, что скоро перестанет быть управляющим банком, так как те данные, которые собрала на него Марина, уже переданы "шахине", которая за приличную сумму продала их тем людям, которые спали и видели, чтобы Владимир Анатольевич перестал быть богатым управляющим банком, а стал бы бедным дворником. Ну, и, естественно, он не подозревал о том, что после того, как в его делах случится крах, он станет очень раздражительным человеком, чем и воспользуется Марина, чтобы его покинуть. Теперь уже очень состоятельной женщиной, так как тех денег, которые она "выкачала" из, теперь уже несчастного, Володи, ей хватит на очень долгое время безбедного существования, даже за минусом тех процентов, которые отдавались "шахине".

## Небольшой комментарий на тему "случайных встреч"

Социальные хакеры – доки в организации "случайных встреч". Ряд приемов заимствован ими, в основном, из арсенала спецслужб, но и в собственной изобретательности многим не откажешь. Конечно, за обольстительницами, о которых мы в данный момент говорим, стоит немало "бойцов невидимого фронта", которые все эти спектакли и ставят. Потому что операция "случайная встреча" – немаловажный этап во всей этой большой игре и планируют ее с учетом рекомендаций психологов, которые на основе данных первого этапа достаточно точно прогнозируют психо– и социотип жертвы и предсказывают поведение клиента в той или иной ситуации. Ведь один "клиент" может "поплыть" сразу после первой встречи, а к другому, более упорному, и подозрительному подходец нужен, – с ним несколько раз нужно встречаться, с ним во время первой беседы вообще ни о чем серьезном говорить не стоит. Значит, нужно, чтобы девушка, которую жертва "случайно" подвозит, "случайно" забыла в его машине свой сотовый телефон, к примеру. Желательно, той же самой модели, что и он предпочитает. Ну чтобы был повод встретиться. А третий, скажем, вообще в свои машины никого не сажает. Значит, нужно у ворот его дома подвернуть ножку или упасть в обморок. И падают, и хорошо падают, потому это все заранее не раз репетируется. А четвертого чужие обмороки, даже в исполнении очень красивых девушек, мало волнуют, потому как человек очень жестокий и предпочитает "стерв", а не размазюнь, в обмороки шлепаю-

щихся в дело и не в дело. Этому устраивается автомобильная подстава, при которой автомобиль девушки врезается в его крутое авто. Он, конечно, сидит в машине, ждет, пока его охрана разберется с "нарушившим правила дорожного движения", и вдруг слышит гортанный женский голос: "Эй, вы бодигарды, кыш отседова. Говорите, сколько я вашему папаше должна, берите деньги, и проваливайте, не мешайте мне наслаждаться моей нелегкой женской долей. А вашему недоумку за рулем скажите, чтоб убирался на своем авто крутом подальше, как только бабу за рулем увидит". Слушает жестокий человек Петр Семенович, владелец нескольких крупных автозаправок в центре столицы и одного небольшого нефтезаводика, этот низкий гортанный голос и уже подсознательно понимает, что этот голос принадлежит "стерве его мечты". И решает он на нее своими глазами взглянуть. И после этого он – пропал. Потому что, как взглянул, уже сознательно понял, что это именно та девушка, которая снилась ему ночами. А для пятого, кроме денег помешенного еще на рукопашном бое и чувстве собственной значимости, устраивается спектакль, в котором участвует девушка его мечты и несколько крутых на вид и неопрятных мужланов. Эти мужланы пристают вон к той красивой девушке, и о, боже, даже рвут на ней платье. Естественно, в зоне видимости "клиента". И решает он броситься в драку и помочь девушке, и бросается и только зубы из-под его кулаков тренированных вылетают, и разлетаются хулиганы в разные стороны от его ударов (потому что проинструктированы на тему того, что "чем дальше и красивее улетят, тем выше гонорар за выступление"). Девушка, естественно, его благодарит сквозь слезы, и он, ее, естественно, подвозит (ну куда ж она в разорванном платье-то сама пойдет), и, конечно, всю дорогу поет ему оды на тему "какой он мужественный, и как он ловко вон тех гадов, которые ее чуть было не…".

***Примечание***

Примерно такие же спектакли, кстати, нередко устраивают некоторые кандидаты перед выборами. Подкупают какую-нибудь шпану, которой говорят, что мол "как вон то авто увидите, сразу бросайтесь… Да не под авто, под авто другие бросаться будут, а на любую красивую девушку. И начинайте ее бить. Без травм, но чтоб кричала. Ясно? А как из этого авто выбежит человек в белых брюках и белом пиджаке, и начнет бить вас, вы ему сразу не поддавайтесь, а тоже слегка помутузьте. Он в курсе и в обиде не будет. А после того, как он вас всех изобьет, чтоб врассыпную бросились с этого места, желательно с криками и стонами, и… Да не домой раны зализывать, он сильно бить не будет, а на вокзал. И чтоб вас до такого-то числа в городе не было. Вот билеты. Все понятно? И если хоть кому слово… Ну, не глупые, сами понимаете". Дальше все идет по плану: завидя авто, "хулиганы" бросаются на девушку, наш герой в белом ее героически вытаскивает из лап "бесчинствующих подростков", пресса, конечно же, тут как тут. Как пресса узнала? А никак. Просто она случайно рядом снимала какой-то репортаж из жизни города, о чем в штабе кандидата, естественно, знали. После этого на всех полосах газет и в первых минутах городских новостей показывают кандидата после драки, в уже не белом пиджаке, утешающего девушку, ставшую "жертвой нападения". Потом берут интервью у кандидата, где он скромно улыбается и говорит, что "он всегда таким по жизни был". Потом сама девушка дает много интервью, в которых чистосердечно (ей же никто не платил) говорит, что "не знаю как другие, но я точно проголосую за Бориса Викторовича, хотя бы просто в знак благодарности. Никто не подошел, а он… Спасибо ему".

## Информация о маркетинговых планах организации

Выведать информацию о маркетинговых планах организации и сыграть на опережение – едва ли не самый лакомый кусок для любого конкурента. Сделать это с помощью методов социальной инженерии проще всего. Не надо ломать сети, обходя бесчисленные количества файрволов и искать, на какой же машине лежит этот документ с маркетинговой стратегией. Не надо подбрасывать подслушивающие устройства на собрание акционеров или на совещание у генерального директора. Не надо снимать информацию по колебаниям оконного стекла лазерным лучом… Это все очень дорогие и не всегда надежные способы. Можно воспользоваться простейшими методами социальной инженерии. Два несложных примера. Я уверил как-то одного генерального директора предприятия о том, что проникну в их компьютерную сеть, и все их маркетинговые планы украду, прочитаю, и им потом перескажу. Он посмеялся, сказав, что это невозможно, что "три межсетевых экрана, целый отдел, занимающийся защитой информации, в котором спецы классные". Не сможешь, мол. Потому что это в принципе невозможно. Но спор, как говорится, принял. Про сеть, разумеется, было сказано для отвода глаз. На самом же деле, никто ни в какие сети проникать не собирался. Все было проще.

***Примечание***

Популярность социальной инженерии среди мошенников, тех, кто занимается конкурентной разведкой и тому подобным, связана, на наш взгляд, с тем, что большинство методов социальной инженерии просты. Иногда просты настолько, что их даже не интересно описывать в книге. Думаешь: ну ведь это же очевидно, какая, к черту, социальная инженерия, ведь этот прием первый раз показали в кино еще году в 50-м. А потом еще сотню раз показывали в тех или иных вариациях. На него то уж точно никто не попадется. И… парадокс, заключающийся в том, что именно на такие простые приемы как раз и попадается большинство. Но даже, когда для проведения того или иного приема требуется проведение сложной комбинации, подразумевающей неплохое владение психологией, все равно для тех, кто занимается, к примеру, конкурентной разведкой, проще применить приемы социальной инженерии, чем заниматься технической разведкой. Исходя, в том числе, и из того немаловажного фактора, что применить социальную инженерию обойдется во много раз дешевле.

## Посещение стендов предприятия на выставке

Для того чтобы собрать большинство информации, оказалось достаточным просто посетить стенд этой организации на ближайшей выставке их продукции. Большинство менеджеров, которые находятся у своего стенда, стоит вам проявить лишь малейшую заинтересованность, с удовольствием расскажут вам все, что они знают о продукции и дальнейших перспективах. Очень часто нужно просто стоять и внимательно слушать (или не просто слушать, а записывать на диктофон, если на память не надеетесь).

***Примечание***

Именно таким образом одна компания из Санкт-Петербурга выкрала секрет производства соусов у своих конкурентов, при этом чуть было их не разорив. Люди весьма удивительные существа, они могут молчать при пытке их сотрудниками конкурирующей фирмы, но при этом с удовольствием выложат все секреты первому встречному на выставке.

Естественно, при этом вы должны выглядеть как солидный клиент, и, желательно, чтобы на вашем бейджике было что-то весьма значительное, вроде "Президент ОАО "Микрон"".

***Примечание***

Но если уж обозвались президентом, то и выглядеть должны, как президент. Это совершенно не значит, что нужно обвешаться перстнями, цепочками, наоборот – одеты вы можете быть скромно: вы уже и так значительный человек, и вам уже незачем производить впечатление. Но одеты должны быть со вкусом, быть очень опрятными и вести себя значительно: как президент. Немного подробнее об этом – далее в примечании "О важности вживания в роль".

Если менеджер не особо разговорчив, можно применить ряд простых уловок, нацеленных на то, что менеджер боится представить организацию в невыгодном свете (в нашей универсальной схеме – это и есть мишень. Аттракцией может являться, к примеру, ваша значимость, хоть и искусственно созданная – с помощью бейджика и поведения). К примеру, вы, представившись каким-нибудь президентом, можете спросить: "А что новенького у вас в этом году появится? Знаешь про это что-нибудь?" Кто-то сразу скажет, кто-то не скажет… Тому, кто молчит, можно сказать: "Ладно, если не знаешь, сам позвоню Марьяшевичу, у него спрошу" (фамилию гендиректора и всех остальных значимых лиц надо знать обязательно). И, уходя, пробормотать, "присылают черте-кого, уж на такие мероприятия могли знающего человека прислать"… Один важный момент: предыдущий вопрос, где вы так разозлились, что вам не ответили, должен быть для вас пусть и значимым, но …не очень. Потому что потом вы походите по другим стендам, через некоторое время вернетесь к интересующему вас стенду и зададите уже действительно значимый для вас вопрос: "А вот про это-то знаешь, вон у тех ребят все как хорошо написано, а вы будете такое же делать или мне сразу с ними договор заключать"? И про это, он уже с большой вероятностью расскажет, потому что боится своего влиятельного директора Марьяшевича, и расскажет даже больше, чем надо.

***Примечание***

Мне только единственный раз встретился менеджер, который, хоть и был крайне доброжелателен, но ничего сверх того, что было можно, не сообщил. Менеджер оказался …генеральным директором этого предприятия, который иногда любил вот так "выйти в народ".

…После того, как было немало узнано от менеджера, я пошел брать интервью у сотрудников предприятия.

## Интервью с ключевыми лицами

Взять интервью – это один из самых простых, но вместе с тем и самых привлекательных способов узнать о том, что творится на предприятии: какие маркетинговые планы, кто против кого дружит, кто кого обидел… Способ действительно простой, но вместе с тем очень действенный. Мишень здесь – чувство собственной значимости людей. Люди хотят чувствовать свою значимость, об этом еще Карнеги превосходно написал, и, чтобы удовлетворить это чувство, нередко забывают обо всем, о любой безопасности. Поэтому интервью с удовольствием дают многие (особенно если это интервью для телевидения). А для социального хакера такое прикрытие очень надежно и выгодно, так как позволяет, не особо стесняясь, задавать практически любые вопросы без риска вызвать подозрение.

***Примечание***

Извлечение полезной информации из разговора с кем-то, кто не подозревает, что является объектом вытягивания информации, называется *скрытым допросом*. Скрытый допрос – это серия приемов, позволяющих ненавязчиво получить нужную информацию. Этой тактикой пользуются психологически грамотные продавцы, которые продают свой товар, психотерапевты, чтобы узнать информацию о пациенте, и многие другие. Естественно, пользуются ей и социальные хакеры.

Для того чтобы интервьюируемый перешел к интересующему вас вопросу, его следует слегка "задеть", для чего иногда достаточно сказать фразу типа "Но вот у организации А (называете конкурирующую организацию), в газете "Вести России" сказано, что их продукция по техническим характеристикам намного превосходит аналогичную продукцию, производимую на вашем предприятии?" чтобы интервьюируемый бросился защищать честь родного предприятия и рассказал все, что он знает о данной продукции. Это уже потом он бросится искать номер этой газеты, чтобы своими глазами убедиться в нахальности конкурентов, и не найдет он этот номер, конечно. Да и газету с таким названием не найдет. Для пущей убедительности можно иногда преднамеренно для интервью распечатать единственный экземпляр данной газеты специально для интервьюируемого или создать сайт газеты, на котором во время интервью продемонстрировать упомянутую вами статью. Конечно, в сумме проработка таких мелочей может занять время и повлечь финансовые затраты, но если дело того стоит, то чем больше таких мелочей предусмотрено, тем лучше. Выглядит гораздо эффектнее и практически сводит к нулю какие-либо подозрения, даже если они были вначале.

***Примечание***

Я полностью верю тому, что немалую часть информации многие и их и наши разведчики берут из газет. Я также верю в то, что слова одного из наших сограждан, которого осудили за шпионаж, что все "секреты" он брал сугубо из газетных материалов – это правда. Вообще, по разным мнениям, около 90% всей **закрытой** информации разведчики всех мастей и рангов получают из **открытых** источников. Мне рассказывали, что многие директора после того, как узнавали, что их сотрудники (иногда на уровне заместителей) понарассказывали в интервью, бросались обрывать телефоны редакций и предлагать любые блага, только бы это интервью не выходило.

Часто бывает выгодным и обратный подход, когда вы не нападаете на интервьюируемого, а, наоборот, разыгрывая из себя "технического дурака", просите объяснить ту или иную деталь. Это тоже весьма действенный способ.

***Примечание***

Забегая вперед, заметим, что в терминах трансактного анализа, вы в этом случае ведете общение по трансакции Дитя – Родитель (о трансактном анализе мы подробно будем говорить в *главе 5)*. Вы находитесь в роли Дитя, отводя интервьюируемому роль Родителя. А куда деваться мудрому Родителю, кроме как не научить Дитя всему, что он сам знает? Трансакция Дитя – Родитель прекрасно подходит для начала многих манипуляций, и об этом мы тоже будем говорить в *главе* 5, в которой изложены основные положения трансактного анализа. Вспомните об этом примере, когда будете изучать эту главу. В том же случае, когда вы сказали интервьюируемому, что, мол, у конкурентов то продукция получше вашей будет, вы проводили обратный прием, и отвели себе роль нападающего Родителя, а того, кто давал

интервью, загнали в роль Дитя, заставив оправдываться. Иначе говоря, ваше общение проходило по линии Родитель – Дитя.

Таким образом, побывав на выставке, взяв за пять дней 10 интервью, попив с некоторыми особо благожелательными интервьюируемыми пива в баре и поговорив "за жизнь", а также почитав все газеты за последние полгода, в которых сообщалось о деятельности этого предприятия, я знал практически все, включая интимные стороны деятельности высшего руководства, о чем этому руководству и доложил в своем отчете.

Спор был выигран, а руководство глубоко задумалось. Потом мы вместе придумывали как минимизировать последствия подобных атак. Которые, правда, и атаками-то сложно назвать. Никто не прорывал оборону противника, рискуя собственной жизнью, никто никого не вводил в транс, и вообще ничего противозаконного не делалось. Все было абсолютно легально и весьма просто. Но от того не менее страшно, потому что вот так, когда крупицы информации начинают складываться в мозаику, может получиться хорошая бомба, которая в умелых руках таких дел натворить может…

***Примечание***

Кроме интервью полезно выполнить и ряд сопутствующих мероприятий. Обязательно постойте в курилках, потолкайтесь у главного выхода. Однажды мы выехали к клиенту, на одно предприятие, а я забыл пропуск, и пару часов мне пришлось поскучать в ожидании коллеги у главного вестибюля предприятия. Так за эти пару часов я, сам того не желая, немало узнал о деятельности предприятия и о тех проблемах, которые у него на данный момент есть.

Теперь несколько небольших комментариев к этому подразделу.

## О важности вживания в роль или об актерском мастерстве социальных хакеров

Кем бы не представлялся социальный хакер, какую бы роль он не играл, играть он ее должен убедительно. А для этого он должен "вжиться" в тот персонаж, который играет. Все успешные социальные хакеры – прекрасные актеры. Вживаясь в роль, они контролируют, в том числе, и свои невербальные реакции.

***Примечание***

О невербальных реакциях см. в *приложении 1*.

Простой пример. Допустим, вы мужчина, и переоделись в женщину, и хотите, чтобы все поверили, что вы – женщина. Вы сами понимаете, что просто переодеться, это мало. Потому что для того, чтобы окружающие поверили, что вы именно тот персонаж, роль которого вы играете, вы должны жить этой ролью. В нашем случае – вы должны вести себя как женщина. Даже если на вас будет работать десяток самых лучших гримеров, которые все сделают так, что "комар носа не подточит". А вы всю их работу угробите, закурив сигарету на типично мужской манер. И так далее. Если вы играете бомжа-алкоголика, значит, как только вы войдете в магазин, от вас должны все шарахаться, кричать на вас, к вам должны подскакивать охранники и под белы ручки выводить из магазина, при этом презрительно морщась.

Если человек хороший актер, то он может считать себя на 50% состоявшимся социальным хакером. Если же он еще и разбирается в психологии, то можно считать, что как социальный хакер он состоялся на 100%, потому что "охмурит" почти любого. Дело здесь в том, что *очень много людей смотрят только на внешнюю атрибутику и не смотрят на суть*. Это одно из основных правил социальной инженерии. Правило, которое давно поняли все, кто так или иначе связан с манипулированием людским сознанием: социальные хакеры, продю-

серы, пиарщики всех мастей и рангов и т. д. Примеры действенности этого правила можно приводить сколько угодно, стоит посмотреть хотя бы результаты прошедших выборов.

***Примечание***

Это же правило прекрасно работает и при проведении переговоров, о которых мы подробно будем говорить в *приложении 1*.

Для того чтобы это правило проиллюстрировать, подробнее рассмотрим следующий пример. Предположим, что один из авторов этой книги придет читать лекцию. При этом войдет он в аудиторию неуверенной походкой, лекцию будет читать заикающимся голосом, в общем будет этаким сосредоточением робости перед слушателями. Но при этом он расскажет, что он лауреат того, сего, пятого и десятого, руководитель там-то, а еще консультант вот здесь и здесь, а также выложит перед собой все написанные научные работы и книги, коих немало. И вот если после лекции слушателям задать несколько вопросов, среди которых "Насколько, как вы считаете, автор разбирается в жизни", подавляющее большинство ответит, что по жизни он "полный дурак". Таким образом, все обратят внимание только на внешние проявления (в данном случае неуверенность), о том же, что премии и награды просто так не выдаются, книжки тоже не сами из-под пера вылетают, консультантам не за красивые глаза деньги платят, да и вообще, чтобы всего этого добиться, надо хотя бы немного "кумекать по-житейски", никто внимания, как правило, не обращает.

***Примечание***

С точки зрения трансактного анализа, о котором чуть позже, это объясняется тем, что в данном случае автор выступил в роли Дитя, а слушателям отвел роль Родителей. Естественно, поскольку люди местами просто помешаны на собственной значимости, Родители они мудрые и много понимающие в жизни (конечно, сточки зрения их субъективного мнения, – как в реальности, можно только догадываться). Ну а какой Родитель скажет, что Дитя разбирается в жизни? Правильно, никакой. Вообще позиция, когда вы находитесь в роли Дитя, а другим отводите роль Родителей, работая при этом в рамках трансакции Дитя – Родитель, – самая удобная для любых манипуляций.

Теперь допустим, что тот же автор перед теми же слушателями будет читать лекцию три дня спустя. Но при этом он уже будет говорить уверенно, четко, слушателей бояться не будет, а наоборот будет вести себя с ними даже слегка надменно, и так далее. И после лекции у слушателей снова спросят насчет понимания автором жизни. И вот теперь большинство ответит, что со времени прошлой лекции автор достаточно "поумнел по жизни". Таким образом, опять почти все обратят внимание только на внешнюю атрибутику, а то, что "поумнеть по жизни" за три дня мало кому удавалось, и лектор остался точно таким же, каким он и был в прошлый раз, никому и в голову не придет.

Если же социальный хакер, кроме актерского мастерства, владеет еще и психологией, то ему, как мы уже говорили, "все возрасты покорны". Потому что он очень хорошо осведомлен еще о двух других людских слабостях, играя на которых можно многого добиться.

Следующее правило социальных хакеров гласит, что ***"Большинство людей отрицательно зависимы от своего чувства собственной значимости"***. А это значит, что эта отрицательная зависимость может быть неплохой мишенью для атаки. Зависимость от чувства собственной значимости вообще сама по себе ничего плохого не означает. Наоборот: любому из нас хочется как-то и чем-то выделиться, то есть хочется чувствовать свою значимость. Вопрос в том, что выделяться можно по-разному и относиться к тому, что как-то нужно выделиться тоже можно по-разному. Отрицательная зависимость наблюдается тогда,

когда человеку хочется выделиться любой ценой и делать это как можно чаще. Любой хакер, к примеру, это человек с отрицательной зависимостью от чувства собственной значимости.

> ***Примечание***
>
> С точки зрения трансактного анализа отрицательную зависимость от чувства собственной значимости можно объяснить тем, что у такого человека слабая Взрослая компонента. Кстати, если у человека анализа слабый Взрослый (или в терминологии Фрейда слабое СуперЭго), то такому человеку достаточно лишь чуть-чуть польстить, и "он ваш". Как говорится, "что и не знал, расскажет, и что не мог, сделает".

Люди, у которых, наблюдается этот, скажем так, недостаток, очень уязвимы для действий социальных хакеров. Им действительно, очень часто достаточно только чуть-чуть польстить, чтобы они сделали для вас все, что вы захотите. Другой недостаток таких людей в том, что они очень завистливы. А зависть, по меткому выражению А. Розенбаума, это такое чувство, которое "из очень хороших людей делает очень больших скотов и подчас за очень короткое время". Зависть – это корень всех интриг. Играя на зависти одного сотрудника предприятия к другому, можно сделать очень многое. В организации распознать сотрудника, склонного к отрицательной зависимости от чувства собственной значимости, можно несложно. Иногда для этого ему достаточно сделать лишь справедливое замечание по его работе. Нормальный человек, если замечание действительно справедливо и сделано в нормальном тоне, подумает, как сделать так, чтобы такого больше не повторялось. Тот же, кто слишком много о себе возомнил, будет реагировать примерно так. Во-первых, сначала он набычится. После этого демонстративно с вами не согласится: любую наукообразную чушь начнет плести, лишь бы продемонстрировать свое несогласие. А потом либо открыто обидится, и всем своим видом будет демонстрировать, как вы его оскорбили в лучших чувствах, либо эту обиду затаит. А теперь представим, к такому "оскорбленному сотруднику" подойдет менеджер конкурирующей организации, которая спит и видит, чтобы увести у вас парочку сотрудников вместе с клиентской базой. Подойдет такой менеджер, немного "за жизнь" поговорит, польстит, а потом и скажет:

– Вижу, что вас здесь не очень-то ценят. А знаете что? Если хотите – пойдемте к нам? А? Зарплата лучше, условия лучше, коллектив лучше, и самое главное, клиентов вы будете искать не бесплатно, как здесь, а за отдельные деньги: 10% от сделки с каждого приведенного клиента (клиентская база то нужна, больше чем сам сотрудник, поэтому нужно его заинтересовать, чтобы он перетащил всех клиентов).

И очень многие пойдут.

Третье правило социальной инженерии гласит, что ***"Многие люди хотят, чтобы все хорошее, что только с ними в жизни может произойти, произошло как можно быстрее и желательно с минимальными усилиями с их стороны".*** Пример действия этого правила – тысячи обманутых вкладчиков того же пресловутого МММ, которые поверили, что вложив 100 рублей (отделавшись минимальными затратами) можно через год (и быстро, главное) получить миллион. Другой всем известный пример, это когда большинство людей голосуют за обещания кандидатов, в которых они на разный манер говорят одно и то же: "как только они придут, то все сразу будет хорошо".

Четвертое правило говорит о том, что ***"многие люди существа исключительно жадные до денег".*** Или говоря по-другому, некоторые утрачивают чувство реальности после того, как перед их носом помахать купюрой. А если не купюрой, а чемоданчиком с купюрами, то чувство реальности утрачивается всерьез и надолго. Игра на этой слабости – один из основных приемов в социальной инженерии. Применяется в разных вариациях: от баналь-

ного подкупа до "писем счастья", в которых сказано, что "если перечислите на этот счет два доллара, то через месяц получите двадцать".

**Социальная инженерия – это за редким исключением почти всегда игра на людских пороках и слабостях.** К редким исключениям можно отнести, к примеру, излишнюю доверчивость. Хотя и здесь как сказать.

## О важности продумывания мелочей

Успешный социальный хакер всегда продумывает все до мелочей. К примеру, если он пошел брать интервью, то у него будет заготовлена визитка, где будет написано, что он корреспондент такой-то газеты. Если вы позвоните по указанному номеру телефона, то тоже ничего странного не обнаружите, потому что трубку снимет девушка и обаятельным голосом произнесет:

– Редакция газеты "Мир города". Светлана Куприянова. Здравствуйте.

Договориться же о том, чтобы кто-то посидел на телефоне в течение пары часов – дело недолгое. Точно так же как договориться не только с девушкой, но и с мужчиной, который в случае чего скажет, что он главный редактор и попросит у интервьюируемого прощения за то, что "вот так вот, без предупреждения, прислали корреспондента, вы уж извините, номер горит, а информация о вашем предприятии как раз очень нужна, потому что ваше предприятие одно из значимых в нашем городе, но если конечно вы против, то Петр Семенович тут же уйдет и не будет вас беспокоить, но я очень вас прошу уделить ему времени, конечно, сколько сможете, я все понимаю, учитывая вашу занятость, как это трудно…". И ошалев от такой льстивой скороговорки генерального директора, вы соглашаетесь уделить время для интервью.

## Несколько правил ведения "интервью"

• ***Обязательно польстите собеседнику, показав, что вы осведомлены о его значимости в компании.*** Делать это лучше или вначале, прямо во время вступления к интервью, или ближе к середине разговора.

• ***Обязательно прорабатывайте все мелкие детали и постарайтесь узнать как можно больше информации об интервьюируемом и его деятельности еще до интервью.*** Люди раскрываются только перед теми, в ком они видят заинтересованного их персоной собеседника. Кроме этого, если вы "в теме", то у вас будет амплуа осведомленного человека, а по отношению к осведомленному человеку и процент доверия больше (мол, свой), и "внутренние тормоза" ослабевают (осведомленному и сболтнуть что-то лишнее не страшно, так как он наверняка и сам все это знает, а то что спрашивает – ну ему по плану его интервью там про это спрашивать положено. Однако не забывайте и говорить заведомо неверные вещи. Это тоже очень хороший прием, так как многим людям присуще желание показать свою значимость, и, как только вы покажете свою некомпетентность, они тут же станут вас поправлять.

• ***Наберитесь терпения.*** Скрытый допрос требует терпения. Никогда не торопите события. Если ваш собеседник поймет, что вам надо от него нечто большее, чем просто интервью, он просто замкнется и начнет говорить о погоде. Из этой же серии совет о том, что на собеседника ни в коем случае не стоит "давить", насильно подводя его к нужному вопросу.

• ***Внимательно слушайте собеседника.*** **В** течение всего времени интервью. Ни в коем случае нельзя делать так, чтобы показать свою заинтересованность каким-то конкретным вопросом. Потому что вас должны интересовать все вопросы, и тот вопрос, который вам

действительно интересен, должен быть просто "одним из" в той череде вопросов, которые вы задаете. Желательно даже спланировать беседу так, чтобы интересующий вас вопрос задали не вы, а о нем стал говорить сам собеседник. Таким образом, вы должны так спланировать беседу, чтобы плавно подвести собеседника к интересующему вас вопросу.

• ***Не оканчивайте интервью, сразу после того, как все узнали.***

После этого перейдите на нейтральные темы, и таким способом завершите разговор. Это важно не только из-за того, чтобы собеседник не заподозрил неладное, а еще и для соблюдения **"закона края",** согласно которому наилучшим образом запоминаются те моменты разговора, которые происходят в его начале и конце. А то, что в середине, соответственно, запоминается намного хуже. Вообще правилом хорошего тона в "вытягивании" информации является построение скрытого допроса так, чтобы собеседник вообще не узнал, что сболтнул что-то лишнее. Для этого надо соблюдать два простых правила, которые в 70% случаев приведут к нужному результату:

– маскируйте значимые для вас вопросы чередой незначимых;

– задавайте нужные вопросы в середине беседы, для того чтобы по закону края интервьюируемый забыл их первыми.

• ***Оставляйте благоприятное впечатление об интервью у своего собеседника.*** Это важно, в первую очередь, для того, чтобы ваш собеседник имел желание продолжить общение в будущем.

> ***Примечание***
>
> О правилах ведения переговоров и о психологических законах, которые лежат в их основе, мы будем подробно говорить в *приложении **1.***

## Простые правила, позволяющие избежать данный вид атак

Существует два очень простых правила, которые позволяют избежать данного вида атак.

• **Правило первое.** Ни один из сотрудников предприятия не должен знать больше, чем ему полагается знать по должности. К сожалению, нередко это правило не соблюдается, и часто бывает так, что любой сотрудник знает не меньше генерального директора. Что, конечно же, не просто неверно, а очень опасно.

> ***Большинство людей не умеют хранить секреты***
>
> Если вы руководитель какого угодно масштаба и ранга, запомните одно из самых важных правил, выполнение которого на много процентов обезопасит вас от многих социоинженерных атак. Правило такое: подавляющее большинство людей не могут хранить даже свои сокровенные секреты, не говоря уже о чужих. Если вы наедине поделитесь какой-либо информацией с сотней лучших сотрудников, предупредив каждого, что информация сугубо секретна, можете быть уверены, что 90 человек ее непременно "сольют на сторону". По самым разным причинам. Кто-то по глупости житейской, кто-то жене за вечерним чаем, кто-то "по пьяни", кого-то будет переполнять чувство собственной значимости, потому что "сам генеральный доверился и рассказал" и об этом, конечно же, нужно рассказать друзьям, которым никто никогда такой важной информации не доверял… Причин тут много. И они не главное – важен результат: большинство не могут хранить секреты. И, конечно, одно из качеств хорошего руководителя, – это умение разбираться в людях, которое полезно

хотя бы для того, чтобы из этой сотки выделить те пять-десять человек, которым действительно не страшно довериться.

• **Правило второе.** Применяемое в том случае, если у кого-то из сотрудников возникнет желание с кем-то поделиться той информацией, которую ему положено знать по должности. В трудовом контракте с сотрудником обязательно должен быть прописан пункт о том, что за разглашение коммерческой информации сотрудника ждет ответственность вплоть до уголовной. Именно так – "ответственность вплоть до уголовной", так как все другие виды наказания (взыскания, штрафы и пр.) легко обходимы. Подумаешь, штраф какой-то. Его же не сотрудник будет платить, а та организация, которая, скажем, заказала ему вашу клиентскую базу данных, потому что к сумме счета за свои "услуги" ваш "сотрудник" просто добавит сумму штрафа.

***Примечание***

И еще. Небольшое добавление ко второму правилу. Вы можете себя не ограничивать в средствах запугивания своих сотрудников на предмет того, что с ними будет после того, как они что-то сворują в вашей организации. Потому что некоторых работников удержать от дурных поступков может только страх. Так как страх за свое дальнейшее будущее для многих это именно то единственное чувство, которое сильнее страсти к деньгам.

## Воровство клиентских баз данных

Продолжим начатый в *главе 1* разговор о воровстве клиентских баз данных. Несмотря на то, что достоянием гласности являются только единичные факты воровства клиентских баз данных, количество даже известных широкой публике случаев за последнее время значительно выросло. Для нас наиболее интересно то, что большинство хищений информации связано с использованием методов социальной инженерии.

***Примечание***

Причина того, что достоянием гласности становится лишь малый процент таких хищений в том, что фирмы, естественно, не желают портить свою репутацию, признаваясь в собственной беспечности.

Наиболее просто добыть клиентские базы данных – это воспользоваться беспечностью сотрудников, работающих на предприятии. Нередко счета фактуры и прочие документы валяются на столах у сотрудников, которые еще имеют привычку выходить из своего кабинета минут на 10 – 30, так что, если и не надо, со скуки все пересмотришь. В некоторых магазинах, допустим по продаже офисной техники, мебели и т. д., многие продавцы оформляют счета, отвернувшись к своему компьютеру, а то, что я, к примеру, могу быть сотрудником конкурирующей фирмы, и мне ничто не мешает постоять за спиной и посмотреть список клиентов, это никого не волнует. Однажды одной даме, которая слишком долго оформляла мою покупку (в компьютерном магазине), я сказал: "Девушка, я вижу, что вы еще не очень освоились с 1С-предприятием, давайте, я вам помогу". Девушка с удовольствием приняла мою просьбу, встала из-за компьютера и …вообще ушла на 15 минут. Вероятно, пить чай. Что еще интереснее, ни один из сотрудников, которые туда-сюда сновали мимо меня (ее компьютер стоял в центре магазина), не поинтересовался, чего это собственно я (посторонний человек) за ним сижу.

Случаи, когда похищаются клиентские базы данных, пользуясь беспечностью работающих на предприятии кадров, очень нередки.

К примеру, для начала можно представиться сотрудником фирмы, которая устанавливает базы данных, и, проникнув таким образом за компьютер, или просто спросив у сотруд-

ников, узнать, какие базы данных уже установлены на пользовательских машинах. А если повезет, то заодно их и скачать.

Можно поступить так, как было в одной энергетической компании Санкт-Петербурга (этот случай мы описывали в *главе 1),* когда человек, представившись другом заболевшего сотрудника (системного администратора), сказал, что друг попросил его сегодня заменить. Хотя выяснить, друг попросил или кто-то еще, можно очень просто: позвонив своему сотруднику и перепроверив информацию. Правда, можно поступить хитрее и действительно сделать так, что друг подтвердит эту информацию. Можно ведь просто стать на некоторое время другом системного администратора. Пусть и не лучшим. Главное, чтобы этой дружбы было достаточно для того, что когда он действительно заболеет (или просто по каким-то причинам не сможет прийти на работу), он обратился за помощью к кому нужно. К другу, то есть, который только этого и ждет. Или не просто ждет, а пытается форсировать ситуацию. К примеру, вам вдруг неожиданно пришла повестка в военкомат, и, надо же какое совпадение, в тот вечер, когда вы обнаружили ее в своем ящике, вы как раз шли к себе домой вместе с другом попить пивка.

– Ой, е…, – говорите вы "другу", – мне же завтра обязательно нужно быть на работе. Чего же делать то…

А друг он на то и друг, чтобы подстраховать товарища в нужную минуту.

– Да ерунда, – говорит он вам, – дел-то на три копейки. Давай я завтра вместо тебя схожу и все сделаю. Позвони своему боссу, предупреди, что, так, мол, и так, у меня такая ситуация и вместо меня придет мой хороший товарищ.

И, радуясь, как удачно все разрешилось, вы вместе с "другом" со спокойной душой идете пить пиво.

Можно на месяц устроиться в фирму, у которой надо украсть базы, менеджером по продажам. И уйти из нее на второй день, сказав, что не устроил коллектив вообще и директор в частности.

> ***Примечание***
>
> Один из самых простых способов своровать нужную базу данных. Таким образом одна московская часовая мастерская своровала клиентскую базу данных у своего конкурента. Цена вопроса составила около $1500.

Ну и, наконец, самый распространенный тип кражи баз данных, это их "уход" с предприятия вместе с сотрудниками, как это произошло некоторое время назад с одной московской фирмой по продаже мебели, когда все ключевые менеджеры ушли и открыли свое дело. Аналогичная ситуация случилась недавно в Санкт-Петербурге у крупной компании, занимающейся продажей сотовых телефонов. В обоих случаях только умение директоров договариваться с партнерами, которым они объяснили ситуацию, помогло спасти дело. Известен случай в Новосибирске, когда из компании, занимающейся корпоративной поставкой компьютеров, ушли ключевые менеджеры и создали собственную фирму, естественно, под работу с теми клиентами, которых они обслуживали, трудясь в прежней организации. Примеры приводить можно долго.

Как же защититься от воровства клиентских баз? Самое простое – соблюдать те правила защиты, о которых мы говорили в предыдущем разделе, дополнив их еще несколькими. Итак.

• Ни один из сотрудников предприятия не должен знать больше, чем ему полагается знать по должности.

• В трудовом контракте с сотрудником обязательно должен быть прописан пункт о том, что за разглашение коммерческой информации сотрудника ждет ответственность вплоть до уголовной.

***Примечание***

Еще раз повторимся, что этот пункт является одним из самых важных в защите компании от подобных случаев. В трудовом договоре с сотрудником должно быть четко прописано, во-первых, что является предметом коммерческой тайны, и, во-вторых, какие неприятности ожидают сотрудника, в том числе и уволившегося после разглашения предмета коммерческой тайны этим сотрудником. Сотруднику нужно четко разъяснить, что согласно ст. 7, 8, 10 и 11 Федерального закона "О коммерческой тайне" работодатель имеет право подписать с сотрудником документ о неразглашении сведений, которые по мнению работодателя составляют предмет коммерческой тайны предприятия, и за разглашение которых он может применить к сотруднику те или иные меры, вплоть до судебного преследования, а согласно ст. 4 этого закона сотрудник обязан будет возместить причиненные фирме убытки, возникшие в результате разглашения им конфиденциальной информации (размер убытков устанавливает суд). Известно, что после такого инструктажа у большинства сотрудников мысль разгласить чего-либо пропадает в момент появления. Специально же для тех, кому этого мало, можно влезть в юридическую казуистику и пояснить, что клиентскую базу данных, вообще-то, можно рассматривать как средство производства, которое является собственностью работодателя. Из чего следует, что воровство этой базы можно уже рассматривать как воровство чужого имущества, что является предметом соответствующей статьи уже Уголовного кодекса (ст. 159 УК РФ). Кроме того, можно сообщить сотруднику, что при большом желании за хищение базы данных вы можете инициировать его судебное преследование аж по четырем статьям Уголовного кодекса: уже упомянутой ст. 159 ("Кража"), ст. 272 ("Несанкционированный доступ к компьютерной информации"), ст. 183 ("Незаконное разглашение и получение сведений, составляющих коммерческую, банковскую или налоговую тайну") и ст. 146 ("Нарушение авторских и смежных прав"). Практика показывает, что когда перед людьми появляется возможность за кражу информации получить уголовное преследование, они становятся намного осмотрительнее в своих действиях.

• Посторонние люди не должны иметь простого доступа в офис.

• Если в комнате находятся посторонние, сотрудники ни при каких условиях не должны выходить из комнаты.

• Нередко бывает так, что доступ к клиентской базе имеет практически любой сотрудник, так как база лежит на общем Doc-сервере, к которому не имеет доступа разве что уборщица. Конечно, такого быть не должно. Доступ к клиентской базе данных должны иметь только те служащие, которым это положено по должности. Это всем известное правило, согласно которому, чем меньше лиц имеет доступ к конфиденциальной информации, тем меньше вероятность, что эта самая информация "уйдет на сторону".

***Замечание***

Многие эксперты в области конкурентной разведки приводят еще правило, согласно которому все компьютеры, которые имеют доступ к клиентской базе, не должны иметь выхода в Интернет, быть без дисководов, приводов CD– и DVD-ROM, USB-входов, с них нельзя ничего распечатать и т. д. На наш взгляд, это правило, во-первых, не реальное, так как подобные меры просто очень сильно затруднят работу, а, во-вторых, ни к чему не

приводящее, поскольку в этом случае компьютеры тогда должны быть еще и без мониторов, чтобы нельзя было перефотографировать информацию с экрана монитора. В настоящее время некоторые эксперты склоняются к тому, что уменьшить потери от воровства клиентских баз с компьютеров поможет внедрение систем *CRM* (систем управления и учета взаимоотношений с клиентами).

## Фишинг

Фишинг на сегодняшний день является одним из самых распространенных видов социальной инженерии. По сути фишинг это выведывание информации для доступа к банковским счетам доверчивых пользователей. Он распространен в тех странах, где пользуются популярностью услуги интернет-банкинга. Чаще всего "фишеры" используют поддельные электронные письма, якобы присылаемые банком, с просьбой подтвердить пароль или уведомление о переводе крупной суммы денег.

***Примечание***

Само слово "фишинг" происходит от английского fishing, что, в свою очередь, переводится как рыбалка. Такое название этому виду мошенничества дали потому, что он на самом деле очень напоминает рыбалку, так как фишер по сути забрасывает наживку (вернее, несколько сотен наживок) и ждет, пока на нее кто-то "клюнет".

Суть фишинга сводится к следующему. Злоумышленник заставляет пользователя предоставить ему какую-либо секретную информацию: информацию о банковских счетах, кредитных картах и т. д. Самое важное в том, что жертва совершает все эти действия абсолютно добровольно, – фишеры хорошие психологи и действуют четко.

Выделяют три основных вида фишинга:

- почтовый;
- онлайновый;
- комбинированный.

*Почтовый фишинг* появился первым, – об этом виде мошенничества общественность узнала еще в 1996 году.

***Примечание***

Тогда сразу несколько тысяч клиентов провайдера America Online получили электронные письма от "представителя компании" с просьбой выслать логин и пароль для входа в систему. И многие выслали.

Суть почтового фишинга в том, что жертве отправляется электронное письмо, в котором содержится просьба выслать те или иные конфиденциальные данные. К примеру, от имени интернет-провайдера с похожего (или идентичного) почтового адреса отправляется письмо, в котором написано, что по провайдеру нужно узнать логин и пароль для доступа в Интернет указанного пользователя, так как сам провайдер по тем или иным техническим причинам (база "рухнула") этого сделать не может. Более интересный пример связан с одним известным американским банком, клиенты которого однажды получили сообщения о том, что на их счет пришло большое перечисление (допустим несколько десятков тысяч долларов), и в соответствии с договором, так как сумма перечисления превышает сумму в $1000, им для подтверждения получения перевода необходимо пройти по ссылке, приведенной в конце письма, и ввести всю необходимую информацию для подтверждения перевода. В противном случае перевод будет отправлен назад. Мало кто смог побороть свою жадность, и несколько тысяч клиентов банка стали объектом фишинг-атаки.

***Примечание***

Это как раз тот случай, когда социальные хакеры блестяще сыграли на одном из людских пороков – жадности.

*Онлайновый фишинг* заключается в том, что мошенники один в один копируют какой-либо из известных сайтов, причем для него выбирается очень похожее доменное имя (или то же самое, только в другой зоне), и создается идентичный дизайн.

***Примечание***

В качестве приманки (аттракции) товары в этих поддельных интернет-магазинах продаются практически по демпинговым ценам, что неудивительно, ведь никто ничего на самом деле реально не продает.

Дальше происходит примерно следующее. Решив совершить в магазине покупку, пользователь вводит свои логин, пароль и номер пластиковой карты, после чего все эти данные становятся известными злоумышленнику. После чего мошенник незамедлительно "обнуляет" кредитную карточку жертвы.

***Примечание***

Данный вид фишинга иногда еще называют *имитацией бренда* (brand spoofing).

*Комбинированный фишинг* является объединением двух предыдущих видов фишинга. Его появление вызвано тем, что почтовый и онлайновый фишинг уже достаточно устарели, да и пользователи стали грамотнее в части информационной безопасности. Поэтому фишеры придумали другую тактику. Так же как в онлайновом фишинге создается поддельный сайт, а потом как в почтовом фишинге пользователям отсылаются письма с просьбой зайти на этот сайт.

***Примечание***

Это достаточно сильный психологический ход, благодаря которому комбинированный фишинг сразу же получил огромное распространение. Дело в том, что посетители стали настороженнее, и уже немногие просто так скажут свои пароли (хотя и такие встречаются). А в комбинированном фишинге эта настороженность как раз и снимается, благодаря тому, что в письме пользователя не просят сообщать какие-либо конфиденциальные данные, а просто просят зайти на сайт. Всего то. Пользователю просто предлагается зайти на какой-либо сайт, и самому проделать все необходимые операции.

Сейчас происходит самый настоящий бум фишинга. Об этом, в частности, могут свидетельствовать следующие цифры: всего с октября по январь 2005 года Федеральная комиссия США по торговле зарегистрировала более 10 млн (!) жалоб от пользователей, ставшими жертвами фишинг-атак. Общая же сумма убытков по данным этой же организации составила около $15 млрд за 2005 год.

***Примечание***

Естественно, законодательства всех стран оказались неприспособленными к этому новому виду мошенничества.

***Из истории Российского фишинга***

В России первый зарегистрированный случай фишинга датируется маем 2004 года, когда клиенты Сити-банка получили по электронной почте

письма с просьбой зайти на сайт банка (лжесайт, естественно) и подтвердить номер своей карты и ПИН-код.

Фишеры в своей деятельности прекрасно используют связь с теми или иными событиями. К примеру, человеку точно в его день рождения приходит поздравительная открытка, в которой написано, что ему ко дню рождения банк, клиентом которого он является, в рамках проводимой акции "День Рождения" перечислил на счет $500. Для того чтобы их получить, нужно зайти на сайт банка (поддельный, естественно) и ввести необходимую информацию. Многие не чураются использовать и такие горестные для всех события, как крупные теракты или стихийные бедствия, когда различные организации просят людей перечислять деньги в фонд помощи пострадавшим. Просят и фишеры. По тем же схемам, что мы рассматривали: зайдите на сайт, зарегистрируйтесь и спишите какую-то сумму со своего счета.

***Примечание***

На момент написания книги единственным браузером оснащенным защитой от фишинга по умолчанию является Opera, начиная с версии 8.0.

В настоящее время многие IT-специалисты по всему миру заняты разработкой способов, позволяющих защититься от атак фишеров. Кроме того, что в браузерах будут создаваться черные списки фишинг-сайтов, предложено еще несколько способов.

• *Генераторы одноразовых паролей*

Поскольку суть фишинга состоит в получении паролей и банковских сведений, необходимых для доступа к электронным счетам пользователей, использование генераторов одноразовых паролей позволяет обойти этот вид мошенничества. Генератор одноразовых паролей на вид напоминает обычный небольшой карманный калькулятор. Когда пользователь заходит на сайт банка, для того чтобы получить доступ к своему счету, ему необходимо ввести показанную генератором последовательность символов. Банк применяет тот же алгоритм для создания пароля. Доступ предоставляется только в том случае, когда оба пароля совпадают. Такой пароль нельзя украсть по той простой причине, что доступ по нему можно получить только один раз. Минусы использования такой системы состоят в дополнительных расходах для клиентов.

***Примечание***

В настоящее время генераторы одноразовых паролей применяют многие банки США и Европы, а также крупные интернет-провайдеры, к примеру, провайдер AOL.

• *Использование USB-устройств*

Суть данного приема сводится к тому, что пользователь не сможет получить доступ к своему счету, если он не подключит USB-устройство к своему компьютеру. В этом случае мошенники также не смогут получить доступ к счету пользователя.

***Примечание***

Наряду с USB-устройствами предлагалось использовать также специальные карты с микросхемами, которые вставляются в считывающее устройство, подключенное к компьютеру. Однако от этого варианта отказываются, как от дорогостоящего.

• *Мобильное подтверждение*

Суть этого приема в том, что доступ к карте осуществляется только после того, как пользователь отправит со своего мобильного телефона, номер которого он сообщил банку, какое-либо сообщение SMS (Short Message Service).

• *Хеширование паролей конкретного Web-сайта*

Хеширование паролей предотвращает кражу конфиденциальных данных путем добавления к паролю информации, специфичной для того сайта, где предполагается применить пароль. Пользователь просто вводит в специальной форме свой пароль, а браузер преобразует его и добавляет необходимую информацию. Суть в том, что Web-сайту, на котором пользователь вводит пароль, этот пароль в чистом виде не сообщается, на сайт приходит уже хешированный пароль. Таким образом, даже если пользователь и введет свой пароль на фальшивом сайте, то хакеры его применить не смогут. На настоящем же сайте применяется та же схема хеширования, что и у владельца карты.

## Фарминг

Более опасным видом мошенничества, чем фишинг, является так называемый *фарминг.* Фарминг заключается в изменении DNS-адресов так, чтобы страницы, которые посещает пользователь, были не оригинальными страницами, скажем, банков, а фишинг-страницами.

Поскольку суть фарминга сводится к автоматическому перенаправлению пользователей на фальшивые сайты, фарминг гораздо более опасен, чем фишинг, так как в отличие от последнего новый метод хищения данных не требует отсылки писем потенциальным жертвам и соответственно их ответа на них. Это, естественно, более изощренный, хотя и технически намного более сложный метод мошенничества, чем фишинг. Но зато при фарминге у пользователя практически нет причин проявлять свою недоверчивость: писем никто не присылал, на сайт никто заходить не просил. Пользователь сам по своему желанию решил зайти на сайт банка, и зашел. Только не на оригинальный, а на поддельный сайт.

Опасность фарминга многие исследователи связывают еще и с тем, что с целью его развития хакеры будут предпринимать все больше атак на DNS-серверы, и эти атаки будут все изощреннее. Опасно же это тем, что если количество взломов DNS-серверов возрастет, то это приведет к настоящему хаосу в мировой сети.

> ***Примечание***
>
> Служба DNS (Domain Name System) предназначена для того, чтобы сопоставить адрес сайта, который пользователь набрал в браузере, реальному IP-адресу того сервера, на котором этот сайт расположен. Службу DNS нередко сравнивают с телефонным справочником, в котором вы сначала выбираете имя, потом смотрите номер и звоните по указанному номеру. Так и здесь: выбираете имя сайта, служба DNS говорит вам его "номер" (IP-адрес), после чего вы идете на указанный сайт.

Кроме роста взлома DNS-серверов, исследователи также прогнозируют рост сетевых взломов типа ARP-spoofing, который, по сути, представляет собой подмену MAC-адреса и предназначен для прослушивания трафика между двумя машинами.

> ***Примечание***
>
> Протокол ARP используется компьютерами для обращения друг к другу в пределах одной сети путем преобразования IP-адреса в MAC-адрес нужного компьютера, после чего происходит связь по протоколу Ethernet.

## Рейдерские атаки

*Рейдеры* – это захватчики предприятий. Соответственно рейдерская атака – это атака по захвату предприятия.

Классическая схема рейдерской атаки выглядит следующим образом.

## 1 этап. Сбор информации о захватываемом предприятии

Как всегда, в любом виде деятельности, сбор информации – самый важный подготовительный этап. На этом этапе собирается и анализируется вся информация о предприятии: финансовая ситуация на предприятии, список контрагентов, список клиентов, список акционеров (реестр акционеров), информация о слабых и сильных сторонах предприятия, о вредных привычках руководства и сотрудников, кто с кем и против кого дружит на предприятии, информация о маркетинговых планах и прочее, прочее. На первом этапе в большинстве своем работают методы социальной инженерии, с помощью которых, как мы уже говорили ранее, собирать информацию легче всего. Как правило, этот этап занимает от одного до трех месяцев в зависимости от масштабов предприятия и от сложности добывания нужной информации. Самое важное для рейдера на этом этапе – получить тем или иным способом копию реестра акционеров.

## 2 этап. Начало атаки

Началом атаки можно считать тот момент, когда рейдер начинает скупку акций у миноритарных акционеров. Миноритарии, как правило, с акциями расстаются очень легко, так как реально ощутимых дивидендов по ним практически не получают, а рейдеры предлагают за акции суммы в размере годового оклада.

> ***Примечание***
>
> *Миноритарные акционеры* – это акционеры с небольшим количеством акций. К примеру, в начале 90-х годов в разгул приватизации очень нередко, когда почти каждый работник какого-то большого предприятия с несколькими тысячами человек сотрудников имел по две-три акции. Вот такие акционеры и называются миноритарными.

Параллельно со скупкой акций у миноритариев проходит работа по "закошмариванию предприятия", если выражаться на рейдерском языке. Основная цель "закошмаривания" – дезорганизация работы предприятия. Кроме этого достигается также побочная цель: колеблющимся акционерам демонстрируется, что на предприятии имеются большие проблемы, после чего они со своими акциями расстаются гораздо охотнее. Второй этап для предприятия это действительно кошмар, лучше слово сложно придумать: руководству вчиняются иски от имени акционеров по поводу нарушения различных операций с акциями, нарушении порядка проведения сделок (о чем рейдер узнает на первом этапе), в отношении руководства и сотрудников предприятия возбуждаются уголовные дела (неважно по реальным поводам или нет – главная цель это издергать людей), инициируются проверки деятельности предприятия различными службами (налоговой инспекцией, санэпидстанцией, противопожарной службой, природоохранной прокуратурой и т. д. – чем больше, тем лучше), для парализации работы предприятия используется тактика гринмейлера, и т.д.

> ***Примечание***
>
> На языке рейдеров *гринмейл* – это корпоративный шантаж, достигаемый реализацией прав мелких акционеров агрессивным образом или "закошмариванием" предприятия.

Способов, причем абсолютно легальных, "закошмарить" практически любое предприятие очень много. По сути, при "закошмаривании" предприятию устраивается классическая DDoS-атака (отказ от обслуживания) на социальном уровне.

> ***Примечание***

Как правило, при "закошмаривании" предприятия основную роль играют именно социальные хакеры, которые используют в своей работе методы социального программирования.

Руководство предприятия, видя, что стало объектом рейдерской атаки, как правило, начинает идти на увольнение работников, продающих свои акции, с целью устрашения тех, кто еще свои акции не продал. Иногда это дает результат, иногда нет. Кроме того, акции предприятия переводятся в доверительное управление или передаются в залог какой-нибудь конторе, подконтрольной предприятию. После этого руководством, как правило, проводится дополнительная эмиссия акций и организуется контрскупка акций.

## 3 этап. Внесение раскола в состав руководства предприятия

Для того чтобы заполучить предприятие практически легально, рейдерам достаточно 30% плюс одна акция. Однако в настоящее время ситуация такова, что управление предприятия держит в своих руках от 70% и более акций (так называемый *консолидированный пакет)*. Поэтому рейдеру необходимо внести раскол между членами управляющего органа предприятия, для чего рейдер пытается расколоть управляющий орган, сыграв на различных внутренних противоречиях между управленцами предприятия (о их внутренних противоречиях тоже узнается на первом этапе). По сути 3-й этап – это этап "плетения интриг" между руководителями предприятия и этап скупки акций у основных держателей, которым делаются различные "интересные предложения".

Кроме того, на этом же этапе формируется оппозиция из недовольных миноритарных акционеров, для того, чтобы под флагом этой оппозиции рейдеры могли проникнуть на предприятие.

Руководство предприятия на этом этапе, как правило, делает два шага:

• пытается теми или иными способами смягчить конфликт между управленцами предприятия;

• идет на уступки миноритарным акционерам с целью смягчения давления оппозиции.

## 4 этап. Работа с активами предприятия

На этом этапе руководство предприятия пытается сделать так, чтобы захват предприятия потерял для рейдера смысл. Для этого руководству нужно либо вывести активы предприятия, либо каким-либо образом их обременить. Рейдеры же, естественно, пытаются этого не допустить.

## 5 этап. Вход на предприятие

Теперь рейдеру нужно легальным образом зайти на предприятие. Основной метод: внеочередное собрание акционеров и переизбрание совета директоров. Делается это примерно следующим образом. Если у рейдера имеется 30% плюс одна акция, то в действующий орган управления предприятием посылается требование о созыве внеочередного собрания акционеров. После того, как основное собрание проигнорирует требование, рейдеры имеют право провести такое собрание самостоятельно.

***Примечание***

Как правило, подобные собрания проводятся скрытно, чтобы на нем могли присутствовать только подконтрольные рейдеру акционеры. Известно немало случаев, когда подобные собрания проводились в воинских частях. Таким образом, рейдеры делают все, чтобы "ненужные акционеры" не попали на собрание. Известны случаи, когда рейдеры для этой цели

разыгрывали целые спектакли. К примеру, перед входом в здание, где должно проходить собрание акционеров, представители рейдера на входе в здание перехватывали ненужных участников собрания и вели их в другой зал этого же здания, где перед ними разыгрывался спектакль под названием "собрание акционеров", а в это время на настоящем собрании в другом зале рейдерская партия большинством голосов переизбирала совет директоров. Иногда применяется обратный подход, при котором, наоборот, оппоненты допускаются на собрание для того, чтобы всему миру показать, что все законно, что на собрании были не только подконтрольные рейдеру оппоненты, но и представители противоположной стороны. Только при этом акции оппонента каким-либо образом "блокируются", т. е. делается так, что оппонент временно не может воспользоваться своими акциями (и, следовательно, иметь право голоса), к примеру, из-за того, что на него заведено уголовное дело на предмет того, что когда-то он добыл эти акции незаконным путем.

На первом собрании 30% плюс одна акция не является достаточным кворумом для принятия решения, поэтому на первом собрании констатируется отсутствие кворума, эта констатация заносится в протокол собрания, и все расходятся. Изюминка в том, что если собрать собрание повторно, 30% плюс одна акция уже будет кворумом, и решения принимаются большинством голосов. Решения и принимаются: прекратить полномочия прежнего совета директоров и избрать новый совет директоров. Таким образом создается параллельный орган управления. Умные рейдеры, как правило, делают еще один остроумный шаг. Они делают так, что один из участников собрания …направляет в суд претензию к проведению собрания и просит признать суд собрание недействительным. Казалось бы: зачем рейдерам это надо? Это же кажется нелогичным. На самом же деле все логично. Повод для претензии выбирается очень формальный, и, желательно, какой-то вздорный, в общем, такой, который суд не признает значимым. Суд и не признает и отказывает в удовлетворении иска. А поскольку заседание суда прошло, то у рейдера появляется документ о том, что фактически суд признал собрание легитимным (это называется словом *преюдиция)*. Документ этот, естественно, очень ценный.

После того, как произошло собрание акционеров с переизбранием совета директоров, по сути, предприятие в руках рейдеров, и параллельный орган управления берет на себя контроль над деятельностью предприятия.

Дальнейшее развитие событий зависит от того, какую цель ставили перед собой рейдеры, захватывая предприятие. Если они захватывали предприятие только из соображений наживы, то после захвата быстро реализуется цепочка по продаже предприятия. Нередко, что в результате реализации этой цепочки предприятие попадает к добросовестному хозяину. Если же целью рейдеров был бизнес предприятия, то после захвата начинается этап "ликвидации последствий военных действий": начинаются выплаты зарплат сотрудникам, делаются перечисления в бюджет и т. д.

***Примечание***

Нередки случаи, когда прежние руководители предприятия переквалифицировались в рейдеров и начинали отбирать у захватчиков свое бывшее родное предприятие по всем правилам рейдерской атаки.

Вот примерно так происходят рейдерские атаки на различные предприятия.

***Примечание***

Естественно, подробное описание всех этапов рейдерской атаки выходит за рамки данной книги, но нам это и не особо важно. Для нас

важно то, что на многих этапах этой атаки используются приемы социальной инженерии и социального программирования.

**Где же применяется социальная инженерия и социальное программирование при организации рейдерских атак?**

Социальная инженерия в классическом виде применяется в основном на первом этапе, то есть тогда, когда собирается информация об организации. А как мы говорили ранее, собирать информацию проще всего методами социальной инженерии. На втором этапе к методам социальной инженерии добавляются методы социального программирования, поскольку второй этап – начало рейдерской атаки это уже не сбор информации, а работа по дестабилизации деятельности предприятия и здесь лучше подходят различные методы социального программирования, один из которых – устройство предприятию атаки "отказ от обслуживания". Методы же социальной инженерии на втором этапе тоже могут применяться, к примеру, для дискредитации компании в сети Интернет. Для этого, как правило, используются форумы на сайте компании и прочие инструменты, посредством которых представители компании общаются в Интернете с посетителями своего сайта. Ну и, конечно, на третьем этапе, этапе интриг и заговоров, без социального программирования тоже никуда (конечно, в области его отрицательного применения). Таким образом, основные и значимые этапы "рейдерского наезда" – это социальное хакерство в чистом виде.

**Почему социальное хакерство и социальное программирование популярный инструмент для рейдерских атак?**

Дело в том, что основная концепция социального программирования состоит в том, что многие поступки людей и групп людей **предсказуемы** и подчиняются определенным законам. Простой и банальный пример. Если на предприятии стало плохо, то люди с него побегут. Совершенно всем понятная вещь. А ведь это социальное программирование в чистом виде. Сотрудники предприятия – это большая социальная группа. А сказав фразу "если на предприятии стало плохо, то люди с него побегут" мы, по сути, сказали, что разработали метод воздействия на большую социальную группу, которой в данном случае является многотысячная армия сотрудников предприятия. Таким образом, мы предсказали, как будет вести себя данная социальная группа под воздействием некоторой внешней силы. Внешняя сила здесь – ухудшение обстановки на предприятии, а прогнозируемый нами способ поведения – это констатация того факта, что при ухудшении условий сотрудники предприятие покинут. Все просто и банально, и, несмотря на это, мы увидели, что даже большой социальной группой можно вполне осознанно управлять, так как ее действия вполне прогнозируемы.

**Как определить начало рейдерской атаки?**

О том, что вас начали атаковать, можно определить по следующим признакам.

• Начались проверки предприятия различными инстанциями: налоговой полицией, санэпидстанцией, МЧС, МВД, различными надзорными организациями и др. Причем проверяющие просят предоставить копии документов, в которых указаны сведения об активах фирмы, о кредиторской задолженности, об акционерах.

• В средствах массовой информации (СМИ) появляются негативные статьи о предприятии, о его руководстве, да и вообще неожиданно ни с того ни с сего СМИ вдруг стали проявлять повышенную активность в отношении предприятия.

***Примечание***

Особенно этот пункт должен вас насторожить, если в СМИ появляются сообщения об ущемлении прав миноритарных акционеров.

• Акционеры вдруг получили заказные письма с уведомлением о вручении, в которых находится, к примеру, поздравление с ближайшим праздником. Или вообще ничего не нахо-

дится. Или находится простой чистый лист бумаги. Не важно. Главное, что таким образом те, кто собрался вас атаковать имитируют формальность, так как согласно закону перед созывом внеочередного собрания акционеров нужно им направить предложение о созыве такого собрания. Вот и направили. А потом в суде атакующие скажут, что акционерам направлялось предложение о продаже их акций, а совету директоров предприятия было направлено предложение о внеочередном созыве собрания акционеров. Судья попросит предъявить доказательства того, что такие письма были направлены. Этим доказательством будет уведомление о вручении письма. А то, что противоположная сторона будет говорить, что, мол, не правда, там открытки лежали, так на это всегда можно сказать, что там лежали реальные документы, а про открытки это все наглая ложь.

• Миноритарные акционеры начинают проявлять интерес к деятельности предприятия, чего за ними никогда не замечалось.

***Примечание***

Особенно надо насторожиться в том случае, когда действуют не они сами, а по генеральной доверенности от их имени действуют какие-то родственники, которые, как нельзя кстати, являются большими специалистами в корпоративном праве.

• Вам стали часто поступать предложения о продаже ваших акций или их доли.

Теперь несколько примеров того, как рейдеры атаковали некоторые предприятия.

К руководителю ООО "Памир"[2] поздно ночью, когда он возвращался с работы, подошли два человека, которые представились сотрудниками правоохранительных органов, и предложили пройти с ними, чтобы подписать документы о передаче его доли акций, мотивировав это тем, что мол, поскольку фирма не платит налогов, у нее скоро начнутся серьезные проблемы. А сотрудники правоохранительных органов, так получилось, являются доброжелателями фирмы, так как сами не раз обращались за услугами в "Памир" и теперь хотят помочь руководству. Мол, у них на конспиративной квартире сидит покупатель, и если продать ему свою долю сейчас, то хоть какие-то деньги получишь, а через полгода вас все равно разорят, и останешься только должен. Фирма налоги платила исправно, грозы ничего не предвещало, серьезной аргументации "сотрудники правоохранительных органов" не имели. Директор от такой сомнительной сделки отказался, и вроде бы все затихло. Но через год после этого случая в 000 "Памир" к руководству пришел человек с предложением продать все предприятие или долю в нем, на что руководитель ему ответил, что никто ничего продавать не собирается. Через некоторое время после этого аналогичные предложения поступили остальным акционерам Общества. Они также отказались от продажи и поставили в известность руководство, которое справедливо заключило, что фирму кто-то взял "на мушку". Руководство, проанализировав ситуацию, поняло, что кому-то стало известно о некоторых пробелах в уставной документации Общества и срочно исправило их. После того, как были приняты изменения в уставе Общества, согласно которым любые изменения в учредительные документы может вносить только лично директор или те, из учредителей, которые получили от него генеральную доверенность, предложения о продаже поступать перестали.

Но так гладко все бывает не всегда. Согласно публикации в одной из газет, у ЗАО "Элерон", которое являлся собственником большого участка земли и недвижимости на нем, рейдерская атака на него последовала даже несмотря на то, что все документы были оформлены идеально. По уставу общества доли в нем могли переходить только между акционерами общества, третьим же лицам, согласно уставу, продажа долей была запрещена. После того как одна из участниц продала свои акции, от ее имени началась рейдерская атака, хотя по закону ее доля перешла остальным членам общества. Рейдеры от ее имени направили иск

[2] Здесь и далее названия компаний, естественно, изменены. Любые совпадения с реально существующими организациями следует считать случайностью. – *Прим. авт.*

в арбитражный суд. Дальше было много неприятностей, и судебных заседаний, и "закошмаривания". Руководство фирмы и ее адвокаты обращались во многие инстанции, но везде им говорили примерно одно и то же, что, мол, пока фирму не отнимут, спокойной жизни не ждите. Ситуация разрешилась только после того, как руководство заручилось поддержкой высших лиц области.

Заметим, что сейчас количество рейдерских атак в рамках рассмотренной классической схемы пошло на убыль. Связано это с тем, что законодательство изменилось в лучшую сторону, оставив для рейдеров уже не такое большое количество законных возможностей по захвату предприятия. Кроме того, в крупных регионах уже почти все захватили. Ну и, наконец, основная причина на наш взгляд в том, что бизнес успешно учится защищаться, и самые лакомые кусочки рейдерам (основной пакет акций и активы предприятия) уже достать очень сложно, потому что активы предприятия, как правило, надежно спрятаны, а основной пакет акций консолидирован у руководства. Поэтому сейчас, как правило, применяется уже не классическая рейдерская атака, а так называемая *тактика гринмейлеров.* Дело здесь в том, что по закону "Об акционерных обществах" владение даже одной акцией позволяет такому акционеру запрашивать любую информацию о сделках компании, информацию об акционерах и т. д. И в принципе, поработав, можно даже с помощью одной акции перехватить власть у реального руководства. Руководство же знает, что связываться с профессиональными шантажистами – себе дороже, поэтому предпочитает от них откупаться. В результате за небольшой пакет акций (или даже за одну акцию гринмейлер получает неплохую сумму). Вот, примерно, таким образом гринмейлеры и зарабатывают.

# Глава 3
# Примеры социального программирования

В этой главе мы рассмотрим различные примеры социального программирования. Примеры и положительного применения, к коим можно отнести превращение агрессивной толпы в оказионную (о различных видах толп см. *далее в этой главе и в главе 8),* и отрицательного, к которым можно отнести, скажем, способы "закошмаривания" предприятий при рейдерских наездах, о них мы говорили в *предыдущей главе.*

Суть этой главы в том, чтобы показать примеры того, что в ряде случаев действительно можно "программировать" поведение людей, причем и одного человека, и большой группы людей. Примеры данного раздела относятся к категории социального хакерства именно по той причине, что во всех из них люди выполняли чью-то чужую волю, как бы подчиняясь написанной социальным хакером "программе". Примеры эти весьма разные. И по цели, которые ставили социальные хакеры, и по способам исполнения, и по последствиям, и по срокам исполнения. Есть и изящные многоходовки, и простые примеры, положительные и отрицательные, к категории социального хакерства относятся и многочисленные примеры черного и белого пиара (PR – сокращение от англ. *Public Relations),* некоторые из которых тоже приведены в *этой главе.*

## "Пожар" в кинотеатре

Классикой социального программирования является пример "с пожаром" в кинотеатре, описанный одной из газет еще в советские времена. Тогда группа шутников кинула в зал кинотеатра во время просмотра одного из фильмов несколько дымовых шашек и истошно завопила "Пожар, пожар!". Естественно, спровоцировав тем самым массовую панику, в результате которой погибло несколько человек. Остается только догадываться, преследовал ли тот "шутник" какие-то конкретные цели или просто так кроваво "пошутил". Единственное, что можно утверждать почти точно, это то, что "шутники" к этой акции подготовились, и провели ее по всем правилам. Во-первых, момент бросания шашки и криков "Пожар!" был выбран весьма точно: это было сделано во время одного из самых драматических моментов фильма, когда зрители находились в большом напряжении и некотором страхе от происходящего на экране. Во-вторых, один из участников этой "шутки", сидевший ближе всех к выходу, как только послышались первые крики о пожаре, бросился к выходу, подав тем самым пример всем остальным людям. Которые, естественно, этому примеру последовали.

***Примечание***

Мог ли тот "шутник" преследовать какие-либо вполне конкретные цели? Конечно, мог. К примеру, он в силу тех или иных причин мог захотеть обанкротить данный кинотеатр. Пара-тройка таких выходок и люди в этот кинотеатр ходить перестанут, т. к. за ним закрепится слава "кровавого кинотеатра".

Классическим этот пример называется потому, что он происходил по классической схеме, согласно которой сначала толпе дается какой-либо внешний стимул, после чего в качестве ответа на этот стимул следовала вполне *прогнозируемая* реакция. Внешним стимулом могут быть и крики "Пожар", и генератор Вуда, и змеи, – все, что угодно. Реакция – массовая паника.

Примерно также любил "шутить", как ни странно, известный физик Роберт Вуд, который приходил в кинотеатры с генератором низкочастотных колебаний, излучающим колебания в диапазоне 7 – 9 Гц. Когда он включал свой генератор, люди начинали метаться в панике и выбегали из кинотеатра на улицу. Несколько раз это приводило к различным телесным повреждениям у зрителей.

***Примечание***

Смысл "шутки" в том, что наши внутренние органы тоже колеблются с определенной низкой частотой, причем для большинства из них частота колебаний составляет как раз 7 – 9 Гц. При включении *генератора Вуда,* который генерировал колебания той же частоты, что и частота колебаний внутренних органов, наблюдался эффект резонанса, в результате которого люди начинали ощущать сильный дискомфорт и паническое настроение.

Гораздо позже "шутка Вуда" была один в один повторена также в кинотеатре одного города, правда уже с более трагическими последствиями.

***Примечание***

В литературе также описывались случаи убийств с применением генератора Вуда. Вернее, доведения до самоубийств. Преступники действовали по следующей схеме. Рядом с квартирой жертвы, психотип которой предполагал склонность к суициду, монтировался генератор, включался и работал практически беспрерывно. Генератор мог размещаться или на чердаке, над квартирой жертвы, если она жила на крайнем этаже, в соседней квартире, а нередко и прямо в квартире. Жертва при работе генератора ощущала дискомфорт, паническое настроение, и нередко принимала решение свести счеты с жизнью.

Известен также случай, когда в качестве причин для паники злоумышленники использовали …змей. Вернее, ужей. Представьте себе, идет кинофильм, главный герой фильма ужасов ищет чего-то на кладбище, тревожная музыка, и вдруг в этот драматический момент один из зрителей ощущает, что у него по ноге что-то ползет. Нагибается посмотреть что же это такое и с ужасом понимает, что это змея. "Змеи, в зале змеи", – кричит он, хватает этого несчастного ужа и бросает подальше от себя. И поближе к голове какого-то зрителя. После чего срывается с места и бежит к выходу. Эффект примерно такой же, как и в том случае, когда кричали "Пожар".

# Как сделать "соляной кризис" методами социального программирования

Всем памятен недавний "соляной кризис", случившийся в нашей стране. Вот, что писало в это время известное интернет-издание Лента.ру. Текст статьи приводится с некоторыми сокращениями с целью восстановления хронологии событий.

"В России набирает силу соляной кризис, грозящий перерасти в соляной бунт. Из ряда областей страны исчезла соль. Поставщики уже подняли цены в несколько раз, а граждане, опасаясь, что этот кризис – надолго, стоят в очередях и покупают товары первой необходимости впрок. Хотя соляной кризис длится уже как минимум неделю, только к середине февраля стало понятно, что очереди не сократятся, страсти не улягутся, а история не останется без внимания властей, вырвавшись с местного на федеральный уровень.

С определенной долей уверенности можно сказать, что все началось 10 февраля, когда нехватку соли обнаружили туляки, а на оптовых базах Тулы цена килограммовой пачки соли составляла 3 рубля 60 копеек. Тогда местные СМИ утверждали, что дефицит соли – чисто тульская проблема, и приводили в пример соседние регионы, где килограмм соли стоил рубль восемьдесят. Власти попытались успокоить туляков, пообещав поставки пятисот тонн к концу недели. Интересно, что в тот же день нехватку соли ощутили в Калуге. С 11 по 14 февраля в Тамбовской области были скуплены трехмесячные запасы соли. Появились и начали распространяться слухи о том, что Украина прекратила или может прекратить поставки соли в Россию. Продавцы и производители объясняли ажиотаж по-своему – изменился технический регламент, что и породило слухи о дефиците соли. 15 февраля тревогу забили нижегородцы. Несмотря на то, что в области скопился полугодовой запас соли, жители региона за день раскупили ее месячный запас. И если в Тамбовской области цена килограмма соли доходила до 30 рублей, то в Нижнем Новгороде она достигала 50 рублей. Не уступали нижегородцам и жители Новгородской области. Они скупили 300 тонн соли за два дня. Администрация области предложила свое объяснение соляному феномену. Там считают, что ажиотаж спровоцировали российские оптовики, у которых на складах скопились излишки соли. Паника достигла апогея к 16 февраля, когда нехватку ощутили в Саратовской и Волгоградской областях, в Чебоксарах и Тюмени. В Москве и Московской области также было не все спокойно. Московским властям даже пришлось объяснить гражданам, что запасов соли в столице хватит на два месяца. Паника, **старательно подогреваемая теленовостями,** привела к образованию огромных очередей. Граждане, стоящие в очередях, занимали места родственникам и соседям. Продавцы, предчувствуя, что вскоре спрос упадет, т. к. запасов соли потребителям хватит надолго, даже начали распространять контрслухи о грядущем понижении цен. Кое-где это сработало. Огромный спрос на соль породил у соотечественников смутные воспоминания о военном времени. Кроме соли граждане начали скупать сахар, спички, муку и крупы – на всякий случай, вдруг пригодятся. Власти Воронежа тем временем усмирили цены на соль. Правда, для этого пришлось нарастить запасы ценного продукта до 600 – 800 тонн, а также силами городского полка милиции провести серию рейдов по рынкам и магазинам. Дошло до того, что проблемой заинтересовались федеральные власти. Госдума 17 февраля поручила одному из комитетов выяснить у правительства причины повышения цен на продукты первой необходимости". Конец цитаты.

Кроме того, отмечается в обозрении, "интересно заметить, что рынок соли обычно не подвержен сильным колебаниям – поставки товара производятся из различных источников, сам товар подчиняется основным рыночным законам, и ажиотаж должен быстро спадать, сменяясь низким уровнем спроса. Однако из каждого правила есть исключения – и непра-

вильно понятая фраза или строчка в документе оборачиваются исчезновением со складов всех запасов соли".

Напомним также, что *федеральная антимонопольная служба* (ФАС) в ходе своего расследования пришла к выводу, что "в соляном кризисе не виноваты ни производители соли, ни предприятия оптово-розничной торговли. Правила конкуренции нарушало только ООО "Соляная компания", зарегистрированная в Тюмени. Но только одна организация не смогла бы вызвать такого масштабного кризиса". Не найдя нарушений среди производителей, ФАС заключила, что виноваты потребители: "Основной причиной повышения цен послужил ажиотажный спрос населения на пищевую соль, вызванный распространением недостоверной информации о недостаче данного продукта на российском рынке", – сказано в официальном пресс-релизе ФАС.

Давайте подумаем, мог ли он быть организован методами социального программирования. И подумав, приходим к выводу, что вполне мог. Более того, скандал такого масштаба, в результате которого чуть не сняли некоторых министров, вполне по силам организовать …одному человеку. Причем самому обычному. В том смысле, что этот человек может быть рядовой человек "с улицы". А сделать это с одним, а не с группой людей, вообще несложно. Рассмотрим гипотетическую схему, как это могло бы быть реализовано.

> ***Примечание***
>
> Авторам совершенно не известно, как это было сделано на самом деле, и чьи интересы при этом преследовались. Не исключено, что таким образом одна из министерских группировок пыталась ослабить влияние, или вообще убрать другую группировку. А в качестве исполнителей выбрали социальных хакеров. Если так оно и было, то, по крайней мере, проделано все было очень красиво.

Общая гипотетическая схема развития такого или подобного скандального кризиса проста.

Сначала делается кризис в одном конкретно взятом городе. Этот кризис подхватывается местным телевидением, которому нужны высокие рейтинги и которое знает, что больше всего аудитория любит всяческие скандалы и сенсации. Поэтому совершенно закономерно, что телевидение мимо скандала не пройдет. И вот в вечернем выпуске новостей диктор взволнованным голосом сообщает, что по неизвестной причине из магазинов города исчезает соль. И добавляет, что аналитики нашего канала, которые, как вы знаете, одни из лучших аналитиков в области (ну как же себя не похвалить и в очередной раз не самопорекламироваться), говорят, что нельзя исключать того, что соляной кризис в нашем городе это начало большой войны между крупнейшими поставщиками соли в Россию. Крупнейшие же поставщики соли, поскольку они не смотрят местное телевидение города Н-ска и незнакомы с заключениями крупнейших аналитиков местного телевидения города Н-ска, совершенно не в курсе, что между ними началась какая-то война. Местные же жители, посмотрев репортаж, обрывают телефоны, звоня своим знакомым и произнося только одну фразу:

– Слышали, а? Соли-то скоро не будет! Вы еще за ней не бежите? А мы уже.

И вот четверть города, несмотря на позднее время, бежит в круглосуточные супермаркеты скупать соль.

Съемочные группы крупных областных каналов дежурят круглосуточно. Потому что областному телевидению то нужны высокие рейтинги, и там тоже знают, что больше всего аудитория любит всяческие скандалы и сенсации, поэтому охота за сенсациями идет круглосуточно. Естественно, как только становится известно, что в Н-ске скупили всю соль, туда направляется съемочная группа, и вот уже сюжет о соляном кризисе в Н-ске транслируется всеми крупными областными каналами. Жители всех других городов, не будучи дураками,

понимают, что то, что случилось в Н-ске, может случиться и с ними. И вот соли нет уже по всей области. Пропадает она и на границах соседних областей, потому что не все жители "обессоленной" области успели закупить соль и теперь совершают набеги в соседние регионы. Те, кому набеги совершать лень, или они этого по каким-то причинам сделать не могут, звонят своим родственникам по всей стране и просят закупить их килограмм двадцать соли, и прислать посылкой.

На центральном телевидении России люди не глупее, чем на местном и областном телевидении и насчет того, как повышаются рейтинги, тоже прекрасно осведомлены. И вот в области, в которой разразился соляной кризис, высаживается десант из нескольких съемочных групп с разных Всероссийских каналов. Благодаря которым весть о том, что "в стране скоро может не быть соли" долетает даже до тех аулов, которых на карте без бинокля не найдешь. В результате чего паника начинает охватывать уже всю страну, и проблема местного и областного уровней становится проблемой федерального масштаба.

А ведь все это могла сделать очень небольшая группа людей, а если очень нужно, – то и один человек. И на то, чтобы все это спровоцировать, им при благоприятном стечении обстоятельств мог понадобиться один день и несколько тысяч рублей. Что, согласитесь, весьма небольшой бюджет для организации кризиса всероссийского масштаба. Как это возможно? А очень просто. Представьте себе, что в супермаркет можно сказать вбегает человек и нервно спрашивает у всех продавщиц: "А где у вас здесь соль?" После того, как ему показали, где соль, он бежит к этому прилавку и скупает ее всю. После этого в супермаркет вбегает другой человек с тем же самым вопросом. Но соли в нем уже нет, или осталось совсем немного. При этом все эти люди говорят покупателям и продавщицам, что "только что по радио передали, что скоро соли в стране совсем не будет". Те, кто это от наших покупателей соли услышал, впадают в легкое беспокойство, и решают на всякий случай прикупить килограмм-второй соли "на черный день". Но в том супермаркете, в котором они находятся, соль уже кончилась. Люди обеспокоиваются чуть больше и идут в другой супермаркет, чтобы прикупить килограмм пять-десять соли. На всякий случай. А наши молодчики тем временем тот же самый трюк проделывают в другом супермаркете, в третьем, десятом, и всем покупателям с удовольствием рассказывают, что "Вот, по радио передали…". Некоторые же покупатели тем временем уже начинают звонить своим знакомым, чтобы посоветовать им прикупить соли, поскольку они в магазине слышали, что ее скоро не будет, и что на их глазах люди скупили всю соль в магазине, и им самим пришлось бежать в другой, где они "чудом урвали". И вот так начинается цепная реакция в одном конкретно взятом городе. И в принципе, наши гипотетические провокаторы соляного кризиса уже могут больше ничего не делать, потому что механизм уже запущен. Но нет, им этого мало. И они еще обзванивают все городские газеты и городское телевидение, где в роли возмущенных жителей советуют обратить внимание СМИ на то, что в городе нигде нельзя купить соли и в качестве доказательства своих слов советуют зайти в ближайший супермаркет. Ну дальше "кризис подхватывается местным телевидением, которому нужны высокие рейтинги и которое знает…", в общем, как сказка про белого Бычка.

Таким образом, даже один человек, владеющий методами социального программирования, может влиять на процессы в государстве.

## Венки на трассе

Одному PR-агентству была поставлена задача сделать так, чтобы по одной из магистральных трасс ездило как можно меньше народу. Предыстория такова. В результате постройки параллельной трассы владельцы магазинов на старой трассе лишились своих доходов, т. к. большинство людей стало ездить по новой трассе, которая была удобнее, шире,

освещеннее и т. д. Владельцы магазинов скинулись и заказали "черную PR-кампанию" этой трассе. Что же сделали пиарщики? Конечно, они не стали прибегать к разрушению дорожного полотна путем раскопок, взрывных работ и прочего. Они просто …закупили несколько сотен венков в ритуальных компаниях. И развесили их практически на каждом третьем дереве новой трассы. В принципе после этого они могли уже ничего не делать. Потому что поток машин по старой трассе и так уже увеличился. Что понятно: людям психологически крайне некомфортно ездить по дороге, на каждом десятом метре которой кто-то "погиб" (о чем и свидетельствовали многочисленные венки). Это все равно, что ехать по кладбищу. И, конечно, люди стали выбирать объездные пути, т. е. старую трассу, "которая хоть и вся в колдобинах, но на ней никто не разбивается". Но пиарщики на этом не остановились. В СМИ тех городов, примыкающих к новой трассе (т. е. жители которых наиболее часто пользуются этим маршрутом), была заказана серия публикаций на тему того, что новая трасса просто какая-то "трагически мистическая". Мол, каждая 10-я машина, которая по ней проедет – разбивается. Причем почти все с летальным исходом. После этих публикаций поток машин на новой трассе еще больше уменьшился, и почти совсем иссяк после того, как к венкам добавились еще и кресты с памятниками, и трасса уже действительно стала напоминать проезжую дорогу по кладбищу.

Когда власти поняли, что к чему, стало уже поздно. Венки снимали, вешали новые… На старую трассу тоже была направлена мощная PR-кампания. Мощная в том смысле, что денег было угрохано много. А так – слабая. Потому что основные ее тезисы были направлены на колдобины на старой трассе, на то, что по ней медленнее ехать, на то, что машины на ней чаще выходят из строя, поскольку опять-таки одни колдобины. Пиарщики старой трассы все это "обрубили" одним ходом. Вернее, одним плакатом, который был поставлен перед развилкой старой и новой трассы. На плакате было написано крупными буквами одна фраза "Хочешь доехать быстро или живым?". Над словом "быстро" была стрелочка на новую трассу, над словом "живым" – на старую.

# Конец ознакомительного фрагмента.