**ХАКЕРСКИЕ ШТУЧКИ,  
ИЛИ КАК ОНИ ЭТО ДЕЛАЮТ**

*В этой главе раскрыты неко-  
торые "хитрости": регист-  
рация под вымышленным  
именем, обход различных  
"подводных камней" (АОН,  
авторизирующиеся програм-  
мы, клавиатурные шпионы,  
ПЭМИН). Особое внимание  
уделено вопросам работы  
с электронной почтой - вы-  
яснению реального отправи-  
теля сообщения, отправле-  
нию анонимных сообщений,  
выбору второго почтового  
адреса.*

***Проверка на отсутствие АОН***

Прежде чем получать адрес и звонить на BBS, нужно убедиться (напри-  
мер, путем звонка с сотового телефона, с телефона-двойника типа  
Panasonic, с таксофона или с телефона, который гарантированно не  
определяется системой АОН), что на данном узле отсутствует система  
АОН. Если в списке BBS (или в рекламе) указан тип модема Russian  
Courier, Zyxell или IDC, с вероятностью 99% на этих станциях исполь-  
зуются АОН. АОН выдает себя характерным щелчком и звуковым сиг-  
налом, как правило, после первого гудка (он снимает трубку, а далее  
идут гудки, выдаваемые самим АОН, как правило, отличающиеся от  
первого гудка по тональности). Если АОН есть, но все же нужно остать-  
ся анонимным (например, хотите провести акцию информационной  
войны, сбросить новый вирус и тому подобное), можно воспользовать-  
ся АнтиАОНом. Эти функции присутствуют практически во всех теле-  
фонных аппаратах с АОН (например, в РУСЬ или в Phone Master).  
Также можно купить приставку-АнтиАОН, которая еще не раз приго-  
диться (в Москве, например, они продаются на радиорынке в Митино).  
Функцию АнтиАОН лучше включать почти сразу после набора номера  
и удерживать ее некоторое время. Если АОН не может определить но-  
мер, то после снятия трубки АОН-ом слышится характерные тональные  
сигналы (порядка 9 штук).

***Советы по регистрации***

Никогда не стоит регистрироваться под настоящим именем, ведь неиз-  
вестно, к кому может попасть эта информация и для чего она будет ис-  
пользована. Можно взять любую телефонную базу, например, КОТИК  
или ее Online версию (http://www.xland.ru:8088/tel\_win/owa/tel.form),  
и ввести любую выдуманную фамилию. Тривиальные фамилии, вроде  
Иванов, Петров, Смирнов, Андреев, Алексеев и так далее, корректнее не  
использовать, лучше что-то не совсем обычное (ну первое, что прихо-  
дить в голову: Левашов, Дубинин, Авдотин, Садовский). Далее записы-  
ваем инициалы, адрес и телефон любого человека из выведенного спис-  
ка. При регистрации на BBS обычно требуется сообщить такие  
сведения:

- имя и фамилию (иногда полное ФИО - полученные инициалы  
нетрудно преобразовать во что либо, например Н.А. в Николая

Алексеевича; более того, инициалы могут и не совпадать, ведь по-  
тенциально квартира может быть зарегистрирована, скажем, на ро-  
дителей или жену) - вводятся полученные из базы;

- домашний адрес - полученный из базы;

- телефон - тоже полученный из базы;

- день рождения - придумываем;

- хобби - придумываем;

- и т.д.

Системные операторы BBS, как правило, очень ленивы, и максимум, на  
что их хватит, так это проверить данные по той же самой базе.

Обязательно нужно все это куда-нибудь записать, можно в файл  
(и хранить его в надежном месте, например, на диске, созданном про-  
граммой BestCrypt). Рекомендуется использовать абсолютно разные  
данные при работе с разными BBS! В FTN-сетях следует регистриро-  
ваться, применяя подобные методы.

Рассмотрим еще один аспект privacy. Это "нехорошие" функции многих  
программ: вести логические протоколы работы и так далее.

***Что "помнит" компьютер***

Некоторые программы обладают на редкость большим количеством все-  
возможных "черных ходов", "люков", "багов" и так далее. Вот лишь не-  
которые примеры:

- Microsoft Outlook Express 4.0 - все письма, которые когда-либо были  
отправлены, получены или удалены, он все равно хранит в своей  
базе. Поэтому рекомендуется периодически удалять (лучше невосста-  
новимыми методами, например, с помощью программы Kremlin 2.1)  
эти файлы. Они расположены в следующих директориях:

\Windows\Aplication\Microsoft\Outlook Express\Mail\ - почта,  
здесь необходимо удалить все файлы с расширениями IDX и МВХ.

\Wmdows\Aplication\Microsoft\Outlook Express\News\ - новости,  
здесь необходимо удалить все файлы с расширениями NCH.

Удалить из базы все удаленные сообщения можно также с помощью  
опции "Сжать папки".

- Microsoft Internet Explorer 4.0:

\Windows\Cookies\ - хранит файлы Cookies (их лучше периодичес-  
ки удалять с помощью программы Kremlin 2.1).

\Windows\Temporary Internet Files\ - хранит все адреса, которые  
посещались в Интернет (их лучше периодически удалять с помо-  
щью программы Kremlin 2.1).

- Microsoft Windows 95:

\Windows\History\ - хранит все файлы истории (их лучше перио-  
дически удалять с помощью программы Kremlin 2.1).

\Windows\name.pwl - в этих файлах Windows хранит имена, теле-  
фоны и пароли для соединения с Интернет, все они легко (с помо-  
щью специальных программ) расшифровываются.

\Wmdows\Pronles\name\ - (вместо name будет указано имя пользо-  
вателя) хранит профили и все установки конкретных пользователей  
(это, кстати, справедливо и для Windows NT)

\Windows\Aplication\Microsoft\Outlook Express\Mail\ - почта  
\Windows\Aplication\Microsoft\Outlook Express\News\ - новости  
\Windows\Aplication\Microsoft\Address Book\ - адресная книга  
\Windows\Cookies\ - файлы Cookies  
\Windows\Favorites\ - файлы закладок Интернет  
\Windows\History\ - файлы истории Windows  
\Windows\user.dat - параметры пользователя  
\Windows\user.daO - резерв

Большинство FTP-клиентов сохраняют в специальной директории все  
места в Интернет, которые посещались пользователем (а иногда сохра-  
няют и нешифрованные имена и пароли). В целях безопасности целесо-  
образно периодически (скажем, раз в неделю) стирать содержимое  
кэша. Например, в Bullet Proof FTP (одной из лучших программ, полу-  
чить которую можно на сервере http://www.bpftp.com), он располагает-  
ся в директории Cache. Лучше производить невосстановимое удаление,  
например, с помощью программы Kremlin 2.1.

***К вопросу о CMOS SETUP***

Вот еще один наглядный пример лазеек для спецслужб. Почти любой  
компьютер имеет возможность установить пароль на вход. Но мало кто

знает, что специально для спецслужб (разработчиками BIOS) были со-  
зданы универсальные пароли, открывающие вход в любой компьютер.  
Вот примеры:

- AWARD BIOS: AWARD\_SW, Ikwpeter, Wodj, aPAf, j262, Sxyz,  
ZJAAADC

- AMI BIOS: AMI, SER, Ctrl+Alt+Del+Ins (держать при загрузке,

иногда просто INS)  
Естественно, что вводить пароль нужно в соответствии с регистром букв.

***Программы, авторизующиеся в Online***

В последнее время все чаще стали появляться программы, которые про-  
веряют через Интернет, зарегистрирована ли данная копия программы.  
Вернее, когда пользователь работает в Интернет, они незаметно это про-  
веряют, а потом радуют сообщением о том что используемая копия не-  
легальна. Наглядный тому пример - Bullet Proof FTP. Но это еще не  
все. Существует мнение, что такие программы, как, например, операци-  
онная система Windows, способны как бы следить за всем, что происхо-  
дит в компьютере (либо сами, либо по команде из Интернет), и отправ-  
лять все собранные данные своим разработчикам. Не так давно  
разразился скандал, когда выяснилось, что один известный FTP-клиент  
отправлял все вводимые имена и пароли своим разработчикам. Так что  
будьте бдительны!

***Клавиатурные шпионы***

Клавиатурные шпионы - это программы, запоминающие, какие клави-  
ши были нажаты в ваше отсутствие, то есть - что творилось на вашем  
компьютере, пока вас не было в офисе. Для этого все, что набирается  
на клавиатуре, заносится специальной программой в текстовый файл.  
Так что набранный на компьютере в бизнес-центре или интернет-кафе  
текст может без особых проблем стать достоянием владельца такого  
компьютера. Технически эта операция выполняется классом программ,  
называемых keyboard loggers. Они разработаны для разных операцион-  
ных систем, могут автоматически загружаться при включении компью-  
тера и маскируются под резидентные антивирусы или еще что-нибудь  
полезное.

Самая лучшая из опробованных программ, Hook Dump 2.5  
(http://www.geocities.com/SiliconValley/Vista/6001/hookdump.zip или  
http://www.halyava.ru/ilya/, для Win 3.1 и Win 95) может автомати-  
чески загружаться при включении компьютера, при этом никак не  
проявляя своего присутствия. Набранный на клавиатуре текст, назва-  
ния программ, в которых набирался текст, и даже скрытый пароль в  
Dial-Up Networking, который вообще не набирался - все записывает-  
ся в файл, расположенный в любой директории и под любым именем.  
Программа имеет много настроек, позволяющих определять нужную  
конфигурацию.

***Защита от ПЭМИН***

Нужно помнить, что за счет побочных электромагнитных излучений  
и наводок (ПЭМИН) можно считывать информацию с монитора компь-  
ютера (разумеется, с помощью специальных технических средств) на  
расстоянии до 200 метров, а то и больше. Также можно считывать ин-  
формацию с процессора, клавиатуры, винчестера, дисковода (когда они  
работают, естественно). Поэтому все криптосистемы становятся почти  
бессмысленными, если не принять соответствующих мер защиты. Для  
защиты от ПЭМИН рекомендуется применять генераторы белого шума  
(в диапазоне от 1 до 1000 МГц) типа ГБШ-1 или Салют. Их (а также  
другие интересные вещи) можно приобрести в фирмах, торгующих  
спецтехникой. А можно заняться творчеством и сделать их самостоя-  
тельно, используя схемы из популярной книги "Шпионские штучки"  
(в Москве ее можно приобрести, например, в СК "Олимпийский" или  
на радиорынке в Митино).

***Пейджинговая безопасность***

Пейджер стал для многих незаменимым средством оперативного обще-  
ния. Но мало кто знает, что технология пейджинга позволяет организо-  
вать прослушивание (мониторинг) пейджинговых сообщений с помощь  
несложной аппаратуры (сканер+компьютер+соответствующее про-  
граммное обеспечение). Поэтому пейджинговые компании контролиру-  
ются не только ФСБ, ФАПСИ и прочими силовыми подразделениями,  
но и всеми, кому не лень, в том числе криминальными структурами  
и новоявленными Джеймс Бондами в лице отечественных фирм, зани-  
мающихся так называемой защитой информации.

***Электронная почта  
Получение E-mail***

Иногда у пользователя возникает ситуация, когда хотелось бы выявить  
реального автора полученного сообщения. Например, получено сообще-  
ние от вашей жены, в котором она пишет, что уходит к другому. Вы  
можете либо вздохнуть с облегчением, выпить на радостях рюмку-дру-  
гую и отправиться с друзьями на дачу праздновать это событие, либо  
попытаться выяснить, не является ли это чьей-то шуткой.

Ваши друзья могли легко изменить поле From в отправленном сообще-  
нии, поставив туда вместо своего обратного адреса хорошо известный  
вам адрес вашей жены, например masha@flash.net. Как это делается,  
можно прочесть в разделе "Отправление e-mail". Так что стоящая перед  
нами задача сводится к следующему: определить, соответствует ли ука-  
занный адрес отправителя адресу, с которого в действительности было  
отправлено сообщение.

Итак, каждое электронное сообщение содержит заголовок (header), ко-  
торый содержит служебную информацию о дате отправления сообще-  
ния, названии почтовой программы, IP-адресе машины, с которой было  
отправлено сообщение, и так далее. Большинство почтовых программ  
по умолчанию не отражают эту информацию, но ее всегда можно уви-  
деть, открыв с помощью любого текстового редактора файл, содержа-  
щий входящую почту, или используя функцию почтовой программы,  
позволяющую просматривать служебные заголовки (как правило, она  
называется Show all headers). Что же видим?

Received: by geocities.com (8.8.5/8.8.5) with ESMTP id JAA16952

for ; Tue, 18 Nov 1997 09:37:40 -0800 (PST)  
Received: from masha.flash.net (really [209.30.69.99])

by endeavor.flash.net (8.8.7/8.8.5) with SMTP-id LAA20454

for ; Tue, 18 Nov 1997 11:37:38 -0600 (CST)  
Message-ID: <3471 D27E.69A9@flash.net>  
Date: Tue, 18 Nov 1997 11:38:07 -0600  
From: masha@flash.net  
X-Mailer: Mozilla 3.02 (Win95; U)  
MIME-Version: 1.0  
To: petya@geocities.com  
Subject: I don't love you any more, you \*&$%# !!!!

Да, много всякого. Не вдаваясь в технические подробности, в общих  
чертах: заголовки Received сообщают путь, который прошло сообщение  
в процессе пересылки по сети. Имена машин (geocities.com,  
endeavor.flash.net) указывают на то, что сообщение, скорее всего, при-  
шло к вам в geocities.com из домена вашей жены flash.net. Если имена  
машин не имеют ничего общего с flash.net (например, mailrelay.tiac.net),  
это повод задуматься о подлинности сообщения. Но самая главная стро-  
ка для нас - последняя из строк, начинающихся со слова Received:

Received: from masha.flash.net (really [209.30.69.99])

Она отражает имя машины (masha.flash.net) и уникальный IP-адрес,  
с которого было отправлено сообщение. Указанный домен (flash.net) со-  
ответствует адресу вашей жены. Впрочем, ваши друзья могли подделать  
и строку masha.flash.net (в Windows 95 это делается через Control  
Panel=>Network=>TCP/IP Properties=>DNS Configuration, указав  
masha и flash.net в полях Host и Domain соответственно), поэтому важ-  
но определить имя, соответствующее данному IP-адресу: 209.30.69.99.

Для определения имени, соответствующего цифровому адресу, можно  
воспользоваться одной из доступных программ, например WS-Ping32  
(http://www.glasnet.ru/glasweb/rus/wsping32.zip), а лучше CyberKit  
(http://www.chip.de/Software/cyber.zip). Набрав цифровой адрес, даем  
команду NS LookUp (Name Server Lookup) и смотрим на полученный  
результат. Когда имя определено, дальше все просто: если получено что-  
либо похожее на рррЗОЗ-flash.net или p28-dialup.flash.net, то сообщение  
отправлено вашей женой (или кем-то, имеющим почтовый адрес во  
Flashnet, но выяснить это подробнее уже нельзя). Если указано нечто  
весьма далекое от flash.net - скорее всего, отправляла сообщение не  
ваша жена. Иногда адрес не определяется. В этом случае можно вос-  
пользоваться функцией TraceRoute той же программы. Эта функция  
поможет проследить путь от вашей машины до указанного IP-адреса.  
Если этот адрес (он будет последним в списке узлов, через которые сиг-  
нал прошел от вашего компьютера до компьютера с указанным IP-адре-  
сом) снова не определяется, то последний из определенных по имени  
узлов все-таки укажет на примерное географическое положение компь-  
ютера отправителя. Еще более простым и изящным способом определе-  
ния страны и даже названия провайдера или сети является использова-  
ния вот этого адреса:

http://www.tamos.com/bin/dns.cgi

Итак, в результате получилось что-то вроде Brasilian Global Network.  
Ваша жена не бывала последнее время в Бразилии? Нет? Ну, тогда она  
от вас и не уходила. Вас разыграли. Будьте бдительны!

***Отправление E-mail***

Даже вполне добропорядочные граждане иногда хотят сохранить в тай-  
не свою личность при высказывании своего мнения, скажем, автору сай-  
та, пропагандирующего фашизм, или президенту Лукашенко. Вопросы  
приобретения второго (анонимного) электронного адреса вынесены  
в отдельный подраздел "Второй адрес".

Remailer (Ремейлер) - это компьютер, получающий сообщение и от-  
правляющий его по адресу, указанному отправителем. В процессе пере-  
адресации все заголовки (headers), содержащие информацию об отпра-  
вителе, уничтожаются, так что конечный получатель лишен всякой  
возможности выяснить, кто является автором сообщения. Таких про-  
грамм в сети много, некоторые из них позволяют указывать фиктивный  
адрес отправителя, большинство же прямо указывают в заголовке, что  
сообщение анонимно. Чтобы узнать, как пользоваться ремейлером, нуж-  
но отправить сообщение по адресу remailer@replay.com, указав в поле  
Subject remailer-help. Через некоторое время придет ответ с подробны-  
ми инструкциями об отправке анонимных сообщений. Еще более про-  
стой способ - это отправиться по адресу

http ://www. replay, com/remai ler/

Там расположен ремейлер, позволяющий посылать сообщения прямо из  
WWW. На этом же сайте также можно воспользоваться цепочкой из  
ремейлеров, так что отправленное сообщение пройдет через несколько  
компьютеров, каждый из которых старательно уничтожит все заголовки  
предыдущего. Но делать это, скорее всего, нецелесообразно. Во-первых,  
одного ремейлера вполне достаточно (если, конечно, отправитель не  
секретный агент), во-вторых, сообщение может затеряться и не дойти до  
получателя, в-третьих, оно может идти очень долго. Вот пример полу-  
ченного сообщения:

Date: Mon, 31 Mar 1997 12:33:23 +0200 (MET DST)  
Subject: The rest is silence:

To: petya@glasnet.ru

From: nobody@REPLAY.COM (Anonymous)

Organization: Replay and Company Unlimited

X-URL: http://www.replay.com/remailer/

X-001: Replay may or may not approve of the content of this posting

X-002: Report misuse of this automated service to abuse@replay.com

Теоретически определить реального отправителя сообщения с использо-  
ванием ремейлера можно, но практически это сделать очень сложно.  
На это способны лишь люди из ФСБ, ФАПСИ, ЦРУ и им подобных  
организаций. Но и они должны будут предварительно запастись реше-  
нием суда, чтобы ремейлер открыл им требуемую информацию. А если  
использовалась цепочка ремейлеров, то придется обойти всю цепочку.  
Но если отправитель к тому же пользовался анонимным proxy-сервером  
и (или) анонимайзером, то шанс найти его становиться еще меньше  
(не забудьте отключить использование файлов Cookies).

Итак, первое апреля. Вы умираете от желания сообщить своему другу  
от имени его провайдера о том, что его счет закрыт за неуплату (сооб-  
щение должно быть с обратным адресом его провайдера). Описанные  
ниже способы хороши для розыгрышей, но мало пригодны, если дей-  
ствительно нужно остаться анонимным. Варианты таковы:

Использование обычной почтовой программы. Самый простой вариант:

поставить в своей почтовой программе в поле Return Address любой  
адрес, и если получатель письма не станет изучать его заголовок, он  
останется в уверенности, что получил сообщение именно от того, чей  
адрес указан в поле From. Очень просто и очень ненадежно.

Использование специальной программы - анонимизатора. Таких про-  
грамм несколько, примером может служить AnonyMail  
(ftp://ftp.tordata.se/www/hokum/amaill0.zip). Заполняются поля From,  
То, Subject (тут все ясно), и поле Host, в котором указывается имя  
хоста, через который будет отправлена почта. Поскольку протокол от-  
правки сообщений SMTP не требует в подавляющем большинстве слу-  
чаев какой-либо авторизации отправителя, смело можно указать прак-  
тически любое имя, желательно такое же, как у предполагаемого  
получателя этого сообщения. Для не очень опытного пользователя оп-  
ределение подлинности сообщения будет значительно затруднено. На-  
пример, если отправляется письмо по адресу kiska@frontier.net, в поле  
Host нужно указать адрес frontier.net. Для проверки можно отправить  
сообщение самому себе. Недостатки: IP-адрес вашей машины все-таки  
будет отражен в заголовке. Кроме того, поле То в полученном сообще-  
нии превратится, скорее всего, в Apparently-To. Правда, мало кто об-  
ратит на это внимание. Эти способы вполне корректно работают

и с русскими кодировками. Поскольку de facto стандартом для пере-  
сылки сообщений между разными компьютерами является KOI8-R,  
при рассылке сообщений рекомендуется использовать именно эту ко-  
дировку - отправленное сообщение, скорее всего, будет правильно пе-  
рекодировано почтовым компьютером получателя.

***Второй адрес***

Проблема защиты частной жизни в сети ставит перед пользователями  
вопрос об обладании вторым (третьим... десятым) электронным адресом.  
Его хорошо иметь там, где почту не будут читать, и в том домене, гео-  
графическая принадлежность которого "нейтральна". В общем, все те  
же требования, что и ко второму паспорту и гражданству. Наличие та-  
кого адреса защищает от попыток выяснить личность пользователя, дает  
возможность предоставлять разные адреса разным корреспондентам  
в зависимости от их статуса, избавляет от необходимости извещать всех  
корреспондентов о новом адресе, если пользователь сменил провайдера  
или переехал в другую страну. Существует довольно много служб, по-  
зволяющих бесплатно получить второй электронный адрес. По способу  
отправки и получения почты эти службы можно разделить на три ос-  
новных типа.

**Тип 1.** Пример: http://www.europe.com. Службы этого типа дают  
пользователю возможность перенаправлять полученную на новый адрес  
корреспонденцию по указанному пользователем адресу. Таким образом,  
в наличии уже должен быть какой-либо адрес почты, поскольку исполь-  
зуя протокол РОРЗ почту забрать нельзя. Отправление почты осуществ-  
ляется напрямую через хост этой службы (протокол SMTP). Существу-  
ет, правда, 60-дневный период, в течение которого можно пользоваться  
и обычным почтовым ящиком (РОРЗ), после истечения периода -  
за деньги. Пользователь самостоятельно выбирает userid, а также домен  
из нескольких (бесплатно) или многих (платно) предложенных имен,  
например: iname.com, writeine.com, girls.com, boys.com. Выполнив не-  
сложные инструкции, можно стать обладателем нового адреса, скажем  
ohhhhhhh@girls.coin. В процессе заполнения анкеты нужно указать свою  
страну (например, Албания), имя (тут вариантов мало, все пишут Иван  
Петров или Петр Иванов) и адрес, на который должна пересылаться  
вся приходящая корреспонденция. Этот адрес впоследствии можно лег-  
ко изменить. Вот и все! Недостаток: настоящий адрес пользователя из-  
вестен сотрудникам службы.

**Тип 2.** Службы этого типа дают пользователю возможность как отправ-  
лять почту напрямую, так и получать ее (РОРЗ и SMTP), так что пер-  
вичный адрес либо совсем не нужен, либо потребуется всего лишь раз,  
при открытии счета. Для этих целей можно использовать адрес прияте-  
ля или адрес в Hotmail (см. ниже). Пример: http://www.geocities.com  
или http://www.netaddress.com (возможности последней даже шире, она  
позволяет помимо РОРЗ и SMTP читать и отправлять почту из окна  
браузера, поэтому службу можно отнести и к типу 3). Технология от-  
крытия счета примерно такая же. Преимущество: настоящий первичный  
адрес неизвестен, единственный "след", который остается, это IP-адрес,  
с которого происходит чтение и отправление почты. Службы также  
дают возможность перенаправлять почту на первичный адрес, если есть  
такое желание. Кроме того, практически почту пользователя смогут  
прочесть только администраторы службы, а не московский провайдер  
или ФАПСИ с ФСБ, хотя теоретически и это возможно.

**Тип 3.** Принципиально другой тип службы. Чтение и отправление почты  
происходят без использования почтовой программы, прямо в окне брау-  
зера. Пример: http://www.hotmail.com. Переадресация на первичный ад-  
рес невозможна. Преимущества: можно читать почту с любого компьюте-  
ра с доступом в WWW, будь то другая страна или Интернет-кафе  
в Южном Бутово, плюс опять же сложности отслеживания почты. Недо-  
статок: не очень удобно пересылать файлы - в каждом письме' можно  
отправить только один файл и только с использованием Netscape  
Navigator 2.0 и выше или Internet Explorer 4.0 и выше. Совсем не слож-  
но, зато как удобно! Стоит также отметить сайт http://www.mailcity.com,  
который позволяет создавать неограниченное количество копий и слепых  
копий адресов. Эта программа на основе Web - воплощенная мечта для  
тех, кто занимается массовой рассылкой писем. И в заключении еще одно  
важное соображение касательно privacy. При отправлении почты через  
любую из этих служб, заголовок сообщения содержит IP адрес, с которо-  
го отправлено сообщение. Даже Hotmail это делает. Но, если при отправ-  
ке сообщения с использованием почтовых служб первых двух типов  
скрыть свой реальный IP адрес нельзя (это связано с самим принципом  
работы протокола SMTP), то при использовании почтовой службы тре-  
тьего типа, то есть при отправлении почты из окна браузера, лазейка все  
же есть. Это говорит о том, что почтовый адрес третьего типа можно сде-  
лать практически полностью анонимным, достаточно лишь воспользо-  
ваться одним из способов анонимизации своих путешествий по сети. Как  
это сделать написано в разделе "На FTP-сервер под чужим IP-адресом".

***Идентификация пользователя по E-mail***

Да, действительно, а зачем устанавливать личность по известному адре-  
су электронной почты?

А зачем устанавливают автоматический определитель номера (АОН)?  
А зачем существует база данных, в которой по телефону можно опреде-  
лить имя и адрес человека? Причин много, начиная от чистого развле-  
чения (кто не хочет поиграть в Пинкертона?), и заканчивая желанием  
выяснить, кто это с адресом someone@oxford.edu поздравляет вас каж-  
дый год с днем рождения и признается в любви. Кроме того, поняв ме-  
тодики поиска информации, становится ясно, насколько уязвима ано-  
нимность такого отправителя в сети. Заметим сразу, что способы  
выяснения личности по известному адресу e-mail весьма разнообразны,  
причем ни один из них не гарантирует успеха. Обратная задача решает-  
ся довольно тривиально: множество E-mail directories (Fourll,  
WhoWhere) позволяют найти по имени человека его адрес (если, конеч-  
но, он сам того захотел). Рассмотрим задачу нетривиальную.

***Pinger***

Воспользовавшись программой CyberKit (http://www.cHp.de/Software/cyberap)  
или, например, WSPing32 (http://www.glasnet.ru/glasweb/rus/wsping32.zip)  
пользователь получает возможность ткнуть пальцем в любой'адрес  
электронной почты и спросить: "А это кто?". Иногда можно даже полу-  
чить ответ. Итак, задаем адрес someone@oxfbrd.edu, получаем:

Login name:someone In real life: John McCartney  
Directory:/usr/someone Shell: /usr/bin/csch  
Last login Fri Aug18, 1995 on ttyv3 from dialup.oxford.edu  
No mail  
No plan

OK, someone@oxfrord.edu принадлежит John McCartney. Дело сделано,  
хотя очень часто никакого результата не будет, либо появится строка  
типа "Forwarding service denied" или "Seems like you won't get what you  
are looking for".

To же самое можно сделать, не забивая компьютер подобными программами  
(хотя они очень полезны и пригодятся не раз), а посетив Web-интерфейс, по-  
зволяющий получить тот же самый результат (http://web.lm.com/sfw.html).  
Следует заметить, что выполнение Pinger с использованием имени хоста

(в данном случае oxford.edu) может не принести никакого результата,  
в то время как использование видоизмененного (альтернативного) имени  
хоста результат даст. Как узнать альтернативное имя хоста? При помощи  
CyberKit, функция NS LookUp. Нужно ввести имя www.oxford.edu  
и посмотреть на полученный результат. Он может содержать альтерна-  
тивные имена хоста, называемые aliases, например panda.oxford.edu. По-  
пробуйте someone@panda.oxford.edu,- может сработать.

Иногда информация в ответ на Pinger-запрос может быть выдана толь-  
ко пользователю из того же домена, к которому принадлежит иденти-  
фицируемый адрес. Решение простое: можно найти пользователя из ис-  
комого домена в Internet Relay Chat и попросить его сделать  
Pinger-запрос. Программа-клиент для IRC содержит функцию Pinger,  
так что никакое специальное программное обеспечение человеку, к ко-  
торому вы обратились, не потребуется.

***Поиск в WWW и Usenet***

Это сделать очень просто:

Нужно набрать адрес http://www.altavista.digital.com и нажать Find!  
Есть вероятность найти домашнюю страницу искомого пользователя  
или упоминание о нем на других страницах. Там вполне может быть  
имя обладателя адреса, а если повезет, и фото.

Если человек с искомым адресом отправлял в какую-нибудь группу  
Usenet сообщение, то его можно разыскать по адресу. Для этого можно  
воспользоваться системой AltaVista (http://www.altavista.digital.com),  
позволяющей производить поиск во всех недавно отправленных  
в Usenet сообщениях. В поле поиска нужно набрать искомый адрес (пе-  
ред адресом необходимо написать from:). После нажатия кнопки Find  
откроется новое окно с результатами поиска.

Поиск в системе DejaNews (http://www.dej anews.com) проводить пред-  
почтительнее, потому что она предлагает поискать нужный адрес  
и среди старых сообщений, если среди недавних он не найден. Поиск  
также можно вести прямо с этой страницы (from: писать не нужно,  
просто адрес).

***Поиск в E-mail Directories***

В Интернет широко представлены службы, позволяющие разыскать  
электронный адрес человека по его имени. Между тем эти же службы  
иногда можно использовать для выполнения обратной задачи. На

какой-либо из указанных ниже страниц можно задать лишь домен иско-  
мого адреса, без имени.

http://www.four11 .corn

http://www. yahoo.com/search/people

http://www.bigbook.com

http://www. bigfoot.com

http://www.bigyellow.com

http://www.infospace.com

http://www.abii.com/lookupusa/adp/peopsrch.htm

http://www. looksmart.com

http ://www. switch board. corn

http://www.whowhere.com

http://www.dubna.ru/eros/ (поиск по русским ресурсам).

Если пользователей, адреса которых принадлежат к искомому домену,  
немного, то система в ответ на запрос выдаст список адресатов. Но, как  
правило, список содержит не более ста имен и адрес, стоящий перед  
знаком @, не указывается. Чтобы выяснить адрес целиком, придется  
следовать по ссылке для каждого имени. Если же людей с таким доме-  
ном больше ста, то поиск таким способом теряет смысл. Другими сло-  
вами, человека из (c)aol.com или (c)netcom.com так не найдешь.

***Защита от SPAM***

Для многих пользователей Интернет SPAM (бесконечные рекламные  
предложения и мусор, рассылаемый по почте) стал настоящим бед-  
ствием. Основные рекомендации для защиты от SPAM следующие:

- пишите письма в конференции Usenet исключительно с ненужных  
(бесплатных) адресов, потому что именно письма в конференции  
Usenet являются основной "засветкой" для спамеров. А если будет  
много SPAM, то такой адрес можно, что называется, выбросить  
и за пару минут сделать другой подобный;

- установите какую-либо программу-фильтр для e-mail. Существует ве-  
ликое множество таких программ, доступных на бесплатных серверах,  
например, на http://www.shareware.com и http://www.download.com.

***На FTP-сервер под чужим IP-адресом***

Путешествуя по Интернет, пользователи часто не задумываются о том,  
что оставляют следы своих посещений каждый раз, когда заходят на  
какой-либо FTP-сайт. Стандартные log-файлы позволяют любопытным  
владельцам сайтов узнать многое, и, прежде всего, IP-адрес, что равно-  
значно, например, тому, что определен номер телефона. Существует не-  
сколько способов защитить privacy от подобных посягательств.

Анонимно путешествовать по сети можно с помощью proxy-сервера.  
Proxy сервер работает, по сути, как Анонимайзер, то есть документ  
с сайта "забирает" он, а не компьютер пользователя. Большинство proxy  
серверов ограничивают доступ на основании IP-адреса, с которого при-  
ходит обращение. Иными словами, если провайдером пользователя яв-  
ляется Demos, то proxy сервер Glasnet его к себе попросту не пустит.  
Но, к счастью, в сети всегда можно найти "добрый" proxy, владельцы  
которого либо открыто заявляют о его доступности для всех желающих,  
либо, по той или иной причине, не ограничивают доступ только своим  
доменом, о чем широкой публике не известно, например:

svc.logan.k12.ut.us: 8001  
proxyl.emirates.net.ae: 8080  
proxy.sysnet.it: 8080  
www.archmate.com.tw: 3128  
www-proxy.global-one.ru: 3333  
sunsite.cs.msu.su: 3128  
www.anonymizer.com: 8080  
squid.nianr.net: 3128

Для настройки FTP-клиентов proxy-сервер надо установить в passive  
режим. Проделав эту нехитрую операцию, можно путешествовать по  
сети, как болгарский или американский пользователь, но... тут есть один  
очень важный момент. Далеко не все proxy серверы являются полнос-  
тью анонимными. Некоторые из них позволяют администратору сайта,  
который пользователь посещаете с использованием proxy, при желании  
определить IP-адрес, с которого происходит обращение к proxy, то есть  
реальный IP-адрес пользователя. Поэтому выбранный proxy-сервер  
нужно проверить на предмет его полной или неполной анонимности.  
Сделать это можно на сервере http://www.tamos.com/bin/proxy.cgi

Если в ответ получено сообщение "Proxy server is detected!", выбран-  
ный proxy имеет "дыру", будет предоставлена информация о реальном  
IP-адресе пользователя, как, впрочем, и об IP-адресе proxy сервера,  
с которого пришел запрос. Если же сообщение гласит "Proxy server is  
not detected" - все в порядке, анонимность обеспечена. Рекомендуется  
периодически (не реже, чем раз в месяц) проверять proxy, с которыми  
ведется работа, на предмет анонимности. В заключение еще несколько  
соображений касательно использования proxy серверов. Работа через  
далеко расположенный proxy снижает .скорость передачи данных и уве-  
личивает время ожидания. Кроме того, если все читатели будут исполь-  
зовать приведенные выше адреса proxy, то очень скоро удовольствие  
кончится, и доступ к ним будет закрыт (если уже не закрыт). Найти  
подходящий proxy несложно, например, приведенные адреса найдены  
всего за пять минут. В поисковой машине (например Alta Vista) указы-  
ваются ключевые слова, что-нибудь вроде proxy+server+coniiguration+  
Netscape. В результате появится список страниц, где провайдеры расска-  
зывают своим пользователям, как настроить браузеры для работы с их  
proxy. Если пробовать все подряд, на пятый или седьмой раз удача  
улыбнется, и proxy-сервер согласится работать.