Евгений Барилюк barilyuk@hi-tech.ua

# Как стать **невидимкой** в Сети

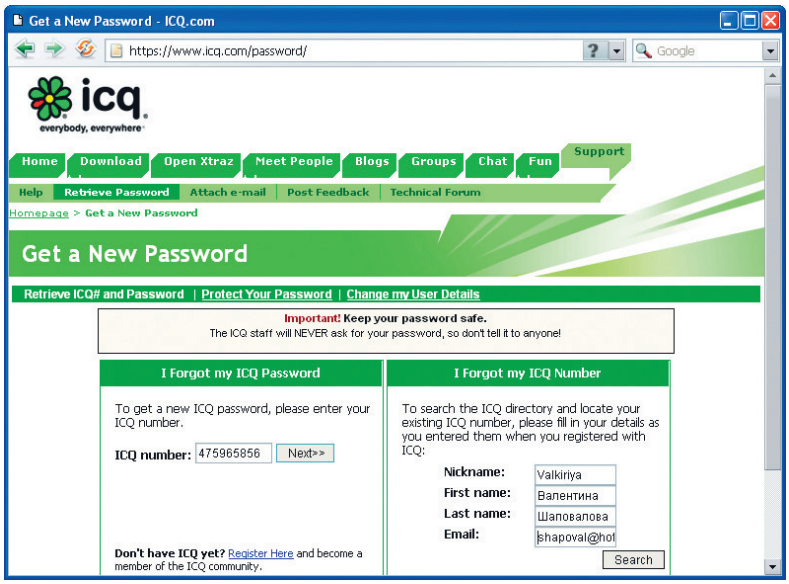
Путешествуя по Интернету вы, сами того не желая, оставляете массу информации потенциальным злоумышленникам. Но скрыться от их взглядов и тем самым обезопасить себя и свой ПК все-таки можно и нужно. Вот пять наиболее распространенных атак и рекомендаций, как не потерять ваше виртуальное, а иногда и реальное имущество в Глобальной паутине

Задумываетесь ли вы, сколько информации о вас и вашем ПК передается в Сеть после одного щелчка мышкой? Оказывается, хотите вы того или нет, вы отправляете много информации о себе: IP-адрес, версию и название операционной системы, конфигурацию браузера (включая название и номер версии) и даже разрешение экрана. По идее, эта информация предназначается лишь для «электронных мозгов» сервера, чтобы он знал, какую веб-страницу вам отправить. Например, некоторые веб-сайты для разных браузеров могут иметь разные варианты веб-страниц. Однако на практике веб-мастеры чаще всего создают лишь одну версию страницы под один браузер (зачастую это Internet Explorer), но хотя для вывода веб-страницы ваши данные уже не нужны, они все равно высылаются серверу.

На первый взгляд, ничего страшного в том, что кто-то узнает ваш IP-адрес, особенно когда при этом вы еще думаете, что ничего такого на вашем ПК нет, и злоумышленников вам бояться не нужно. Но недоброжелатель, зная высылаемые серверу параметры, может вычислить ваш адрес электронной почты, географическое местоположение, и, что самое важное, паспортные данные. Кроме того, он может просто ограничиться атакой на ПК для пополнения своей бот-сети, рассылающей спам. Поэтому имеет смысл скрыть часть отправляемой информации, а также принять меры для повышения уровня безопасности вашей личной информации от кражи.

# 1 Угнать тетю Асю

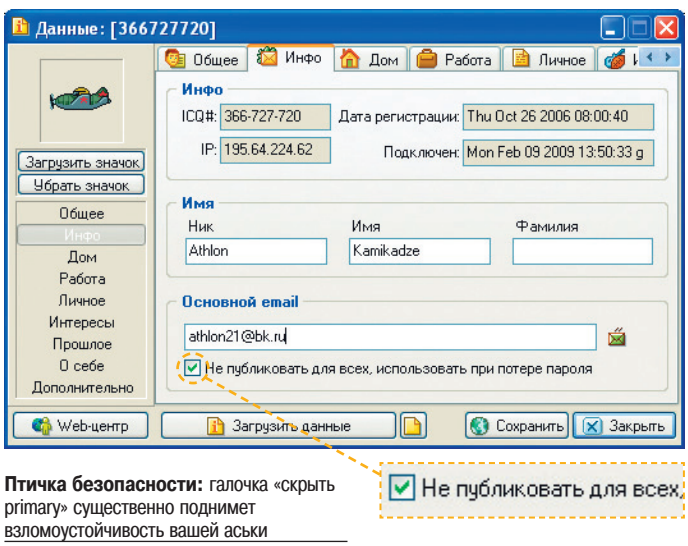
Большинство отечественных пользователей сети воспринимают сервис обмена мгновенными сообщениями ICQ как нечто должное и даже не представляют, что идентификационный номер аськи может стать объектом виртуальной охоты с целью последующей перепродажи. Еще меньше пользователей помнят, что идет активная охота практически на все номера сервиса. Продается все: от девяток (девятизначных номеров) для спама до пятерок. Только на памяти автора числится два угона, владельцы которых поленились использовать пароль посложнее, чем «123456» (на взлом ICQ с таким паролем уходит не больше десяти секунд). Так как же защитить свой UIN (user identification number — идентификационный номер пользователя) от угона (будь то свежекупленный или кровно зарегистрированный номер)? **Для этого вам нужно соблюдать несколько простых правил, которые снизят риск угона до минимума**.




**Превратности безопасности:** восстановить пароль аськи можете не только вы, но и злоумышленник

**Первое:** не используйте простой пароль: он не должен содержать часто произносимые слова, имена, даты рождения, числа, названия мест, городов и популярных музыкальных групп. Например, такой пароль как «boombox» современный двухъядерный компьютер подберет за 13 минут. Никогда не используйте один пароль на форумах и других программах: очень часто бывало, что хакеры взламывали форум, а потом по его базе подбирали пароли на номера ICQ пользователей, и иногда пароли совпадали.

Конечно, запомнить пароль вида «m@Z!138#» просто нереально, но зато все тот же двухъядерный ПК потратит на его взлом аж 23 года — но, скорее всего, хакеры оставят эту затею раньше ☺. А чтобы лучше запоминалось, следует использовать осмысленные слова, добавляя к ним пару спецсимволов и чередуя регистр. Например, фраза «kRiShKa@17» если и не является абсолютным паролем, то, по крайней мере, доставит существенные хлопоты взломщикам. И, наконец, самое главное: пароли рекомендуется менять один раз в месяц или даже чаще.




**Птичка безопасности:** галочка «скрыть primary» существенно поднимет взломоустойчивость вашей аськи

**Второе:** по возможности не пользуйтесь своим номером в интернет-клубах, кафе, компьютерных клубах и пр. Для этих целей заведите себе простой девятизначный номерок, который не жалко и потерять.

**Третье:** служба ICQ позволяет в случае утраты пароля восстановить его (*icq.com/password*), отправив ответ на секретный вопрос и на указанный e-mail (он называется primary — первичный). Даже если вы укажете несколько e-mail-адресов, пароль будет высылаться только на primary. Однако используемая система несовершенна. Например, в качестве primary e-mail часто указывают ящик на бесплатном хостинге, о котором потом забывают. Со временем хостинг-провайдер удалит ящик как неиспользуемый. В итоге взломщик может повторно зарегистрировать этот ящик и затребовать новый пароль. Как видите, с таким заданием справится и ребенок. Поэтому рекомендуется скрывать адрес primary e-mail (эта настройка есть во всех современных IM-клиентах), а также не использовать его для регистрации на форумах.

## Полезные ссылки

- *http://ru.wikibooks.org/wiki/Защита_конфиденциальных_данных_и_анонимность_в_интернете* — детальная информация об анонимности и безопасности в Сети
- *http://ru.wikipedia.org/wiki/SOCKS* — подробная информация о socks, особенностях их работы и использования
- *http://proxyfree.ru* — здесь всегда есть свежие прокси-серверы
- *http://ip-whois.net* — узнать чей-нибудь IP-адрес и географическое расположение можно с помощью этого сервиса
- *http://russianproxy.ru/socks5_proxy_list_fastest* — список доступных socks-серверов

## 2 Зомби из ПК

В последнее время не только в электронной почте и ICQ, но и социальных сетях стали появляться различные программы, «сенсационные новости», фотографии знаменитостей и прочая интересная информация. Но не доверяйте и никогда не запускайте подобные ссылки (даже если антивирус проверил и сказал, что в письме вирусов нет). Дело в том, что вместе с присланным ПО вы в нагрузку получите и троянского коня, а ссылка на сайт с сенсациями превратит компьютер в зомби (звено бот-сети). Тогда вы наверняка лишитесь и номера ICQ, и почтового ящика, а ПК будет использоваться для рассылки спама. Плюс ваши друзья начнут получать от вас письма с вредоносным ПО или ссылки на сенсационные новости. **Поэтому ни в коем случае не открывайте неизвестные приложения, даже если письмо пришло от человека, которого вы давно знаете.** Все просто — его компьютер взломали и от его имени рассылают трояны по всему контакт-листу.

Кроме того, полностью доверять антивирусам и файрволу вообще не следует — самым слабым звеном в системе компьютерной безопасности, как всегда, остается человек, а самое главное оружие против компьютерных злоумышленников — ваш здравый рассудок. Дело в том, что в Сети есть огромное количество программ, которые просто перемешивают код зловредного ПО, и эвристические анализаторы и проактивная защита зачастую «не узнают» давно известного троянского коня.

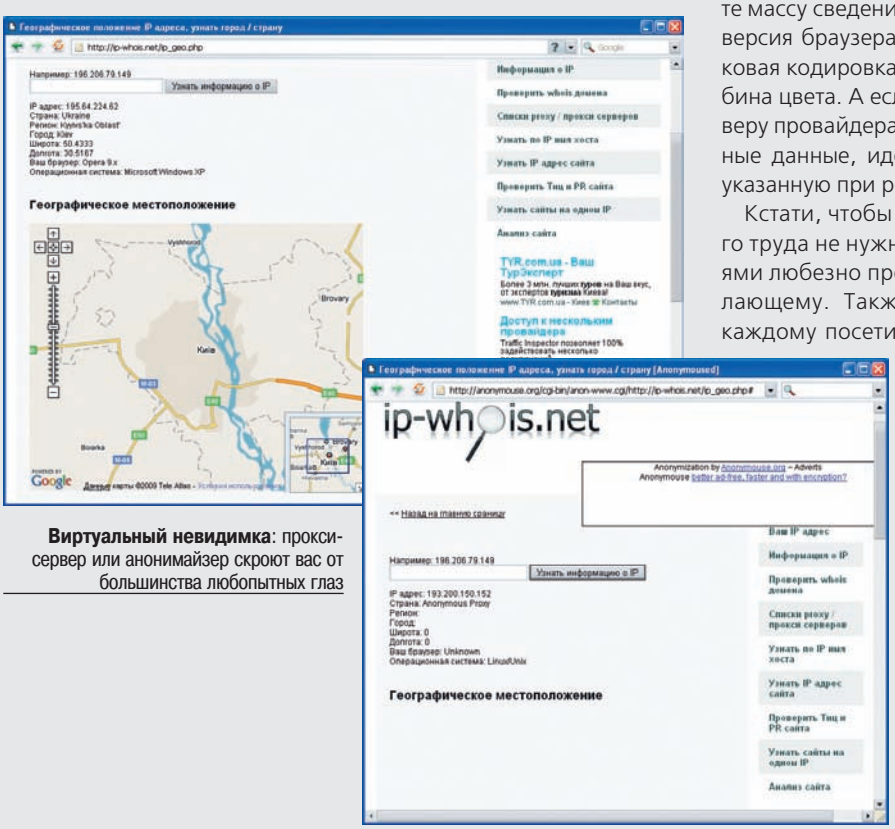
Но поскольку большинство спамеров не используют самые передовые наработки вирусописателей, то регулярное обновление антивирусов и установленный файрвол снизят риск зомбирования вашей машины как минимум вполовину. Кстати, эксперты по безопасности утверждают, что лишь использование учетной записи без прав администратора повышает безопасность Windows на 60 %.

### Популярные Socks-клиенты

**SocksCap** — *www.vpnservice.info/sockscap.html*
**FoxyProxy** — *http://foxyproxy.mozdev.org*
**FreeCap** — *www.freecap.ru*
**Proxifier** — *www.proxifier.com*
**Anonymous Guest Professional** — *www.spszone.com/anguest*

## 3 Алло, это кто?

Говоря о сетевой безопасности, стоит для начала развеять самый устойчивый миф, касающийся анонимности в Интернете. Нет, не о том, что еще многие люди думают, будто в Сети о человеке ничего нельзя узнать. Очень часто можно услышать: «Мне не нужна анонимность, ведь я не занимаюсь ничем предосудительным. Пусть хакеры об этом беспокоятся...». А теперь подумайте, понравится ли вам, если прохожие будут знать ваш адрес, следить за вами и стараться проникнуть к вам домой? Поэтому обеспечению анонимности в Интернете следует уделять должное внимание.




**Виртуальный невидимка**: прокси-сервер или анонимайзер скроют вас от большинства любопытных глаз

Нажимая мышкой на ссылку, вы, хотите того или нет, передаете массу сведений о своем ПК, как то IP-адрес, используемая ОС, версия браузера, URL предыдущей посещенной страницы, языковая кодировка, часовой пояс и даже разрешение экрана и глубина цвета. А если заинтересованное лицо получит доступ к серверу провайдера, то по IP-адресу сможет получить ваши паспортные данные, идентификационный код и другую информацию, указанную при регистрации у провайдера.

Кстати, чтобы получить о вас подробную информацию, много труда не нужно: ICQ и другие программы обмена сообщениями любезно предоставляют IP-адрес собеседника любому желающему. Также некоторые форумы показывают IP-адреса каждому посетителю, а после написания комментария вы можете с удивлением обнаружить, что рядом с никнеймом выводится и ваш IP-адрес

Для начала можно попробовать «спрятаться» с помощью прокси-сервера, который является посредником между компьютером пользователя и серверами Сети. Но это лишь на первый взгляд использование прокси-сервера — гарантия анонимности. Оказывается, подавляющее большинство прокси-серверов в своих запросах передают в специальном поле IP-адрес конечного пользователя. Правда, есть и анонимные службы, вот только найти их не так уж и просто, так как они обычно закрываются в течении недели после публикации. Взять себе свежий прокси можно по адресу http://*ip-whois.net/proxy.php*.

## Ручная дезинфекция

Довольно часто бывает, что даже новейшие версии антивирусов рапортуют о безвирусной системе, которая тем временем выдает глюк за глюком. Как отловить заразу? Достаточно простым, но эффективным тестом на внедрение вирусов был и остается поиск по вновь созданным файлам. Почти все троянские и шпионские компоненты не утруждают себя модификацией даты создания файла, а потому обнаруживаются в момент. Все, что нужно после посещения подозрительных уголков Сети, — как можно быстрее нажать на «*Пуск — Найти — Файлы и папки*». Ищем файлы, созданные за последний день на диске C: (для надежности можно охватить и другие диски). Там будет много всего, но нас в первую очередь интересуют исполняемые файлы (EXE), динамические библиотеки (DLL) и прочие программные компоненты, расположенные в *Program Files* и каталоге *Windows*.

Далее необходимо избавиться от инфицированных файлов, предварительно отослав их в антивирусную лабораторию на анализ, и восстановить «чистые» компоненты с диска установки Windows.

Для восстановления компонентов Windows вставьте компакт-диск с дистрибутивом, а в меню *Пуск-Выполнить* наберите команду *sfc /scannow*. Запустится утилита *Защита файлов Windows*, которая проведет сканирование и предложить заменить отсутствующие или поврежденные файлы на оригинальные.

Другой вариант сохранения анонимности в Интернете — использование анонимайзеров (anonymizer). Анонимайзеры — это, по сути, просто анонимные прокси-серверы, имеющие собственный веб-интерфейс. И работать с ними очень просто. Заходим на сайт, вводим в специальное поле адрес нужного нам сервера — и все, запрашиваемая страничка загружается. Правда, при использовании анонимайзеров придется смириться с парой недостатков. Во-первых, скорость загрузки страниц может значительно уменьшиться. А во-вторых, на сегодняшний день уже практически невозможно найти бесплатный анонимайзер. Конечно, когда эти службы только появились, никому и в голову не могла прийти мысль о сборе денег за свои услуги. Максимум, что владельцы могли себе позволить, — это «повесить» несколько рекламных баннеров. Теперь же пользователям приходится платить за роскошь остаться неузнанным.

Логичным будет объединение нескольких прокси-серверов по всему миру в последовательную цепочку, что существенно затруднит поиск отправителя. Эта задумка реализована в проекте Tor (*www.torproject.org*). Tor работает со многими существующими приложениями, включая веб-браузеры, системы мгновенного обмена сообщениями и другим ПО, использующим протокол TCP.

Существует еще один способ обеспечения анонимности в Интернете, который является на сегодняшний день самым надежным. Речь идет о socks-протоколах. Принцип действия этой технологии в общем-то похож на работу прокси-сервера. Правда, есть несколько серьезных различий. Так, «общение» клиентского компьютера и socks-сервера происходит не по общепринятым, а по специальным протоколам (socks4, socks5 и т. д.). В результате передача IP-адреса пользователя невозможна в принципе. Кроме того, socks-сервер сам преобразовывает информацию от пользователя в запросы для общепринятых протоколов. А это значит, что ни один сервер «не догадается», что отправляет данные не конечному пользователю, а посреднику. Да и работать с технологией socks очень удобно — достаточно скачать любой Socks-клиент (см. вставку «Популярные Socks-клиенты»). Установив клиент, настройте его — и можно больше ни о чем не беспокоиться.

## Безопасность без прав

Практически все пользователи используют дома лишь одну учетную запись, имеющую права администратора, и продолжают ругать Windows за «дырявость», не догадываясь, что для существенного повышения безопасности Windows вовсе не требуется иметь продвинутые знания по администрированию ПК, а достаточно лишь использовать учетную запись с ограниченными правами.

Как подсчитали в компании BeyondTrust, если бы пользователи работали в Windows без административных полномочий, то для них 92 % из обнаруженных в системе за год критических уязвимостей оказались бы не столь опасны или вообще не имели бы значения.

В компании изучили бюллетени по безопасности Windows, выпущенные корпорацией Microsoft за 2008 год. Как выяснилось, в подавляющем большинстве из них в разделе о мерах по снижению и устранению риска атаки говорилось, что пользователи, работающие без привилегий администратора, менее уязвимы. Это касается 92 % критических уязвимостей и 69 % от всех 154 ошибок, выявленных и исправленных за прошлый год.

Когда же исследователи перешли к изучению браузера Internet Explorer и офисного пакета Microsoft Office, выяснилось, что и здесь доли уязвимостей, от которых можно защититься отказом от привилегий администратора, составляют соответственно 89 и 94 %.

Кстати, недавно опубликованный способ обхода системы UAC в Windows 7 (*www.thevista.ru/page.php?id=10752*) тоже касается только пользователей с правами администратора.

И напоследок: если вам никак нельзя обойтись без учетной записи с правами администратора, используйте как можно более сложный пароль.

# 4 Виртуальный дядя-миллионер

В наш прогрессивный XXI век даже мошенники переходят на электронную форму работы. Сейчас они активно рассылают спам-письма, в которых пишут, что вы являетесь дальним родственником миллионера из Великобритании, предлагая оплатить офисные расходы по получению денег богатого родственника. И если в это вряд ли кто поверит, то в выигрыш в лотерее поверят многие. Поэтому такие письма стоит просто удалять не читая, особенно если вы не принимали участия ни в каких розыгрышах.

Лучше внимательно читайте бланки уведомлений банков, копии счетов и прочую конфиденциальную информацию, приходящую к вам по электронной почте. Документы могут быть подделками, с помощью которых злоумышленник пытается узнать ваши персональные данные. Если есть сомнения, обратитесь в свой банк за подтверждением.

Возьмите за правило: никому в Сети нельзя доверять свои персональные данные – номера счетов, веб-кошельков, пароли доступа и пр. А участвуя в онлайн-аукционах или покупая товары в Интернете, никогда не соглашайтесь на предоплату товара, так как потом будет проблематично вернуть свои деньги.

И помните, мошенники эксплуатируют самые простые человеческие чувства – жадность, гордость, любовь к «клубничке», лень. Если вы видите какое-то «странное» сообщение, которое давит как раз на них, – это тоже повод задуматься, не пытаются ли вами манипулировать. Если вам предлагают удивительно выгодные условия сделки, скорее всего, вас хотят обмануть.

Вообще, социальная инженерия – один из самых продуктивных (и иногда единственный) способ взлома, так как жертва сама выдает все, что нужно. Суть метода проста: вор заговаривает зубы, вытягивая требуемую информацию. Допустим, что вы получили письмо, в котором администрация ICQ, приносит свои извинения, сообщает о каких-то технических неполадках и просит вас повторно выслать им пароль. Не верьте, на 100 % это обман. Или помните, как регистрируясь на бесплатном mail-сервере, вы заполняли поле «секретного вопроса»? К примеру, это мог быть вопрос: «Как зовут мою собаку?». Вор запросто может в милом разговоре по аське аккуратно вытянуть из вас имя вашего питомца.

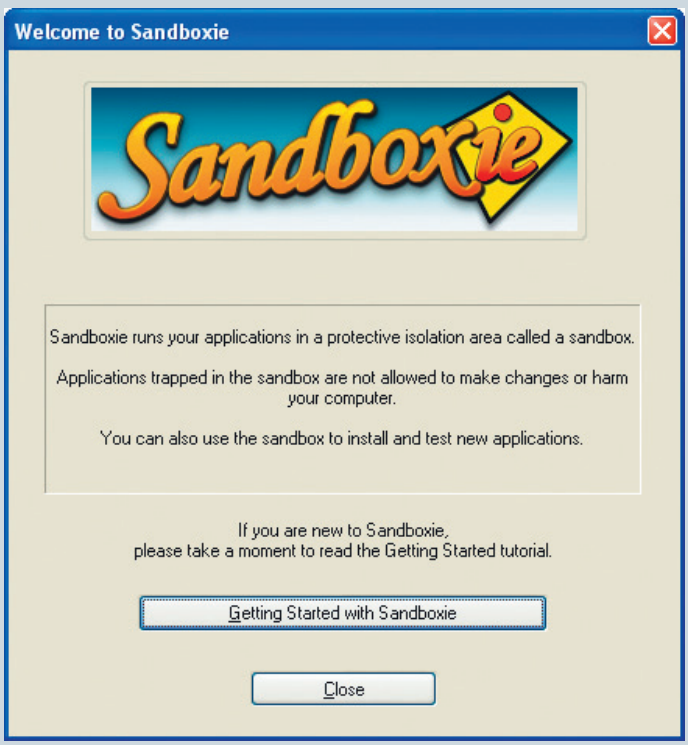
## Безопасная песочница

Тем пользователям, которые не смогли воспользоваться технологией VirtualSurf (см. вставку на следующей странице) для защиты компьютера во время серфинга, хорошо подойдет программа Sandboxie (*www.sandboxie.com*). При этом установка и настройка, в отличие от VirtualSurf, займет всего несколько минут.

Утилита предназначена для контроля за работой других программ, которые через нее запущены. При этом результаты работы этих программ не влияют на работу системы в целом, а сохраняются в отдельной папке. Таким образом, это ПО собой своеобразный фильтр, в котором задерживаются все изменения, производимые программами. Основная функция Sandboxie — защита и сохранение вашего компьютера в рабочем состоянии, поэтому о защите конфиденциальных данных нужно будет позаботиться отдельно.

Ценность данной утилиты заключается в том, что можно вообще не выполнять ее настройку. Скачали, установили, пользуетесь. Sandboxie создает в меню быстрого запуска и в меню «Пуск» ярлык «Sandboxed Web Browser», который запускает ваш браузер по умолчанию через программу. Это уже будет защищать вашу систему от вирусов, троянских коней и их последствий.

Правда, при настройке по умолчанию защита ваших конфиденциальных данных минимальна. Поэтому сразу же рекомендуется заблокировать для доступа папки и файлы с конфиденциальными данными. Для этого нужно их добавить в список «Blocked Access», который доступен в настройках SandBoxie.




Sandboxie позволяет запускать каждую программу так, что любые изменения в системе сохраняются в ограниченной среде («песочнице») и их можно отменить

## 5 Дырявое окошко

Браузер поистине может считаться окном в Сеть, через которое не только мы выходим в Интернет, но и могут войти к нам. Сделать это можно, например, атакой на сам браузер с засылкой троянской программы или сбором данных о пользователе (с какой страницы пришел, под каким IP). Кроме того, не забывайте, что все браузеры сохраняют компрометирующие данные о посещенных страницах на жестком диске.

Internet Explorer — до сих пор самый популярный сетевой обозреватель всех времен и народов. Но это же и сделало его самым небезопасным. Практически каждую неделю в нем обнаруживается свежая порция новых «дыр». Но «дыры» — это еще не все. Хуже всего, что IE страдает хроническим недержанием конфиденциальной информации. В первую очередь это относится к кешу и истории. По умолчанию кеш размещается в каталоге *Documents and Settings\user-name\Local Settings\Temporary Internet Files* и, по идее, в любой момент может быть удален по команде. Но не все так просто! Из-за ошибок в системе индексации часть файлов порой просто не удаляется (в чем легко убедиться, заглянув в указанный каталог после его очистки). Туда же попадают и вложения электронной почты при открытии вложений в Outlook Express, причем штатными средствами IE они не удаляются. Самое интересное, что индексный файл index.dat, находящийся в том же подкаталоге, вообще не очищается и продолжает хранить адреса посещенных сайтов.

Решение проблемы состоит в ручном удалении всего содержимого папки Temporary Internet Files, но при этом необходимо выйти из системы и войти под именем другого пользователя, поскольку в противном случае доступ к части файлов будет заблокирован. Кроме того, можно пойти радикальным путем и заменить себе браузер. Например, Internet Explorer 8 и Firefox 3.1 имеют функцию приватного серфинга, удаляя всю информацию о посещенных страницах при выходе.

## Универсальная защита

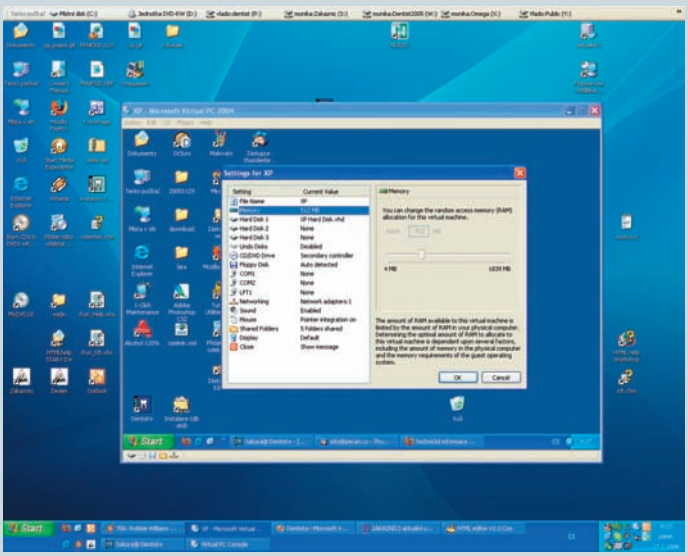
Говорят, что ничего абсолютного в мире нет, однако абсолютную защиту во время серфинга в Сети получить можно. Это обеспечивает технология VirtualSurf. При этом, хотя время настройки равно времени установки Windows + дополнительного ПО, данный метод гарантирует 100 % сохранность данных вашего компьютера и защиту конфиденциальных данных от кражи.

Для этого вам нужно создать виртуальную машину, на которой будут открываться сайты. Виртуальная машина (ВМ) — это программа, которая создает на вашем компьютере еще один компьютер, который запускается в окне программы. Фактически специальное ПО эмулирует аппаратную начинку виртуального ПК, поэтому его настройка ничем не отличается от настройки реального компьютера. Фишка в том, что виртуальный ПК и физический могут не иметь никакой связи. Поэтому при наличии на сайте вредоносного кода последствия его выполнения будут отражаться только на виртуальной машине, не принося вашему компьютеру никакого вреда. А настроив виртуальную машину соответствующим образом, можно избавиться и от этих последствий — при выключении ВМ все изменения будут стираться и возвращаться к первоначальным настройкам, когда никаких вирусов на ВМ еще не было. В безопасности будет и личная информация, которая хранится на компьютере-хозяине и недоступна из ВМ.

Создать и настроить на своем компьютере виртуальную машину совсем несложно. Достаточно скачать бесплатную утилиту VirtualPC от Microsoft (*www.microsoft.com/windows/downloads/virtualpc/default.mspx*). В итоге вы получите инструмент, который позволит вам не бояться кражи личной информации и зловредного ПО.

**Настройка ВМ заключается в следующем:**

1. Установите эмулятор компьютера (виртуальную машину) VirtualPC.
2. Установите ОС на виртуальную машину и все нужные вам программы (браузеры, антивирус, файрвол и т. д.).



Потратив пару часов на настройку виртуальной машины, вы сэкономите гораздо больше времени на переустановке ОС и программ на своем реальном ПК

3. Разрешите в настройках ВМ доступ к сетевой карте вашего ПК для виртуальной операционной системы.
4. Включите опцию создания дисков отмены (для возврата к изначальным настройкам при повреждении операционной системы зловредным ПО).
5. Настройте сетевое подключение (введите логин, пароль, адрес прокси-сервера и т. д.) и начинайте безопасный серфинг в Сети.