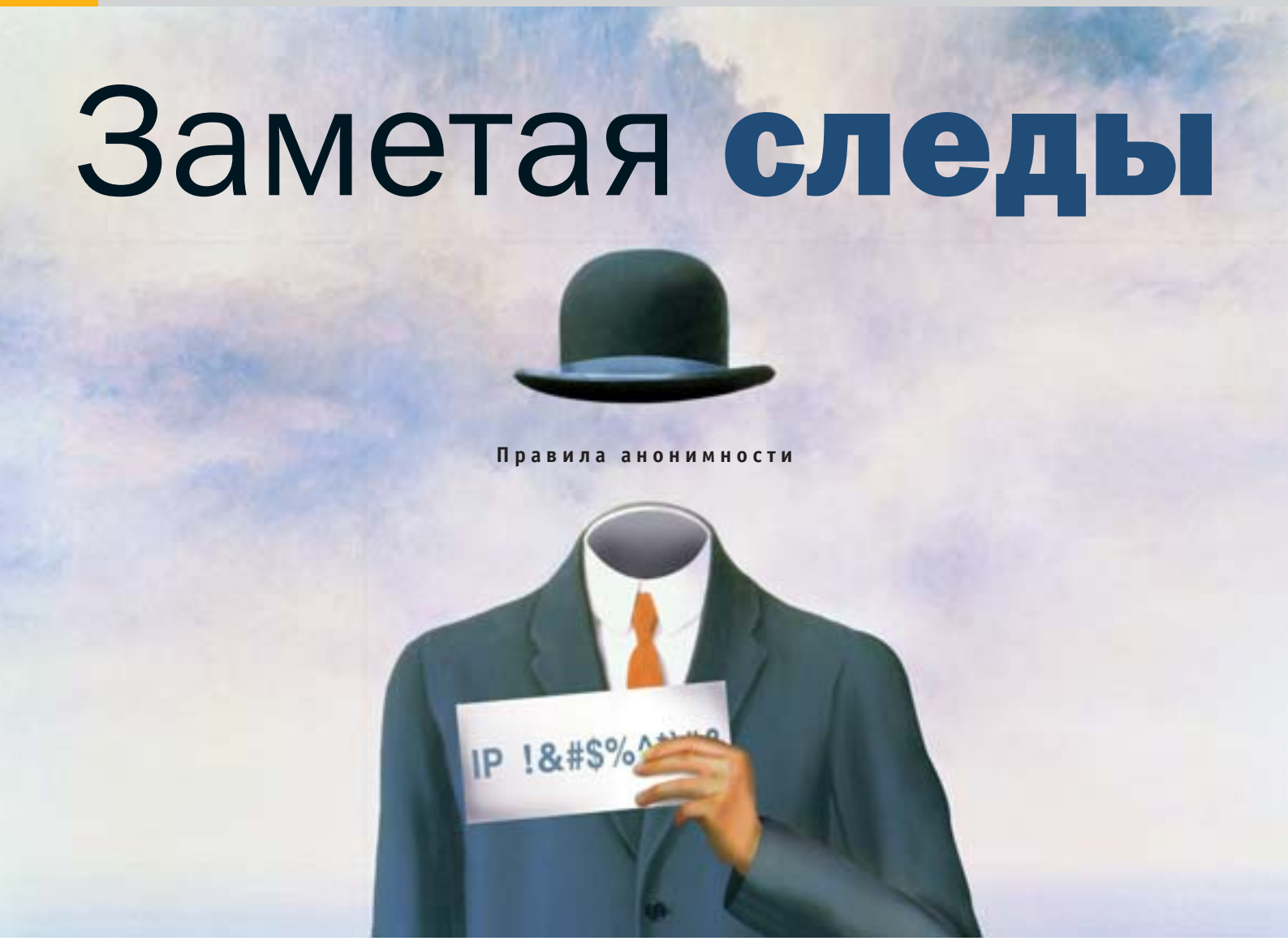
Заметая следы



Правила анонимности

Пользователь в Интернете неизбежно оставляет следы. Его компьютеру могут угрожать спам, опасные скрипты или шпионские программы. Рассказ о том, как в Сети надеть шапку-невидимку.

По примерным оценкам, Интернетом пользуются около 700 миллионов человек. Если вы считаете, что в этой массе передвигаетесь абсолютно анонимно, это не более чем заблуждение. Дело в том, что при путешествиях от сайта к сайту за вами тянется предательский след информации. Даже ваш браузер откровенничает про детали системных настроек, выставляет напоказ информацию, какую страничку вы только что посетили или что искали в Google. А уж через IP-адрес вас можно идентифицировать однозначно.

Spyware, cookies, спам

Для многих сайтов вы уже стали хорошим знакомым. Вы можете это заметить, когда при проверке почты через веб-интерфейс ваш логин автоматически появляется в окне ввода. Такие знаки внимания относятся к безвредным последствиям слежки за пользователем. Однако дело принимает неприятный оборот, когда рекламщики начинают охоту за данными с помощью cookies и spyware. Ваши любимые сайты, последние онлайн-покупки, используемое аппаратное и программное обеспечение — вся информация считывается третьими лицами без вашего ведома. На ее основе действующие по всему миру маркетинговые агентства создают детальные профили пользователей. Как следствие — на каждом шагу вы натыкаетесь на рекламные баннеры, завлекающие вас более или менее подходящими предложениями. Не менее усердно работают спамеры: »

» с помощью маленьких невидимых жучков они, к примеру, могут узнать, открывали ли вы сообщение со спамом и даже когда это было, — таким образом будет понятно, проверяете ли вы почту, приходящую на этот адрес.

Анонимный серфинг

При навигации по Сети происходит фоновый обмен данными. Так, сервер запрошенного вами сайта узнает через ваш IP-адрес, в какой стране вы находитесь и услугами какого провайдера пользуетесь. Кроме того, в каждом запросе содержится информация о вашем браузере и операционной системе, о системных настройках, а также о том, с какого сайта вы пришли. Но это еще не все: сервер, как правило, оставляет cookie-файл на вашем жестком диске, чтобы впредь было известно, как прошли ваши предыдущие посещения этого сайта. Вы хотите положить конец этим онлайн-откровениям?

Замаскировать IP-адрес

При каждом заходе в Интернет вы получаете от своего провайдера новый IP-адрес. Это необходимо, так как предоставляемых согласно интернет-стандарту IPV4 одновременно на всех пользователей адресов не хватает. В лог-файлах серверов отмечается, каким IP-адресом и какие данные были затребованы. Хотя сервер и не знает, как вас зовут, в случае чего вас вполне можно идентифицировать — ведь провайдер следит за тем, когда вам был присвоен тот или иной IP-адрес.

Серфинг через прокси-сервер

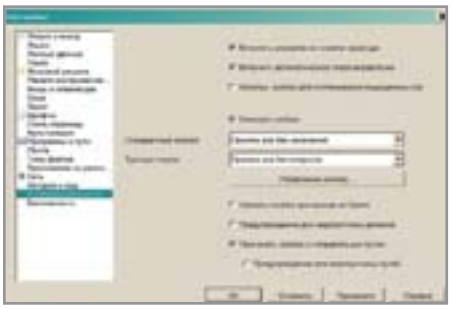
IP-адрес можно изменить, используя «обходной путь» через прокси-сервер. Прокси-сервер берет на себя роль так называемого промежуточного звена: он принимает запрос браузера пользователя и передает его на сервер. Ответ от сервера происходит по тому же пути. Польза от такой переадресации заклю- »

Программа JAP

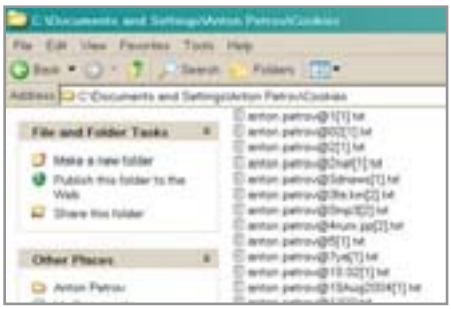
Безопасность на высшем уровне

Многие утилиты-анонимайзеры перенаправляют данные через прокси-серверы, которые не всегда заслуживают доверия из-за неясной степени конфиденциальности. Совсем другое дело — JAP: потоки информации через надежное соединение попадают на серверы службы, там шифруются и дальше передаются смешанно на компьютеры предприятий и организаций, которые владельцы JAP считают крайне надежными. Здесь входящие пакеты данных всех пользователей проходят через сложную процедуру перемешивания друг с другом. Эту путаницу шлюзует каскад компьютеров, пакеты данных снова и снова перемешиваются. Только последний компьютер знает ключ, чтобы распутать клубок данных. Кроме него после этой процедуры никто уже не сможет определить происхождение этих данных. Несмотря на сложную систему, работать в JAP очень просто и удобно. Все нужные настройки браузера выполняются автоматически. Только в случае, если вы находитесь в Интернете через вынужденный прокси-сервер, вам надо будет вручную занести его адрес в настройки JAP.

▸ **http://anon.inf.tu-dresden.de**



▲ Opera позволяет в своих настройках заблокировать команду Referer



▲ Многие сайты без спроса записывают cookies на ваш компьютер

▲ Пример безопасной и анонимной почты — Hushmail.com

» чается в том, что веб-сервер узнает не ваш IP-адрес, а лишь IP-адрес прокси.

Как выбрать прокси-сервер

Если вы хотите путешествовать по Сети анонимно через прокси-сервер, активируйте в вашем браузере опцию «Соединение → Настройки LAN → Использовать прокси-сервер» и укажите IP-адрес сервера. В Сети есть списки прокси (к примеру, на сайте www.multiproxy.org или www.atomintersoft.com), но перечисленные там серверы часто бывают слишком загружены, и поэтому их использование может существенно затормозить ваше соединение. Будет ли соединение через данный прокси-сервер проходить на высокой скорости, можно выяснить только на собственном опыте. Еще одно препятствие, с которым вы можете столкнуться: не все прокси-серверы обеспечивают полную анонимность. Многие прокси, например, добавляют к HTTP-запросу переменную HTTP_X_FOR WARDED_FOR с указанием вашего IP-адреса.

Анонимайзеры

Если поиск прокси-сервера кажется вам слишком обременительным занятием, вы можете использовать такие утилиты для обеспечения анонимности как Get Anonymous или Steganos Internet Anonym Pro. Эти программы автоматически перенаправляют ваши запросы прокси-серверам, они удобны и просты в использовании. Однако публичные серверы, установленные по умолчанию в настройках того или иного анонимайзера, часто бывают перегружены, и, как результат, скорость интернет-соединения от этого сильно страдает. Еще один недостаток этих утилит состоит в том, что они используют публичные серверы, поэтому анонимность вам не гарантируется. Если при работе в Интернете необходима полная секретность, лучше воспользоваться программой JAP.

Отключение cookies

Сервер сохраняет данные не только у себя, но и на вашем компьютере. Так появляются файлы cookies. С помощью этих небольших текстовых файлов веб-сервер распознает вас при следующем заходе на сайт. В этих случаях cookies нужны и полезны. Самое неприятное в них то, что их сохранение и чтение не очевидны для пользователя, ведь они оказываются у вас на компьютере без спроса. Вам не сообщают ни про содержание, ни про цель, ни про длительность сохранения этих файлов. Проблема в том, что cookies нельзя взять и заблокировать. Если пользователь запретит их в настройках браузера, он сам себе откажет в доступе ко многим сайтам. Например, вы не сможете войти в свой профиль в Живом журнале или пользоваться почтовым ящиком Mail.ru.

Удалить существующие cookies

Но что же делать с файлами cookies, которые уже прочно обосновались на вашем жестком диске? Сотрите их! Для этого щелкните в Internet Explorer в меню «Настройки → Параметры Интернета → Удалить cookies». После этого действия вы окажетесь неопознанным для всех сайтов. Чтобы окончательно уничтожить все cookies, не забудьте стереть и файл Index.dat — в этом файле Windows указывает все ранее принятые пакеты данных. Так как операционная система не даст вам разрешение на доступ к этому файлу, для его удаления вам понадобится ути- »

Hushmail

Бесплатно, анонимно и безопасно

С помощью Hushmail вы можете анонимно посылать зашифрованные электронные письма. Анонимность обеспечивается за счет того, что для создания профиля пользователя не обязательно указывать личные данные. Это практично в том случае, когда использование римейлера слишком сложно. Шифрование сообщений в службе Hushmail производится по стандарту Open PGP. Он использует метод публичных ключей. При этом для каждого пользователя создаются два индивидуальных ключа — публичный и частный. Публичный ключ сообщается всем пользователям, которые имеют право расшифровывать сообщения, а личный ключ остается у пользователя. Для шифрования сообщения отправитель использует публичный ключ получателя, и тот может расшифровать послание только с применением своего личного ключа.

Hushmail функционирует так же просто, как и любая другая почтовая служба. Через POP3 с почтовым ящиком можно работать также и в Outlook или в другой клиентской программе. Немного сложнее работа с PGP, потому что сперва каждому получателю сообщения необходимо отправить публичный ключ. Бесплатный почтовый ящик на Hushmail имеет размер 2 Мбайт. Увеличение объема почтового ящика до премиум-класса кажется нам не очень разумным — так как при оплате этой операции используется пластиковая карточка, ни о какой анонимности речь уже не идет. Увеличение памяти и не нужно: хотя, конечно, объем почтового ящика 2 Мбайт — не так уж и много, этого вполне достаточно, если вы используете его только для секретной переписки по электронной почте.

▶ **www.hushmail.com**

» лита TIF-Loscher 2.0. При запуске системы программа создаст новый, пустой файл Index.dat и удалит тем самым и все следы cookies. Наш совет: если вы хотите блокировать cookies и в будущем, то сделайте Index.dat доступным только для чтения. Для этого найдите файл в каталоге «Документы и настройки/[Ваше имя пользователя]/ Cookies». Правой клавишей мышки щелкните на значок файла и в пункте «Свойства» поставьте галочку напротив строчки «Только чтение». Теперь ваш браузер не сможет вносить новые записи в этот файл.

Как отключить Referrer

Владельцы сайтов используют эту команду для сбора статистики. В браузере Opera ее можно отключить, а в Mozilla Firefox и Internet Explorer такой возможности нет. Однако не стоит делать из этого трагедию: во-первых, это безопасно, а во-вторых, владельцам сайтов эти данные нужны обычно только для того, чтобы узнать, какие сайты дают ссылку на их страничку.

Анонимные римейлеры

Так называемые римейлер-системы удаляют сведения об отправителе из заголовка сообщения и заменяют их другим адресом. Существуют различные технические варианты, как послать анонимное письмо, однако, в принципе, все они сводятся к одному и тому же методу: информация передается не от одного почтового сервера к другому, а проходит через еще один сервер-посредник или даже через несколько серверов. Примерно так же работает и JAP. Какой именно «поставщик» этой услуги заслуживает вашего доверия, решать только вам, как и в случае с прокси-серверами. К примеру, анонимность гарантирует Hushmail.com — бесплатная почтовая служба, которая одновременно предлагает и анонимность, и шифрование сообщений.

Блокировка веб-жучков

Веб-жучки, или Clear GIF — это прозрачные картинки, которые часто бывают спрятаны в спам-сообщениях и которые незаметно собирают и пересылают информацию от вас спамерам. Если вы откроете такое электронное письмо, жучок загрузится с сервера, однако вы его не увидите. В чем же тогда смысл его использования? Подкарауливающие вас в спаме веб-жучки могут служить, к примеру, подтверждением прочтения для того, кто отправил вам это сообщение, и он таким образом будет знать, что ваш адрес еще действует и вы принимаете с него почту. Однако все может быть гораздо хуже: вполне вероятно, что через веб-жучок можно прочитать cookies, хранящиеся на вашем жестком диске. Если сервер, который снабдил электронное письмо веб-жучком, найдет у вас в компьютере cookie, это было бы с точки зрения защиты информации настоящим ЧП.

Разблокировать веб-жучки

Спам никогда нельзя открывать, надо сразу же его удалять. Ведь даже просто при открытом списке сообщений веб-жучки могут начать действовать, например, отослав подтверждение прочтения. Для входящих сообщений рекомендуется включить текстовый режим просмотра — тогда HTML-файл, в котором скрывается жучок, будет прикреплен к сообщению. CHIP