КОМПЬЮТЕР ГЛАЗАМИ ХАКЕРА

3-е издание

Михаил Флёнов

Модификация операционной системы Windows

Разгон компьютера

Атаки хакеров и защита

Форсирование Интернета

Компьютерные шутки

Материалы на www.bhv.ru

bhv®

Михаил Флёнов

КОМПЬЮТЕР ГЛАЗАМИ ХАКЕРА

3-е издание

Санкт-Петербург
«БХВ-Петербург»
2012

УДК 681.3.06
ББК 32.973.26-018.2
Ф70

Флёнов М. Е.

Ф70 Компьютер глазами хакера. — 3-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2012. — 272 с.: ил.

ISBN 978-5-9775-0790-5

Рассмотрены компьютер, операционные системы Windows XP/Vista/7 и Интернет с точки зрения организации безопасной и эффективной работы на ПК. Описаны основные методы атак хакеров и рекомендации, которые позволят сделать компьютер быстрее, надежнее и безопаснее. Представлены примеры накручивания счетчиков на интернет-сайтах и методы взлома простых вариантов защиты программ Shareware. Приведены советы хакеров, которые позволят при путешествии по Интернету не заразиться вирусами и не стать добычей сетевых мошенников, владеющих методами социальной инженерии. Показано, как сделать интерфейс Windows более удобным и привлекательным, компьютер — надежнее и быстрее, а работу в сети — более эффективной. В третьем издании добавлены новые примеры для операционной системы Windows 7. На сайте издательства находятся программы, описанные в книге, а также используемые файлы и дополнительные статьи.

Для пользователей ПК

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Игорь Шишигин*
Зав. редакцией	*Григорий Добин*
Редактор	*Анна Кузьмина*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Наталия Першакова*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Марины Дамбиевой*
Зав. производством	*Николай Тверских*

Подписано в печать 31.01.12.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 21,93.
Тираж 2000 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0790-5

Оглавление

Введение

Первое издание книги я начинал с того, что компьютер становится неотъемлемой частью нашей жизни. Прошло уже несколько лет, и сейчас можно смело говорить, что компьютер уже стал неотъемлемой частью нашего бытия. Лично у меня дома один стационарный компьютер и три ноутбука. Стационарный компьютер у детей, по ноутбуку у меня с женой и один ноутбук с Linux, который используется мною для моих рабочих дел. Вот думаем еще купить один ноутбук дочке, чтобы не дралась с братом за стационарный компьютер.

А ведь в доме есть еще Xbox360, который так же можно назвать полноценным компьютером, просто заточенным под игры, PSP. Ах да, я еще забыл о китайском планшетнике, который тоже является компьютером.

Не забываем и про смартфоны, которые начинают вытеснять простые телефоны. Нынешние смартфоны по своей мощности уже догнали те персональные компьютеры, которые существовали во времена написания первого издания. На моем HTC Surround установлен процессор с одним гигагерцем и видеоускорителем. Я писал первое издание на ноутбуке с процессором Pentium M 1,6 ГГц. Уже появляются смартфоны на процессорах с двумя ядрами, и о такой мощности я мог только мечтать в 90-х годах, а сейчас я эту мощь ношу с собой каждый день в кармане и использую для звонков и серфинга по Интернету.

Каждый день я иду на работу, а за спиной в рюкзаке находится ноутбук HP. Выдалась свободная минутка — так, крышка ноутбука открывается и начинает переливаться разными цветами, показывая загрузку Windows. Теперь творить можно где и когда угодно, лишь бы хватило заряда аккумулятора. Практически каждый день я разбираю почту в метро или работаю над очередной заметкой для своих блогов, а в ближайшие дни собираюсь тратить свое время в пути на работу и домой на написание этой книги.

Темп жизни растет с каждым днем, и постоянного наличия ноутбука под рукой, например мне, уже не хватает. Люди начинают окружать себя дополнительными цифровыми устройствами, такими как планшетники, смартфоны и игровые приставки. Компьютеры внедряются в жизнь все активнее, и их отказы, кража, взлом и другие неприятности могут привести к катастрофе. Именно поэтому все связанное с хакерами все ярче описывается в прессе.

Эта книга полезна абсолютно всем, кто хоть как-то связан с компьютерами. Специалистам некоторые вещи покажутся слишком простыми, хотя мой опыт говорит, что мелочей в нашей жизни не бывает. Но даже если вы хорошо знакомы с компьютером, то данная книга будет вам интересна, как веселое повествование о том, что вы уже знаете. Ну а если вы знакомы с компьютерами и хакерами поверхностно, то помимо хорошего времяпровождения сможете узнать и полезную информацию. Надеюсь, что вы не пожалеете потраченных времени и денег.

Компьютер глазами хакера

Не знаю почему, но у некоторых людей очень странная реакция на слово "хакер", особенно на обложке книги. Некоторые почему-то считают, что в такой книге обязательно должно описываться написание вирусов, другие предполагают, что там должен обсуждаться изощренный взлом сайтов или программ. Но ничего из этого не имеет отношения к книге. Для подобных тем книга называлась бы по-другому. Например, как приемы взлома и защиты от взлома сайтов я описывал в книгах "PHP глазами хакера" [7] и "Web-сервер глазами хакера" [6]. Взломами программ я не интересуюсь, хотя и был опыт много лет назад.

Так о чем же эта книга? Мы будем говорить о компьютере вообще и ОС Windows в частности. И чем же она будет отличаться от других самоучителей/книг по компьютерам? Мы будем говорить о безопасности, о компьютерных приколах и об оптимизации компьютера. Хакерство — это не просто взлом программы или сервера, это образ жизни.

Если вас смущает слово "хакер" в названии книги, то просто проигнорируйте его. Читайте самое важное для себя, и надеюсь, что она будет для вас интересна и познавательна.

Хакеры — это не ботаны, которые сидят с сигаретой в руках по ночам в рваных джинсах в нищих квартирах. Это такие же люди, как мы с вами. Они так же зависимы от общества, в котором живут, и бывают совершенно разными. Бывают хакеры, которые действительно зарабатывают копейки и работают за обеды, устанавливая ОС в школах, а бывают очень богатые и обеспеченные люди. Так что ломайте стереотипы, которые созданы в СМИ.

Мне приходилось общаться в своей жизни с большим количеством людей, которые являются профессионалами в ИТ и которых я бы без проблем называл хакерами. У меня был большой опыт работы в журнале "Хакер", и я могу сказать, что все там достойны, чтобы их называли хакерами. Возможно, не все ломали сайты, возможно, не все ломали программы, но это не является показателем какой-то элитности. И во время общения с этими людьми трудно не заметить одну особенность — они все обладают хорошим чувством юмора. Есть хакеры-ботаники, но такие как раз почему-то не любят журнал "Хакер".

Я никогда не был ботаником и люблю прикалываться, поэтому этой составляющей хакерского мира мы тоже уделим небольшое внимание. Вы увидите, как можно подшутить над друзьями или коллегами, используя компьютер, узнаете некоторые

секреты использования Интернета и сможете повысить эффективность своего пребывания в сети. Помимо этого, вас ждет множество интересных и веселых ситуаций, компьютерных шуток из моей жизни и многое другое.

Возможно, где-то книга даже покажется немного философской, но это только третье издание. Первое было больше практическим. Это во втором издании я решил поговорить чуть больше.

Книга стоит на трех китах: компьютер, ОС Windows и Интернет. Это действительно значимые понятия современной эпохи, и именно их мы будем рассматривать с точки зрения хакера. А если конкретнее, нам предстоит узнать про тюнинг (настройка, оптимизация и ускорение), взлом и защиту компьютера, ОС Windows и Интернета.

Эта книга отличается от других тем, что здесь полезные знания можно приобрести, совмещая процесс познания с отдыхом и развлечением. Вы узнаете, как сделать свою работу за компьютером лучше, интереснее, эффективнее и безопаснее.

Но работа должна приносить удовольствие. Постоянно трудиться за одним и тем же рабочим столом утомляет. Вы же делаете дома перестановку, обновляете интерьер, чтобы четыре стены не докучали своим видом? То же самое и с компьютером. Однообразные окна надоедают, а смена только обоев рабочего стола и окраски окон не приносит нужного эффекта. Хочется чего-то большего.

Компьютер сейчас — не просто дань моде, для меня это источник дохода, средство отдыха и развлечения, инструмент для получения информации и обучения, ну и, конечно же, способ самовыражения. Он позволяет реализовать многие мои желания. В этой книге я поделюсь с вами самым интересным из того, что знаю о "внутренностях" ОС Windows, с точки зрения пользователя. Это поможет придумать новые компьютерные шутки, использовать железо по максимуму или просто разнообразить вашу жизнь.

Вы узнаете, как сделать интерфейс приложений более удобным и изящным. Свои любимые программы я под Новый год раньше украшал гирляндами, а летом на диалоговых окнах рассаживал цветы. Это делает жизнь приятнее и красивее. Почему "раньше"? Сейчас времени как-то нет, а жаль. Это интересное занятие.

Многие люди, покупая новый автомобиль, сразу же приступают к тюнингу. Это позволяет через машину продемонстрировать свою индивидуальность и выделиться среди окружающих. Почему не поступить так и с компьютером? Он ведь тоже является отражением наших характерных особенностей, и мы имеем на это полное право.

Некоторые хакеры занимаются модингом, украшая системный блок, а кто-то предпочитает улучшать ОС. Я больше люблю все же программные украшения, потому что именно с ОС приходится работать чаще, а системный блок больше стоит под столом и никому не виден, но от тюнинга железа все равно не отказываюсь. Именно поэтому первым делом мы будем украшать Windows, а заодно познакомимся с универсальными способами изменения и других программ. Конечно же, эти приемы применимы не ко всем программам, но к большинству — это уж точно.

Я провожу за компьютером по 10—12 часов, а когда еще не было ни жены, ни детей, то у монитора просиживал до 16 часов, в основном ночью, когда тихо и спокойно. Я даже кушал, держась одной рукой за клавиатуру, а отходил от компьютера только, чтобы поспать. Так как в игры я практически не играю, то получалось, что большая часть времени уходила на программирование и изучение системы. Но надо же как-нибудь отдыхать и развлекаться! Вот я и начал создавать маленькие смешные программы, с помощью которых легко подшутить над друзьями и коллегами по работе. Большинство таких программ или трюков рождалось именно на работе, где был "испытательный полигон" для новых идей. Всегда хочется показать свои знания и умения (и даже превосходство), и юмор позволяет это сделать как нельзя лучше. А главное, на работе есть корпоративная сеть, в которой много компьютеров, а значит и потенциальных "жертв". Именно сеть позволяет сделать шутки более интересными.

Мне в те времена повезло с заместителем начальника моего отдела, потому что он тоже был любителем подшутить над ближним. Нужно действовать по великой заповеди хакеров: "Подшути над ближним своим, ибо он подшутит над тобой и возрадуется".

Однажды у меня перестал работать монитор, и я долго не мог понять почему. Оказалось, что монитор работал, просто над ним "поколдовал" мой шеф (про эту шутку читай в *главе 3*). После этого между нами развернулась настоящая война. Мы постоянно искали новые способы "напакостить" друг другу. С каждым днем шутки становились все интереснее и изощреннее.

Некоторые вещи, которые мы будем рассматривать, могут нарушать какое-либо лицензионное соглашение разработчика программы, ОС или компьютера, поэтому прежде чем приступать к действиям, следует внимательно с ним ознакомиться. Например, мы узнаем, как можно изменить ресурсы приложения (окна, меню, значки и т. д.), что противоречит лицензионному соглашению на использование разработок большинства крупных производителей программного обеспечения. Небольшие фирмы или программисты-одиночки делают соглашения более мягкими или вообще не используют их в своей практике, и самое интересное из того, как их можно настроить на свой вкус, я раскрою на страницах этой книги.

Правило использования

Лично я не понимаю, почему нам запрещают изменять что-то в программе, которую мы честно купили. Производители телевизоров не запрещают перекрашивать его в другой цвет, да и с автомобилями можно делать все, что угодно (теряется только гарантия). Так почему же нельзя то же самое сделать с Windows?

Но необходимо отдавать себе отчет в том, что, нарушив лицензию, вы можете лишиться поддержки. Я, да и многие другие, этой поддержкой не пользуюсь, поэтому смело изменяю все, что захочу.

Помните, что большинство примеров приводится только в информационных целях, для лучшего понимания системы и компьютера. За использование этих знаний

в незаконных целях автор и издательство ответственности не несут. Я всегда говорил, что даже безобидный предмет может стать оружием уничтожения или разрушения.

Кто такие хакеры?

Это довольно спорный вопрос, и я достаточно много писал о том, кто такие хакеры и как ими стать. Давайте разберем понятие "хакер" с позиции, с которой я буду рассматривать его в данной книге. Именно из-за того, что у некоторых людей другое понимание слова "хакер", начинаются непонятные вопросы к названию этой книги или к его содержимому.

Но для начала надо углубиться немного в историю. Понятие "хакер" зародилось, когда только начинала распространяться первая сеть ARPANET. Тогда это понятие обозначало человека, хорошо разбирающегося в компьютерах. Некоторые даже подразумевали под хакером человека, "помешанного" на компьютерах. Понятие ассоциировали со свободным компьютерщиком, человеком, стремящимся к свободе во всем, что касалось его любимой "игрушки" — компьютера. Собственно благодаря этому стремлению и тяге к свободному обмену информацией и началось такое бурное развитие всемирной сети. Я считаю, что именно хакеры помогли развитию Интернета и создали FIDO. Благодаря им появились UNIX-подобные системы с открытым исходным кодом, на которых сейчас работает большое количество серверов.

В те далекие времена еще не было вирусов и никто даже не думал о взломе сетей, сайтов или отдельных компьютеров. Образ хакера-взломщика появился немного позже. Но это только образ. Настоящие хакеры никогда не имели никакого отношения к взломам, а если хакер направлял свои действия на разрушение, то это резко осуждалось виртуальным сообществом. Даже самые яркие представители борцов за свободу не любят, когда кто-либо вмешивается в их личную жизнь.

Так что если вы купили книгу в надежде, что тут будет что-то о взломе чего-либо, только из-за слова "хакер" на обложке, вы можете разочароваться. Но я все же постарался сделать книгу как можно интереснее и полезнее, поэтому все же надеюсь, что вы не разочаруетесь.

Настоящий хакер — это творец, а не разрушитель. Так как творцов оказалось больше, чем разрушителей, то истинные хакеры выделили тех, кто занимается взломом, в отдельную группу и назвали их крэкерами (взломщиками) или просто вандалами. И хакеры, и взломщики являются гениями виртуального мира. И те, и другие борются за свободу доступа к информации. Но только крэкеры взламывают сайты, закрытые базы данных и другие источники информации с целью собственной наживы, ради денег или минутной славы, такого человека можно назвать только преступником (кем он по закону и является!).

Если вы взломали программу, чтобы увидеть, как она работает, то вы — хакер, а при намерении ее продать или просто выложить в Интернете crack (крэк) — становитесь преступником. Но если вы взломали сервер/компьютер/веб-сайт и сообщили владельцу ресурса об уязвимости, то вы, несомненно, — хакер.

Жаль, что многие специалисты не видят этой разницы и путают хакерские исследования с правонарушениями. Хакеры интересуются безопасностью систем и серверов для определения ее надежности (или в образовательных целях), а крэкеры — с целью воровства или уничтожения данных.

Итак, к крэкерам относятся:

- вирусописатели — программисты, которые применяют свои знания на то, чтобы написать программу разрушительной направленности;
- вандалы — эти люди стремятся уничтожить систему, удалить все файлы или нарушить работу сервера;
- взломщики компьютеров/серверов — они совершают "кражу со взломом" с целью наживы, выполняя зачастую чьи-либо заказы на получение информации, но очень редко используют свои знания в разрушительных целях;
- взломщики программ — такие крэкеры снимают защиту с программного обеспечения и предоставляют его для всеобщего использования. Этим они приносят ущерб софтверным фирмам и государству. Программисты должны получать зарплату за свой труд.

Чтобы еще раз подчеркнуть разницу между хакером и крэкером, можно сравнить их с взломщиками программ. Все прекрасно понимают, что многие софтверные фирмы завышают цены на свои программные продукты. Крэкер будет бороться с ценами с помощью снятия защиты, а хакер создаст свою программу с аналогичными функциями, но меньшей стоимости или вообще бесплатную. Так, движение Open Source можно причислить к хакерам, а те, кто пишет крэки, относятся к взломщикам, т. е. крэкерам.

Мне кажется, что путаница в понятиях отчасти возникла из-за некомпетентности в этом вопросе средств массовой информации. Журналисты популярных СМИ, не вполне разбираясь в проблеме, приписывают хакерам взломы, делая из них преступников.

Истинные хакеры никогда не используют свои знания во вред другим. Именно к этому я призываю в данной книге, и никакого конкретного взлома или вирусов в ней не будет описано. Вы найдете только полезную и познавательную информацию, которую сможете использовать для умножения своих знаний.

Так как в нашей жизни злостный образ хакера уже устоялся и от него уже не избавиться, то их разделили на White Hat (белые шапки) и Black Hat (черные шапки). К черным шапочкам относятся как раз хакеры, которые все взламывают. К белым шапочкам (почему-то возникает ассоциация с врачами) относятся добрые и пушистые хакеры, которых я уважаю и о которых мы будем говорить.

Есть еще красные шапочки (Red Hat), но это отдельная элитная категория, которая носит бабушкам пирожки, а всем остальным открытый код :). Шутка конечно же. На счет пирожков я не уверен, а вот открытый код Red Hat все же несет миру. С этими шапками связан самый знаменитый дистрибутив Linux, который в свое время наделал много шума.

Хакеры должны очень хорошо знать компьютер и в особенности ОС, а также желательно знание программирования и лучше на нескольких языках. Когда мы будем рассматривать атаки, которые используют хакеры, то вы увидите, что без навыков программирования реализовать большинство из этих приемов будет невозможно. Если вы заинтересовались и решили повысить свой уровень мастерства, то могу посоветовать прочитать мои книги "Программирование в Delphi глазами хакера" [2] и "Программирование на C++ глазами хакера" [1]. Надеюсь, это поможет вам научиться создавать собственные шуточные программы и хакерский софт. Для понимания материала не надо иметь глубоких знаний в программировании. Компьютерные шутки, которые мы будем рассматривать в данной книге, хороши, но не менее интересно самостоятельно сотворить забавную программу и подбросить ее друзьям.

Напоследок я хочу дать вам одну ссылку на одну статью энциклопедии Wiki: **http://ru.wikipedia.org/wiki/%D5%E0%EA%E5%F0**. Выглядит страшно и не понятно, но на самом деле это то же самое, что написать: **http://ru.wikipedia.org/wiki/хакер**. Просто, если ввести этот адрес в браузере, сайт переведет русское слово в URL в закодированный формат (коды букв вместо реальных букв) и загрузит уже эту страницу. В этой статье промотайте немного вниз, и напротив раздела "Известные хакеры" вы должны увидеть фото Линуса Торвальдса (рис. В1).

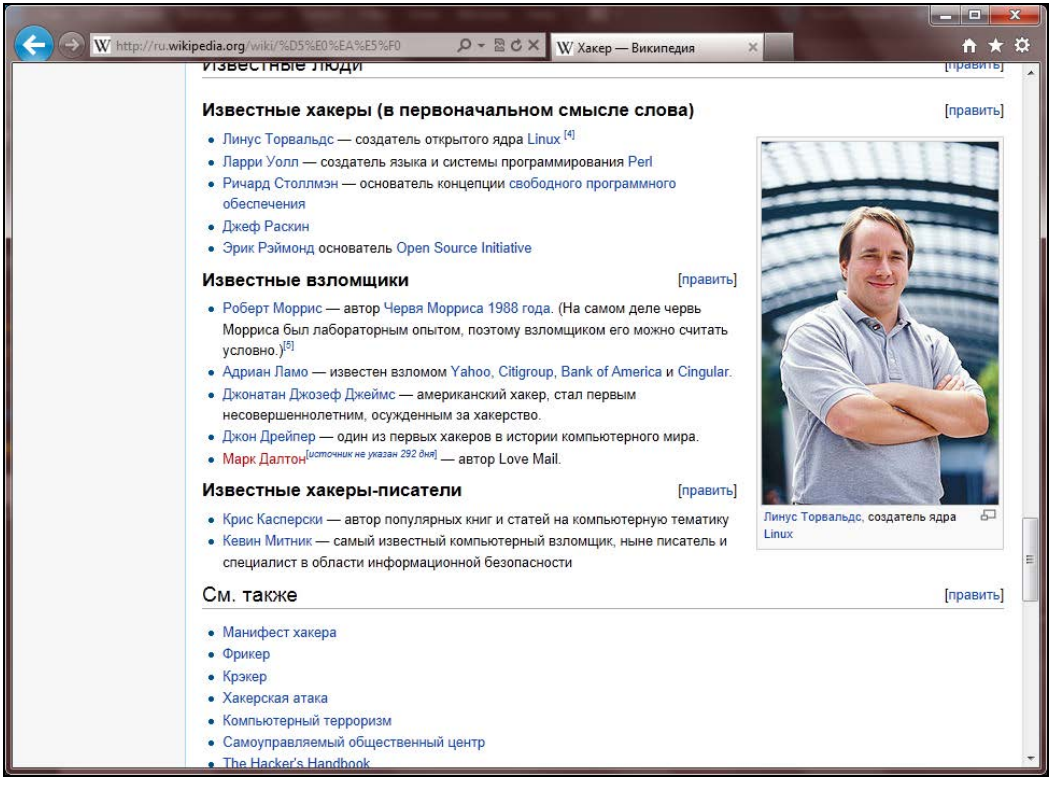

Рис. В1. Известный хакер Линус Тррвальдс

Не думаю, что Линус когда-то и что-то взламывал, но очень много людей, которые разделяют мою точку зрения, без сомнений назовут его хакером. Я понимаю, что энциклопедия Wiki не всегда показательна и тем более, не является законом, потому что ее пишут люди, которые могут ошибаться. Но все же в целом эту энциклопедию рецензирует большое количество людей.

Так, самое главное — существует множество понятий и ни одно из них не является единственным верным. Но я считаю правильной мою точку зрения и именно с этой точки пишу эту книгу. Надеюсь, что мы смотрим на мир с одной и той же позиции, и тогда вам эта книга понравится.

Как стать хакером?

Этот вопрос задают себе многие, но точного ответа вам не даст никто. Есть ответы, которые могут нравиться, но реальность намного более сурова. Данная книга не сделает из вас хакера, как никто не сможет этого сделать. Только труд сотворил из обезьяны человека, и только работа сделает из простого юзера элитного хакера.

Нужно просто как можно больше изучать, читать, пробовать, практиковаться. Желательно общение с другими людьми, потому что обмен опытом — наиболее важный ресурс информации. Не ограничивайтесь только одним автором книг или только одной книгой. Прочитав лишь эту книгу, вы познакомитесь с опытом и узнаете мнение только одного автора, но оно не всегда является лучшим. Аккумулируйте информацию, анализируйте и принимайте решение сами.

Я всегда люблю говорить: "не стоит тупо делать что-то, потому что это тупо". Прежде чем что-то сделать, желательно все же подумать самому, а не доверяться какой-то книжке (даже этой) или автору. Не доверяйте мне, потому что я сам себе не доверяю, пробуйте сами и проверяйте, и тогда вы получите неоценимый опыт, который пригодится в будущем.

В этой главе мы постараемся выделить некоторые общие аспекты, но все зависит от конкретной области, в которой вы хотите стать лучшим. Да, существует множество областей безопасности и хакерства, вот только некоторые:

- сетевой — рассматривает безопасность сетевых протоколов и интернет-приложений;
- кернел (kernel) — ядро ОС, переполнения буфера, ошибки выполнения программ;
- криптография — вопросы и проблемы безопасности шифрования, стойкости и передачи зашифрованных данных;
- веб-сайты — это отдельный класс безопасности, который мне интересен больше всего;
- вирусы — этот класс мне интересен меньше всего. Во времена MS-DOS мне было интересно экспериментировать с системой, и я даже пробовал написать вирус, но дальше размножения дело не дошло, потому что мне это показалось очень скучным и глупым занятием;

- программный — сюда бы я отнес как безопасность программ, так и стойкость ко взлому авторизации/проверки ключей.

Названия и классификацию я придумал сейчас налету, потому что делить области можно как угодно и по какому угодно признаку. Смысл тут в том, что стать специалистом в разных областях одновременно очень и очень сложно. Уж слишком разные нужны тут знания.

Сравним компьютерного специалиста со строителем. В каждой профессии существует некая специализация (разная направленность). Хорошим строителем может быть отличный каменщик или штукатур. Точно также и хакером может быть специалист по операционным системам (например, UNIX) или программист (приложений или веб-сайтов). Все зависит от ваших интересов и потребностей.

После выхода первого издания книги ко мне пришло несколько писем, в которых читатели были недовольны тем, что я в своей книге не уделил внимание вирусам/взлому программ или чему-то еще, и поэтому слово "хакер" на обложке не должно находиться. Видимо, авторы писем ограничены только одной областью хакерства, но тут все намного сложнее.

Итак, вот некоторые рекомендации, которые помогут вам стать настоящим хакером и добиться признания со стороны друзей и коллег.

1. Вы должны знать свой компьютер и научиться эффективно им управлять. Если вы будете еще и знать в нем каждую железку, то это только добавит к вашей оценке большой и жирный плюс.

   Что я подразумеваю под умением эффективно управлять своим компьютером? Это значит знать все возможные способы для выполнения каждого действия и в каждой ситуации уметь использовать наиболее оптимальный из них. В частности вы должны научиться пользоваться "горячими" клавишами и не дергать мышь по любому пустяку. Нажатие клавиши выполняется быстрее, чем любое, даже маленькое перемещение мыши. Просто приучите себя к этому, и вы увидите все прелести работы с клавиатурой.

   Лично я использую мышь очень редко и стараюсь всегда применять клавиатуру. Если быть точнее, то дома я вообще не использую мышь, потому что у меня ее нет. Дома я использую ноутбук и touch pad.

   Маленький пример на эту тему. У меня был один начальник, который всегда копировал и вставлял данные из буфера обмена с помощью кнопок на панели инструментов или команд контекстного меню, которое появляется при щелчке правой кнопкой мыши. Но если вы делаете так же, то, наверное, знаете, что не везде есть кнопки **Копировать**, **Вставить** или соответствующие пункты в контекстном меню. В таких случаях мой начальник набирает текст вручную. А ведь можно было бы воспользоваться копированием/вставкой с помощью "горячих" клавиш <Ctrl>+<C>/<Ctrl>+<V> или <Ctrl>+<Ins>/<Shift>+<Ins>, которые достаточно универсальны, а их работа реализована практически во всех современных приложениях (даже там, где не предусмотрены кнопки и меню).

   За копирование и вставку в стандартных компонентах Windows (строки ввода, текстовые поля) отвечает сама операционная система, и тут не нужен дополни-

тельный код, чтобы данные операции заработали. Если программист не предусмотрел кнопку, то это не значит, что данное действие не предусмотрено вовсе. Оно есть, но доступно через "горячую" клавишу. Если соответствующие "горячие" клавиши не переопределены в программе (им не даны другие действия), то команды будут работать.

Еще один пример. Я работал программистом на крупном предприятии (более 20 000 работников). Моей задачей было создать программу ведения базы данных для автоматизированного формирования отчетности. Большое количество параметров набиралось вручную, и для этого использовались операторы. Первый вариант программы работал без "горячих" клавиш, и для ввода данных требовалось 25 операторов. После внедрения "горячих" клавиш производительность возросла, и с программой работало уже менее 20 операторов. Экономия заметна даже без увеличительного стекла.

2. Вы должны досконально изучать все, что вам интересно о компьютерах. Если вас интересует графика, то вы должны освоить лучшие графические пакеты, научиться рисовать в них любые сцены и создавать самые сложные миры. Если вас интересуют сети, то старайтесь узнать о них все. Если вы считаете, что познали уже все, то купите более толстую книгу по данной теме, и вы поймете, что сильно ошибались. Компьютеры — это такая сфера, в которой невозможно знать все!!! Даже в отдельно взятой области очень тяжело быть всезнающим специалистом.

   Хакеры — это, прежде всего, профессионалы в каком-нибудь деле. И тут даже не обязательно должен быть компьютер или какой-то определенный язык программирования. Хакером можно стать в любой области, но мы в данной книге будем рассматривать только компьютерных хакеров.

3. Желательно уметь программировать. Любой хакер должен знать как минимум один язык программирования. А лучше даже несколько языков. Лично я рекомендую всем изучить для начала Borland Delphi или C++. Borland Delphi достаточно прост, быстр, эффективен, а главное, это очень мощный язык. C++ — признанный стандарт во всем мире, но немного сложнее в обучении. Но это не означает, что не надо знать другие языки. Вы можете научиться программировать на чем угодно, даже на языке Basic (хотя использовать его не советую, но знать не помешало бы).

   По ходу изучения книги вы увидите, что без навыков программирования некоторые приемы были бы невозможны. Используя готовые программы, написанные другими хакерами, вы можете стать только взломщиком, а для того чтобы стать хакером, нужно научиться создавать свой код.

   Хакер — это творец, человек, который что-то создает. В большинстве случаев это касается кода программы, но можно создавать и графику, и музыку, что тоже относится к искусству хакера.

4. Не тормозите прогресс. Хакеры всегда боролись за свободу информации. Если вы хотите быть хакером, то тоже должны помогать другим. Хакеры обязаны способствовать прогрессу. Некоторые делают это через написание программ с открытым кодом, а кто-то просто делится своими знаниями.

Открытость информации не означает, что вы не можете зарабатывать деньги. Это никогда не возбранялось, потому что хакеры тоже люди, хотят кушать и должны содержать свою семью. Самое главное — это созидание. Вот тут проявляется еще одно отличие хакеров от крэкеров: хакеры "создают", а крэкеры "уничтожают" информацию. Если вы написали какую-нибудь уникальную шуточную программу, то это вас делает хакером. Но если вы изобрели вирус, который с улыбкой на экране уничтожает диск, то вы — крэкер-преступник.

В борьбе за свободу информации может применяться даже взлом, но только не в разрушительных целях. Вы можете взломать какую-либо программу, чтобы посмотреть, как она работает, но не убирать с нее систем защиты. Нужно уважать труд других программистов, не нарушать их авторские права, потому что защита программ — это их хлеб.

Представьте себе ситуацию, если бы вы украли телевизор. Это было бы воровство и преследовалось бы по закону. Многие люди это понимают и не идут на преступления из-за боязни наказания. Почему же тогда крэкеры спокойно ломают программы, не боясь закона? Ведь это тоже воровство. Лично я приравниваю взлом программы к воровству телевизора с полки магазина и считаю это таким же правонарушением.

При этом вы должны иметь право посмотреть на код купленной программы. Ведь вы же можете вскрыть свой телевизор, и никто не будет вас преследовать по лицензионным соглашениям. Кроме того, вас же не заставляют регистрироваться, когда вы честно приобрели товар, как делают это сейчас с активацией.

Когда я говорю, что вы должны иметь право посмотреть на код, я не призываю писать и использовать только проекты с открытым исходным кодом. Ни в коем случае. Можно смотреть во внутренности программ с помощью дизассемблеров. На ассемблере читать код программ намного сложнее, но тут будет самое настоящее соединение с хакерской культурой (как красиво сказал, аж сам не верю).

Я понимаю разработчиков программ, которые пытаются защитить свой труд. Я сам программист и продаю свои программы. Но я никогда не делаю сложных систем защиты, потому что любые попытки "предохранения" усложняют жизнь законопослушным пользователям, а крэкеры все равно их обойдут. Какие только "замки" не придумывали крупные корпорации, чтобы защитить свою собственность, но crack существует на любые программы, и большинство из них взломано еще до официального выхода на рынок. С нелегальным распространением программ нужно бороться другими методами, а системы активации или ключей бесполезны.

В цивилизованном мире программа должна иметь только простое поле для ввода некоего кода, подтверждающего оплату, и ничего больше. Не должно быть никаких активаций и сложных регистраций. Но для этого и пользователи должны быть честными, потому что любой труд должен оплачиваться. А то, что какой-то товар (программный продукт) можно получить бесплатно, это не значит, что вы должны это делать.

5. Знайте меру. Честно сказать, я уважаю Билла Гейтса за то, что он создал Windows и благодаря этой операционной системе сделал компьютер доступным для каждого в этом мире. Если раньше пользоваться компьютерами могли только люди с высшим образованием и математическими способностями, то теперь он доступен каждому ребенку.

   Единственное, что я не приветствую, — это методы, которыми продвигается Windows на компьютеры пользователей. Мне кажется, что уже давно пора ослабить давление, и Windows наоборот станет более популярной, а у многих пропадет ненависть к корпорации и ее руководству. Хотя судя по последним тенденциям именно это и происходит.

   Нельзя просто так лишать денег другие фирмы только из-за того, что ты проиграл конкуренцию, как это произошло с Netscape Navigator. Тогда Microsoft не удалось победить фирму Netscape в честной борьбе, и Microsoft сделала свой браузер бесплатным, потому что у корпорации достаточно денег, и она может себе это позволить. Но почему нельзя было просто уйти от борьбы и достойно принять проигрыш? Ведь доходы фирмы от перевода браузера на бесплатную основу не сильно увеличились, а интеграция Internet Explorer в ОС — чистый фарс.

6. Не изобретайте велосипед. Тут опять действует созидательная функция хакеров. Они не должны стоять на месте и обязаны делиться своими знаниями. Например, если вы написали какой-то уникальный код, то поделитесь им с ближними, чтобы людям не пришлось создавать то же самое. Вы можете не выдавать все секреты, но должны помогать другим.

   Ну а если вам попал чужой код, то не стесняйтесь его использовать (с согласия хозяина!). Не выдумывайте то, что уже сделано и обкатано другими пользователями. Если каждый будет изобретать колесо, то никто и никогда не создаст повозку, и тем более автомобиль.

7. Хакеры — не просто отдельные личности, а целая культура с собственными магическими заклинаниями и танцами с бубнами, которые позволяют добиться нужного результата (например, заставить программу работать). Но это не значит, что все хакеры одеваются одинаково и выглядят на одно лицо. Каждый из них — отдельный индивидуум, и не похож на других. Не надо копировать другого человека. Удачное копирование не сделает вас продвинутым хакером. Только ваша индивидуальность может сделать вам имя.

   Если вы известны в каких-либо кругах, то это считается очень почетным. Хакеры — это люди, добывающие себе славу своими познаниями и добрыми делами. Поэтому любого хакера должны знать.

   Как определить, являетесь ли вы хакером? Очень просто, если о вас говорят, как о хакере, то вы один из них. Жаль, что этого добиться очень сложно, потому что большинство считает хакерами взломщиков. Поэтому, чтобы о вас заговорили как о хакере, нужно что-то взломать или уничтожить. Но это неправильно, и не надо поддаваться на этот соблазн. Старайтесь держать себя в рамках дозволен-

ного и добиться славы только хорошими делами. Это намного сложнее, но что поделаешь... Никто и не обещал, что будет просто.

8. Чем отличаются друг от друга программист, пользователь и хакер? Программист, когда пишет программу, видит, какой она должна быть, и делает на свое усмотрение. Пользователь не всегда знает, что задумал программист, и использует программу так, как понимает.

   Программист не всегда может предугадать действия своих клиентов, да и приложения не всегда тщательно оттестированы. Пользователи имеют возможность ввести параметры, которые приводят к неустойчивой работе программ.

   Хакеры намеренно ищут в программе лазейки, чтобы заставить ее работать неправильно, нестабильно или необычно. Для этого требуется воображение и нестандартное мышление. Вы должны чувствовать исполняемый код и видеть то, чего не видят другие.

   Если вы нашли какую-то уязвимость, то необязательно ее использовать. Об ошибках лучше сообщать владельцу системы (например, администрации сайта). Это весьма благородно, а главное, — создаст вам имя, и при этом можно не опасаться оказаться в зале суда. Хотя, те, кто оказываются в суде, быстрее получают популярность, потому что о таких людях пишут в газетах и им начинают подражать "чайники". Но кому в тюрьме нужно признание общественности? Мне оно абсолютно не нужно. Тем более что после отбывания срока очень часто тяжело найти себе работу. Мало кто захочет содержать в штате бывшего преступника, да и после пребывания в местах не столь отдаленных могут еще долго не разрешать пользоваться любимыми компьютерами. Лучше быть здоровым и богатым, т. е. пусть не знаменитым, но на свободе.

Некоторые считают, что правильно надо произносить "хэкер", а не "хакер". Это так, но только для английского языка. У нас в стране оно обрусело и стало "хакером". Мы — русские люди, и давайте будем любить свой язык и признавать его правила. Хотя, некоторые читатели могут быть и с Украины, Белоруссии и других стран бывшего СНГ, и тогда произносите это слово так, как уже устоялось в вашем языке, и не копируйте с американцев.

Тут же возникает вопрос: "Почему же автор относит к хакерскому искусству компьютерные шутки и сетевые программы?" Попробую ответить на этот вопрос. Во-первых, хакеры всегда пытались доказать свою силу и знания методом написания каких-либо интересных, веселых программ. К этой категории я не отношу вирусы, потому что они несут в себе разрушение, хотя они тоже бывают с изюминкой и юмором. Зато простые и безобидные шутки всегда ценились в узких кругах.

Мне кажется, что в ИТ-областях вообще очень хорошо с чувством юмора, и хакеры — не исключение, чтобы писать только серьезные вещи. Поэтому не будем ботаниками, а будем чаще улыбаться, это полезно для кожи лица, чтобы не было морщин.

Таким способом хакер демонстрирует не только знания особенностей операционной системы, но и старается заставить ближнего своего улыбнуться. Так как многие

хакеры обладают хорошим чувством юмора, и он поневоле ищет своего воплощения во всем. Я советую шутить с помощью безобидных программ, потому что юмор должен быть здоровым.

Пользуйтесь собственным умом

Читать чужие идеи и мысли очень хорошо и полезно, потому что, изучая опыт других людей, можно узнать много нового. Но с другой стороны, не стоит принимать все на веру без самостоятельного анализа. Даже эту книгу нужно профильтровать через собственный мозг, потому что я где-то могу ошибаться или заблуждаться.

Вы также должны понимать необходимость использования различных технологий. Я по образованию экономист-менеджер и 6 лет проучился в институте по этой специальности. Но даже до этого я знал, что заказчик всегда прав. Почему-то в компьютерной области стараются избавиться от этого понятия. Например, Microsoft пытается заставить программистов писать определенные программы, не объясняя, зачем это нужно пользователям. Многие тупо следуют этим рекомендациям и не задумываются о необходимости того, что они делают.

Тут же приведу простейший пример. Совсем недавно все программисты вставляли в свои продукты поддержку XML, и при этом никто из них не задумывается о целесообразности этого. А ведь не всем пользователям этот формат нужен, и не во всех программах он востребован. Следование рекомендациям не означает правильность действий, потому что заказчик — не Билл Гейтс, а ваш потребитель. Поэтому надо всегда делать то, что требуется конечному пользователю. А если заказчику не нужен XML, то не надо и внедрять его поддержку в программу.

Сейчас нас зомбируют с экранов телевизоров и интернет-сайтов облачными технологиями и тучами. А оно вам нужно? Придумали какие-то красивые слова, а все это как было клиент-серверной технологией, так и осталось. Если нужны интернет-вычисления, то используйте интернет-серверы, а как вы их назовете — облако, туча или мясорубка, клиенту все равно. Не обязательно задействовать сложные системы, которые строят Amazon и Microsoft, когда нужен всего лишь веб-сайт или небольшой веб-сервис.

Я рекомендую не обращать особого внимания на корпорацию Microsoft (хотя некоторые ее разработки гениальны), потому что считаю определенные ее действия тормозом прогресса. И это тоже можно доказать на примере. Сколько технологий доступа к данным придумала Microsoft? Просто диву даешься: DAO, RDO, ODBC, ADO, ADO.NET, и это еще не полный список. Корпорация Microsoft регулярно выкидывает на рынок что-то новое, но при этом сама этим не пользуется. При появлении новой технологии все программисты кидаются переделывать свои программы под новоиспеченный стандарт и в результате тратят громадные ресурсы на постоянные переделки. Таким образом, конкуренты сильно отстают, а Microsoft движется вперед, потому что не следует своим собственным рекомендациям и ничего не переделывает. Если программа при создании использовала для доступа к данным DAO, то можно спокойно оставить ее работать через DAO, а не переделывать на

ADO, потому что пользователю все равно, каким образом программа получает данные из базы, главное, чтобы данные были вовремя и качественно.

Могу привести более яркий пример — интерфейс. В программах, входящих в пакет MS Office, постоянно меняется интерфейс, и при этом всем говорят, что именно он самый удобный для пользователя и именно за ним будущее. Все бегут переводить свои программы на новый внешний вид меню и панелей, а тот же Internet Explorer и многие другие программы выглядят, как 10 лет назад, в них практически ничего не меняется. Microsoft не тратит на это время, а конкуренты месяцами переписывают множество строчек кода.

Да, следование моде придает вашим программам эффектность, но при этом вы должны суметь сохранить индивидуальность.

Компания Microsoft постоянно что-то переписывает и переделывает в спецификациях, но при этом сама очень сильно топчется на месте и программы меняет только по мере необходимости. В этом смысле Apple поступила мудрее и постоянно движется вперед. Если на настольных системах яблочный гигант пока отстает, но на мобильном рынке он с большим отрывом обошел Microsoft и заставил конкурента шагнуть не то, что на шаг назад, а отступить к самому началу. Мобильная платформа MS была практически полностью переписана и запущена с нуля под новым именем Windows Phone без совместимости с предыдущей платформой Windows Mobile.

Возможно, сложилось впечатление, что я противник Microsoft, но это не так. Мне очень нравятся некоторые ее продукты, например Windows, Office, C#, Visual Studio или MS SQL Server, но я не всегда согласен с ее методами борьбы с конкурентами. Это жестокий бизнес, но не до такой же степени.

Программисты и хакеры навязывают другим свое мнение о любимом языке программирования, как о единственно приемлемом, обычно добиваясь успеха, потому что заказчик часто не разбирается в программировании. На самом же деле заказчику все равно, на каком языке вы напишете программу, его интересуют только сроки и качество.

Если я могу обеспечить минимальные сроки написания приложения, сохраняя хорошее качество, работая на Borland Delphi, то я буду использовать его. Такое же качество на C++ я (да и любой другой программист) смогу обеспечить только в значительно большие сроки. Правда сейчас я нашел для себя другой язык программирования, который мне больше подходит — C#, и с его помощью я пишу свои нынешние проекты.

Вот когда заказчик требует минимальный размер или наивысшую скорость работы программы, тогда я берусь за C (не путать с C++) и ASM (встроенный ассемблер). Но это бывает очень редко (последний раз было, наверное, лет 6 назад), потому что сейчас носители информации уже практически не испытывают недостатка в размерах, и современные компьютеры работают в миллионы раз быстрее своих предшественников. Таким образом, размер и скорость программы уже не являются критичными, и на первый план выдвигаются скорость получения готового продукта и качество выполнения заказа.

Какие требования перед вами ставят, такие требования и выполняйте. Не пытайтесь забивать гвозди отверткой, используйте молоток. Точно так же и при выборе программных продуктов, с помощью которых вы будете реализовывать задачу — нужно выбирать то, что подходит лучше, а не то, что круче.

Предыстория

Чтобы лучше понимать мир хакера, нужно оглянуться назад и увидеть, как все развивалось, начиная с зарождения Интернета и появления первых хакерских программ, первых взломов и т. д.

В 1962-м году директор агентства ARPA (Advanced Research Projects Agency, Управление передовых исследовательских проектов) Дж. С. Р. Ликлидер (J. C. R. Licklider) предложил в качестве военного применения компьютерных технологий использовать имеющиеся компьютеры, взаимосвязанные выделенной линией. Целью такого применения компьютеров стало создание распределенных коммуникаций. А в основу ноу-хау был положен принцип функционирования системы, устойчивой к отказам линий связи. Благодаря этому ключевым направлением исследований агентства стали компьютерные сети. Это время можно назвать началом появления сети ARPANET (Advanced Research Projects Agency NETwork, сеть коммутации пакетов).

С этой ошибки и началось развитие Интернета. Почему ошибки? В основу был положен принцип функционирования системы при отказе отдельных ее блоков, т. е. уже в самом начале заложили вероятность отказа отдельных компонентов!!! Во главу угла должна была стать безопасность системы, ведь она разрабатывалась для военных нужд США. Но как раз на этот аспект никто не обращал внимания. И это понятно, ведь компьютеры были доступны только профессионалам, о домашних компьютерах только мечтали. А о том, чтобы подключить домашний компьютер к сети, использовавшейся для военных и исследовательских целей, никто и не задумывался. Дальше еще хуже.

Разные специалисты признают различные события как рождение сети. В различных источниках можно найти даты, начиная с 1965 до 1970 года. Но многие признали 1969 год — период появления ARPANET, и именно тогда зарождается ОС UNIX, на основе которой и создавался Интернет в ближайшие десятилетия.

В начале 70-х годов ARPANET стала расширяться и объединять различные исследовательские институты. Сеть вышла за пределы одного здания и начала опутывать США. Изначально никто даже не предполагал, что рост пойдет такими быстрыми темпами и сеть объединит такое большое количество компьютеров. Поэтому первые технологии, которые использовались для связи и обмена данными, устарели в течение первых 10 лет.

С 1970 года начинается десятилетие фрикеров. Их тоже относят к категории хакеров, хотя они напрямую не связаны с компьютерами. Основное направление их деятельности — телефоны, услуги по использованию которых стоили дорого, поэтому молодые ребята (и не очень молодые, и иногда не очень ребята :)) старались

снизить эти затраты. Не знаю, какие расценки сейчас в США, а в Канаде до сих пор цены на телефонную связь очень высокие. Домашняя линия стоит минимум 10 долларов, а хороший безлимитный тариф — 30 долларов. Сотовая связь так же очень дорогая. Средняя стоимость разговора в месяц обходится в 70 долларов на одну телефонную линию.

Эпоху фрикеров начинают отсчитывать с момента, когда компания Bell опубликовала в журнале "Technical Assistance Program" частоты тональных сигналов, которыми управляется телефонная сеть. В 1971 году появилась "синяя коробка" (Blue Box), с помощью которой можно было генерировать сигналы нужных тонов. Следующие 10 лет такие коробки позволили экономить людям немалые деньги на телефонных разговорах, телефонные компании стали терять деньги. После 1980 года эта болезнь начинает проходить, потому что фрикеров начали активно ловить, и это стало небезопасно.

Среди фрикеров были замечены достаточно знаменитые личности, например основатели Apple Computers. Они продавали студентам электронные приборы, среди которых были и "синие коробки".

В 1972 году появилось первое приложение для передачи электронных сообщений, а через год сеть вышла за пределы США, и к ней подключились компьютеры из Англии. В том же году начались первые разговоры и предложения по построению международной сети.

Только в 1981 году был создан Defence Security Center (DSC, центр компьютерной безопасности министерства обороны США). Этот центр должен был определить степень пригодности предлагаемых систем для их ведомства.

16 декабря 1981 года начался судебный процесс против самого знаменитого фрикера Льюиса де Пейна, более известного под кличкой Роско. В этом же деле участвовал и известный хакер Кевин Митник, но ему повезло, — тогда он проходил в качестве свидетеля. Не прошло и года, как знаменитый хакер попался на другом деле и все же сел в тюрьму для подростков.

В 1982 году в основу Интернета был положен протокол передачи данных TCP/IP (Transmission Control Protocol/Internet Protocol). Количество хостов росло, а для обращения к компьютерам использовались их адреса. С появлением TCP/IP началась разработка DNS (Domain Name System, система доменных имен), что позволило обращаться к компьютерам по именам, а система сама переводила их в адреса компьютеров.

Несмотря на то, что к этому времени мир уже узнал о том, что компьютерные технологии могут быть опасны, протокол TCP разрабатывался как открытый и с большим количеством недостатков с точки зрения безопасности. И только при разработке IPv6 безопасности было уделено достаточно много внимания.

1983 год возвращает Кевину Митнику свободу. Но ненадолго, потому что руки хакера тянутся к взлому, и он снова попадается, из-за чего ему приходится скрываться вплоть до 1985 года.

В 1984 году система DNS вводится в эксплуатацию. Проходит еще четыре года, и весь мир узнает, что существует угроза червя. В 1988 году происходит одно из са-

мых масштабных заражений "червем" компьютеров, подключенных к Интернету. Молодой выпускник Корнельского университета по имени Роберт Моррис, являющийся сотрудником фирмы Digital, пишет программу-"червя", которая должна была самостоятельно перемещаться по сети и заражать файлы всех взломанных компьютеров.

Для внедрения на чужой компьютер "червь" использовал подбор пароля. В теле программы находилось несколько наиболее часто употребляемых паролей, и именно они применялись для проникновения в другой компьютер. Если напрямую пароль не удавалось подобрать, то подключался системный словарь слов. Таким простым способом было взломано более 7% всех компьютеров в сети. Это достаточно большая цифра. "Червь" был запущен по случайной ошибке, и его код еще не был закончен. Трудно предположить последствия, если бы Роберт Моррис смог дописать программу до конца.

Но и это еще не все. 1988 год оказался самым продуктивным с точки зрения взлома и громких судебных дел. Именно в этом году в очередной раз был пойман Кевин Митник, и на этот раз он уже надолго был отлучен от компьютеров.

Начиная с 1990 года, сеть ARPANET перестает существовать, потому что ее просто съедает Интернет. Всемирная сеть начинает поглощать все отдельные сети.

В 1991 году мир первый раз увидел веб-страницы, без которых сейчас уже никто не может себе представить Всемирную сеть. Интернет-сообщество начинает смотреть на сеть по-новому. В том же году появляется одна из самых мощных систем шифрования — PGP (Pretty Good Privacy, набор алгоритмов и программ для высоконадежного шифрования сообщений с использованием открытых ключей), которая постепенно становится стандартом в большинстве областей, в том числе и в шифровании электронных сообщений e-mail.

В 1994 году количество пользователей Интернета уже исчисляется миллионами. Чтобы народ не просиживал за монитором зря, предпринимаются первые попытки полноценной коммерческой деятельности через сеть, которая постепенно перестает быть исключительно инструментом для обмена информацией, теперь это еще и средство рекламы и способ продвижения товара в массы.

В 1995 году регистрация доменных имен перестает быть бесплатной, и начинается эра войны за домены. Хакеры стремятся скупить все доменные имена, похожие на торговые марки, или просто легко запоминающиеся слова. Компании, которые хотят, чтобы доменное имя совпадало с их торговой маркой, тратят большие деньги для их выкупа.

Этот же год стал знаменит и тем, что я купил себе модем и влился в Интернет. До этого я появлялся в сети очень редко и ненадолго, потому что для меня это было слишком дорогое удовольствие.

Итак, на такой деловой ноте мы закончим вводную лекцию и перейдем к практическим упражнениям по воинскому искусству, где часто главное — это скрытность и победа минимальными силами.

ГЛАВА 1

Интересные настройки Windows

Будем двигаться от очень простого к простому, ведь все на самом деле очень примитивно, если не усложнять себе жизнь. Поэтому после прочтения книги даже на те вопросы, на которые вы не знали ответа, вы сможете воскликнуть: "Как же это было просто!" Я ничего особого изобретать не намерен, а просто соберу интересные (на мой взгляд) темы относительно компьютера в одной книге. И начнем мы с интерфейса ОС Windows и его программ.

Когда я первый раз познакомился с Windows 95, то понял, что полюбил эту ОС по самые иконки. Несмотря на то, что она была нестабильна и выдавала синие экраны, да и переустанавливать ее приходилось раз в пару месяцев, в ней было очень много удобных для простого пользователя и заядлого хакера вещей.

С появлением следующих версий, таких как Windows 98, 2000, моя любовь только укреплялась. С каждой новой версией система усложнялась, и появлялись новые, интересные возможности для выражения своей индивидуальности. Нестабильность и проблемы иногда склоняли меня установить Linux и работать в нем, но с появлением Windows XP я понял, что ни о каком дистрибутиве в "красной шапке" можно больше и не думать. Лучше заплатить подороже, но получить отличную, удобную и стабильную систему. Главное — подойти с правильной стороны и все строго настроить. А тут есть где "разгуляться", и не только для повышения надежности, но и с целью улучшения внешнего вида.

Начиная с Windows Vista, количество интересных изменений, которые можно выполнить в визуальном интерфейсе, сильно сократилось, поэтому и эта глава сильно изменилась по сравнению с предыдущими изданиями. На момент написания этих строк во всем мире семимильными шагами идет переход на Windows 7, а через год нам обещают еще одну новую версию — Windows 8. Архитектурно Windows уже не должна так сильно меняться, как это произошло при переходе с Windows XP на Vista, поэтому бóльшая часть описываемого здесь может быть применима и в ближайших будущих версиях ОС от Microsoft.

Но вернемся к Linux, который я только что упомянул. Если честно, то в Linux я иногда посиживаю, но в последнее время все реже и реже. Процентов 90 своего

компьютерного времени я провожу непосредственно в Windows, и только 10 процентов уходит на Linux в его различных проявлениях.

В предыдущем издании эта глава содержала много информации, касающейся Windows XP и IE версии 6.0, которые сейчас используются все меньше и меньше. Я думаю, что к моменту выхода книги на полки магазинов количество компьютеров на Windows XP сократится еще сильнее, поэтому оставлять устаревшую информацию не имеет смысла. Но чтобы не терять ее вовсе, я вынес все, что касается Windows XP и Internet Explorer до версии 7, в архив, который можно найти на FTP-сервере издательства (см. **ftp://85.249.45.166/9785977507905.zip**, ссылка доступна также со страницы книги на сайте **www.bhv.ru**). Ищите там множество дополнительной информации в папке Doc.

В этом издании я решил значительно сократить этот раздел, потому что параметры постоянно изменяются, и не хотелось бы, чтобы большая часть книги устарела уже завтра. Вместо этого мы рассмотрим наиболее интересные настройки системы.

1.1. Internet Explorer

Большинство программ устанавливается с настройками по умолчанию. И если в основном производители программного обеспечения предоставляют к своим настройками полный визуальный интерфейс, то Microsoft почему-то решила не делать этого. Не все настройки можно изменить визуально в окне параметров, иногда приходится изменять что-то напрямую в реестре. Как любит говорить qa (quality assurance), с которым я сотрудничаю сейчас на работе: "Don’t ask me why it works this way". Реально, иногда очень сложно объяснить, почему менеджеры проектов или разработчики приняли именно такое решение.

Популярный (пока еще) в Windows-мире браузер Internet Explorer, который устанавливается с ОС по умолчанию, грешит такой же проблемой. У него далеко не все параметры можно изменять в окне настроек. Некоторые (иногда очень интересные и полезные параметры) доступны для изменения только напрямую в реестре.

1.1.1. Убить нельзя, помиловать

Среди настроек есть такой параметр, который запрещает пользователю закрывать окна Internet Explorer. Во время путешествия в сети на многих сайтах выскакивает масса всплывающих окон, которые засоряют экран. Если использовать возможность такой настройки, то окна будут только плодиться, а при попытке закрытия появится окно с предупреждением, как на рис. 1.1.

Чтобы сделать Internet Explorer незакрываемым, нужно перейти в реестре в раздел **HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions**. Этот путь может отсутствовать, и нужно будет добавить недостающие разделы. Для этого достаточно щелкнуть правой кнопкой мыши на нужном разделе и в появившемся меню выбрать **Создать | Раздел** (New | Key). Например, если у вас существует только путь **HKEY_CURRENT_USER\Software**

Policies\Microsoft, то щелкните правой кнопкой на строке **Microsoft** и создайте раздел **Internet Explorer**, а затем в нем — **Restrictions**. Когда все разделы будут существовать, создайте параметр **NoBrowserClose** типа `DWORD` и со значением `1`.

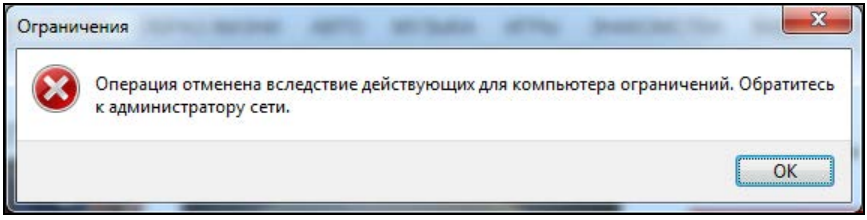

Рис. 1.1. Предупреждение о невозможности закрытия окна IE

Все эти действия можно проделать на компьютере своего друга и посмотреть за его реакцией, когда он попытается закрыть окно. Я однажды подшутил так над своими коллегами по работе. Реакция их была разнообразной. Большинство посчитало, что это было вмешательство вируса.

Чтобы внести все эти изменения на компьютере пользователя, нужно достаточно много времени, а его может и не быть. Чтобы сделать все быстро и незаметно, можно поступить следующим образом:

1. Внести изменения сначала в свой компьютер.
2. Выполнить экспорт файла реестра с опцией **Выбранная ветвь** (в данном случае ветвь **HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions**).
3. Записать получившийся файл на флешку.

Теперь идите к компьютеру пользователя, над которым вы намереваетесь подшутить, и говорите, что хотите что-то показать. Вставляете флешку и запускаете файл с расширением reg. Вся необходимая информация будет автоматически добавлена. Не надо больше ничего делать, даже запускать Internet Explorer. Просто скажите, что это не та флешка, и уходите. Ждите, пока пользователь сам не запустит браузер и не встретится с проблемой закрытия программы.

Мне интересно узнать, чем руководствовался тот человек, который придумал ограничение, запрещающее закрывать IE? Я бы с удовольствием поговорил бы с этим человеком, чтобы узнать, для чего это было сделано. А те, над кем подшутили подобным образом, наверно открутили бы нерадивому разработчику голову.

Этот параметр существовал в IE6, и я думал, что его добавили по глупости и уберут из Internet Explorer уже в 7-й версии. Сегодня я проверил 9-ю версию и трюк все еще работает. Немного странно он начинает работать, совсем не сразу. Видимо, браузер кеширует свои параметры и не читает их каждые пять минут или при каждом запуске. Я даже сначала подумал, что параметр не работает, и уже собирался удалить этот раздел из книги. Но прошло некоторое время и я не смог закрыть браузер, а раздел вернулся в книгу.