Михаил Фленов

КОМПЬЮТЕР ГЛАЗАМИ ХАКЕРА

2-е издание

Санкт-Петербург
«БХВ-Петербург»
2009

УДК 681.3.06
ББК 32.973.26-018.2
Ф69

Фленов М. Е.

Ф69 Компьютер глазами хакера. — 2-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2009. — 352 с.: ил. + CD-ROM

ISBN 978-5-9775-0117-0

Рассмотрены компьютер, операционные системы Windows XP/Vista 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. Во втором издании уделено больше внимания вопросам безопасности и добавлены новые примеры для операционных систем Windows XP и Vista.

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	*Юрий Якубович*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 25.03.09.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 28,38.
Тираж 2500 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.60.953.Д.003650.04.08 от 14.04.2008 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.

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

ISBN 978-5-9775-0117-0

Оглавление

Введение

Компьютер становится уже неотъемлемой частью нашего бытия, и лично я всегда ношу с собой свой ноутбук, т. к. даже не представляю себе жизни без него. Выдалась свободная минутка, — крышка ноутбука сразу открывается и начинает переливаться разными цветами, показывая загрузку Windows XP. Теперь творить можно где и когда угодно, лишь бы хватило заряда аккумулятора.

Темп жизни растет с каждым днем, и постоянного наличия ноутбука под рукой мне, например, уже не хватает. Мне нужно работать быстрее и успевать больше, поэтому я начинаю задумываться о наладоннике, который позволит мне более эффективно использовать свободное время в транспорте или в очередях, правда денег на него пока не хватает.

Компьютеры внедряются в жизнь все плотнее и плотнее, 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 веселая книга о том, что вы уже знаете. Ну а если вы знакомы с компьютерами и хакерами поверхностно, то, помимо хорошего времени провождения, сможете узнать и полезную информацию. Надеюсь, что вы не пожалеете потраченного времени и денег.

Компьютер глазами хакера

В данной книге описываются составные части ОС Windows, интересные приемы настройки компьютера и операционной системы. 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.

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.

Рис. В1. Вот так красиво может загружаться Windows XP

Чтобы проведенное за компьютером время стало приятней, надо научиться украшать ОС Windows и ее программы. Пример того, чего можно достичь, показан на рис. В1. Сначала, в *главе 1*, я покажу простые методы тюнинга с использованием специализированных утилит, позволяющих упростить и украсить работу. В *главе 2* вы познакомитесь с составом стилей рабочего стола, загрузчиков и программ входа в Windows XP и способами их редактирования напрямую.

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 я 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 иногда украшаю гирляндами, а летом на диалоговых окнах рассаживаю цветы. Это делает жизнь приятнее и красивее.

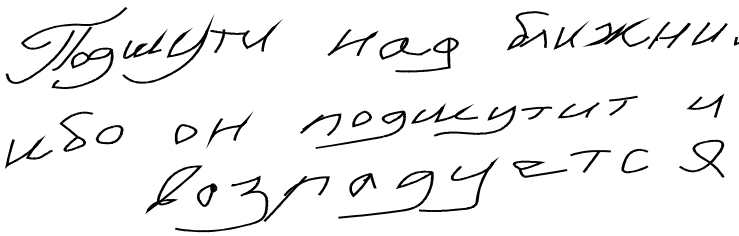
Многие люди, покупая новый автомобиль, сразу же приступают к тюнингу. Это позволяет через машину продемонстрировать свою индивидуальность и выделиться среди окружающих. Почему не поступить так и с компьютером? Он ведь тоже является отражением наших характерных особенностей, и мы имеем на это полное право.

Некоторые хакеры занимаются модингом, украшая системный блок, но ведь он очень часто стоит под столом и незаметен. Да и по 8 часов на работе мы смотрим не на эту "коробку", а на монитор и окна, которые там находятся. 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 писать маленькие смешные программы, с помощью которых легко подшутить над друзьями и коллегами по работе. Большинство таких программ или трюков рождалось именно на работе, где есть "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.



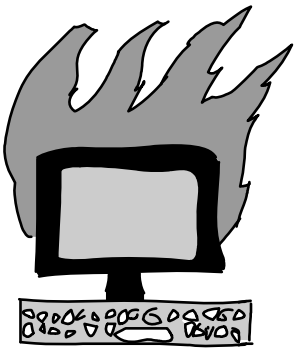
Однажды у меня перестал работать монитор, и я долго не мог понять почему. Оказалось, что монитор работал, просто над ним "поколдовал" мой шеф (про эту шутку читай в *главе 3*). После этого между нами развернулась настоящая война. Мы постоянно искали новые способы "напакостить" друг другу. С каждым днем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



Огненный разгон

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.

Когда мы будем рассматривать разгон компьютера, то при практическом использовании этой возможности вы нарушите гарантию производителя. Если по вашей вине сгорит компьютер, то никто уже не примет его в ремонт. Если у вас нет достаточного опыта работы с железом компьютера, то воспринимайте эту информацию как познавательную. Большинство начинающих при экстремальных разгонах обязательно что-нибудь сжигают (материнскую плату или процессор), и замена будет производиться только за их счет, поэтому практический опыт окажется дорогим. Если у вас есть лишние деньги, то можно потренироваться. Я в основном занимаюсь этим на машинах, которые уже свое отработали (их, если что, и выкинуть не жалко). Если компьютер новый и работает быстро и стабильно, то и разгон ему не нужен.

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.

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". Собственно благодаря этому стремлению и тяге к свободному обмену информацией и началось такое бурное развитие Всемирной сети. 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 не внедрилась практика взломов сетей 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.

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. Ежели вы взломали сервер и сообщили администрации об уязвимости, то вы, несомненно, — хакер, но коли уничтожили информацию и скрылись, то это уже преступление.

Жаль, что многие специалисты не видят этой разницы и путают хакерские исследования с правонарушениями. Хакеры интересуются системой безопасности 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.

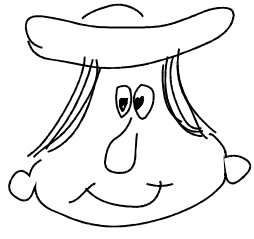
Мне кажется, что путаница в понятиях отчасти возникла из-за некомпетентности в этом вопросе средств массовой информации. Журналисты популярных СМИ, не вполне разбираясь в проблеме, приписывают хакерам взломы, делая из них преступников.

На самом же деле хакер — это просто гений. 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.

Хакеры должны не просто знать компьютер. 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.

Как стать хакером?

Этот вопрос задают себе многие, но точного ответа вам не даст никто. Данная книга не сделает из вас хакера, как никто не сможет этого сделать. Только работа сделала из обезьяны человека.



И работа сделает из человека хакера

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 Web-приложений;
- кернел — ядро ОС, переполнения буфера, ошибки выполнения программ;

- криптография — вопросы и проблемы безопасности шифрования, стойкости и передачи зашифрованных данных.

Названия и классификацию я придумал сейчас на лету, потому что делить области можно как угодно и по какому угодно признаку. Смысл 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 так же и хакером может быть специалист по операционным системам (например, UNIX) или программист (приложений или Web-сайтов). Все зависит от ваших интересов и потребностей.

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 по "хакерству" 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.

   Маленький пример на эту тему. Мой начальник всегда копирует и вставляет 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 и работа которых 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 ну-

жен дополнительный 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 всегда.

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 знать 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). Хотя я не очень люблю Visual Basic за его ограниченность, неудобность и сплошные недостатки, я видел несколько великолепных программ, которые были написаны именно на этом языке. Глядя на них, сразу хочется назвать их автора хакером, потому что это действительно виртуозная и безупречная работа. Создание из ничего чего-то великолепного как раз и есть искусство хакерства.

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.

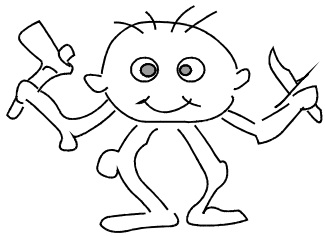
Хакер — это творец, человек, который что-то создает. В большинстве случаев это касается кода программы, но можно создавать и графику, и музыку, что тоже относится к искусству хакера. Но даже если вы занимаетесь компьютерной музыкой, знание программирования повысят ваш уровень. Сейчас писать свои программы стало гораздо легче. С помощью таких языков, как Borland Delphi, можно создавать простые утилиты за очень короткое время, и при этом вы не будете ни в чем ограничены. Так что не поленитесь и изучите программирование.

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, и тоже хотят кушать, и должны содержать свою семью. Но деньги не должны быть основополагающим в вашей жизни. 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.



Отдай исходный код

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.

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 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.

   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 придумывайте 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 подели-

тесь 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 вам определить, являетесь ли вы хакером? Очень просто, если о вас говорят, как о хакере, то вы один из них. Жаль, что такого добиться очень сложно, потому что большинство считает хакерами взломщиков. Поэтому, чтобы о вас заговорили как о хакере, нужно что-то вскрыть. Но это неправильно, и не надо поддаваться на этот соблазн. Старайтесь держать себя в рамках дозволенного 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. Но кому в тюрьме нужно признание общественности? Я думаю, что никому. 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. знаменитым и 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.

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.

Таким способом хакер демонстрирует не только знания особенностей операционной системы, но и старается заставить ближнего своего улыбнуться. Не секрет, что многие хакеры обладают хорошим чувством юмора, и он поневоле ищет своего воплощения. Я советую шутить с помощью безобидных программ, потому что юмор должен быть здоровым.

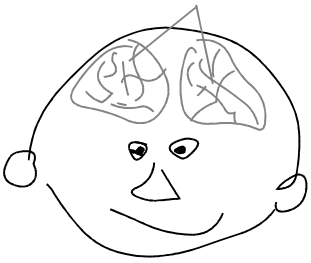
Пользуйтесь собственным умом

Читать чужие идеи и мысли это 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. Сейчас все программисты вставляют 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 нужно XML, то не нужно и внедрять его поддержку в программу.

Я рекомендую не обращать особого внимания на корпорацию Microsoft (хотя некоторые их разработки гениальны), потому что считаю определенные их 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.

Возможно, сложилось впечатление, что я противник Microsoft, но это не так. Мне очень нравятся некоторые их продукты, например Windows или MS SQL Server, но я не всегда согласен с их 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 об 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. Лично я могу обеспечить минимальные сроки написания приложения, сохраняя хорошее качество, только работая на Borland Delphi. Такое же качество на C++ я (да и любой другой программист) смогу обеспечить только в значительно большие сроки.

Вот когда заказчик требует минимальный размер или наивысшую скорость работы программы, тогда я берусь за C (не путать C и C++) и ASM (встроенный ассемблер). Но это бывает очень редко, 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 и качество выполнения заказа.

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) J. C. R. Licklider предложил в качестве военного применения компьютерных технологий использовать взаимосвязанные выделенной линией имеющиеся компьютеры. 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 главе 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 разные 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 будет создаваться 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 не очень ребята :) старались снизить эти затраты.

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 появляется первое приложение для передачи электронных сообщений, а через год сеть вышла за пределы США, и к ней подключились компьютеры из Англии. В этом 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.

1983 год возвращает Кевина Митника на 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 самых 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 Web-страницы, без которых сейчас уже никто не может себе представить Всемирную сеть. Интернет-сообщество начинает смотреть на сеть по-новому. В этом 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.

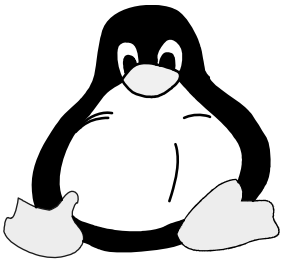
Этот же год стал знаменит и тем, что я купил себе модем и влился в Интернет. До этого я появлялся в сети очень редко и ненадолго, потому что для меня это было слишком дорогое удовольствие.

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

Когда я первый раз познакомился с Windows 95, то понял, что полюбил эту ОС. 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.



Обманываешь, по ночам пингвинов разводишь

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.

Ну если честно, то да, в Linux я иногда посиживаю. Ну хорошо, не иногда, а довольно часто. Но если сравнить с окнами, то в них я трачу больше времени.

В начале этой главы мы будем рассматривать настройки Internet Explorer, которые спрятаны от пользователя и к которым можно получить доступ только через реестр. Описывать все параметры я не буду, потому что их очень много, но самое интересное, что может пригодиться хакеру, разберем достаточно подробно.

В дальнейшем большое внимание будет уделено настройке внешнего вида Windows и, конечно же, Windows XP, потому что именно эта версия позволяет сделать интерфейс максимально красивым и удобным при минимальных затратах.

1.1. Собственный Internet Explorer

Первое, с чего я начинаю тюнинг своей ОС — изменяю Internet Explorer (IE). Некоторые программисты пишут собственный браузер на движке IE, но я не понимаю, зачем это делать, когда и так изменить можно практически все. Сейчас мы рассмотрим, как трансформировать главное окно браузера до неузнаваемости, после чего вы сможете говорить друзьям, что это ваша собственная разработка.

На данный момент уже существуют специальные программы, которые умеют делать некоторые настройки автоматически, но когда-то приходилось работать руками. Я вам продемонстрирую второй вариант, потому что ручной способ помогает понять, как все работает, не ограничивает в возможностях и не требует затрат на покупку чужих программ.

Большинство настроек мы будем проводить в реестре, и для их вступления в силу может понадобиться перезапуск компьютера. Я тестировал предлагаемые установки на Windows XP с установленным Internet Explorer 6.0, и перезагрузка не понадобилась ни разу.

1.1.1. Мой логотип в IE

Анимация в Windows в большинстве случаев создается из простых растровых изображений в формате BMP. Почему-то Microsoft очень редко использует анимационные форматы типа GIF или видеоформат AVI. Если первый перешел на платную основу и для его использования требуются отчисления, то второй пока что еще открыт, но используется крайне редко. Кстати, формат AVI, кажется, был создан в лабораториях самой Microsoft, и поэтому не совсем понятно, почему они стесняются использовать собственные же разработки?

Как же тогда статичные картинки начинают двигаться? Это делается, как и в играх 90-х годов, на основе спрайтовой анимации. Спрайт — это не то, что не дает многим засохнуть в жаркое лето, и производящая данный напиток компания абсолютно ни при чем. Спрайт — это отдельный кадр анимации или мультипликации.

На рис. 1.1 показано несколько изображений самолета в разных фазах поворота. Каждое представление имеет размер 180×90 пикселов, и все они

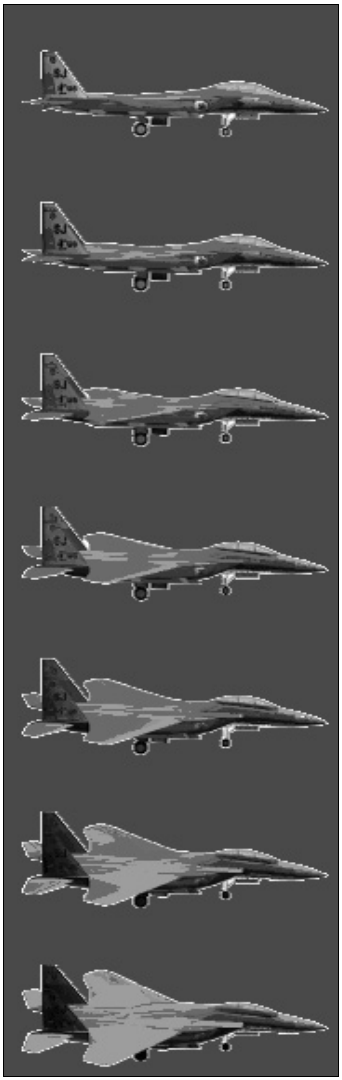


Рис. 1.1. Анимация самолета

выстраиваются по горизонтали или вертикали (в данном случае выбран второй способ, как и в Internet Explorer). Чтобы добиться эффекта анимации, программа последовательно выводит изображения из такого массива картинок, создавая иллюзию движения. Все происходит точно так же, как при создании анимации в мультфильмах.

В программе Internet Explorer также формируется в столбик массив изображений. Размер их не имеет особого значения, главное, чтобы они были квадратными. Чтобы не было проблем (чуть позже я их покажу), лучше всего подготовить картинки размером 26×26 пикселов и расположить их по вертикали. Количество изображений не имеет значения. Чем больше картинок и более плавно изменяется положение самолета на них, тем более качественной будет анимация. Но с другой стороны, файл будет занимать много места и негативно повлияет на загрузку. Так что не стоит даже пытаться в него поместить все кадры из фильма "Матрица".

Сохраните подготовленную ленту картинок в файл с расширением bmp. Я советую размещать такие вещи в директории Windows, чтобы они не мешались или их случайно не удалили.

Теперь нужно подключить картинку к Internet Explorer. Для этого запустите программу regedit.exe, для чего выберите меню **Start | Run** (Пуск | Выполнить), в появившемся окне наберите команду `regedit` и нажмите кнопку **ОК**. Перед вами откроется окно редактора реестра (рис. 1.2). Перейдите в раздел **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar**.

По этому пути реестра нужно создать два новых ключа. Для этого щелкните правой кнопкой мыши в правой половине окна и выберите в появившемся меню **New | String Value** (Создать | Строковый параметр). Будет создан новый параметр, который надо переименовать в **BrandBitmap** и установить в качестве значения путь к вашему BMP-файлу. Точно так же создайте параметр **SmBrandBitmap** с указанием того же пути.

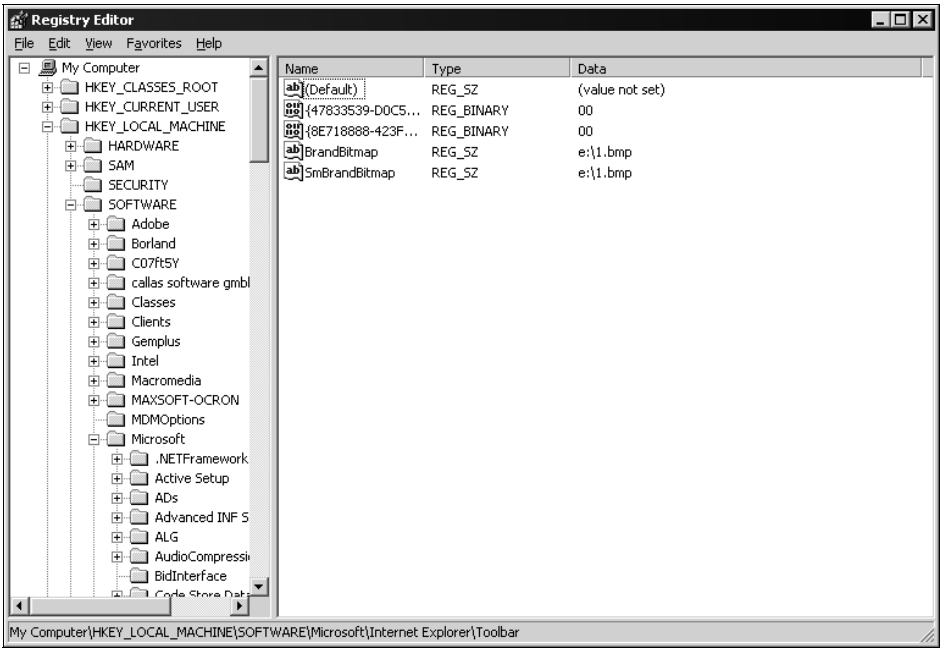


Рис. 1.2. Программа редактирования реестра

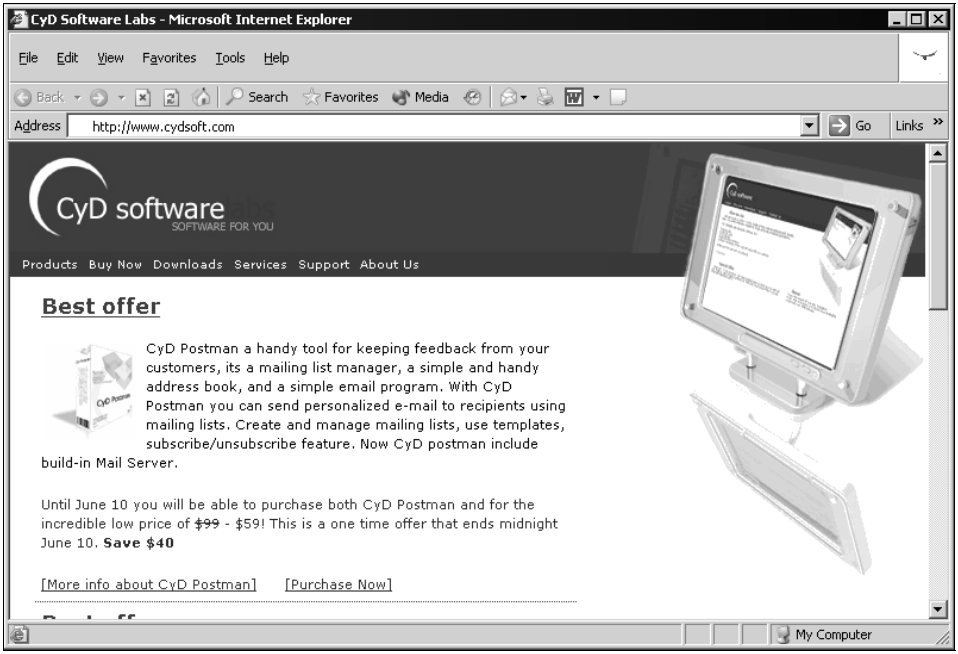


Рис. 1.3. Слишком большой рисунок заставляет меню программы увеличиться по вертикали