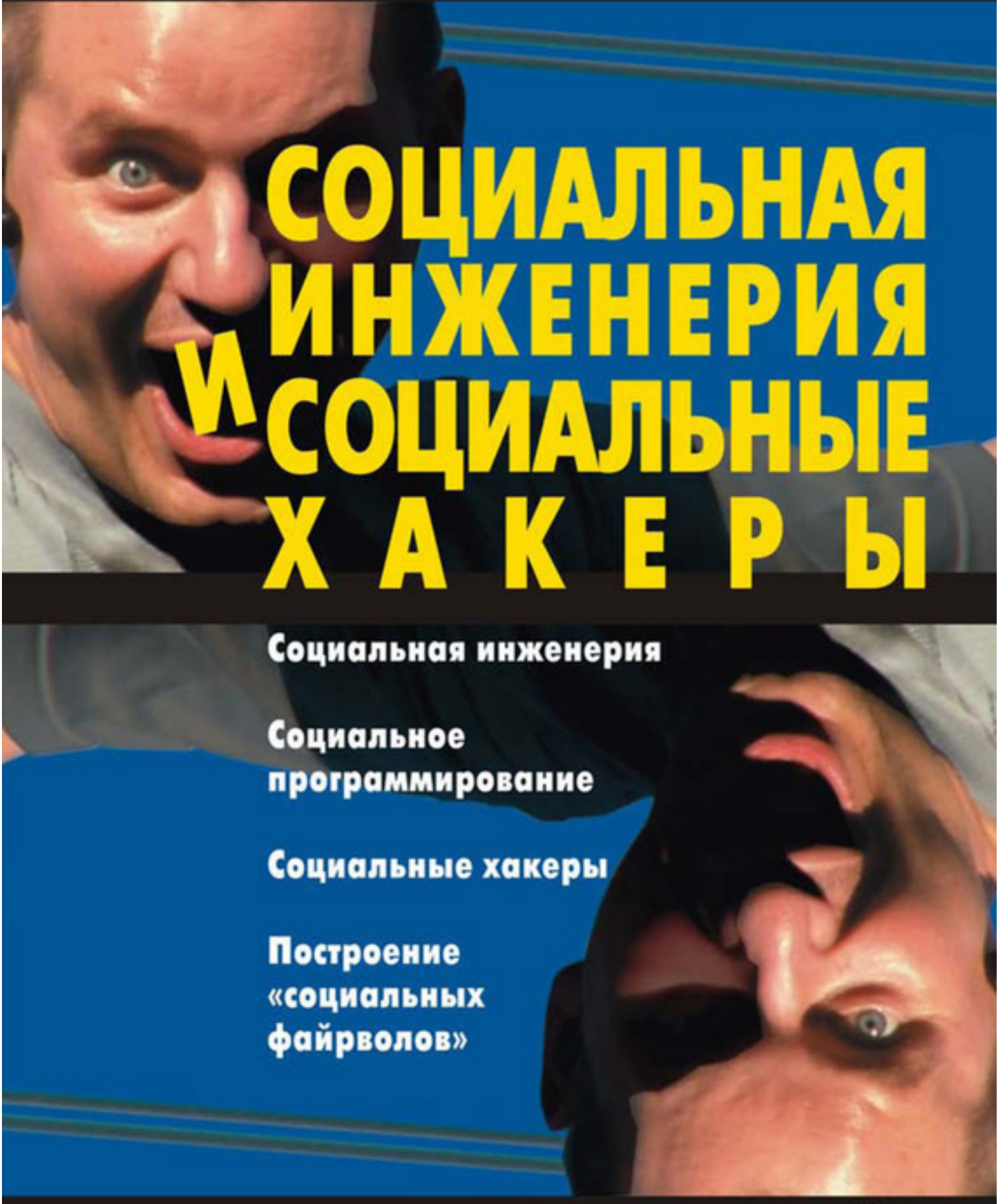


**МАКСИМ КУЗНЕЦОВ
ИГОРЬ СИМДЯНОВ**



СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ И СОЦИАЛЬНЫЕ ХАКЕРЫ

Социальная инженерия

**Социальное
программирование**

Социальные хакеры

**Построение
«социальных
файрволов»**

Максим Кузнецов

**Социальная инженерия
и социальные хакеры**

«БХВ-Петербург»

2007

Кузнецов М. В.

Социальная инженерия и социальные хакеры / М. В. Кузнецов — «БХВ-Петербург», 2007

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 (транзактный 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.

© Кузнецов М. В., 2007

© БХВ-Петербург, 2007

Содержание

Введение	5
Для кого и о чем эта книга	5
Благодарности	8
Часть I	9
Глава 1	10
Основная схема воздействия в социальной инженерии	13
Основные отличия социальной инженерии от социального программирования	18
Глава 2	22
Об истории социальной инженерии	22
Основные области применения социальной инженерии	22
Финансовые махинации	23
Конец ознакомительного фрагмента.	29

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 отве-

тило 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 попадают 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 таким 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 обнаружится? 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 покриковать К. Митника – каждого из нас есть за что покриковать – 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).

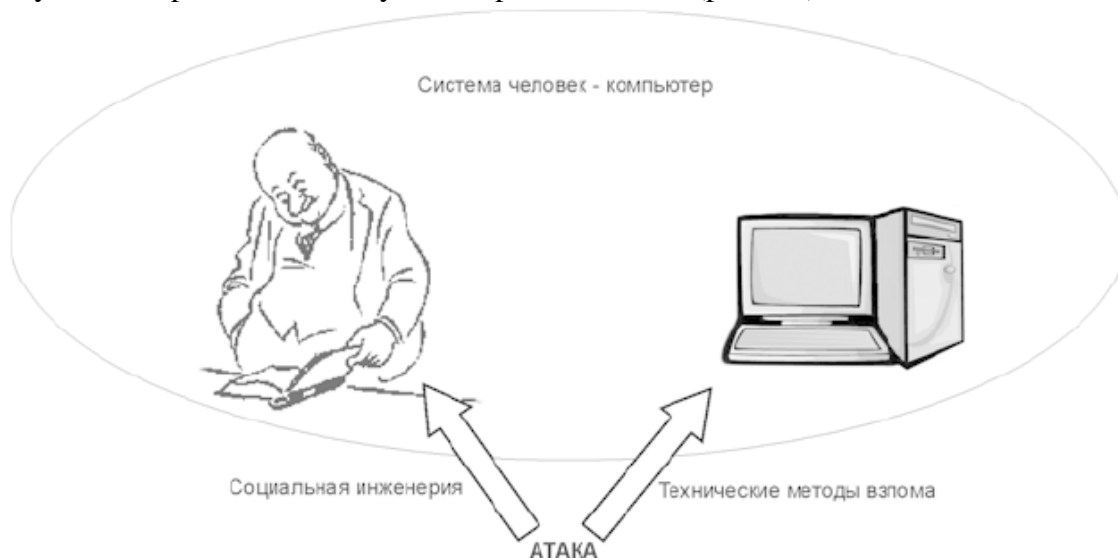


Рис. 1.1. Основные варианты взлома компьютерной системы (человек – с карикатуры Х. Бидструпа)

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" просит 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 поддаваться 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 удилицем, 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 дан-ных*.

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 ИТ. 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 ИТ. 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 радишума. 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 невозможно. 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 органи-

зации 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 выводится 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 нередко случается, 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 я¹ 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 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

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.*

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 случится 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.

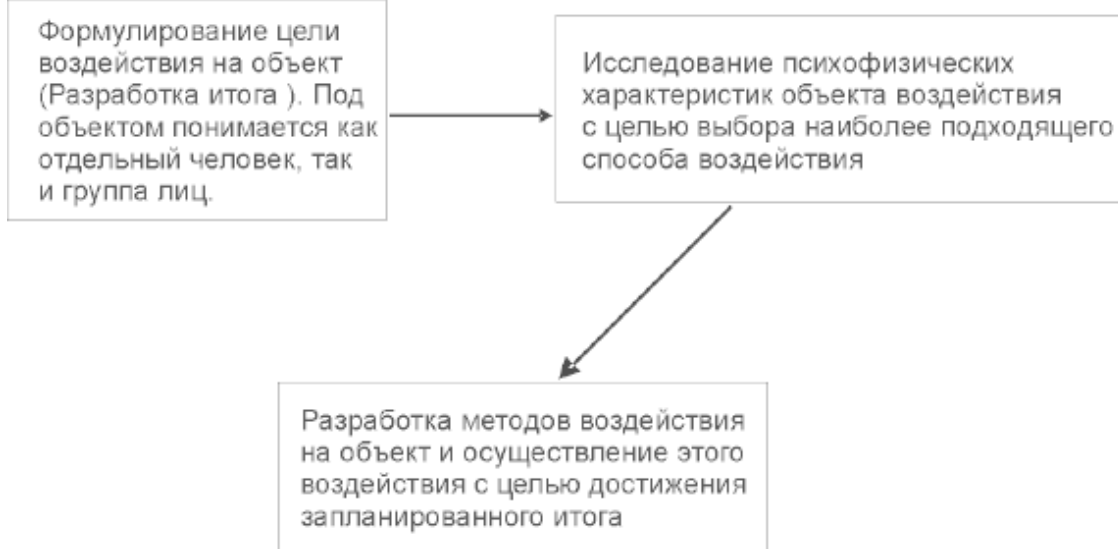


Рис. 1.3. Общая схема методов работы социальных программистов

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 – пойдя, 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. Далее 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:

- транзактном 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 набег 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 матча 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.

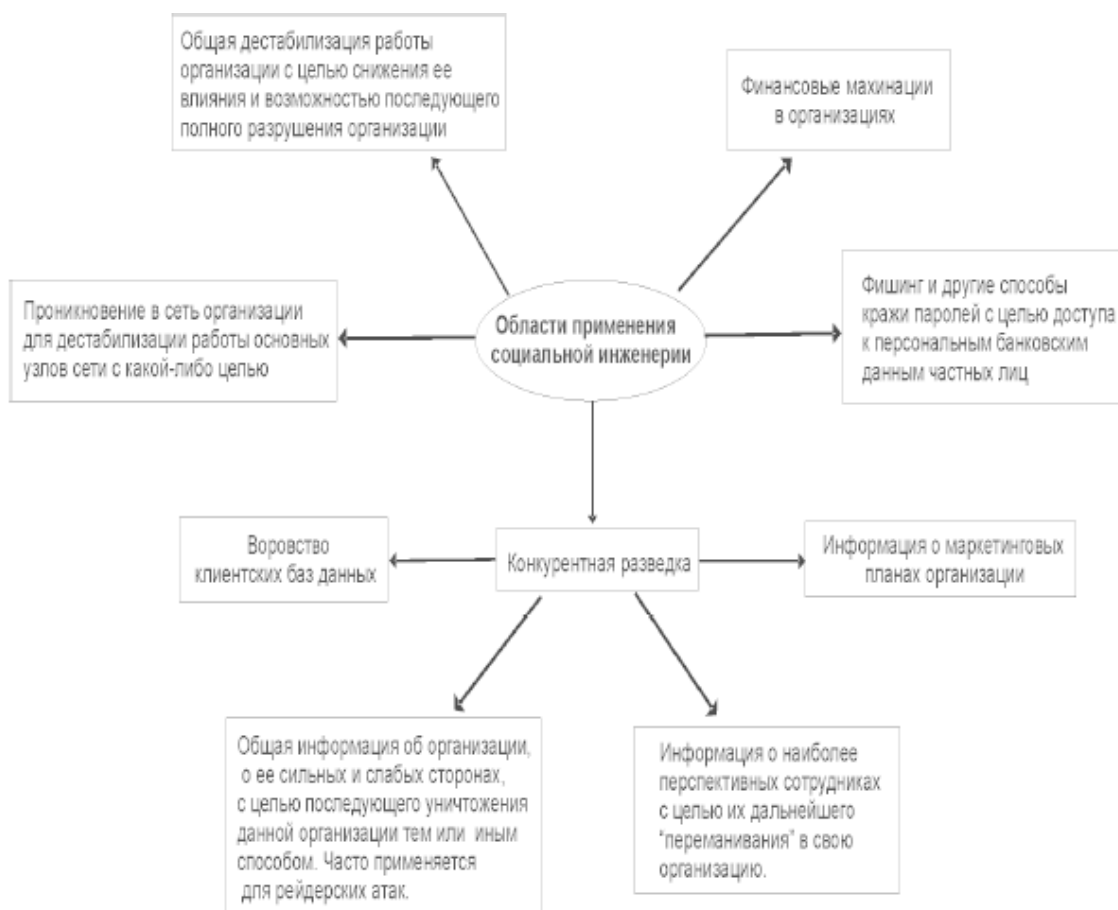


Рис. 2.1. Основные области применения социальной инженерии

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 поддельным, 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 "откатали 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 влюбились не девушку Наташу, а директора. И представьте послед-

ствия. 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 обольстителей 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 мгновение 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 подседа 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 Кашенку 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 симитирована, 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 что 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 шлепающихся 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 нефtezаводика, 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...".

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

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

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