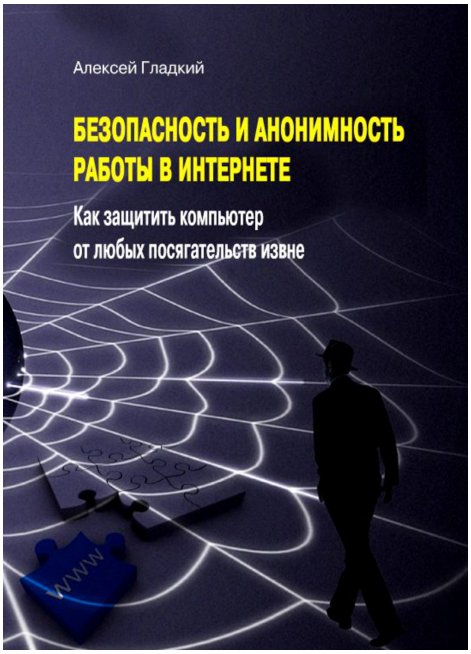
Алексей Анатольевич Гладкий

# Безопасность и анонимность работы в Интернете. Как защитить компьютер от любых посягательств извне




## Введение

Вопрос обеспечения безопасности и анонимности своего пребывания в Интернете волнует многих пользователей: ведь это позволяет заходить на любые сайты, свободно общаться и работать, получать доступ к веб-ресурсам, которые закрыты для обычного доступа (например, заблокированы системным администратором), отправлять анонимные почтовые сообщения, и т. д. В любом случае, в Сети лучше не оставлять следов своего пребывания – этим могут воспользоваться те же злоумышленники.

Кстати, в последние годы мошенничество в Интернете цветет махровым цветом, а количество обманутых и пострадавших от него людей растет не по дням, а по часам. Хищение денег, кража конфиденциальной информации, вымогательство, откровенный обман и элементарное «кидалово» – несть числа приемам и способам, которыми оперируют современные Остапы Бендеры для «сравнительно честного отъема денег у населения».

Причем далеко не всегда они действуют нагло и стремительно (хотя такого тоже хватает). Современный интернет-злоумышленник умеет расположить к себе потенциальную жертву, и вызвать полное доверие к себе. Когда же наступает «прозрение» и жертва осознает, что ее обманули – предпринимать что-либо очень сложно, а зачастую – почти нереально.

Лучший способ обезопасить себя от интернет-мошенников состоит в том, чтобы не попадаться на их уловки. И в этой книге, помимо прочего, мы расскажем о некоторых распространенных способах, которыми пользуются злоумышленники с целью обмана

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

излишне доверчивых граждан.

## Глава 1. Общие сведения о работе в Интернете

Интернет давно и прочно проник в нашу жизнь, и без него уже невозможно представить существование человечества. Им активно пользуются представители самых разных слоев нашего общества – независимо от возраста, рода занятий, профессиональной принадлежности, социального положения и иных факторов. Более того – многие приобретают себе компьютер исключительно для того, чтобы иметь постоянный доступ к Интернету.

Однако вначале необходимо усвоить несколько рекомендаций и правил, которые неукоснительно должен соблюдать каждый пользователь Всемирной Паутины. Об этом и пойдет речь в первом разделе данной главы.

### Рекомендации по Интернет-безопасности

Каждый пользователь Интернета должен четко осознавать, что Интернет может не только принести пользу, но и причинить немалый вред. Чтобы избежать неприятностей, строго соблюдайте перечисленные ниже рекомендации и правила.

♦ Для безопасной работы в Интернете обязательно наличие хорошей антивирусной программы. При этом необходимо, чтобы установленный антивирус мог работать в режиме мониторинга – это позволит выявлять опасность сразу при ее возникновении.

♦ Стоит соблюдать предельную осторожность при посещении неизвестных ресурсов в Интернете. В настоящее время получили распространение вирусы и вредоносные программы, для заражения которыми достаточно просто посетить определенную веб-страницу.

♦ Если вы подключены к Интернету через телефонную линию, динамик модема должен быть включен. Это позволит своевременно выявить попытки сетевых злоумышленников подключить данный компьютер к тому или иному ресурсу путем набора заданного телефонного номера (часто это практикуют распространители порнографических сайтов и услуг аналогичного характера). Если в процессе работы слышно, что модем начал произвольно набирать какой-то номер без участия пользователя, необходимо немедленно отключиться от Сети путем отсоединения сетевого кабеля. После этого нужно проверить компьютер специальной программой категории Antispyware – скорее всего, в компьютер внедрен шпионский модуль автоматического дозвона.

♦ После скачивания из Интернета файлов, архивов и т. п. необходимо сразу же проверить их антивирусной программой, и лишь после этого запускать на выполнение, распаковывать и т. д. Многие вирусы и вредоносные программы могут представлять собой исполняемый файл либо архив.

♦ Почтовые письма, полученные от неизвестных и сомнительных отправителей, перед открытием нужно обязательно проверить хорошей антивирусной программой (с обновленными антивирусными базами). Если этого не делать, то можно в короткие сроки превратить свой компьютер в рассадник вирусов.

♦ Никогда не отвечайте на письма, в которых содержится просьба прислать конфиденциальные данные (логин, пароль и т. п.) по указанному адресу. С помощью такого нехитрого приема злоумышленники завладевают чужими логинами и паролями.

♦ Также настоятельно не рекомендуется отвечать на письма, которые являются спамом – в противном случае спамер будет знать, что ваш почтовый ящик функционирует (а это важная информация для любого спамера). В результате количество получаемого спама будет многократно увеличиваться.

♦ Если при посещении различных ресурсов в Интернете (форумы, порталы, сайты и т. д.) требуется оставить о себе некоторые данные, то такая информация должна быть минимальна (например, совершенно необязательно сообщать свои паспортные данные, домашний адрес, различные пароли и т. п.). Несмотря на то, что на многих Интернет-ресурсах гарантируется полная конфиденциальность, не стоит быть наивным – если кому-то надо получить эту информацию, он ее получит. Причем варианты утечки информации могут быть самыми разными. Кто же может получить конфиденциальную информацию?

• Хакер. Он просто взломает систему защиты сайта либо портала (или сотворит нечто подобное).

• Шантажист. Если кто-то заводит в Интернете различные фривольные знакомства, указывая при этом в качестве средства связи номер телефона либо адрес основного почтового ящика, то по этим данным легко собрать на человека компромат. Это достигается за счет широких возможностей современных мощных поисковых систем.

• Лицо (или группа лиц), собирающее информацию индивидуального характера о людях (например, те же паспортные данные). В этом случае будет заинтересован (чаще всего – подкуплен) сотрудник портала, имеющий доступ к этим данным. В результате через некоторое время беспечный пользователь узнает (как правило, от правоохранительных органов), что, например, на его паспортные данные открыта оффшорная (ищи еще какая-нибудь) фирма, через которую каждый день «отмывается» десяток-другой миллионов долларов. Нетрудно догадаться, что ответственность за все это ляжет именно на пользователя, который легкомысленно доверил свои личные данные администрации Интернет-ресурса.

• Представитель известных силовых структур. Он просто свяжется с администрацией сайта (портала) и вежливо попросит предоставить ему всю информацию о зарегистрировавшихся на сайте пользователях (и, разумеется, получит ее в кратчайшие сроки).

♦ По окончании работы в Интернете всегда отключайте сетевой кабель от телефонной линии или от локальной сети.

А вообще одним из главных правил работы в Интернете является постоянная бдительность. Помните: то, что вы видите на экране монитора – это лишь верхушка айсберга, и от ваших глаз скрыто огромное количество происходящих процессов, многие из которых имеют откровенно деструктивную направленность.

### Как отредактировать параметры подключения к Интернету

Иногда в процессе работы возникает необходимость изменить те или иные параметры созданного ранее подключения к Интернету. Характерные примеры – изменение телефонного номера, через который осуществляется подключение, учетных данных, и т. п.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Чтобы перейти в режим просмотра и редактирования свойств подключения, необходимо в окне подключения нажать кнопку Свойства. Можно также в списке подключений щелкнуть на значке подключения правой кнопкой мыши и в открывшемся контекстном меню выбрать команду Свойства. При выполнении любого из этих действий отобразится окно, которое показано на рис. 1.1.

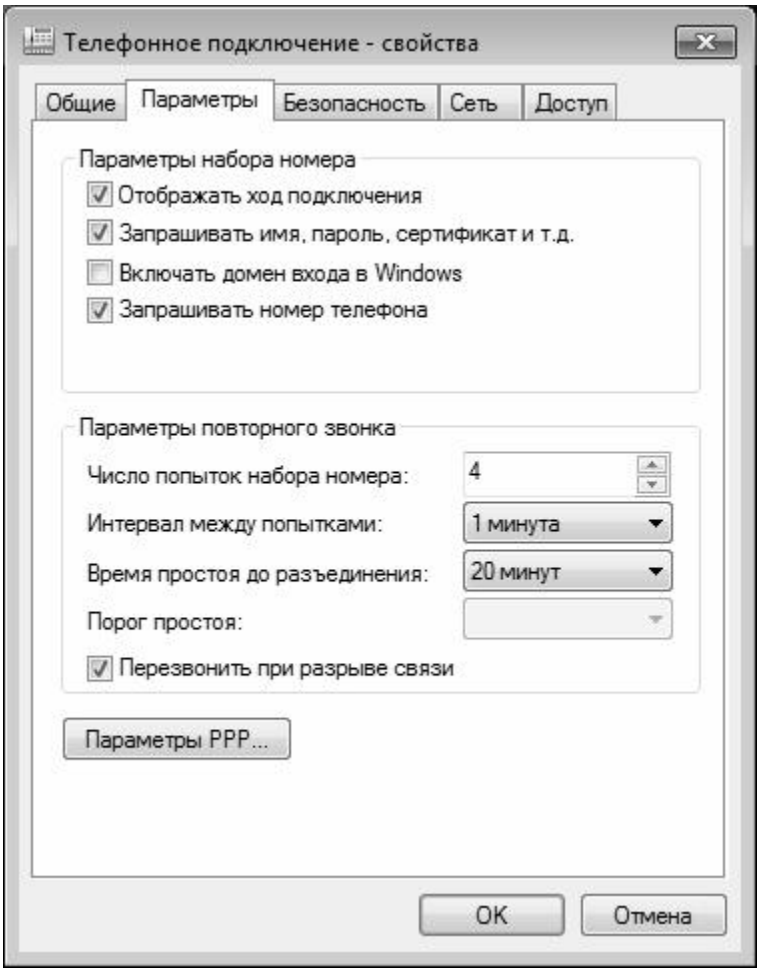



Рис. 1.1. Просмотр и редактирование свойств подключения к Интернету

Как видно на рисунке, это окно содержит несколько вкладок. Каждая из этих вкладок содержит однотипные, сходные по назначению и функциональности параметры настройки. Рассмотрим некоторые наиболее востребованные у большинства пользователей параметры.

На вкладке Общие отображается название устройства, с помощью которого осуществляется подключение к Интернету (модема) и общие параметры подключения. Кнопка Настроить (она доступна для подключений через телефонную линию) позволяет открыть режим настройки параметров работы модема. При этом на экран выводится окно Конфигурация модема, в котором определяется максимальная скорость работы модема, а также с помощью соответствующих флажков включается/выключается аппаратное управление потоком, обработка ошибок и сжатие данных модемом. Слева внизу данного окна находится флажок Включить динамик модема, который обязательно нужно установить.

Параметры набора номера телефона (они также отображаются только для телефонных подключений) включают в себя поле Номер телефона (именно по этому номеру

производится выход в Интернет), а также поля Код города и Код страны или региона, которые доступны только при установленном флажке Использовать правила набора номера. С помощью кнопки Другие можно перейти в режим настройки дополнительных телефонных номеров, которые могут использоваться в данном подключении. При этом на экране отображается окно Дополнительные номера телефонов, изображенное на рис. 1.2.

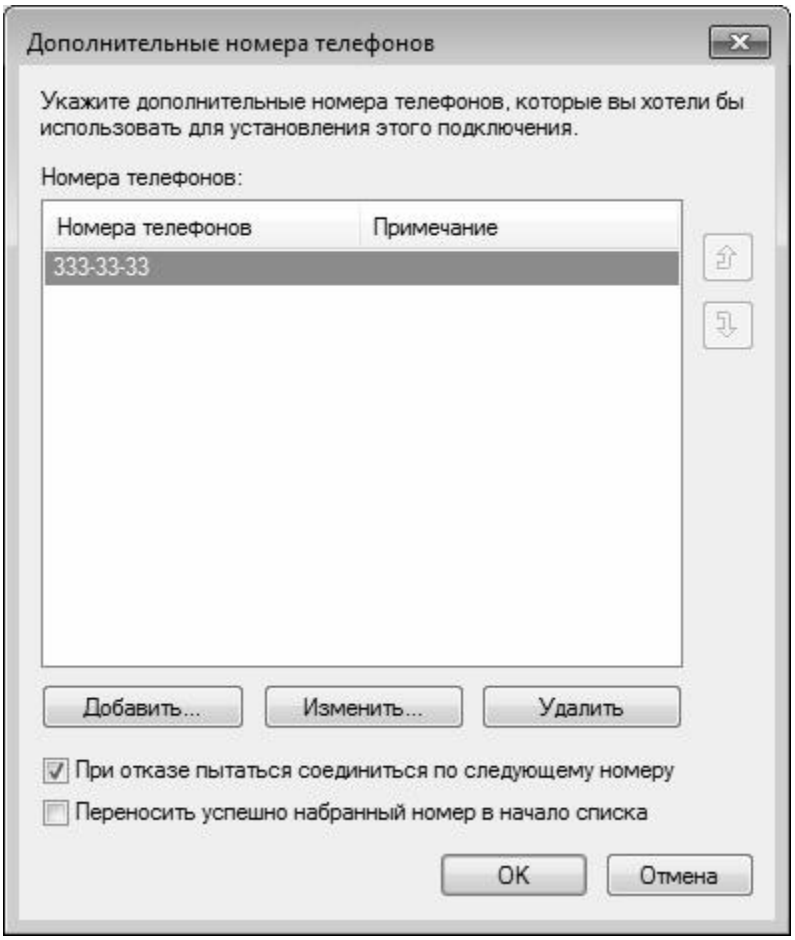



Рис. 1.2. Настройка дополнительных телефонных номеров

В данном окне с помощью кнопок Добавить, Изменить и Удалить осуществляется соответственно добавление новых номеров, редактирование и удаление из списка текущего номера. В режиме добавления либо изменения телефонных номеров можно ввести с клавиатуры произвольный комментарий.

С помощью установки соответствующих флажков можно включить режим соединения по следующему номеру в случае сбоя при первоначальном соединении, а также режим переноса успешно набранного номера в начало списка (использование данных режимов имеет смысл только в том случае, когда список содержит более чем один телефонный номер).

На вкладке Параметры (см. рис. 1.1) производится настройка параметров набора номера и повторного звонка. В выделенной области Параметры набора номера содержатся следующие флажки:

♦ Отображать ход подключения – при установленном данном флажке процесс подключения сопровождается появлением на экране информационных окон, в которых последовательно отображаются этапы подключения (набор номера, регистрация

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

компьютера в сети и др.);

♦ Запрашивать имя, пароль, сертификат и т. д. – если данный флажок установлен, то перед соединением система запросит подтверждение имени пользователя, пароля и иных параметров защиты (при их наличии);

♦ Включать домен входа в Windows – если данный флажок установлен, то перед соединением система запросит имя домена. Установка данного флажка срабатывает только при установленном флажке Запрашивать имя, пароль, сертификат и т. д.;

♦ Запрашивать номер телефона – если данный флажок установлен, то перед соединением система запросит подтверждение номера телефона. Данный параметр отображается только для телефонных подключений.

В выделенной области Параметры повторного звонка (см. рис. 1.1) настраиваются следующие параметры:

♦ Число попыток набора номера – в данном поле указывается количество попыток автоматического подключения, когда с первого раза соединиться не удается;

♦ Интервал между попытками – в данном поле указывается промежуток времени, через который производится очередная попытка подключения. Использование данного параметра имеет смысл в том случае, когда в поле Число повторений набора номера указано любое значение, кроме 0;

♦ Время простоя до разъединения – через промежуток времени, указанный в данном поле, соединение будет разорвано при условии простоя компьютера.

Если установлен флажок Перезвонить при разрыве связи, то при непреднамеренном разрыве соединения будет производиться автоматическое подключение для восстановления соединения.

### Что делать, если отсутствует связь с Интернетом

Каждый пользователь Интернета хотя бы раз сталкивался с ситуацией, когда по каким-то причинам Интернет был недоступен или скорость передачи данных неоправданно снижалась. Далее мы рассмотрим наиболее характерные причины подобных явлений, а также проанализируем сообщения об ошибках, выдаваемых операционной системой при возникновении проблем с Интернетом.

### Причины отсутствия доступа к Сети

Одно из распространенных явлений – когда попытка соединиться с Интернетом по телефонной сети заканчивается неудачей уже на стадии набора телефонного номера модемом. Обычно это происходит в случаях, когда модем либо не подключен к телефонной линии (возможно, для решения проблемы будет достаточно просто вставить штекер телефонного провода в соответствующий разъем), либо не настроен, либо используется другим приложением. Отметим, что в первом случае модем обычно начинает набор номера, и только после этого сообщает об отсутствии связи. Если телефонный номер для выхода в Интернет начинается с «восьмерки» (по аналогии с тем, как это делается для выполнения междугородних звонков) – то сообщение об отсутствии

гудка может появиться как до, так и после набора «восьмерки» модемом.

Чтобы диагностировать неполадку, откройте Диспетчер устройств, дважды щелкните в дереве устройств на позиции модема, затем в открывшемся окне откройте вкладку Диагностика и нажмите кнопку Опросить модем. Если модем настроен правильно, через некоторое время (обычно – в пределах нескольких секунд) на экране отобразится результат опроса. Если ничего не получилось – перезагрузите компьютер и выполните данную операцию повторно.

Иногда обрыв связи случается в процессе набора телефонного номера. Как показывает практика, в большинстве случаев это происходит по вине провайдера. Попробуйте позвонить по номеру, используемому для доступа в Интернет, с обычного аппарата. Если вы не смогли дозвониться (короткие гудки или вообще нет ответа), либо дозвониться получилось, но характерный звук работающего модема не слышен – значит, сбой возникает либо по причине проблем с телефонной линией, либо модем провайдера не работает либо перегружен.

Если же вы смогли дозвониться провайдеру – значит, проблема на вашей стороне. В этом случае следует проверить настройки подключения к Интернету, в частности – правильно ли указан телефонный номер для соединения в Интернетом. Есть и еще один важный нюанс: если АТС, через которую вы выходите в Интернет, не поддерживает тональный набор телефонных номеров – нужно в настройках подключения добавить перед номером телефона латинскую букву P и попробовать соединиться вновь.

Почти все модемы имеют динамик, с помощью которого пользователь прослушивает процесс набора номера и подключения к Интернету. Некоторые пользователи умеют на слух определить набор номера и ответ модема провайдера, благодаря чему они могут с высокой степенью достоверности диагностировать неполадку.

Также на стадии набора номера связь может обрываться по причине неполадок и помех на телефонной линии, либо из-за неправильных настроек модема.

Еще одна распространенная ситуация заключается в том, что само соединение появляется, но при проверке учетных данных (логина и пароля) связь самопроизвольно обрывается.

Если ранее вы подключались к Интернету под своими учетными данными, которые сохранены в системе, и при этом их проверка занимала много времени – перезагрузите компьютер и попробуйте соединиться еще раз. Если же учетные данные вводятся при каждом подключении – проверьте, правильно ли вы их вводите. При этом проверьте регистр символов (при вводе учетных данных прописные и строчные буквы различаются), а также убедитесь в том, что режим Caps Lock отключен. Также проверьте раскладку клавиатуры (возможно, вы вводите учетные данные русскими буквами).

И еще одна распространенная причина, по которой соединение разрывается на этапе проверки учетных данных – это отсутствие денежных средств на счету пользователя.

Бывают случаи, когда подключение к Интернету происходит без проблем, но вот сервисами воспользоваться невозможно (система выдает информационное сообщение об ошибке). Такое может происходить по причине отсутствия TCP/IP-соединения. В первую очередь проверьте правильность настроек данного подключения к Интернету. Для проверки наличия соединения нужно в окне Запуск программы, которое вызывается с помощью команды Пуск ▸ Выполнить, ввести значение ping google.com. Если соединение функционирует исправно, то вы должны получить примерно следующий ответ (может

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

отличаться IP-адрес и время):

Обмен пакетами с google.com [74.125.232.18] с 32 байтами данных;

Ответ от 74.125.232.18: число байт=32 время=214мс TTL=250;

Ответ от 74.125.232.18: число байт=32 время=2214мс TTL=250;

Ответ от 74.125.232.18: число байт=32 время=2514мс TTL=250;

Ответ от 74.125.232.18: число байт=32 время=236мс TTL=250.

При отсутствии соединения вы получите следующий ответ: Неизвестный IP-адрес google.com.

Иногда соединение бывает нестабильным или не устанавливается вообще, оно часто разъединяется, а скорость работы необъяснимо мала. Обычно причина кроется в плохом качестве телефонной сети или в некорректных настройках самого модема. Часто такое можно заметить при попытке подключения через старую аналоговую телефонную станцию. Для устранения неполадки установите оптимальные настройки модема, которые лучше всего подходят для данной телефонной линии. В частности, при плохом качестве подключения на скорости 33,6 Кбит/с можно уменьшить ее, соответствующим образом откорректировав параметры настройки модема. Для этого в настройках подключения на вкладке Общие нажмите кнопку настройки модема, и в появившемся окне измените значение параметра Наибольшая скорость. При уменьшении скорости передачи данных можно добиться более стабильной работы соединения.

Если при попытке соединения на экране отображается следующее информационное сообщение: «Ошибка при соединении с сервером» или «Модем не был обнаружен», еще до того, как модем успевает набрать телефонный номер – вероятно, появились неполадки с настройкой удаленного доступа к операционной системе. В такой ситуации проблему можно решить путем переустановки данного компонента системы.

**Расшифровка кодов ошибок удаленного доступа**

Если при попытках подключения к Интернету возникают проблемы, то на экране отображается не только сообщение об ошибке, но и ее код. Этот код позволяет с высокой степенью достоверности установить истинную причину неисправности, и определить методы ее устранения. Далее мы приведем расшифровку кодов наиболее часто встречающихся при подключении к Интернету ошибок.

♦ 600 Начатая операция не закончена – сообщение свидетельствует о том, что произошла внутренняя ошибка. Для устранения проблемы обычно бывает достаточно перезагрузить систему.

♦ 602 Указанный порт уже открыт – в данном случае COM-порт, через который обычно происходит подключение, уже занят другим процессом, подключением или приложением (например, это может быть программа, которая используется для отправки факсов). В данном случае проблема решается закрытием программы, которая заняла COM-порт.

♦ 606 Указанный порт не подключен – здесь также причина кроется во внутренней ошибке, для устранения которой достаточно перезагрузить систему. В некоторых случаях перезагрузка может и не потребоваться – при попытке повторного подключения все проходит нормально.

♦ 628 Подключение было закрыто – если данное сообщение появилось при попытке подключения через телефонную сеть, то попробуйте соединиться еще пару раз. Если все

повторяется – отключите дополнительные настройки модема и уменьшите его скорость.

♦ 629 Подключение было закрыто удаленным компьютером – в данном случае причины ошибки могут быть разными: это и помехи на линии, и непоправимая ошибка в телефонной сети, и неудавшаяся попытка соединения с удаленным модемом на текущей скорости. Попробуйте дозвониться еще раз, нажав кнопку Перенабрать. Если все повторилось вновь – уменьшите скорость подключения модема до 9,6 Кбит/с, и попытайтесь соединиться вновь. Иногда прояснить ситуацию можно, попробовав подключиться к удаленному модему через другую телефонную линию.

♦ 634 Не удалось зарегистрировать компьютер в удаленной сети – этот сообщение говорит о том, что ваш компьютер не получается зарегистрировать в Сети. Как правило, это происходит при наличии проблем с протоколом NetBIOS, но иногда такую ошибку вызывают также сбои с протоколами TCP/IP или IPX. Причиной обычно является то, что данный IP-адрес уже кем-то занят в Интернете. Для устранения проблемы обращайтесь к своему Интернет-провайдеру.

♦ 636 Устройство, подключенное к порту, не соответствует ожидаемому – такое сообщение выдается в случаях, когда аппаратная часть вашего компьютера несовместима с настройками конфигурации для подключения. Обычно это происходит после экспериментов с «железом», в частности – когда было заменено какое-то сетевое оборудование (модем или последовательный порт). В данном случае рекомендуется проверить настройки и конфигурацию удаленного доступа к сети.

♦ 646 Вход в это время дня для пользователя с данной учетной записью не разрешен – это сообщение говорит о том, что пользователь имеет доступ в Интернет только в определенное время суток, и в данный момент ему доступ закрыт.

♦ 647 Учетная запись отключена – данное сообщение свидетельствует о блокировке данной учетной записи. Проблему можно решить только через провайдера – возможно, администратор закрыл пользователю доступ за неуплату или по причине совершения пользователем каких-либо нарушений (например, рассылка спама, и др.).

♦ 676 Телефонная линия занята – это сообщение дополнительных пояснений не требует. В данном случае либо повторно вручную запустите процесс набора номера, либо в настройках подключения установите режим автоматического дозвона.

♦ 678 Ответ не получен – в данном случае проблема может быть как на вашей стороне, так и на стороне провайдера. Причина в том, что модем или другое устройство не отвечает на телефонный звонок, следовательно – соединение установить не удается. Если номер телефона в настройках подключения указан верно, а телефонный кабель вставлен в то гнездо, в которое нужно – скорее всего, проблема на стороне провайдера.

♦ 680 Отсутствует гудок – это сообщение также особых пояснений не требует. Видимо, модем просто не подключен к телефонной сети.

♦ 691 Доступ запрещен, поскольку такие имя пользователя и пароль недопустимы в этом домене – такое сообщение появляется при наличии проблем с учетными данными. В первую очередь проверьте правильность их ввода, а также раскладку клавиатуры и режим Caps Lock. Не исключено, что истек срок действия ваших учетных данных (например, закончился период оплаченного доступа к Интернету, и др.).

♦ 720 Попытка подключения не удалась, поскольку подключенному и локальному компьютерам не удалось согласовать управляющие протоколы PPP – это сообщение информирует об отсутствии сетевых протоколов управления PPP, настроенных для

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

данного подключения. Такое же сообщение появится и в том случае, когда соответствующий сетевой протокол вообще не был установлен. Подобный сбой может появляться после корректировки сетевого протокола при обновлении ПО.

♦ 721 Удаленный компьютер не отвечает – такое сообщение появляется в случае, когда при попытке начать PPP-диалог ответ с удаленного сервера получен не был. В данном случае проблемы могут быть как на вашей стороне, так и на стороне провайдера.

♦ 736 Удаленный компьютер завершил работу протокола управления – такое сообщение выдается в случае, когда диалог протокола управления каналом PPP начался, но был прекращен удаленным сервером. Как правила, этот сбой возникает по причине неполадок на удаленном компьютере.

♦ 770 Удаленный компьютер отверг попытку подключения – уже из формулировки сообщения об ошибке можно понять, что при попытке подключения что-то не понравилось удаленному компьютеру. Возможно, это настройки вызывающего приложения, либо прочие аппаратные настройки локального компьютера.

♦ 771 Попытка подключиться не удалась, поскольку сеть перегружена – эта ошибка обусловлена перегрузкой телефонной сети (подобное может возникать и при попытке обычного телефонного звонка). Подождите пару минут и попробуйте подключиться к Интернету повторно.

### Как правильно настроить интернет-обозреватель

Безопасность и анонимность работы в Интернете во многом зависят от текущих настроек интернет-обозревателя. Пользователь самостоятельно может выставить требуемые параметры и, тем самым, обеспечить как требуемый уровень безопасности, так и максимально адаптировать программу к своим потребностям. Далее мы расскажем, как выполняется настройка популярных обозревателей Internet Explorer и Mozilla Firefox.

### Настройка Internet Explorer

Для перехода в режим настройки параметров Internet Explorer необходимо выполнить команду главного меню Сервис ▸ Параметры. При активизации данной команды на экране отображается окно, изображенное на рис. 1.3.

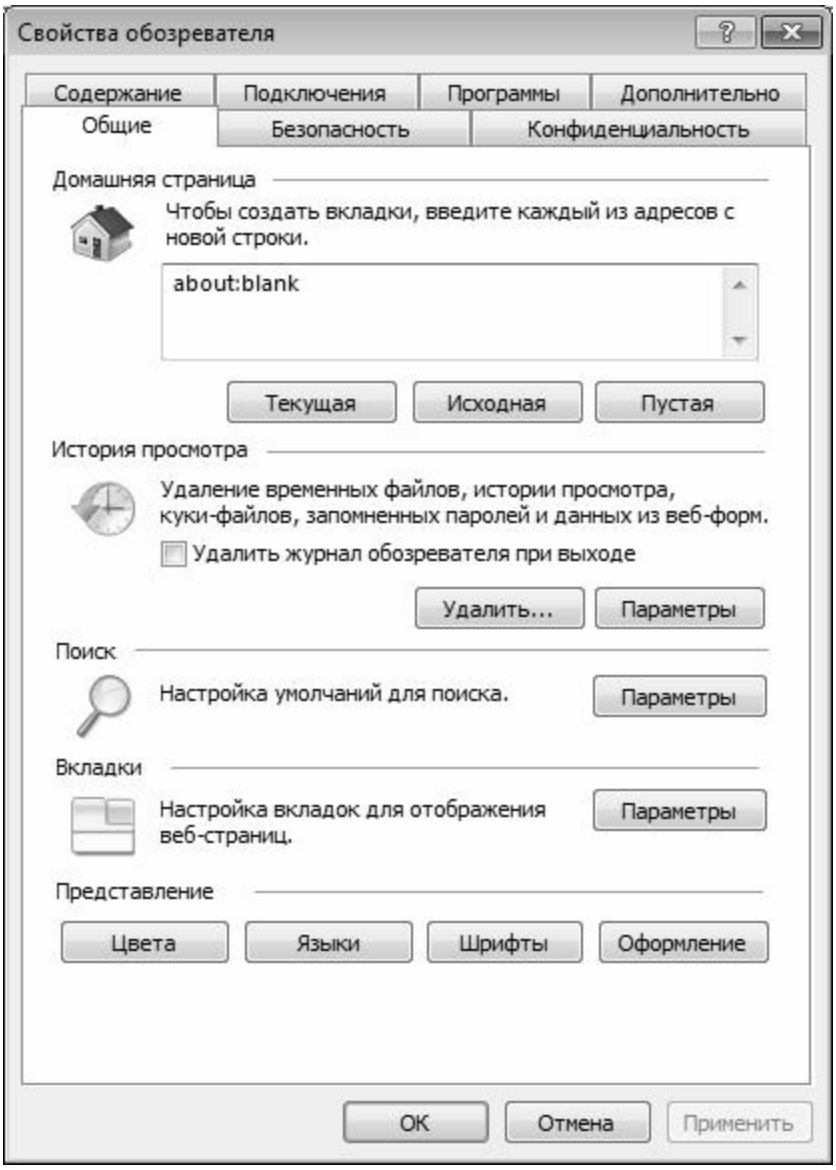



Рис. 1.3. Настройка Internet Explorer

Как видно на рисунке, данное окно состоит из нескольких вкладок. Каждая вкладка содержит параметры настройки соответствующего назначения. Далее мы рассмотрим те параметры, которые являются наиболее востребованными у большинства пользователей.

На вкладке Общие (она открыта на рис. 1.3) выполняется настройка параметров общего назначения.

В верхней части вкладки указывается адрес веб-страницы, которая выбрана пользователем в качестве домашней. Домашняя веб-страница – это страница в Интернете, которая по умолчанию открывается при каждом запуске обозревателя. К данной странице можно вернуться в любой момент, выполнив команду главного меню Вид ▸ Переход ▸ Домашняя страница. Нажатие кнопки Текущая позволяет выбрать в качестве домашней ту страницу, которая открыта в данный момент. Кнопка Исходная восстанавливает в качестве домашней ту страницу, которая была задана при установке интернет-обозревателя. Если домашняя страница не нужна, то следует нажать кнопку Пустая. В этом случае при запуске интернет-обозревателя будет открываться пустая страница.

СОВЕТ

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Вы можете выбрать сразу несколько домашних страниц – в этом случае каждая из них будет открываться в отдельной вкладке. Для этого на вкладке Общие сформируйте список страниц, разделяя их нажатием Enter (чтобы каждый новый адрес был введен с новой строки).

Для удаления временных файлов Интернета, истории посещенных веб-страниц и прочей информации предназначена кнопка Удалить. При ее нажатии отображается окно, в котором путем установки соответствующих флажков нужно отметить данные, которые должны быть удалены, и нажать кнопку Удалить.

С помощью кнопки Параметры, которая находится справа от кнопки Удалить, осуществляется переход в режим настройки и редактирования параметров папки временных файлов Интернета. При этом на экране открывается окно Параметры, которое показано на рис. 1.4.

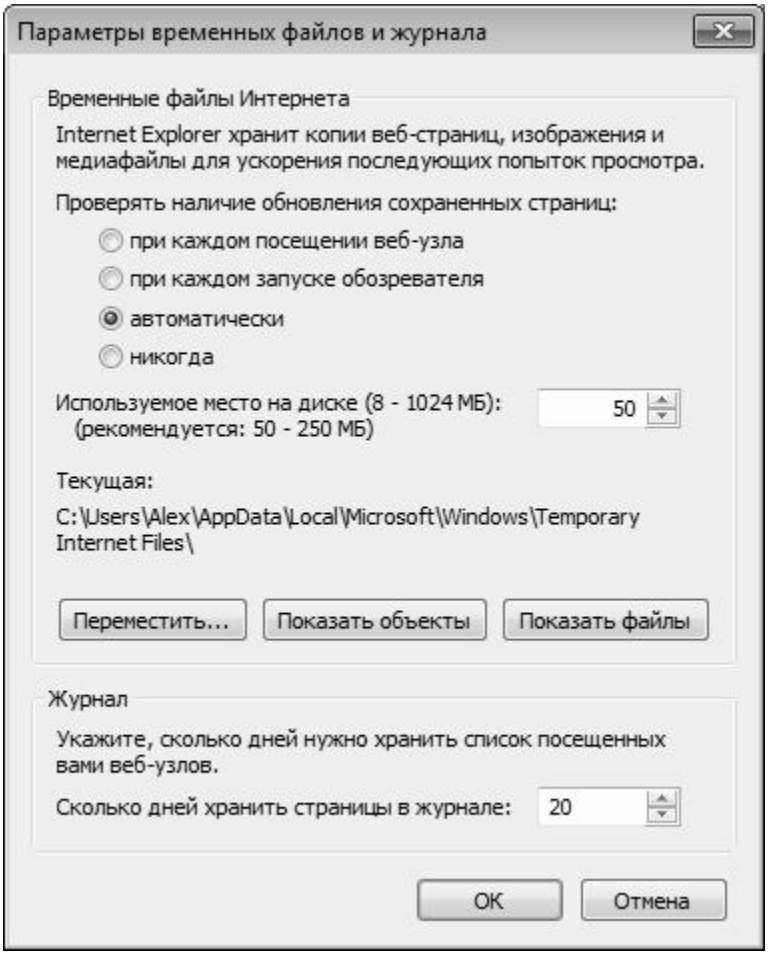



Рис. 1.4. Настройка параметров папки временных файлов Интернета

В данном окне устанавливается требуемый режим проверки обновления сохраненных страниц, отображается расположение папки, содержащей временные файлы Интернета, и указывается максимальный объем места на жестком диске, предназначенного для этой папки. С помощью кнопки Переместить можно переместить папку временных файлов Интернета в указанное место; при этом на экране открывается окно Обзор папок, в котором следует указать требуемый путь. Для немедленного открытия папки с временными файлами Интернета используйте кнопку Показать файлы.

В поле Сколько дней хранить страницы в журнале указывается количество дней, в течение которых должны храниться ссылки на недавно посещаемые страницы (по умолчанию предлагается хранить их в течение 20 дней).

С помощью кнопки Цвета (см. рис. 1.3) осуществляется переход в режим выбора цветов, предназначенных для отображения веб-страниц. При нажатии на данную кнопку на экране открывается окно, в котором выполняются необходимые действия.

Для настройки параметров шрифтов, используемых при отображении веб-страниц, на вкладке Общие следует воспользоваться кнопкой Шрифты, а для выбора языка – кнопкой Языки. С помощью кнопки Оформление осуществляется переход в режим настройки стиля отображения веб-страницы.

Если говорить непосредственно о параметрах безопасности работы в Интернете, то ряд из них вынесены на вкладку Безопасность, содержимое которой показано на рис. 1.5.

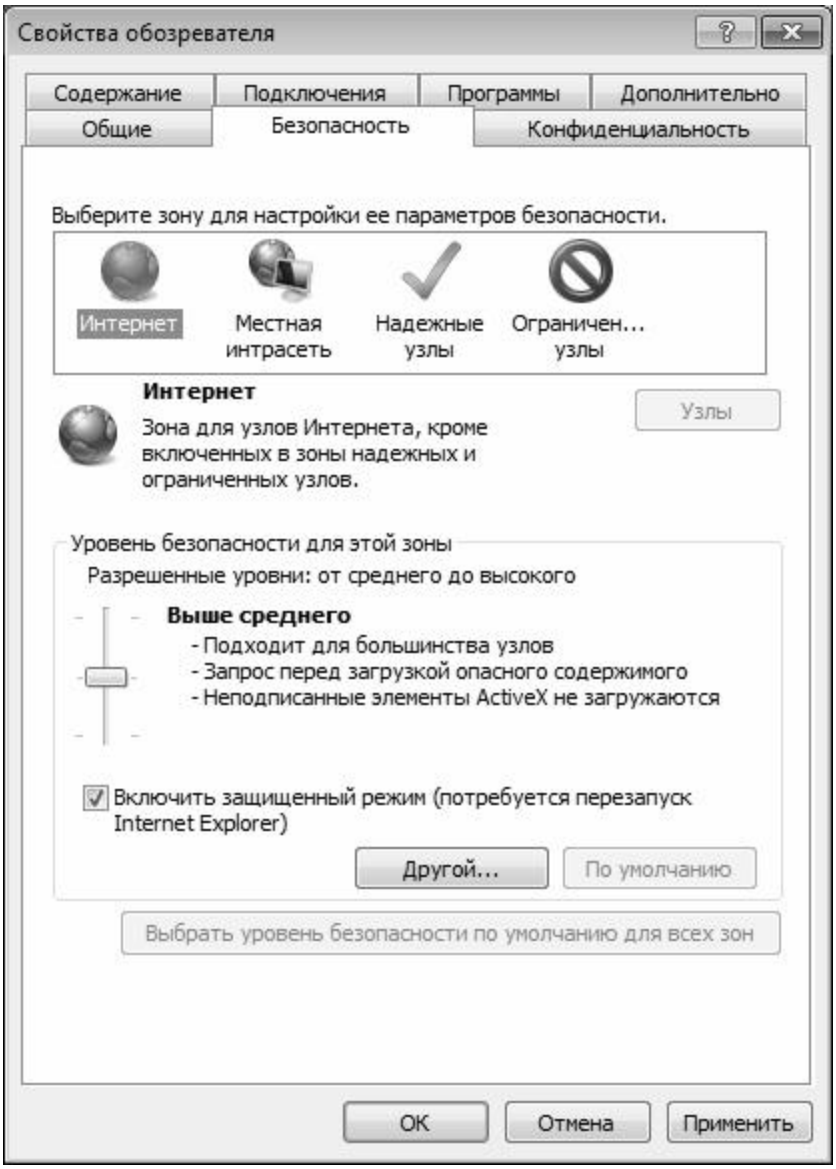



Рис. 1.5. Настройка параметров безопасности

В верхней части данной вкладки приводится перечень зон Интернета, доступных с данного локального компьютера, в нижней – для каждой зоны настраивается уровень безопасности. Для этого следует выделить значок зоны Интернета и с помощью кнопки

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Другой перейти в режим редактирования уровня безопасности для этой зоны.

При необходимости можно восстановить стандартные параметры безопасности для каждой зоны. Это осуществляется нажатием кнопки По умолчанию (предварительно следует выделить значок той зоны Интернета, для которой выполняется данная операция). Чтобы применить используемые по умолчанию параметры сразу для всех зон, нажмите кнопку Выбрать уровень безопасности по умолчанию для всех зон.

Также некоторые параметры безопасности находятся на вкладке Дополнительно, содержимое которой представлено на рис. 1.6.

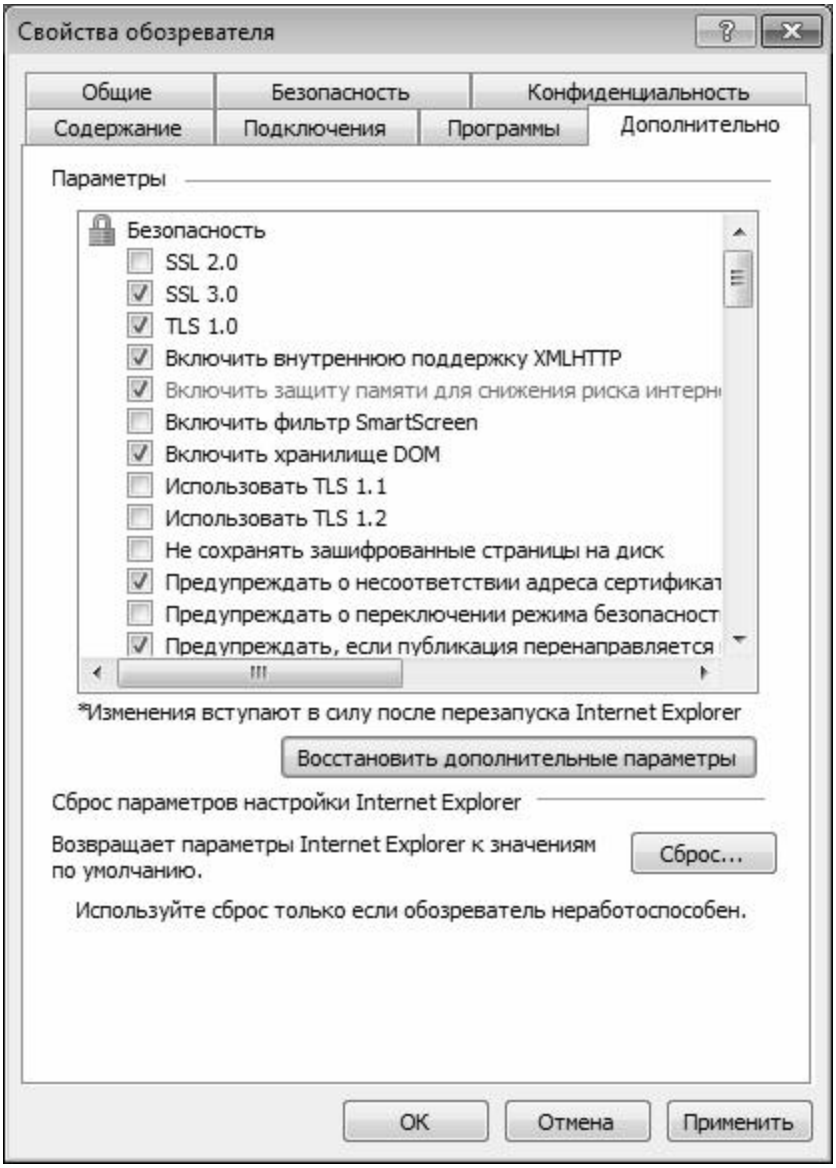



Рис. 1.6. Вкладка Дополнительно

Помимо прочего, здесь с помощью соответствующих флажков можно включать/выключать отображение рисунков и их рамок, воспроизведение анимации, звуков и видео на веб-страницах, использовать автоматическую проверку обновления Internet Explorer и т. д. В отдельный раздел вынесены параметры безопасности. При необходимости можно восстановить значения параметров, предлагаемые системой по умолчанию – для этого следует нажать кнопку Восстановить дополнительные параметры.

Все параметры данной вкладки в зависимости от функционального назначения

разделены в группы: Безопасность, Международный, Мультимедиа, Настройка HTTP 1.1, Обзор, Печать и Специальные возможности. Далее мы рассмотрим наиболее значимые параметры, с которыми приходится работать многим пользователям.

Параметры группы Безопасность предназначены для настройки дополнительных параметров безопасности.

♦ SSL 2.0, SSL 3.0 и TLS 1.0 – установка данных флажков включает режим, при котором отправка и получение конфиденциальной информации будет осуществляться с использованием протоколов соответственно SSL 2.0, SSL 3.0 и TLS 1.0. При этом необходимо учитывать следующее:

• Протокол SSL 2.0 поддерживается всеми безопасными веб-узлами.

• Протокол SSL 3.0 имеет более высокую степень защиты, чем протокол SSL 2.0, но некоторые веб-узлы его не поддерживают.

• Протокол TLS 1.0 имеет степень защиты, сравнимую с протоколом SSL 3.0, и также может поддерживаться не всеми веб-узлами.

♦ Не сохранять зашифрованные страницы на диск – при установке данного флажка включается запрет на сохранение секретных сведений в папке с временными файлами Интернета. Этот режим полезно устанавливать в том случае, когда к компьютеру и к выходу в Интернет имеют доступ несколько пользователей.

♦ Предупреждать о переключении режима безопасности – если установлен этот флажок, то при переключении между безопасными и небезопасными узлами Интернета на экране будет отображаться соответствующее предупреждение.

♦ Проверка подписи для загруженных программ – при установленном данном флажке в Internet Explorer включается режим проверки подлинности загружаемых программ.

♦ Проверят, не отозван ли сертификат сервера – при установке данного флажка Internet Explorer будет выполнять проверку действительности сертификатов узлов в Интернете. Изменение данного параметра начинает действовать только после перезапуска Internet Explorer.

♦ Удалять все файлы из папки временных файлов Интернета при закрытии обозревателя – если установлен данный флажок, то при закрытии окна Internet Explorer будет выполняться автоматическая очистка папки временных файлов Интернета (эта папка называется Temporary Internet Files).

Группа Мультимедиа включает в себя параметры, определяющие порядок отображения мультимедийного содержимого на веб-страницах. Эти параметры перечислены ниже.

♦ Включить автоматическую подгонку размеров изображения – с помощью данного флажка включается такой режим отображения веб-страниц, при котором слишком большие изображения автоматически подгоняются под размер окна интернет-обозревателя.

♦ Воспроизводить анимацию на веб-страницах – этот флажок используется для включения/выключения режима воспроизведения анимации на веб-страницах. Необходимость данного параметра (кстати, его изменение вступает в силу после перезапуска Internet Explorer) обусловлена тем, что некоторые веб-страницы, содержащие анимацию, загружаются очень медленно, поэтому ее воспроизведение иногда имеет смысл отключить.

♦ Воспроизводить звуки на веб-страницах – с помощью этого флажка вы можете включать/выключать воспроизведение звуковых файлов на веб-страницах.

♦ Показывать изображения – с целью ускорения загрузки веб-страниц можно отключить

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

режим отображения графических изображений путем снятия данного флажка.

♦ Показывать рамки рисунков – если данный флажок установлен, то во время загрузки рисунков будут отображаться их рамки. Это позволит получить представление о расположении элементов веб-страницы до ее полной загрузки. Включение данного режима имеет смысл только при установленном флажке Отображать рисунки.

♦ Улучшенная передача цветовых оттенков – при установленном данном флажке включается режим сглаживания изображений.

Группа Настройка HTTP 1.1 содержит два параметра. С помощью флажка Использовать HTTP 1.1 включается режим использования протокола HTTP 1.1 при подключении к веб-узлам, а если установлен флажок Использовать HTTP 1.1 через прокси-соединения, то при подключении к веб-узлам через прокси-сервер будет использоваться протокол HTTP 1.1.

Что касается группы Обзор, то здесь стоит обратить внимание на перечисленные ниже параметры.

♦ Включение стилей отображения для кнопок и иных элементов управления на веб-страницах – если установлен данный флажок, то при отображении веб-страниц для оформления будут применяться параметры настройки экрана Windows.

♦ Выводить подробные сообщения об ошибках http – если установлен данный флажок, то в случае возникновения ошибок при подключении к какому-либо серверу будет отображаться подробная информация об ошибке и советы по ее устранению. В противном случае показывается только код и название ошибки.

♦ Использовать пассивный FTP-протокол (для совместимости с брандмауэрами и DSL-модемами) – при установленном данном флажке используется пассивный FTP-протокол, при котором не требуется определение IP-адреса компьютера. Данный режим считается более безопасным.

♦ Использовать одно и то же окно для загрузки ссылок (если вкладки отключены) – если этот флажок снят, то при открытии веб-страниц с помощью ссылок они будут открываться не в уже открытом окне интернет-обозревателя, а в новом (если отключен режим работы с вкладками).

♦ Подчеркивать ссылки – с помощью данного переключателя выбирается подходящий режим подчеркивания ссылок. Возможные варианты:

• Всегда – ссылки подчеркиваются все время (этот режим установлен по умолчанию).

• Никогда – ссылки не подчеркиваются никогда.

• При наведении – ссылки подчеркиваются только при подведении к ним указателя мыши.

♦ Разрешение сторонних расширений обозревателя – если этот флажок снят, то использование средств сторонних разработчиков (не корпорации Microsoft), предназначенных для Internet Explorer, будет невозможно. Изменение значения данного параметра начинает действовать только после перезапуска Internet Explorer.

♦ Уведомлять по окончании загрузки – если установить этот флажок, то по окончании загрузки файлов на экране будет отображаться соответствующее сообщение.

Группа Печать включает в себя один параметр – флажок Печатать цвета и рисунки фона. Если этот параметр включен, то при печати веб-страницы будет также распечатываться фоновое изображение либо фоновые рисунки. При включении данного режима следует учитывать, что в зависимости от используемого принтера возможно ухудшение скорости и качества печати.

Последняя группа параметров на вкладке Дополнительно называется Специальные

возможности. Если в ней установлен флажок Всегда расширять текст для изображений, то при снятом флажке Показывать изображения (его описание приведено чуть выше) размер рисунка будет увеличиваться для отображения всего связанного с ним текста. Если установлен флажок Перемещать системную каретку вслед за фокусом и выделением, то системная каретка будет перемещаться в зависимости от изменения фокуса или выделения. Данный параметр важен при использовании программ, использующих системную каретку для определения нужной области экрана.

### Настройка Mozilla Firefox

Чтобы перейти к настройкам программы, используйте команду главного меню Инструменты ▸ Настройки – при ее активизации на экране откроется окно настройки параметров Mozilla Firefox, изображенное на рис. 1.7.

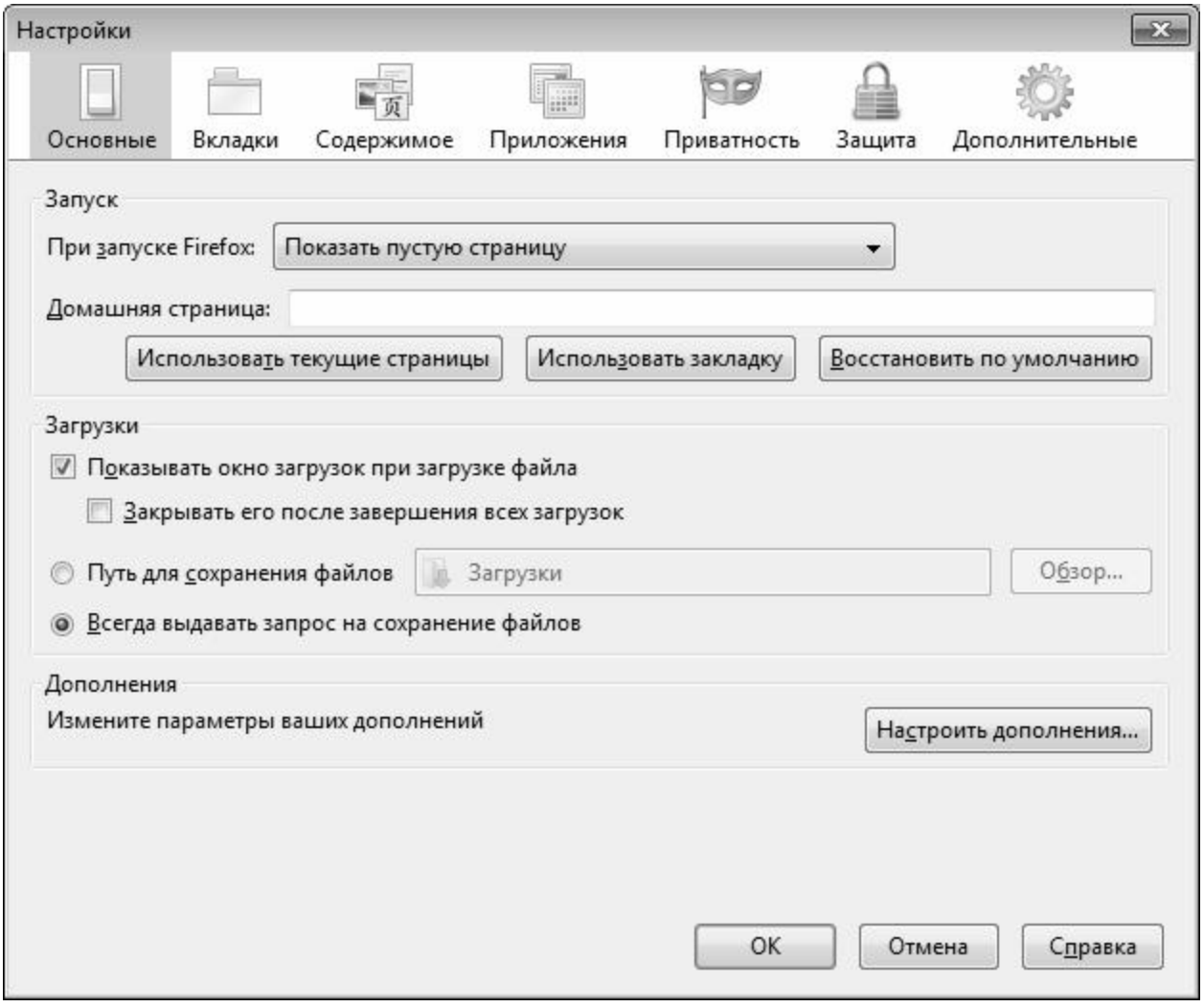



Рис. 1.7. Настройка параметров Mozilla Firefox

Окно настройки состоит из нескольких разделов: Основные, Вкладки, Содержимое, Приложения, Приватность, Защита и Дополнительные. Названия разделов отображаются вверху окна, для перехода к разделу нужно щелкнуть мышью на его значке. Параметры

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

выбранного раздела представлены в окне настроек (например, на рис. 1.7 отображаются параметры раздела Основные). Далее мы рассмотрим самые востребованные параметры настройки Mozilla Firefox.

Раздел Основные содержит параметры, к которым пользователи обращаются в первую очередь. Например, многим сразу хочется отключить автоматическую загрузку стартовой страницы, которая предложена авторами программы по умолчанию. Для решения этой задачи нужно в разделе Основные в поле При запуске Firefox из раскрывающегося списка выбрать значение Показать пустую страницу (это значение выбрано на рис. 1.7). Если же вы хотите, чтобы при запуске программы автоматически загружалась какая-то страница, выберите в данном поле значение Показать домашнюю страницу, после чего в поле Домашняя страница введите ее точный адрес. В данном поле можно выбрать и еще одно значение – Показать окна и вкладки, открытые в прошлый раз: в данном случае при запуске Mozilla Firefox будет автоматически загружаться страница (или несколько страниц, открытых на разных вкладках), которые были открыты в момент завершения последнего сеанса работы с программой.

Если в разделе Основные установлен флажок Показывать окно загрузок при загрузке файла, то при попытке скачать какой-либо файл на экране отобразится окно загрузок, в котором нужно будет либо указать параметры загрузки, либо оставить значения, предложенные по умолчанию. Чтобы по окончании всех текущих загрузок это окно закрывалось автоматически, установите флажок Закрывать его после завершения всех загрузок (он доступен только при установленном флажке Показывать окно загрузок при загрузке файла).

С помощью расположенного ниже переключателя указывается, каким образом программа должна определить место, в которое необходимо помещать загружаемые из Интернета объекты. Если переключатель установлен в положение Путь для сохранения файлов, то в расположенном справа поле нужно указать путь для сохранения, куда автоматически будут помещаться все загружаемые объекты. Чтобы ввести этот путь, нужно нажать расположенную справа кнопку Обзор, после чего в открывшемся окне указать требуемый каталог и нажать кнопку ОК. Если же выбран вариант Всегда выдавать запрос на сохранение файлов, то при каждой загрузке нужно будет вручную указывать путь для сохранения. По умолчанию переключатель установлен в положение Путь для сохранения файлов, а в расположенном справа поле указан путь Рабочий стол, но практика показывает, что большинство пользователей предпочитают пользоваться вторым вариантом, поскольку это позволяет соблюдать определенный порядок при скачивании файлов на компьютер, а не загромождать ими Рабочий стол.

В разделе Вкладки, содержимое которого показано на рис. 1.8, выполняется настройка использования вкладок.

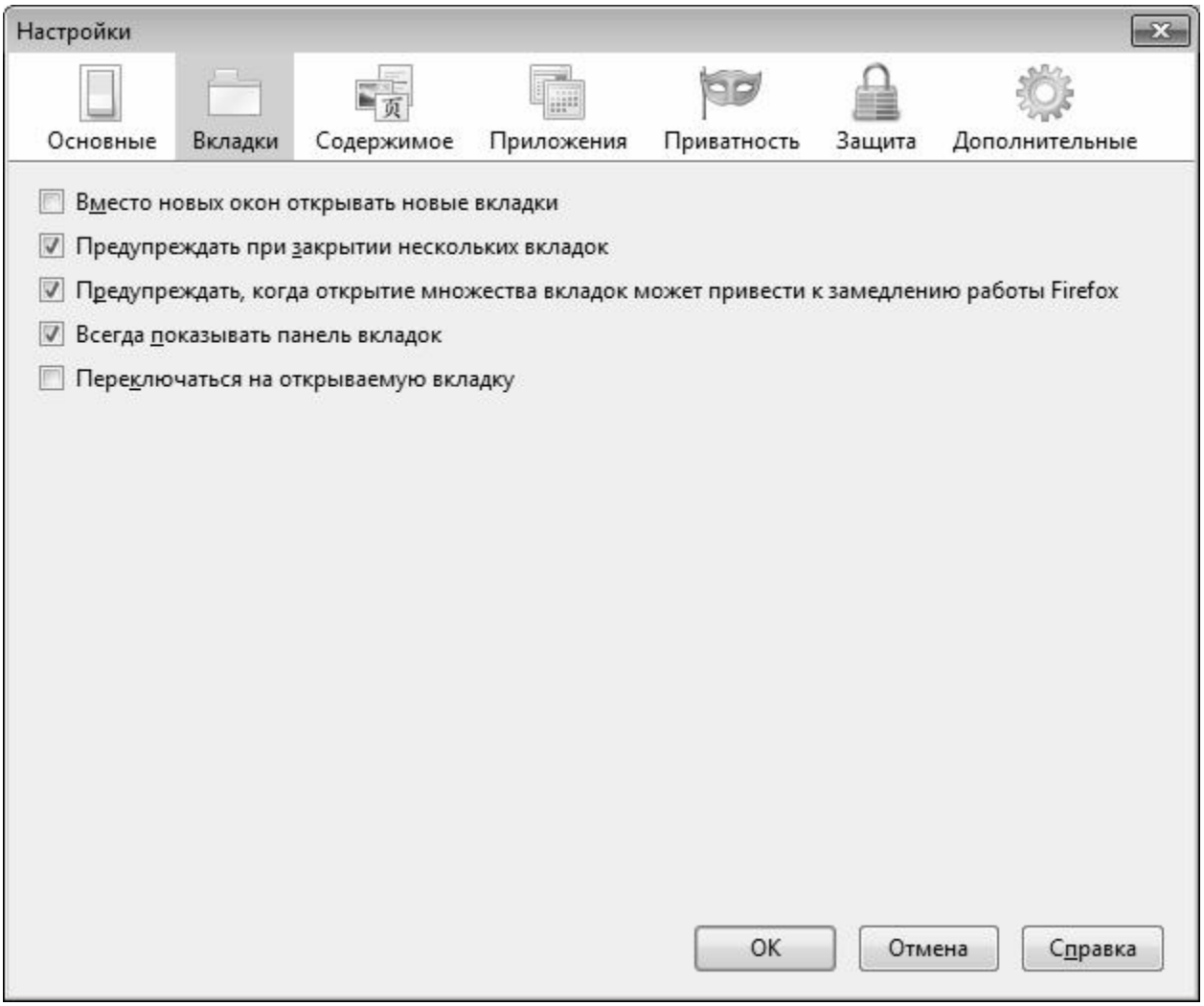



Рис. 1.8. Настройка Mozilla Firefox, раздел Вкладки

Если в данном разделе снят флажок Вместо новых окон открывать новые вкладки, то при щелчках на ссылках для перехода на новые страницы они будут открываться в новом окне. Если же этот флажок установлен, то для открытия ссылок в текущем окне программы будут автоматически создаваться новые вкладки (иначе говоря, после щелчка мышью на ссылке в окне автоматически появится новая вкладка).

В процессе работы может возникать следующая ситуация: пользователь открыл несколько вкладок, затем одна из них ему оказалась не нужна, и он решил ее закрыть. Но машинально он закрывает не вкладку, а окно программы, в результате чего, разумеется, автоматически закрываются и все остальные вкладки. Во избежание подобных ситуаций в разделе Вкладки имеется флажок Предупреждать при закрытии нескольких вкладок: если он установлен, то в случае, когда пользователь пытается закрыть окно программы с открытыми несколькими вкладками, на экране будет отображаться соответствующее предупреждение с запросом на подтверждение данной операции. Окно со всеми вкладками будет закрыто только при положительном ответе на данный запрос.

Если в разделе Вкладки установлен флажок Всегда показывать панель вкладок, то панель вкладок в окне программы будет присутствовать постоянно, даже если ни одна страница не открыта (т. е. даже когда рабочая область пуста). Если же этот флажок снят, то панель вкладок будет появляться автоматически только после открытия какой-либо

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

страницы.

В разделе Содержимое (рис. 1.9) выполняется настройка отображения содержимого веб-страниц, а также некоторых параметров безопасности.

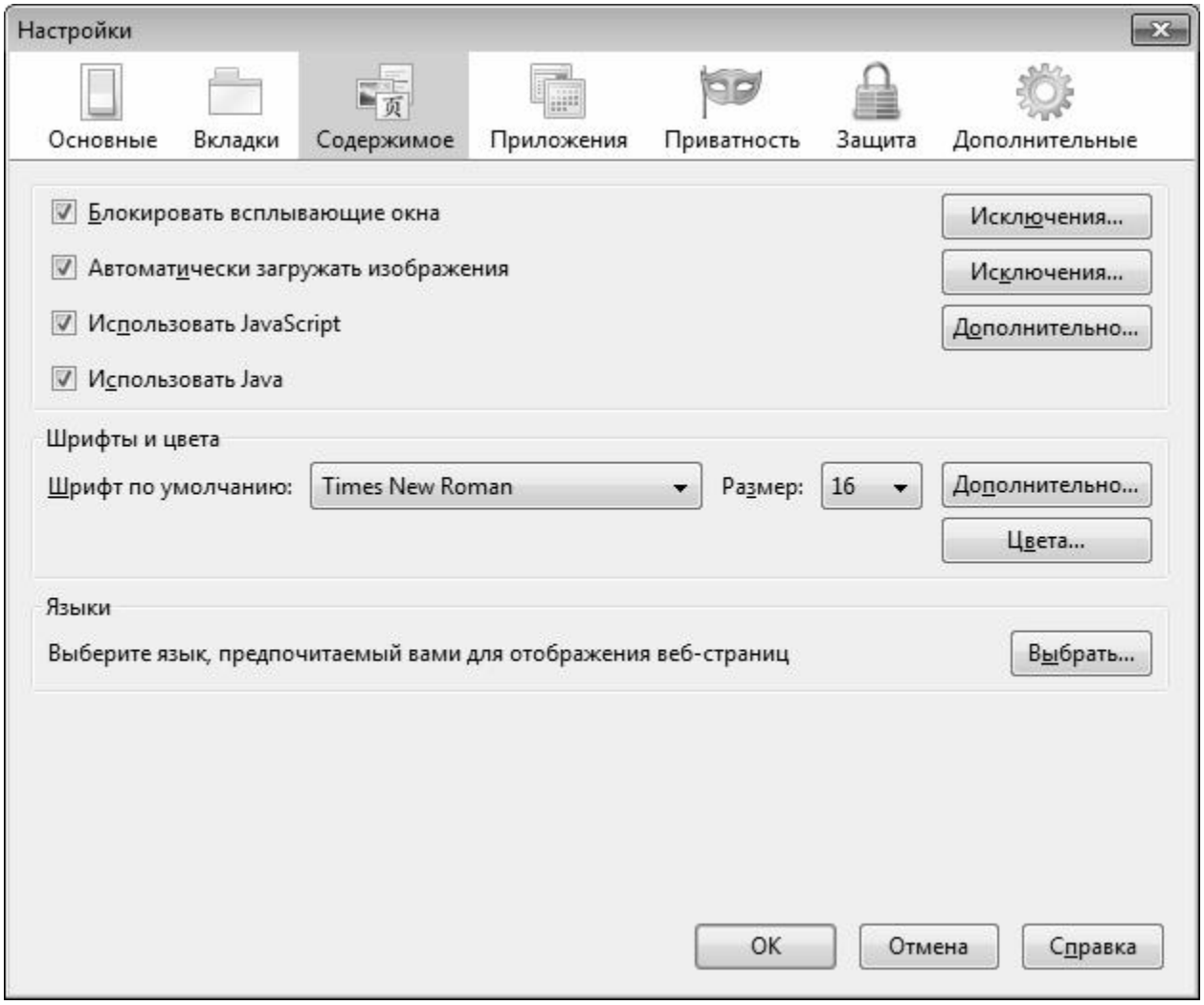



Рис. 1.9. Настройка Mozilla Firefox, раздел Содержимое

Если на данной вкладке установлен флажок Блокировать всплывающие окна, то программа будет автоматически блокировать всплывающие окна, которые почти всегда носят рекламный характер и только мешают работе. Если вы хотите разрешить использование Java-сценариев, то установите соответствующие флажки.

С помощью параметра Шрифт по умолчанию осуществляется выбор шрифта, который будет использоваться по умолчанию для отображения веб-страниц. С помощью расположенной справа кнопки Размер выбирается подходящий размер шрифта, а с помощью кнопки Цвета осуществляется переход в режим настройки цветового оформления. Кнопка Дополнительно предназначена для перехода в режим настройки дополнительных параметров шрифта.

В разделе Приложения осуществляется выбор приложений, которые в процессе работы будут использоваться совместно с Интернет-обозревателем Mozilla Firefox. Как правило, то в данном разделе можно ничего не менять и оставить те значения параметров, которые предложены по умолчанию.

Параметры, находящиеся в разделе Защита, предназначены для обеспечения безопасности вашей работы в Интернете. Начинающим пользователям не рекомендуется менять значения этих параметров без серьезных на то оснований.

Многие дополнительные параметры настройки, в том числе и касающиеся безопасности работы в Интернете, вынесены в раздел Дополнительные, содержимое которого показано на рис. 1.10.

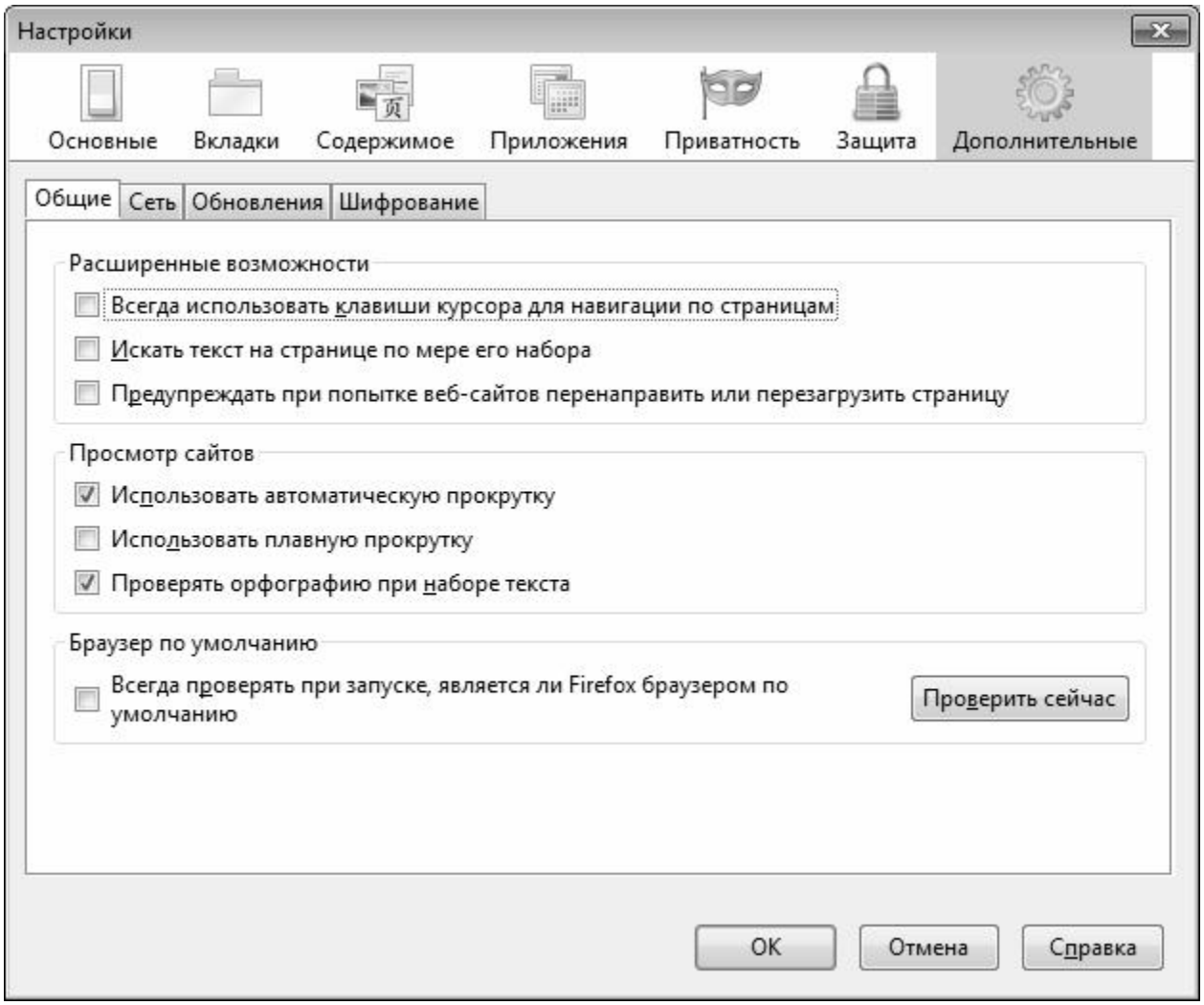



Рис. 1.10. Настройка Mozilla Firefox, раздел Дополнительные

Как видно на рисунке, содержимое раздела располагается на четырех вкладках: Общие, Сеть, Обновления и Шифрование.

Чтобы при работе в Интернете вас случайно не перенаправили на вредоносный или просто ненужный вам сайт, установите на вкладке Общие флажок Предупреждать при попытке веб-сайтов перенаправить или перезагрузить страницу. При каждом запуске программы можно проверять, является ли Mozilla Firefox обозревателем, используемым по умолчанию – для этого достаточно установить соответствующий флажок, расположенный в области Браузер по умолчанию.

На вкладке Сеть можно указать размер дискового пространства, выделяемого для хранения кэша (по умолчанию – 50 Мб). Здесь же путем установки соответствующего флажка можно включить настройку, при которой программа будет предупреждать вас обо

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

всех случаях, когда веб-сайт будет запрашивать разрешение на сохранение данных для последующего автономного просмотра.

На вкладке Обновления содержатся параметры, определяющие порядок поиска и установки обновлений Mozilla Firefox в Интернете. Если установлены флажки Браузера Firefox, Установленных дополнений и Поисковых плагинов, то программа будет автоматически искать соответствующие обновления при каждом подключении к Интернету. Если же вы не желаете расходовать свой Интернет-трафик на эти цели – снимите данные флажки. Отметим, что вы в любой момент можете просмотреть журнал обновлений – для этого достаточно нажать кнопку Показать журнал обновлений. Если на данной вкладке установлен флажок Браузера Firefox, то становятся доступными для редактирования еще два параметра – переключатель При обнаружении обновлений для Firefox и флажок Предупреждать, если при данном действии будут отключены какие-либо дополнения, который доступен только в том случае, когда переключатель установлен в положение Автоматически загружать и устанавливать дополнения. Если же переключатель установлен в положение Предоставлять выбор действия пользователю, то при обнаружении обновлений пользователю будет предложено выбрать вариант дальнейших действий.

Что касается вкладки Шифрование, то в большинстве случаев рекомендуется оставить значения параметров, предложенные по умолчанию. С помощью этих параметров определяются протоколы, а также определяется порядок отправки личного сертификата (автоматически или по запросу, причем по умолчанию предлагается второй вариант). Кнопки, расположенные на данной вкладке, позволяют перейти в режим более тонкой настройки параметров шифрования, но опять же – если вы не являетесь специалистом в этом вопросе, то экспериментировать не рекомендуется.

Все изменения, выполненные во всех разделах окна настройки программы, вступают в силу только после нажатия кнопки ОК. С помощью кнопки Отмена осуществляется выход из данного режима без сохранения выполненных изменений.

## Глава 2. Спам, вирусы, компьютерный шпионаж

В данной главе мы поговорим о таких явлениях, как навязчивая реклама и спам, компьютерный шпионаж, и, конечно, не оставим без внимания тему компьютерных вирусов. Кроме этого, мы научимся самостоятельно бороться со всеми перечисленными явлениями.

### Компьютерные вирусы

Наверное, невозможно сегодня встретить пользователя компьютера, который не слышал бы о компьютерных вирусах. Эти вредоносные программы в огромном количестве

«представлены» в Интернете, и их количество растет с каждым днем. Самое неприятное, что многие распространители вирусов успешно применяют в своей практике передовые достижения IT-индустрии – в результате то, что должно служить во благо пользователям, в конечном итоге может обернуться для них большими проблемами.

Что же включает в себя понятие «компьютерный вирус»? Многие специалисты расходятся во мнениях на этот счет и предлагают разные формулировки. Мы же будем считать, что вирус – это вредоносная программа, проникающая на компьютер без ведома пользователя (хотя, возможно, при невольном его участии) и выполняющая определенные действия разрушительной направленности, нередко умеющая размножаться и самораспространяться.

Первый компьютерный вирус был написан в начале 80-х годов прошлого столетия. Тогда это не было попыткой навредить кому-либо, а сделано просто из интереса. Этот вирусописатель явно не подумал о возможных последствиях: сегодня известно несколько миллионов вирусов, и их количество растет с каждым днем.

Каковы же причины возникновения вирусов? Когда-то это было не более чем шалостью. Постепенно пользователи, умеющие писать вирусы, стали применять свое умение на практике, и вирусы стали создаваться с конкретными целями. Например, сотрудник, вынужденный уволиться с работы и считающий себя обиженным, с помощью вируса мог «отомстить» своему бывшему работодателю либо коллегам по работе. Кстати, подобные ситуации возникали и в корпорации Microsoft – известны случаи, когда бывшие ее сотрудники создавали вирусы, используя свои знания уязвимых мест операционной системы Windows либо офисных приложений.

В настоящее время в мире развелось великое множество «вирусописателей». Одни из них занимаются созданием и распространением вирусов в качестве хобби, другие просто желают сделать «всем плохо», третьи хотят отомстить, четвертые имеют вполне конкретные коммерческие цели – хищение информации либо денежных средств, вывод из строя сетей, веб-ресурсов и т. п. за солидное вознаграждение (в частности, это одно из проявлений современной конкурентной борьбы), и др.

**Виды компьютерных вирусов**

Специалисты выделяют несколько категорий компьютерных вирусов, среди которых можно выделить следующие: файловые вирусы, сетевые вирусы (черви), загрузочные вирусы, макровирусы и так называемые «троянские кони» (трояны).

Файловые вирусы были широко распространены в конце 80-х – начале 90-х годов прошлого столетия. Их отличительная черта – то, что они активизируются при запуске инфицированной программы. При этом программный код вируса скрывается либо в исполняемом файле, либо в динамических библиотеках (dll). После активизации такой вирус способен инфицировать и иные приложения, установленные на компьютере.

Стоит отметить, что время файловых вирусов уже практически ушло. Исключением являются вирусы, которые по своей природе относятся к скриптам. Такие вирусы обычно прячутся в веб-страницах, их программный код написан с использованием скриптового языка программирования (один из самых известных таких языков – JavaScript).

Одним из наиболее неприятных и опасных видов вредоносного программного обеспечения по праву считаются сетевые вирусы (черви). Уже по названию нетрудно

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

догадаться, что их «среда обитания» – это локальная сеть. Сетевому червю для распространения по локальной сети достаточно попасть в один компьютер – и уже через короткое время вся сеть будет инфицирована.

ВНИМАНИЕ

Нередки случаи, когда сетевые вирусы используют хитроумную приманку для того, чтобы пользователь выполнил их активизацию. Например, на рабочем столе зараженного компьютера может внезапно появиться значок с изображением стодолларовой купюры и азартным названием вроде Вы выиграли приз, Возьми меня или т. п. Если на этом значке щелкнуть мышью (а это первое естественное желание у подавляющего большинства пользователей, и об этом прекрасно осведомлены разработчики вредоносного программного обеспечения), то сетевой червь моментально активизируется и начинает распространение по всем компьютерам, подключенным к локальной сети.

Характерной особенностью загрузочных вирусов является то, что они заражают загрузочную область диска. Действует такой вирус примерно так: при загрузке операционной системы сведения из зараженной загрузочной области попадают в память компьютера. После этого инфицируются загрузочные области всех доступных дисков (как жестких, так и гибких). Правда, в настоящее время подобные вирусы встречаются очень редко, поскольку их основной метод размножения – через загрузочные гибкие диски, а таким способом компьютеры сегодня почти никто не загружает (исключением могут являться различного рода нештатные ситуации).

Большинство независимых исследователей сходятся во мнении, что немалая опасность в ближайшем будущем будет исходить от макровирусов. Конструктивно они подобны файловым вирусам, так как тоже прячутся в программном коде. «Ореол обитания» макровирусов – это макросы, то есть приложения, написанные на языке программирования Visual Basic Application. Макросы используются в программах офисного пакета MS Office для расширения их имеющихся функциональных возможностей.

Еще одним опасным видом вирусов являются так называемые «троянские кони», попросту говоря – трояны. Их отличительной особенностью является то, что они обычно не вредят компьютеру либо хранящейся в нем информации. Основная цель этих вирусов – предоставление к данному компьютеру удаленного доступа через Интернет, используя который злоумышленник может осуществлять с инфицированным компьютером любые действия: уничтожать и записывать данные, редактировать настройки, запускать программы, и т. д.

Главное коварство «троянских коней» состоит в том, что пользователь инфицированного компьютера может ничего не подозревать о том, что его компьютер используется в каких-то целях (рассылка спама, реклама порнографических сайтов, рассылка призывов к массовым противоправным действиям, и т. п.). Для надежного противодействия троянам мало установить антивирусную программу – необходимо еще иметь на компьютере сетевой экран (файрволл).

Также здесь можно отметить бессмысленные, шутливые и т. п. вирусы – они, как правило, не осуществляют особых деструктивных действий, а просто периодически выдают на экран сообщения о каких-либо несуществующих «катаклизмах» в компьютере (например, Ваш компьютер заражен вирусом; через 15 минут начнется автоматическое

форматирование диска C). Не исключено, что, получив такое сообщение, испуганный пользователь начнет лихорадочно сохранять всю более-менее ценную информацию на внешних носителях, да и вообще сделать массу ненужных действий. Возможно также, что, не дождавшись обещанного форматирования диска, пользователь сам запустит этот процесс – как говорится, «от греха подальше» (такое паникерство обычно свойственно новичкам).

**Как защититься от компьютерных вирусов**

Для борьбы с вредоносным программным обеспечением в настоящее время существует немало специально предназначенных программных средств, относящихся к категории антивирусов.

Высокой степенью эффективности отличается удобная и недорогая антивирусная программа NOD 32. Ее автором и разработчиком является известная компания ESET, занимающая одну из лидирующих позиций на рынке программного обеспечения. NOD 32 успешно справляется с различного рода вирусами, шпионскими и рекламными модулями, червями, троянами и прочими вредоносными программами. Кроме этого, NOD 32 является надежным сетевым экраном, блокируя любое проникновение в компьютер извне. Среди прочих преимуществ данного продукта стоит отметить простоту и удобство в эксплуатации, а также то, что его функционирование не замедляет работу операционной системы.

Еще один полезный и эффективный защитный продукт – программа Virus Scan, разработчиком которой является американская корпорация McAfee. В данной программе, как и во многих других, реализовано два основных направления – для домашних пользователей и для офисного применения. Для предварительного знакомства с ее возможностями предоставляется бесплатная демонстрационная версия, которую можно скачать с сайта разработчика. Программа обладает достаточно удобным, современным и эргономичным пользовательским интерфейсом, а также простым и понятным инструментарием. Антивирусную программу Virus Scan можно приобрести как отдельно, так и в комплексе с другими программами от этого же разработчика, предназначенными для защиты компьютера и информации – в частности, с антиспамовым фильтром и файрволом. Управление всеми режимами осуществляется из одного интерфейса, а переключение между ними выполняется с помощью соответствующих инструментов.

Одним из распространенных и эффективных антивирусных средств является программа Avast. Как показывает практика, она способна распознавать и успешно бороться с вирусами, перед которыми оказываются бессильны иные антивирусные программы. Отметим, что Avast – это не только собственно антивирус, но еще и сканер электронной почты, а также надежный сетевой экран. В настоящее время имеется как платная, так и бесплатная версия этой программы.

Программа Panda Antivirus – еще один представитель семейства антивирусных продуктов. Ее разработчиком является испанская фирма Panda Software. В состав программы входят модули сканирования и мониторинга (эти функции в Panda Antivirus объединены в одну), модуль почтового сканирования (для проверки электронной корреспонденции) и модуль автоматического обновления антивирусных баз.

Отличительной чертой программы является то, что после установки ее практически не

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

нужно настраивать. Конечно, при необходимости пользователь может изменить любые параметры настройки в соответствии со своими потребностями, но предлагаемые значения по умолчанию подобраны настолько оптимально, что в большинстве случаев программу можно использовать сразу после установки. Это и является одним из приоритетных направлений, заложенных в программе – она должна быть проста и удобна в применении даже для неопытных и начинающих пользователей.

Особо следует отметить возможность программы восстанавливать поврежденную вирусом систему. Иначе говоря, после обнаружения вируса и его обезвреживания (удаления, лечения и др.) программа ликвидирует все сделанные им изменения в системных файлах, системном реестре, настройках системы и т. д., и возвращает операционную систему в то состояние, в котором она была до появления вируса.

Еще одной популярной антивирусной программой является «Антивирус Касперского», автором и разработчиком которой является лаборатория Касперского. Первый релиз продукта увидел свет еще в 1994 году. С тех пор «Антивирус Касперского» претерпел множество изменений и к настоящему времени стал качественным современным средством защиты. Стоимость программы и комплект поставки зависят от того, какую конфигурацию приобретает пользователь.

Также немалой популярностью пользуется антивирус, который называется Dr.Web. Он относится к числу первых российских продуктов аналогичного назначения, и сегодня считается одним из самых эффективных. Отметим, что от многих конкурентов Dr.Web выгодно отличается высоким быстродействием. Параметры сканирования устанавливаются в настройках программы. В частности, там указываются объекты, которые нужно проверить, определяется порядок действия в случае обнаружения вируса (переименовать зараженный объект, удалить его либо вылечить, или поместить в указанную папку), устанавливается количество ресурсов компьютера, выделяемых на сканирование, и др.

Антивирусное приложение Norton Antivirus также имеет немалое число поклонников во всем мире. Ее автором является знаменитая корпорация Symantec. Продукт выпускается в разных конфигурациях – для домашних пользователей и для офисного применения. Средняя стоимость «домашней» версии составляет около 50 долларов США. Программа имеет приятный и эргономичный пользовательский интерфейс – по мнению многих пользователей, он выглядит намного современнее, чем интерфейсы конкурентов, но на момент написания данной книги русский язык в ней не поддерживается. Отличительной чертой Norton Antivirus является наличие очень мощной функциональности проверки электронной почты (многие конкуренты по этому показателю уступают). При этом поддерживается работа со всеми наиболее популярными почтовыми программами – Outlook Express, Microsoft Outlook, The Bat и др. Использование программы практически полностью исключает возможность приема и отправки зараженных вирусами электронных сообщений. Обнаруженные в процессе сканирования вирусы и зараженные файлы помещаются в специальную папку, где пользователь может досконально с ними разобраться и, в зависимости от полученного результата – либо удалить их, либо отменить решение Norton Antivirus о причислении их к числу вирусов.

**Как предотвратить заражение компьютера**

Несмотря на обилие антивирусного ПО, стопроцентной защиты от вирусов сегодня не существует. Тем не менее, соблюдение перечисленных ниже правил поможет многократно снизить риск заражения.

♦ Если возможности используемой антивирусной программы предусматривают использование постоянного мониторинга, то данный режим обязательно должен быть включен при работе в Интернете. Это поможет своевременно обнаружить зараженные файлы, пытающиеся проникнуть в компьютер.

♦ Ни в коем случае нельзя запускать внезапно появляющиеся иконки и значки на рабочем столе – многие вирусы (особенно это относится к сетевым червям) специально помещают на рабочий стол заманчивую иконку, при щелчке на которой вирус активизируется и начинает распространяться по сети.

♦ Периодически нужно выполнять полное сканирование компьютера хорошей антивирусной программой. Периодичность сканирования зависит от того, как часто и с какой загрузкой работает компьютер, а также – выходит ли пользователь в Интернет.

♦ При получении из Интернета либо локальной сети файлов каких-либо приложений пакета Office (Word, Excel и др.) следует в первую очередь проверить их надежной антивирусной программой, и лишь затем открывать. Такие файлы могут содержать макровирусы – это один из наиболее распространенных и коварных видов вирусов.

♦ То же самое относится и к другим скачиваемым из Интернета файлам (дистрибутивы либо исполняемые файлы приложений, самораспаковывающиеся архивы и др.) – перед выполнением их обязательно нужно проверить антивирусом (не забыв перед этим обновить антивирусные базы).

♦ Избегайте компьютеров «общего пользования» – т. е. установленных в студенческих аудиториях, в Интернет-кафе, и т. п. За день таким компьютером воспользуется неизвестно сколько человек, и любой из них может занести вирус со своей дискеты либо компакт-диска. Поэтому записывать с такого компьютера информацию на свою дискету – примерно то же самое, что в разгар эпидемии гриппа посещать многолюдные места.

♦ При работе с внешними носителями информации (дискеты, компакт-диски и др.) обязательно проверять их на наличие вирусов антивирусной программой (особенно если это не собственный диск либо дискета, либо если он новый).

♦ При работе с файлами, расположенными в Интернете, настоятельно рекомендуется не запускать их сразу, а предварительно сохранить на своем компьютере и проверить антивирусной программой.

♦ Еще раз напомним, что по окончании работы в Интернете необходимо обязательно отключить шнур, соединяющий компьютер с Интернетом – если этого не сделать, то вирус может проникнуть даже в выключенный компьютер.

**Компьютерный шпионаж**

Основное отличие шпионских модулей Spyware от компьютерных вирусов заключается в том, что они, как правило, не наносят вреда программному обеспечению и данным, хранящимся в компьютере (если не считать того, что на них отвлекается определенное количество ресурсов оперативной памяти и места на жестком диске). Задача шпионских

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

модулей заключается в том, чтобы собирать некоторую информацию о пользователе (адреса электронной почты, содержимое жесткого диска, список посещаемых страниц в Интернете, информация личного характера и т. д.) и отправлять ее по определенному адресу. При этом пользователь даже не подозревает, что за ним ведется своего рода тайное наблюдение. Полученная таким способом информация может использоваться в самых разнообразных целях, которые могут быть как относительно безобидными (анализ посещаемости тех либо иных сайтов), так и весьма опасными (например, если полученная информация будет использована в противозаконных целях либо в ущерб пользователю).

Каким образом же шпионские модули проникают в компьютер? В большинстве случаев это происходит в процессе инсталляции нужных и полезных приложений, которые пользователь устанавливает самостоятельно. Есть, например, бесплатные программы, которые можно использовать только вместе с встроенной программой-шпионом; если же шпион будет удален, то и основную программу использовать будет невозможно. Кроме этого, нужно соблюдать внимание при установке программ: некоторые шпионы проникают в компьютер, например, после того, как пользователь, не задумываясь, утвердительно ответил на какой-либо запрос, который появился на экране в процессе инсталляции. Некоторые разработчики вставляют в дистрибутив своих продуктов собственную программу-шпиона, а некоторые обращаются за помощью к фирмам, которые создают и поставляют программы-шпионы разработчикам программного обеспечения. Кроме этого, программы-шпионы могут проникать в компьютер из Интернета (от подобных проникновений и защищает брандмауэр).

**Классификация шпионского ПО**

В настоящее время существует несколько видов шпионского ПО. Например, у многих злоумышленников пользуются популярностью так называемые кейлоггеры – клавиатурные шпионы. Их характерной особенностью является то, что они могут иметь как программное, так и аппаратное исполнение. Главная задача клавиатурного шпиона – собирать и высылать своему заказчику информацию обо всех нажатиях клавиш на компьютере, за которым ведется слежка. Это один из самых опасных видов шпионских модулей, поскольку он способен похищать секретную информацию, вводимую пользователем с клавиатуры: логины и пароли, пин-коды кредитных карт, конфиденциальную переписку, и т. д. Часто кейлоггеры используются для похищения программных кодов создаваемого программного обеспечения.

Если клавиатурный шпион имеет аппаратное исполнение, то обнаружить его несложно. Просто следите за своим компьютером, если в помещение, где он находится, имеют доступ другие лица (это особенно актуально по отношению к офисным компьютерам). Следите за тем, чтобы между клавиатурой и системным блоком не появилось какое-то устройство (обычно аппаратный кейлоггер имеет небольшие размеры, меньше спичечного коробка), а при обнаружении непонятных устройств немедленно обратитесь к системному администратору.

Если же кейлоггер представляет собой программу, то для его обнаружения и нейтрализации используйте специальное программное обеспечение категории AntiSpyware.

Еще один известный вид шпионского ПО – сканер жесткого диска. Этот шпион

тщательно изучает все содержимое жесткого диска вашего компьютера (какие программы установлены, какие файлы и папки хранятся, и др.) и отсылает собранные сведения своему хозяину.

Информацию о том, чем вы занимаетесь на компьютере, может собирать экранный шпион. Сущность его состоит в том, что он периодически через определенные промежутки времени (которые заданы злоумышленником) делает снимки экрана (на компьютерном сленге – скриншоты), и отсылает их хозяину. Кстати, этот вид шпионов иногда используется в офисах: с его помощью начальство узнает, чем занимаются подчиненные во время работы.

Также немалой популярностью у злоумышленников пользуются так называемые «прокси-шпионы». После того как такой spyware проникает в компьютер, то этот компьютер будет выполнять роль прокси-сервера (о том, что представляет собой прокси-сервер, мы говорили ранее). На практике это означает, что злоумышленник при работе в Интернете сможет прикрываться вашим именем, и если его действия будут носить деструктивный или противозаконный характер – отвечать придется именно вам. Самый типичный пример – когда с зараженного компьютера рассылается спам, что может привести к появлению проблем со своим провайдером.

Еще один популярный у злоумышленников вид spyware – это почтовые шпионы. Их главная задача – сбор сведений об адресах электронной почты, хранящихся в данном компьютере, и отсылка этой информации хозяину. Сведения собираются обычно в почтовых программах и адресных книгах, а также органайзерах. Такая информация имеет высокую ценность для тех, кто занимается рассылкой спама. Кроме этого, почтовые шпионы могут вести откровенно деструктивную деятельность: менять содержимое писем, вставлять в них рекламные блоки, и т. д.

**Кейлоггер, или клавиатурный шпион**

Несмотря на то, что выше мы уже упоминали о клавиатурных шпионах, на них имеет смысл остановиться подробнее. В первую очередь это обусловлено тем, что клавиатурные шпионы являются одними из самых коварных из всего многообразия шпионских модулей и программ.

В общем случае клавиатурному шпиону можно дать следующее определение:

Клавиатурный шпион – это программа либо устройство, с помощью которого осуществляется постоянное наблюдение за всеми нажатиями клавиш на клавиатуре (а во многих случаях – и за всеми щелчками мыши) с целью получения информации обо всех набираемых пользователем текстах. Зачем это нужно? Ответ на данный вопрос у каждого злоумышленника свой: одному нужно перехватывать чужие почтовые сообщения, другому – получить номера кредитных карт, третьему – взломать пароли, четвертому – украсть у разработчика исходные тексты еще не вышедшей программы, а пятому – все вместе взятое, и еще что-нибудь.

Характерной особенностью клавиатурных шпионов является то, что они могут выступать не только в виде внедренного в компьютер вредоносного программного обеспечения, но и в виде отдельных устройств. Такие устройства обычно устанавливаются между клавиатурой и системным блоком и, поскольку имеют весьма небольшие размеры, могут долго оставаться незамеченными. Однако чтобы установить такое устройство,

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

необходим доступ к компьютеру в отсутствие пользователя. Поэтому на домашних компьютерах такой вид клавиатурных шпионов встречаются редко, чаще – на офисных и рабочих компьютерах, а также на компьютерах «общественного пользования»: в студенческих аудиториях, на почте, в интернет-клубах и др. Чтобы своевременно обнаружить такой «сюрприз», рекомендуется почаще обращать внимание на то, не появилось ли новое устройство между клавиатурой и системным блоком.

Достаточно широко распространены в настоящее время так называемые перехватывающие клавиатурные шпионы. Такие шпионы в большинстве случаев представляют собой программу, состоящую из исполняемого файла с расширением *.exe, и dll-библиотеки, с помощью которой осуществляется управление процессами записи информации. Перехватывающий клавиатурный шпион без проблем запоминает практически любой набранный текст: документы, письма, исходные коды программ (данная возможность нередко используется для кражи исходников еще не вышедших программ), номера кредитных карт, пароли (в том числе и самозаполняющиеся) и т. д.

Клавиатурный шпион (имеется в виду программа, а не устройство) может проникнуть в компьютер разными способами: например, как и любой другой шпионский модуль – в составе какой-либо устанавливаемой на компьютер бесплатной программы (как правило – от неизвестного либо сомнительного разработчика), либо через программу обмена сообщениями, и т. д. В последнее время нередки случаи, когда для «получения» в свой компьютер клавиатурного шпиона достаточно было просто зайти на определенный сайт.

Стопроцентной защиты от клавиатурных шпионов, как и от других вредоносных программ, в настоящее время не существует – ведь известно, что на каждое противоядие можно найти новый яд. Однако при соблюдении мер предосторожности можно свести к минимуму их вероятность их появления на компьютере.

Что касается аппаратных клавиатурных шпионов, то для защиты от них рекомендуется по возможности минимизировать доступ к компьютеру посторонних лиц – это в первую очередь относится к компьютерам, которые установлены на рабочих местах (разумеется, не нужно впадать при этом в крайности – например, системного администратора отгонять от компьютера не стоит). Ну и, конечно, периодически нужно проверять, не появилось ли между клавиатурой и системным блоком какое-нибудь неизвестное устройство. Иногда это касается и домашних компьютеров – вспомните, кто имеет доступ к вашему компьютеру? Одно дело – если только вы, и другое – если, например, к вашему сыну-студенту периодически приходят «продвинутые» в компьютерном отношении друзья и возятся около компьютера. В последнем случае вполне возможно, что вам потехи ради (или с более серьезными намерениями) вставят какого-нибудь «жучка».

Что же делать, если предполагается, что в компьютер уже проник клавиатурный шпион? Конечно, в первую очередь необходимо просканировать компьютер специально предназначенной программой. Для поиска и уничтожения клавиатурных шпионов можно использовать некоторые программы из числа тех, что предназначены для борьбы и с другими Spyware; кроме этого, есть программы, специализирующиеся именно на клавиатурных шпионах (одна из таких программ рассматривается чуть ниже). Однако бывают ситуации, когда выполнение немедленного сканирования невозможно, и в то же время необходимо срочно выполнить какие-либо действия с конфиденциальными данными. Как же поступить в таком случае?

При возникновении подобных ситуаций рекомендуется использовать так называемую

виртуальную клавиатуру. Виртуальная клавиатура – это программа, интерфейс которой представляет собой изображение клавиатуры, а ввод нужных символов осуществляется с помощью мыши. Поскольку принцип действия большинства клавиатурных шпионов заключается в перехвате вводимых с клавиатуры символов, то использование виртуальной клавиатуры достаточно эффективно.

Однако необходимо учитывать, что некоторые клавиатурные шпионы снимают копии экрана еще и после каждого щелчка мыши. Для защиты от таких шпионов предусмотрены виртуальные клавиатуры, в которых для ввода символа достаточно просто подвести указатель мыши к соответствующей позиции. Благодаря этому можно ввести информацию без единого щелчка мышью.

При частой или регулярной работе с конфиденциальными данными рекомендуется постоянно использовать виртуальную клавиатуру – ведь никогда нельзя полностью быть уверенным в том, что в компьютер не проник клавиатурный шпион.

Для борьбы с клавиатурными шпионами можно использовать программы, предназначенные для борьбы и с другими Spyware (описание некоторых из них приведено выше), а также специализированные программы, которые называются анти-кейлоггеры. Одной из таких программ является Anti-keylogger, которую разработали российские специалисты.

Характерной особенностью программы Anti-keylogger является то, что для ее работы не предусмотрено использование сигнатурных баз. Это позволяет ей выявлять и блокировать любые виды клавиатурных шпионов, как известные большинству аналогичных программ, так и нет.

Программа обладает простым и дружественным пользовательским интерфейсом. В разделе Опции предусмотрена возможность настройки параметров работы программы. Кроме этого, в разделе Лист исключений реализована возможность ведения списка исключений; в этот список можно включать программы, которые не должны распознаваться как клавиатурные шпионы.

Помимо программы Anti-keylogger, в Интернете можно найти еще множество программ (как платных, так и бесплатных), специально предназначенных для борьбы с клавиатурными шпионами.

**Как самостоятельно поймать и нейтрализовать компьютерного шпиона?**

Отличительной чертой Spyware является то, что их трудно распознать с помощью штатных антивирусных программ. Поэтому для борьбы с ними рекомендуется использовать специальные утилиты, которые во множестве представлены в Интернете. Однако при этом обязательно нужно учитывать следующее: многие шпионские программы искусно маскируются именно под утилиты для борьбы с ними. Иначе говоря, установив на свой компьютер утилиту для борьбы с Spyware, можно вместо нее заполучить сам шпионский модуль. Поэтому – для распознавания и устранения Spyware рекомендуется либо использовать средства известных разработчиков, либо воспользоваться рекомендациями других пользователей, уже столкнувшихся с подобной проблемой ранее.

Но в некоторых случаях наличие в компьютере шпионского ПО можно обнаружить по характерным признакам, которые перечислены ниже.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

♦ Сразу после запуска Интернет-обозревателя начинает загружаться посторонняя и незнакомая веб-страница (вместо той, которая определена в качестве домашней).

♦ Заметно возрастает исходящий трафик.

♦ Windows работает нестабильно, часто «падает» и «зависает».

♦ При выходе в Интернет через телефонную линию заметно и необъяснимо увеличиваются суммы в счетах за телефонную связь (скорее всего, причиной этого стало наличие в компьютере шпионского модуля автоматического дозвона).

♦ В Интернет-обозревателе непонятно откуда появились новые элементы управления (панель инструментов, команда в контекстном меню, кнопка, и др.);

♦ В списке Избранного появились незнакомые элементы, причем удалить их никак не получается.

♦ В Диспетчере задач на вкладке Процессы видно, что какой-то новый процесс практически полностью задействовал ресурсы компьютера.

♦ На экране время от времени отображаются непонятно откуда взявшиеся рекламные окна, причем даже тогда, когда компьютер отключен от Интернета.

♦ На Рабочем столе появились новые ярлыки или значки, при щелчке мышью на которых выполняется автоматический переход на незнакомую веб-страницу.

Если вы подозреваете, что в компьютер проник Spyware – проверьте папку Program Files, каталог автозагрузки, а также содержимое раздела Программы и компоненты в Панели управления. Некоторые Spyware автоматически помещают свой значок в правую часть панели задач (рядом с часами), и по этому признаку их можно обнаружить. Также рекомендуется проанализировать подменю Пуск ▸ Все программы – некоторые Spyware могут «наследить» здесь. В Интернет-обозревателе проверьте, какая страница выбрана в качестве домашней, а также содержимое папки Избранное.

**Автоматическое обновление Windows как средство защиты компьютера от шпионов и вирусов**

Любой программный продукт постоянно дорабатывается и совершенствуется (если, конечно, он не снят с обслуживания и поддержки ввиду появления новых версий или по иным причинам). Это касается и операционной системы Windows 7: разработчики постоянно выпускают обновления (патчи), которые в большинстве своем предназначены для решения следующих задач:

♦ доработка и улучшение функциональности операционной системы;

♦ устранение имеющихся ошибок;

♦ повышение надежности операционной системы;

♦ повышение уровня безопасности системы от внешних угроз.

Помимо перечисленных, с помощью обновлений можно решать и другие задачи, в зависимости от специфики ситуации. Отметим, что главная задача большинства обновлений – это повышение уровня защиты компьютера от внешних угроз, и прежде всего именно с этой точки зрения важно своевременно скачивать и устанавливать обновления.

В операционных системах семейства Windows реализована возможность автоматического получения и установки всех обновлений, выпускаемых разработчиком (компанией Microsoft). В этом случае при наличии доступа к Интернету система будет

автоматически искать и устанавливать все необходимые патчи, не требуя никакого участия пользователя. Однако при желании пользователь может либо отключить эту возможность, либо взять ее под свой контроль – в этом случае система будет выдавать ему запросы на подтверждение скачивания и инсталляции обновлений.

Чтобы перейти в режим работы с обновлениями, нужно в Панели управления открыть категорию Система и безопасность, и выбрать в ней раздел Центр обновления Windows. Содержимое этого раздела показано на рис. 2.1.

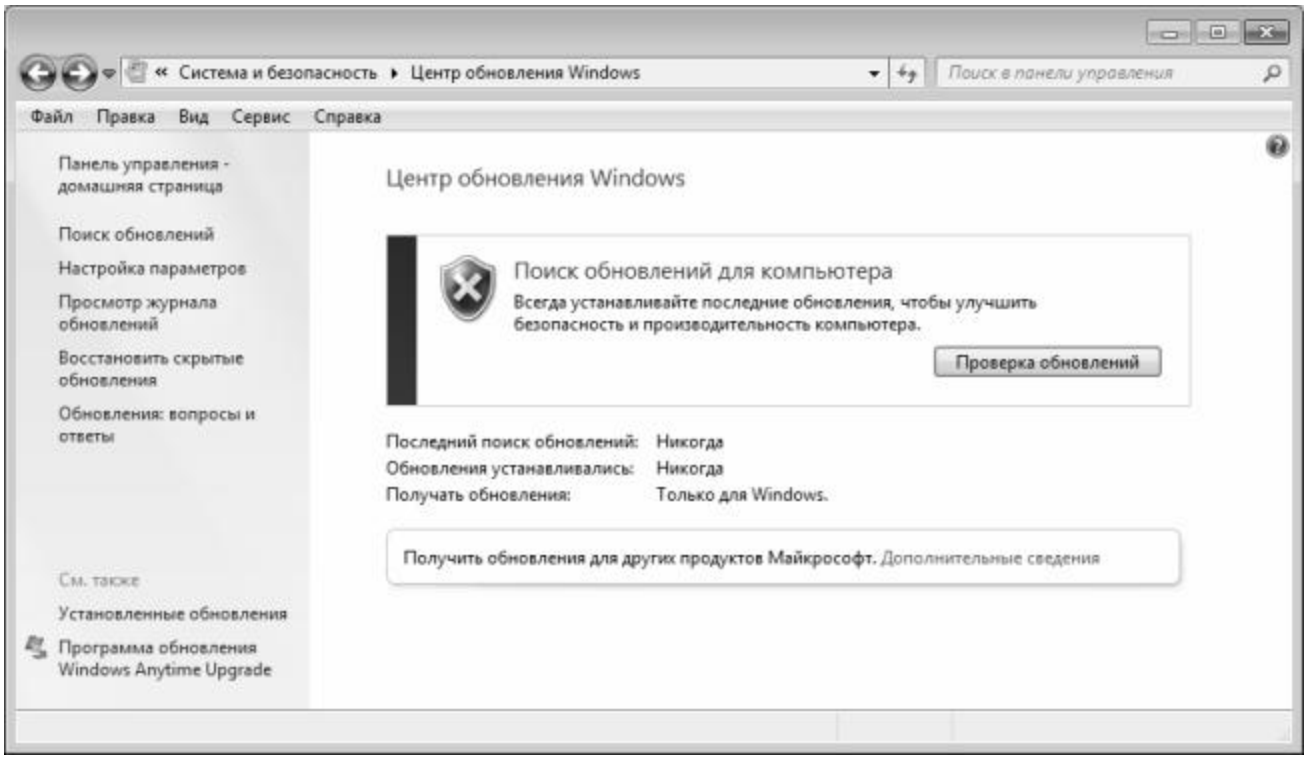



Рис. 2.1. Центр обновления Windows

В данном окне с помощью кнопки Проверка обновлений вы можете в любой момент проверить наличие свежих обновлений, после чего скачать их и установить на компьютер. Помните, что для этого необходимо наличие действующего подключения к Интернету. Также для выполнения этой операции можно воспользоваться ссылкой Поиск обновлений, которая находится в левой части данного окна.

Вы можете самостоятельно настроить параметры обновления операционной системы. Для перехода в соответствующий режим щелкните на ссылке Настройка параметров, которая также расположена в левой части окна. При этом на экране откроется окно, изображенное на рис. 2.2.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

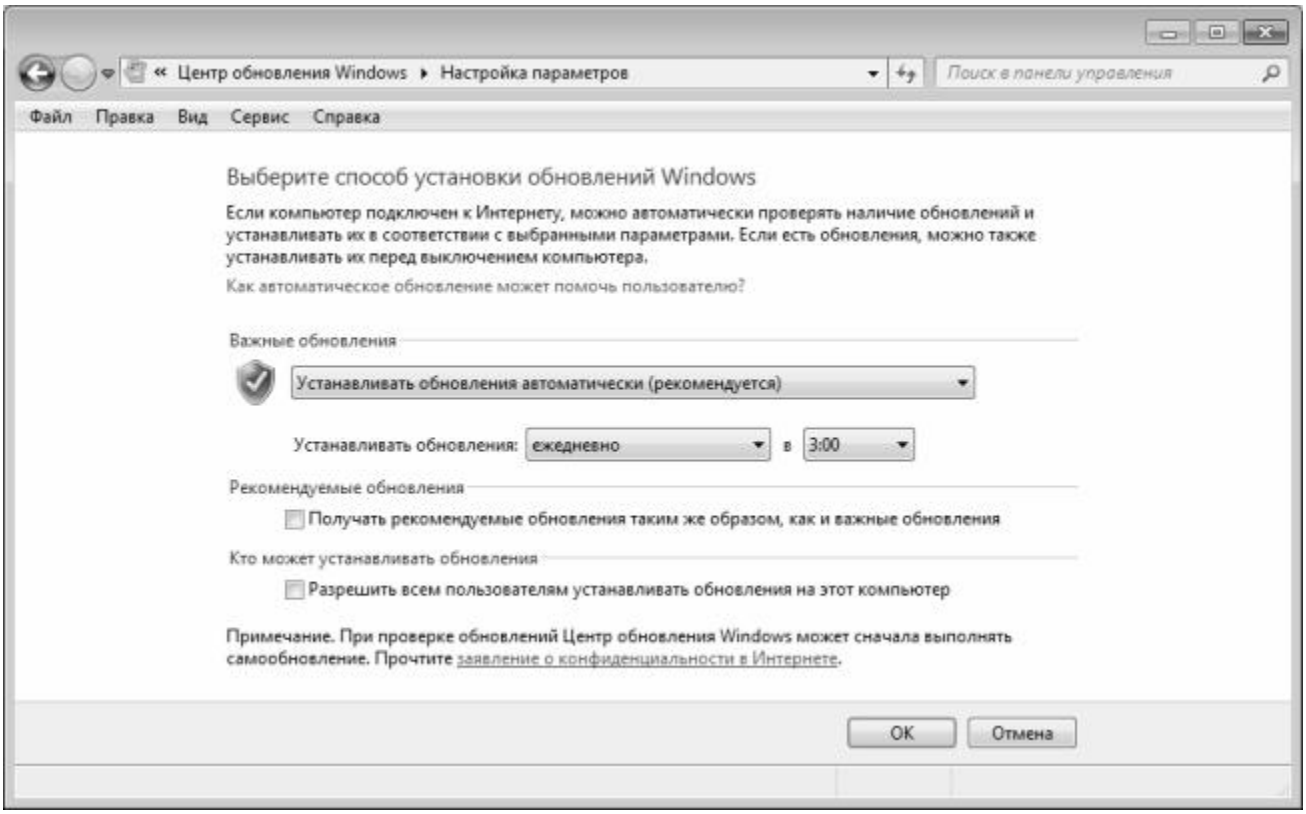



Рис. 2.2. Настройка параметров обновления Windows 7

В данном окне из раскрывающегося списка выбирается подходящий режим обновления операционной системы.

♦ Устанавливать обновления автоматически (рекомендуется) – в данном случае все обновления будут скачиваться и устанавливаться на компьютер в автоматическом режиме, без участия пользователя. Система будет осуществлять автоматический выход в Интернет, и, при обнаружении свежих обновлений, будет их скачивать и устанавливать на компьютер в соответствии с установленным расписанием (о том, как составлять расписание, мы расскажем чуть ниже). Именно этот вариант автоматического обновления рекомендуется к применению большинству пользователей.

♦ Загружать обновления, но решение об установке принимается мной – данный вариант обновления системы отличается от предыдущего тем, что система автоматически в соответствии с установленным расписанием будет выходить в Интернет и скачивать требуемые обновления, но устанавливать их не будет. Решение об установке (или – об отказе от установки) обновлений будет принимать пользователь при появлении на экране соответствующего запроса.

♦ Искать обновления, но решение о загрузке и установке принимается мной – данный вариант обновления системы отличается от предыдущего тем, что система автоматически в соответствии с установленным расписанием будет выходить в Интернет и искать свежие обновления, но загружать их в компьютер и устанавливать их не будет. Решение о загрузке и установке найденных обновлений будет принимать пользователь при появлении на экране соответствующего запроса.

♦ Не проверять наличие обновлений (не рекомендуется) – при выборе данного значения автоматический поиск обновлений выполняться не будет. Это чревато тем, что возможные ошибки в системе не будут своевременно устранены, а уровень безопасности останется

прежним и не улучшится. Отметим, что в системе безопасности Windows всегда были и будут прорехи (в первую очередь «благодаря» деятельности хакеров и прочих злоумышленников), которые устраняются именно в результате установки соответствующих обновлений (их иногда называют «заплатками»). Если не установить такое обновление – система останется уязвимой для внешних угроз. В первую очередь именно по этой причине разработчики не рекомендуют отключать режим автоматического обновления системы.

Если выбран режим обновления Устанавливать обновления автоматически (рекомендуется), то ниже открываются для редактирования параметры настройки расписания, в соответствии с которым система будет автоматически устанавливать скачанные обновления. Устанавливать обновления можно как ежедневно, так и еженедельно – по указанным дням недели. Что касается времени обновления, то из раскрывающегося списка вы можете выбрать любое время суток. Можно оставить компьютер включенным на ночь, и задать время установки обновлений, например, в 3 часа ночи. Дело в том, что установка обновлений может потребовать дополнительных системных ресурсов, и если это будет выполняться параллельно с работой пользователя на компьютере, возможны проблемы с быстродействием. Если же компьютер свободен, то процесс установки обновлений пройдет быстрее.

Обновления системы могут иметь статус важных, а могут – статус рекомендуемых. Например, обновления, касающиеся безопасности работы системы или устранения ошибок, всегда считаются важными, а касающиеся доработки функциональности могут быть рекомендуемыми. Если вы хотите, чтобы рекомендованные обновления загружались и устанавливались в таком же порядке, как и важные – установите флажок Получать рекомендуемые обновления таким же образом, как и важные обновления.

Если к компьютеру имеют доступ несколько разных пользователей, то имеет смысл разрешить каждому из них устанавливать обновления. Поскольку этот процесс почти всегда автоматизирован (а при выборе рекомендуемого режима обновления он автоматизирован полностью), специфических знаний или наличия каких-то особенных прав доступа для этого не требуется. Чтобы разрешить всем пользователям устанавливать обновления системы, включите параметр Разрешить всем пользователям устанавливать обновления на этот компьютер.

Выполненные настройки автоматического обновления вступают в силу после нажатия в данном окне кнопки ОК. Кнопка Отмена предназначена для выхода из режима настройки без сохранения изменений.

Стоит отметить, что существуют так называемые скрытые обновления. О них система вас не уведомляет, а также не выполняет их автоматическую установку, даже если это предусмотрено настройками. Для повышения степени надежности защиты компьютера, а также улучшения его производительности рекомендуется восстановить все важные и рекомендуемые скрытые обновления. Для перехода в соответствующий режим щелкните на ссылке Восстановить скрытые объявления, которая расположена в левой части окна Центра обновления Windows (см. рис. 2.1). Затем в открывшемся окне нужно путем установки соответствующих флажков выбрать требуемые обновления, и нажать кнопку Восстановить.

Стоит отметить, что некоторые из восстанавливаемых обновлений могут отсутствовать в списке обновлений, предлагаемых системой. Как правило, это случается тогда, когда система находит более новое обновление, устраняющее ту же неполадку, что и

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

обновление, которое пользователь намеревался восстановить.

В операционной системе Windows 7 реализована возможность автоматического ведения журнала обновлений. В нем фиксируется информация о каждом обновлении, и фактически данный документ представляет собой подробный протокол обновлений. Вы можете в любой момент просмотреть его содержимое – для этого щелкните на ссылке Просмотр журнала обновлений, которая расположена в левой части окна Центра обновления Windows (см. рис. 2.1). В результате на экране отобразится окно, которое показано на рис. 2.3.

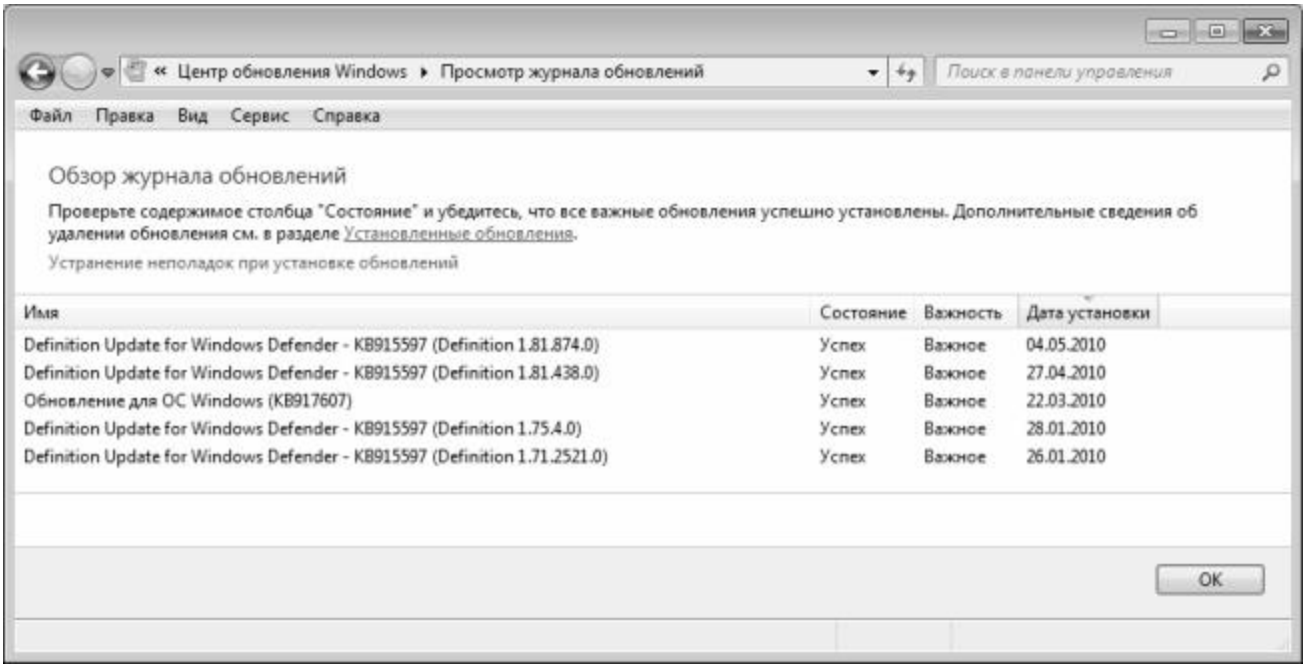



Рис. 2.3. Журнал обновлений

В данном окне представлен список всех выполненных обновлений, начиная с момента установки системы. Для каждой позиции списка в соответствующих колонках последовательно отображается имя обновления, его текущее состояние (если в данной колонке отображается значение Успех, значит обновление успешно установлено), степень важности (например, Важное или Рекомендуемое), а также дата установки.

Чтобы просмотреть более подробную информацию об обновлении, щелкните на соответствующей позиции списка правой кнопкой мыши и в открывшемся контекстном меню выберите команду Подробности. В результате на экране отобразится окно, в котором, помимо прочего, будет содержаться ссылка на страницу в Интернете, где можно просмотреть дополнительные сведения о данном обновлении.

Однако бывают ситуации, когда в силу тех или иных причин установить обновление не удается. Подобные сбои в большинстве случаев носят временный характер и могут быть вызваны перегрузками веб-сайтов и подключений к Интернету, а также иными факторами. Обычно для устранения таких проблем нужно повторно запустить обновление (если у вас включен режим автоматического обновления, то все равно в данном случае нужно будет сделать это вручную).

Для этого нажмите кнопку Проверка обновлений или щелкните мышью на ссылке Поиск обновлений (см. рис. 2.1). Возможно, некоторое время придется подождать – пока

операционная система будет осуществлять поиск новых обновлений. Если таковые будут обнаружены – установите их, утвердительно ответив на соответствующий запрос системы.

ПРИМЕЧАНИЕ

Помните, что в некоторых случаях завершение установки происходит только после перезагрузки компьютера. Перед перезагрузкой закройте все работающие приложения и сохраните текущие данные, поскольку в процессе перезагрузки и завершения установки обновлений возможна потеря несохраненных данных.

Иногда не удается установить обновления по весьма банальной причине – недостатку свободного дискового пространства. В этом случае придется высвободить требуемое количество места путем удаления какой-то ненужной информации, в частности – временных файлов Интернета, содержимого Корзины, прочих ненужных и устаревших данных, а также путем деинсталляции неиспользуемых программных продуктов. Отметим, что в системе Windows 7 предусмотрен штатный механизм очистки жесткого диска. После того как вы освободили место на диске, повторно выполните установку обновлений.

Иногда в процессе скачивания и установки обновлений происходит неожиданный разрыв связи с Интернетом. В этом ничего страшного нет – просто нужно будет при возобновлении связи выполнить повторную проверку наличия обновлений.

Еще одна распространенная проблема – когда компьютер во время установки обновления автоматически выключается в соответствии с установленным для него расписанием. В данной ситуации система начнет автоматическую проверку обновлений сразу после загрузки. Вы можете инсталлировать обновления немедленно или временно отложить их установку. Если компьютер будет включен во время очередного обновления, выполняемого в соответствии с заданным расписанием, то обновления будут установлены автоматически. Если свежие обновления полностью готовы к инсталляции, вы можете установить их непосредственно перед выключением компьютера.

Бывают случаи, когда после установки очередного обновления возникают проблемы с работой тех или иных устройств (это может происходить также после обновления драйвера). Причины этому могут быть разными. Если данное устройство было приобретено вместе с компьютером, сначала следует проверить наличие драйвера у производителя компьютера. Дело в том, что многие производители используют в выпускаемых компьютерах устройства сторонних производителей (в частности, это касается видеоадаптеров и звуковых плат). Иногда производитель дорабатывает и обновляет драйверы для использования с данным компьютером, в то время как сторонний разработчик оставляет прежнюю версию драйвера без изменений. При инсталляции стандартной версии драйвера, даже в том случае, когда она выпущена производителем устройства, могут появляться проблемы.

Еще одна распространенная причина – когда данная версия драйвера несовместима с используемым устройством или компьютером. Нередко изготовители дорабатывают и совершенствуют устройства, не меняя их названия. Бывают ситуации, когда самая свежая версия драйвера инсталлируется без видимых проблем, но впоследствии работает некорректно (или вообще не работает).

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

**Защитник Windows 7**

В состав операционной системы Windows 7 включена программа категории AntiSpyWare, которая называется Защитник Windows.

Функциональные возможности Защитника Windows предусматривают два способа борьбы со шпионским программным обеспечением.

♦ Защита в режиме реального времени. В данном случае Защитник Windows уведомляет пользователя о том, что на компьютер пытается установиться шпионская программа, либо она уже есть и намерена запуститься на исполнение. Аналогичное информационное сообщение появится на экране в случае, когда какой-либо приложение попытается отредактировать важные параметры операционной системы.

♦ Сканирование компьютера в автоматическом режиме.В данном случае Защитник Windows обеспечивает поиск шпионских модулей, которые могли проникнуть в компьютер, планирование регулярных проверок, а также автоматическое удаления шпионского программного обеспечения, найденного в процессе сканирования.

Помните, что эффективность использования Защитника Windows самым непосредственным образом зависит от наличия последних версий определений. В данном случае определения – это, попросту говоря, сигнатурные базы, содержащие постоянно пополняющиеся сведения о потенциально опасных программах. Здесь можно провести аналогию с антивирусными базами, используемыми антивирусными программами. С помощью сигнатурных баз Защитник Windows своевременно распознает опасность и выдает пользователю соответствующее информационное сообщение. Обновление определений происходит автоматически в процессе получения и установки обновлений операционной системы (об этом шла речь в предыдущем разделе). Также вы можете настроить Защитник Windows на поиск обновленных определений в Интернете непосредственно перед началом проверки (о том, как настраивать программу, мы расскажем чуть ниже), либо вручную запускать проверку наличия обновлений тогда, когда посчитаете нужным.

ВНИМАНИЕ

Учтите, что Защитник Windows обеспечивает защиту только от шпионского программного обеспечения, и некоторых подобных вредоносных программ. Он не может использоваться вместо антивирусной программы, поскольку таких функций в нем не заложено.

Как мы уже отмечали ранее, Защитник Windows входит в комплект поставки Windows и инсталлируется на компьютер автоматически вместе с установкой операционной системы. Чтобы запустить программу, наберите в строке поиска меню Пуск запрос Защитник Windows – в результате в верхней части данного меню появится команда для запуска. При ее активизации на экране открывается окно, изображенное на рис. 2.4.

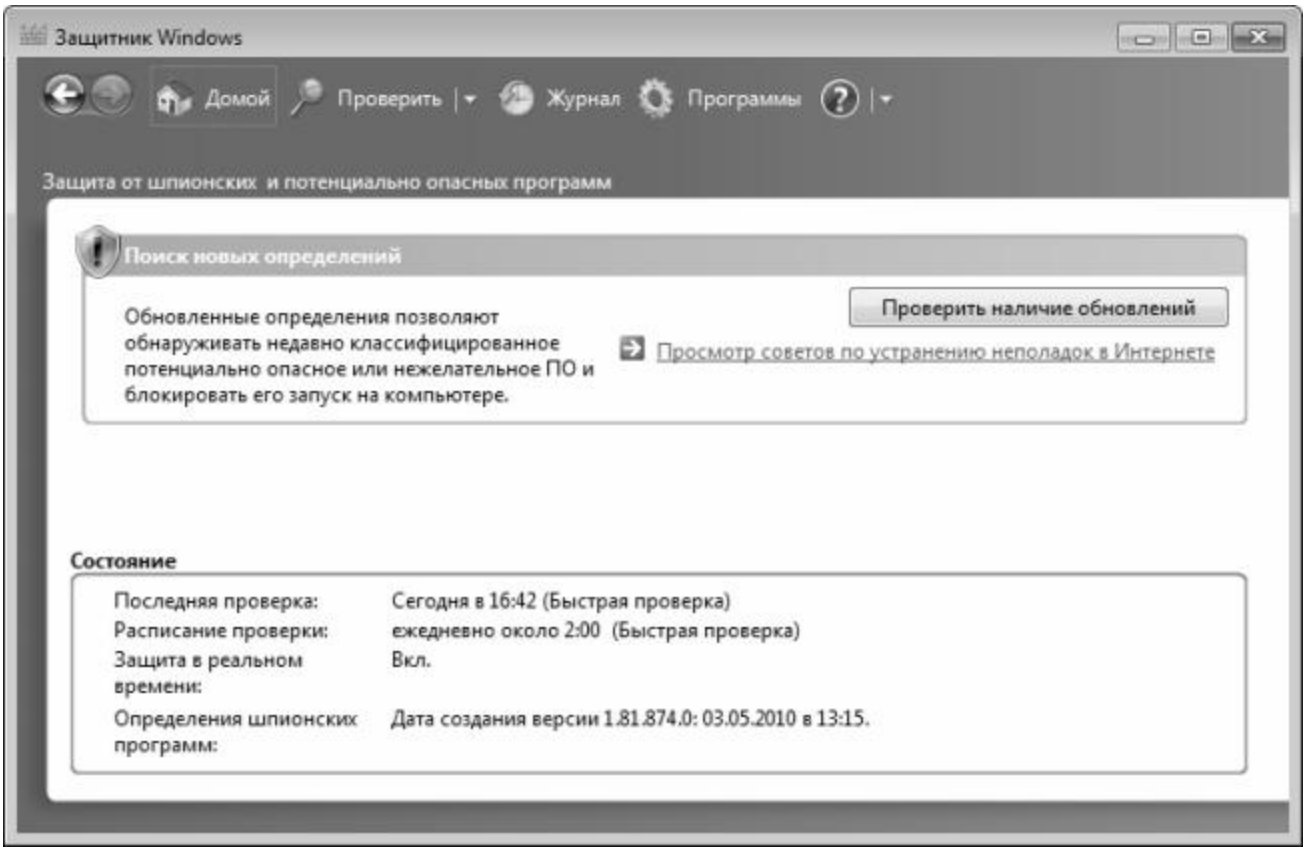



Рис. 2.4. Защитник Windows

Это стартовый интерфейс программы, который открывается по умолчанию. С помощью кнопки Проверить наличие обновлений вы можете в любой момент запустить процесс проверки наличия свежих обновлений сигнатурных баз (определений).

СОВЕТ

Рекомендуется проверять наличие свежих обновлений каждый раз перед запуском проверки – это позволит своевременно актуализировать их содержимое, что, в свою очередь, намного повысит эффективность проверки.

В верхней части окна программы находится главное меню, которое представляет собой перечень ссылок, используемых для выбора режимов работы и активизации соответствующих функций программы. Ссылка Домой открывает стартовый интерфейс программы (см. рис. 2.4), с помощью ссылки Проверить запускается процесс проверки компьютера на предмет обнаружения вредоносных программ. При этом будет использован режим проверки, который используется по умолчанию, а если вы хотите выбрать другой режим проверки – щелкните на стрелочке, расположенной справа от ссылки Проверить, и в открывшемся меню выберите требуемый вариант: Быстрая проверка, Полная проверка или Выборочная проверка.

С помощью ссылки Журнал осуществляется переход в режим просмотра информации обо всех действиях, выполненных над потенциально опасными программами. В частности, они могут удаляться с компьютера, помещаться в карантин, и т. д.

Ссылка Программы предназначена для перехода в режим настройки параметров программы, а также для просмотра помещенных в карантин объектов и дополнительной

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

справочной информации. Поскольку программа фактически функционирует в автоматическом режиме, то грамотная настройка параметров во многом определяет эффективность ее работы.

Чтобы перейти к настройкам программы, щелкните на ссылке Программы, и в открывшемся окне щелкните на ссылке Параметры. В результате на экране отобразится окно, изображенное на рис. 2.5.

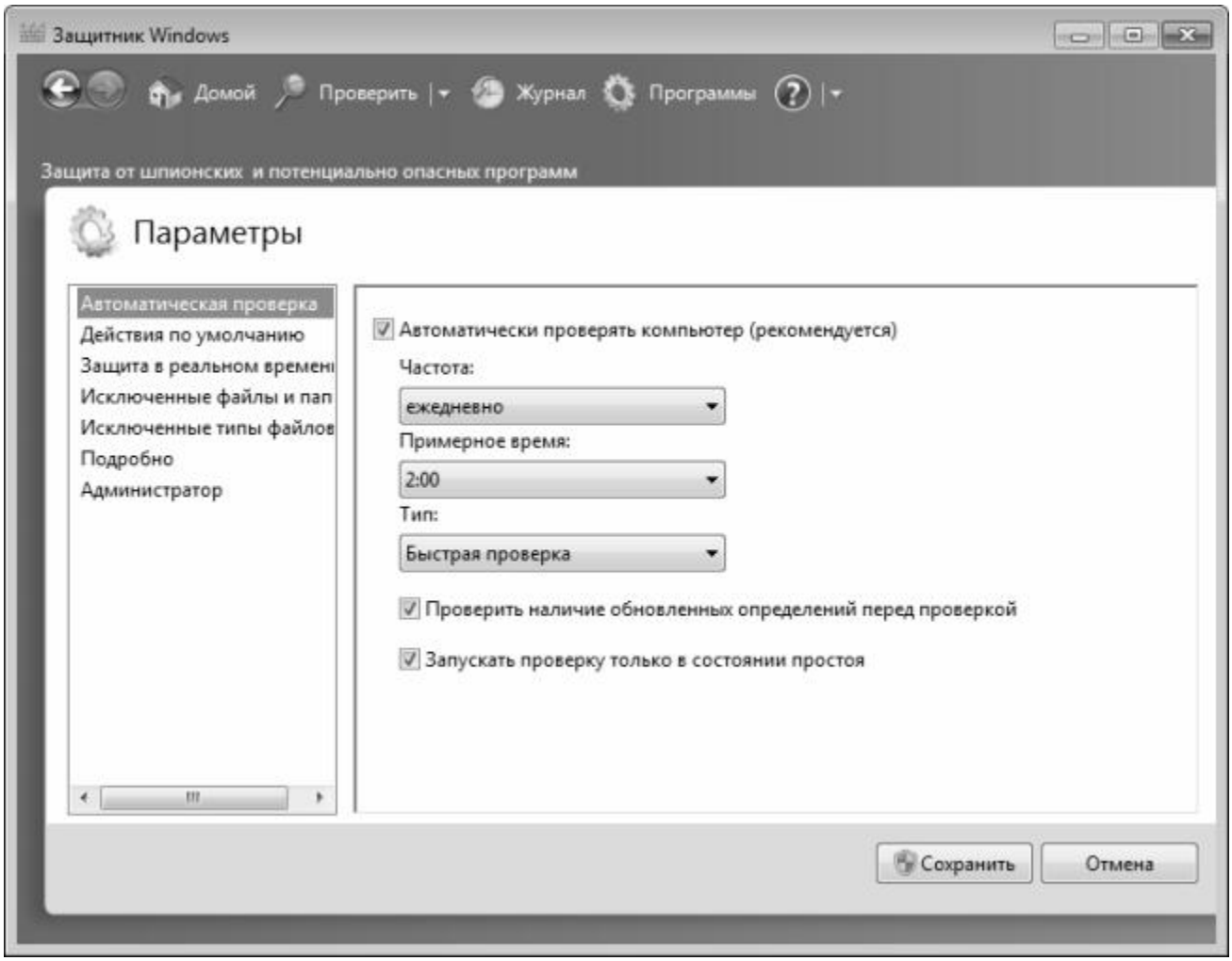



Рис. 2.5. Настройка параметров программы

В левой части данного окна представлен перечень разделов настройки. Каждый раздел содержит однотипные, сходные по назначению и функциональности параметры настройки. Далее мы рассмотрим те их них, которые являются наиболее востребованными для большинства пользователей.

Параметры автоматической проверки компьютера на предмет обнаружения вредоносных программ настраиваются в разделе Автоматическая проверка, содержимое которого показано на рис. 2.5. Если вы хотите, чтобы Защитник Windows автоматически проверял компьютер через определенные промежутки времени, установите флажок Автоматически проверять компьютер (рекомендуется). Учтите, что если данный параметр отключен, то все остальные параметры данного раздела становятся недоступными для редактирования.

В поле Частота из раскрывающегося списка выбирается частота проведения

автоматических проверок. Это можно делать как ежедневно (данный вариант предлагается использовать по умолчанию), так и еженедельно – по указанным дням недели (например, если в раскрывающемся списке выбрано значение понедельник, то автоматическая проверка компьютера будет запускаться каждый понедельник).

В поле Примерное время из раскрывающегося списка выбирается время начала проверки. Например, если в поле Частота выбрано значение понедельник, а в поле Примерное время – значение 15:00, то автоматическая проверка будет начинаться каждый день в 3 часа дня.

В поле Тип из раскрывающегося списка выбирается тип проверки – Быстрая проверка или Полная проверка. В первом случае проверка будет выполнена относительно быстро, но она затронет только основные компоненты, файлы и службы системы. Полная же проверка предусматривает сплошное сканирование всего содержимого компьютера, но она может занять много времени. В целом продолжительность как быстрой, так и полной проверки зависит от ряда факторов (количество установленного на компьютере программного обеспечения, быстродействие и производительность компьютера, и др.).

Ранее мы уже отмечали, что непосредственно перед проверкой рекомендуется проверить наличие обновлений определений (сигнатурных баз). Но если у вас включен режим автоматической проверки компьютера, вы можете автоматизировать и предварительную проверку наличия обновлений – для этого в разделе настройки Автоматическая проверка нужно установить флажок Проверять наличие обновленных определений перед проверкой. По умолчанию данный флажок установлен.

Если установить флажок Запускать проверку только в состоянии простоя, то автоматическая проверка компьютера будет осуществляться только при условии отсутствия активности пользователя (то есть когда мышь и клавиатура находятся в состоянии покоя). Дело в том, что процесс сканирования компьютера требует дополнительных ресурсов, что может сказаться на быстродействии и производительности компьютера. Это особенно актуально для маломощных компьютеров, а также для компьютеров, на которых установлено много разного программного обеспечения. Если во время вашей работы на компьютере начнется автоматическая проверка – это может привести к серьезному замедлению работы вплоть до полной невозможности что-либо делать. В подобных случаях рекомендуется настраивать автоматическую проверку таким образом, чтобы она проводилась, например, в ночное время.

В разделе Действия по умолчанию определяются действия программы по отношению к подозрительным программам в зависимости от степени опасности, которую они представляют.

Всю опасность, которая может исходить от потенциально опасных программ, Защитник Windows делит на три категории: высокий уровень опасности, средний уровень опасности и низкий уровень опасности. Высокий уровень опасности представляют собой программы, которые могут выполнять сбор личных и конфиденциальных сведений, либо причинить вред компьютеру или операционной системе путем, например, изменения параметров системы, причем всегда это делается без ведома и согласия пользователя. Средний уровень опасности исходит от программ, которые могут отрицательно сказаться на сохранности конфиденциальных сведений, а также изменить параметры системы таким образом, что это может стать причиной серьезных проблем с производительностью. Что касается программ, представляющих низкий уровень опасности, то к ним относятся приложения, которые могут выполнять сбор сведений о пользователе или компьютере

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

либо редактировать параметры работы операционной системы, но в то же время работающие в соответствии с лицензионным соглашением, текст которого выводился на экран в процессе их установки.

Для вредоносных программ, представляющих высокий уровень опасности, в разделе Действия по умолчанию из раскрывающегося списка выбирается один из трех возможных вариантов поведения программы:

♦ Рекомендуемое действие на основе определений – в данном случае Защитник Windows примет решение о том, как поступить с вредоносной программой, на основании сведений, содержащихся в сигнатурных базах.

♦ Удалить – при выборе этого варианта подозрительная программа будет немедленно удалена с компьютера. Отметим, что этот вариант является оптимальным для большинства вредоносного программного обеспечения, представляющего высокий уровень опасности.

♦ Карантин – при установленном данном значении подозрительная программа будет автоматически помещена в карантин. При этом она не будет удалена с компьютера, то будет полностью обезврежена.

Что касается приложений, представляющих средний и низкий уровень опасности, то для них, помимо перечисленных вариантов, имеется также вариант Разрешить. В данном случае Защитник Windows проигнорирует данное приложение (то есть распознает его как безвредное), и оно сможет функционировать в штатном режиме.

Если в нижней части раздела установлен флажок Применить рекомендуемые действия, то для всех видов вредоносного программного обеспечения, независимо от степени исходящей опасности, Защитник Windows по умолчанию будет применять вариант Рекомендуемое действие на основе определений.

В разделе Зашита в режиме реального времени осуществляется настройка работы программы по обеспечению защиты компьютера от вредоносного программного обеспечения в режиме он-лайн. Данный раздел включает в себя три флажка, которые перечислены ниже.

♦ Использовать защиту в режиме реального времени (рекомендуется) – при включении этого параметра включается режим защиты компьютера в режиме он-лайн. Отметим, что остальные параметры раздела становятся доступными для редактирования только при установленном данном флажке.

♦ Проверка загруженных файлов и вложений – если установлен это флажок, то Защитник Windows будет в режиме он-лайн проверять все уже загруженные файлы и вложения.

♦ Проверять выполняемые на компьютере программы – при включении этого параметра Защитник Windows будет проверять в режиме он-лайн все выполняемые в данный момент приложения.

По умолчанию все перечисленные флажки установлены, что обеспечивает постоянную защиту компьютера в режиме реального времени.

В разделе Исключенные файлы и папки можно сформировать список исключений. В этот список вносятся каталоги и файлы, которые Защитник Windows в процессе проверки сканировать не должен. Это позволяет исключить из области проверки объекты, которые заведомо не представляют опасности, благодаря чему можно сократить продолжительность проверки.

Чтобы добавить объект в список исключений, нажмите кнопку Добавить. В результате

на экране откроется окно Обзор файлов и папок, в котором нужно указать путь к объекту, исключаемому из области проверки. Это может быть, например, исполняемый файл программы, какой-либо каталог, или раздел жестко диска.

Чтобы удалить объект из списка исключений, выделите его щелчком мыши и нажмите кнопку Удалить. При этом соблюдайте осторожность, поскольку программа не выдает дополнительный запрос на подтверждение операции удаления.

Можно сформировать также список исключений по типам файлов. Например, вы можете указать, что файлы с расширением *.doc и *.txt в процессе проверки следует игнорировать. Для формирования списка исключений по типам файлов перейдите в раздел Исключенные типы файлов.

Чтобы добавить тип файла в список исключений, введите с клавиатуры его расширение и нажмите кнопку Добавить. Если системе знаком такой тип файла, то в списке для него автоматически появится соответствующее краткое описание. Например, для файла с расширением *.doc система сформирует подсказку Документ Microsoft Word, и т. д.

Чтобы удалить тип файла из списка исключений, выделите его в списке щелчком мыши и нажмите кнопку Удалить. При этом будьте внимательны, поскольку он сразу будет удален, без дополнительного предупреждения.

В разделе Подробно выполняется настройка ряда дополнительных параметров Защитника Windows. Здесь содержатся перечисленные ниже флажки.

♦ Проверять архивные файлы – если установлен этот флажок, то поиск вредоносных объектов будет осуществляться также в архивных файлах (RAR, ZIP, CAB и др.).

♦ Проверять сообщения электронной почты – при установленном данном флажке Защитник Windows будет проверять все почтовые сообщения, включая вложения.

♦ Проверять съемные носители – в данном случае Защитник Windows будет осуществлять поиск вредоносных объектах в том числе и на съемных носителях информации (флэш-память, компакт-диск, и др.).

♦ Использовать эвристику – с помощью данного флажка включается механизм эвристического анализа. В данном случае Защитник Windows будет относить к вредоносным программам те приложения, которые не только полностью, но и частично соответствуют имеющимся определениям.

♦ Создать точку восстановления – в данном случае перед каждым действием применительно к обнаруженному вредоносному объекту (удаление, помещение в карантин и др.) система будет автоматически создавать контрольную точку восстановления. О том, что представляют собой контрольные точки восстановления и для чего они нужны, будет рассказано ниже, в главе, посвященной обслуживанию системы и компьютера.

По умолчанию в данном разделе установлены все флажки, кроме Проверять сообщения электронной почты и Проверять съемные носители.

В разделе Администратор можно настроить некоторые параметры администрирования Защитника Windows. Здесь содержится два флажка: Использовать эту программу и Показать элементы всех пользователей компьютера.

Если вы хотите защитить свой компьютер от шпионского программного обеспечения, установите флажок Использовать эту программу. В этом случае Защитник Windows будет оповещать вас обо всех попытках запуска или установки на данном компьютере шпионского программного обеспечения или иных подобных программ. При снятом данном флажке защита работать не будет.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Параметр Показать элементы всех пользователей компьютера позволяет управлять конфиденциальностью пользователей в части защиты от шпионского программного обеспечения. Если этот флажок установлен, то можно будет просматривать журнал, список помещенных в карантин объектов, а также список исключений для всех пользователей системы. Если же данный параметр отключен, то можно будет просматривать эти данные только для текущего пользователя.

По умолчанию флажок Использовать эту программу установлен, а флажок Показать элементы всех пользователей компьютера – снят.

Все изменения, выполненные в окне настройки параметров программы, вступают в силу после нажатия кнопки Сохранить. Кнопка Отмена предназначена для выхода из данного режима без сохранения выполненных изменений. Эти кнопки доступны во всех разделах окна настройки программы.

Как мы уже отмечали ранее, возможности программы предусматривают проведение проверок трех типов: быстрая, полная и выборочная. Требуемый вариант выбирается в меню, которое открывается нажатием стрелочки, расположенной рядом со ссылкой Проверить. При выборе быстрой или полной проверки процесс сканирования начинается сразу. Если же выбран вариант Выборочная проверка, то на экране открывается окно, изображенное на рис. 2.6.

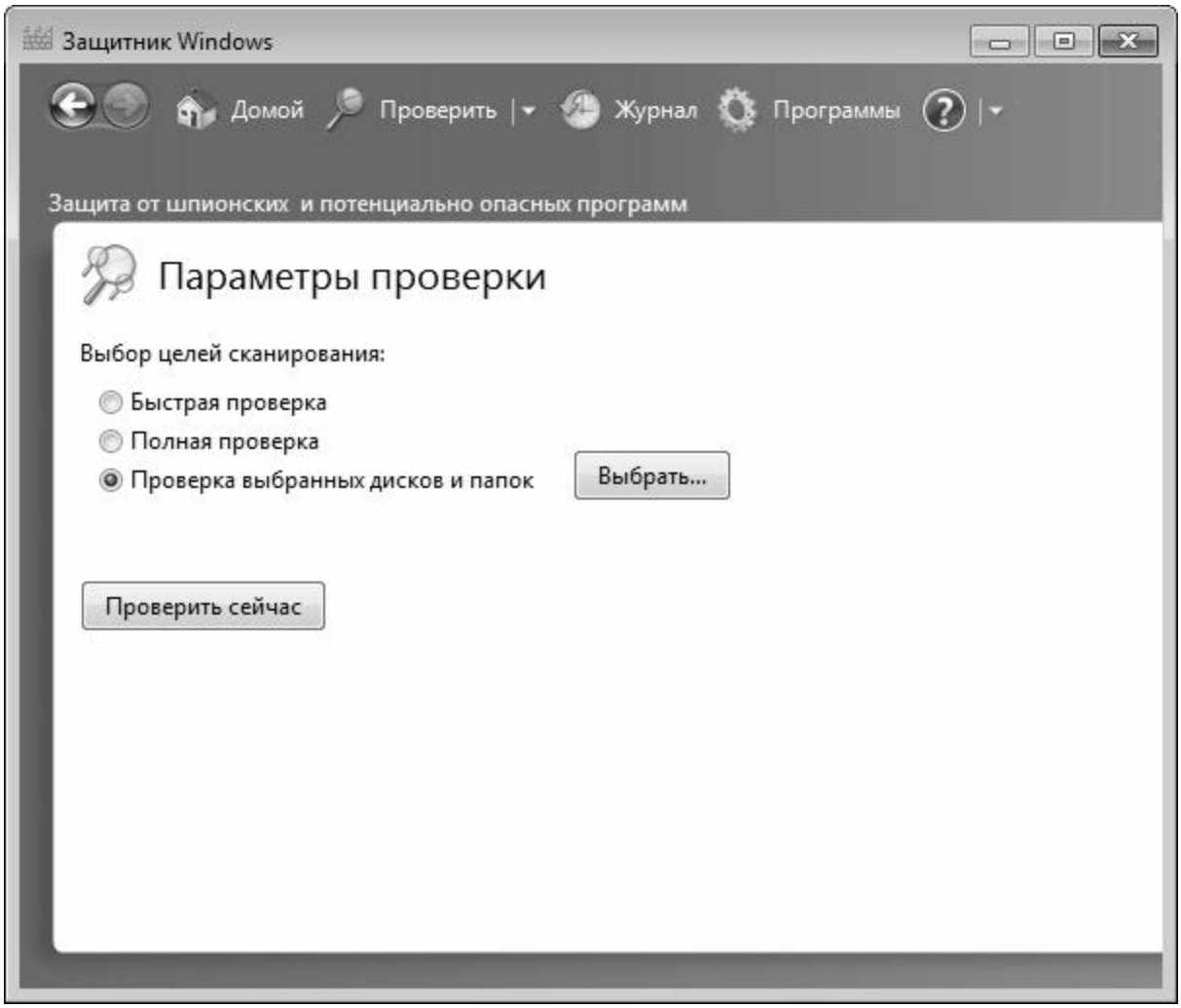



Рис. 2.6. Выборочная проверка

Смысл выборочной проверки заключается в том, что Защитник Windows будет сканировать только те объекты, которые указал пользователь. Поэтому в данном окне нужно установить переключатель в положение Проверка выбранных дисков и папок, и нажать расположенную справа кнопку Выбрать. В результате на экране откроется окно, в котором путем установки соответствующих флажков нужно выбрать объекты для проверки и нажать кнопку ОК. Чтобы запустить процесс выборочной проверки немедленно, нажмите кнопку Проверить сейчас.

**Прочее программное обеспечение для борьбы с компьютерным шпионажем**

В завершение темы компьютерного шпионажа кратко рассмотрим две популярные утилиты, специально предназначенные для поиска и удаления шпионских модулей. Следует учитывать, что каждую из них необходимо периодически обновлять – по аналогии с антивирусными программами.

**Программа SpywareBlaster**

Одним из эффективных антишпионских средств по праву считается программа SpywareBlaster, разработчиком которой является фирма JavaCoolSoftware. Она предназначена для использования в операционных системах Windows любой версии, начиная с Windows 95.

Программа отличается эргономичным и в то же время простым и интуитивно понятным пользовательским интерфейсом, в котором большинство параметров настраиваются путем установки/снятия соответствующих флажков либо переключателей. Среди всего многообразия параметров работы программы особо следует отметить возможность блокировки настроек домашней страницы (в результате чего уже ни один шпионский модуль не сможет изменить, например, адрес страницы, загружаемой по умолчанию). Также в программе реализована возможность создания «отката» для настроек интернет-обозревателя (кстати, данная утилита поддерживает работу не только с Internet Explorer, но и с другими популярными интернет-обозревателями – в частности, Netscape, Mozilla). В данном случае достаточно зафиксировать текущие настройки интернет-обозревателя (причем можно сохранить несколько различных конфигураций настроек), и при необходимости вернуться к ним в любой момент (обычно – при возникновении подозрений на то, что в настройки интернет-обозревателя без участия пользователя внесены нежелательные изменения).

Кроме упомянутых выше, программа SpywareBlaster имеет еще ряд интересных возможностей.

**Программа AVZ**

Еще одна полезная утилита для борьбы со шпионскими модулями – программа AVZ, которая распространяется бесплатно. Многие пользователи считают ее одной из лучших

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

программ для поиска и удаления не только программ-шпионов, но и рекламных модулей (о них мы поговорим ниже). Кстати, помимо борьбы со шпионскими и рекламными модулями, эта программа успешно борется и с некоторыми вирусами.

Русскоязычный интерфейс программы удобен и понятен пользователю. Предварительная настройка AVZ проста, причем во многих случаях параметры, предложенные по умолчанию, являются оптимальными. Для каждого типа вредоносного объекта, который был обнаружен в процессе сканирования (вирус, программа-шпион и др.), можно указать, каким образом с ним поступить: удалять, выдать только отчет, и др. Кроме этого, можно настроить сканирование на выборочный поиск вредоносных программ – например, искать и удалять только шпионские модули, а все остальное игнорировать.

В программе автоматически ведется протоколирование процесса сканирования. Полученный протокол при необходимости можно сохранить в отдельном файле для последующего изучения.

**Борьба с рекламными модулями Adware**

Помимо вирусов, модулей SpyWare и прочего вредоносного софта в настоящее время широко распространены так называемые рекламные модули – Adware. Они, в отличие от компьютерных вирусов, не вредят компьютеру и хранящимся в нем данным, и не ведут шпионской деятельности, подобно SpyWare. Задача рекламных модулей заключается в рекламировании товаров и услуг, предлагаемых разными фирмами и организациями, путем навязчивой демонстрации рекламных материалов (баннеров, popup-окон, ссылок и т. п.) пользователям.

**Проникновение Adware в компьютер**

Рекламные модули могут проникать в компьютер в процессе установки некоторых бесплатных программ; иногда это является главным условием возможности эксплуатации устанавливаемой программы. Это был один из основных способов распространения первых Adware. Причем нередко в процессе инсталляции пользователю сообщалось о том, что такое Adware и с какой целью он включен в дистрибутив программы (например, Установка данного модуля является платой за использование программы). В наиболее «продвинутых» программах пользователю при инсталляции даже предлагалось выбрать вариант использования программы – бесплатно с рекламным модулем Adware либо на платной основе. При деинсталляции программы вместе с ней удалялся и рекламный модуль.

Однако в настоящее время Adware такими цивилизованными способами уже почти не распространяются. Нередко рекламный модуль устанавливается на компьютер даже после того, как пользователь от этого отказался. Попавший в компьютер рекламный модуль нелегко обнаружить и удалить (для этого нужно использовать специально разработанные

утилиты, о которых будет рассказано ниже). Если Adware проник в компьютер в процессе инсталляции какой-то программы, то при ее удалении уже и речи не идет о том, чтобы такой вместе с ней удалился рекламный модуль.

Рекламные модули, созданные с применением современных технологий, по умению проникнуть в компьютер и вести там свою деятельность сравнимы с «троянскими конями» и иными современными вирусами. Самые «продвинутые» Adware способны вступать в своего рода «схватки» с конкурентами, которые ранее проникли в компьютер, и уничтожать их. При этом пользователь может ничего не подозревать о подобных «сражениях» и иной бурной деятельности, которую ведут рекламные модули в его компьютере. И лишь периодически появляющаяся реклама, раздражающая с каждым разом все сильнее и сильнее, наводит пользователя на мысли, что, видимо, кто-то в его компьютере все-таки «прижился».

Каким же образом действуют рекламные модули? Все зависит от их направленности, а также от фантазии разработчика. Например, весьма раздражает пользователей появление всплывающих рекламных popup-окон. Как правило, они появляются именно тогда, когда их хочется видеть меньше всего. Созданные с применением передовых технологий рекламные popup-окна трудно убрать с экрана, и нередко они перемещаются по странице при ее «прокрутке» вместе с остальным содержимым.

Разновидностью рекламных popup-окон являются переходные и дополнительные окна. Переходные окна появляются после щелчка мышью на какой-либо ссылке и отображаются до открытия следующего окна, а дополнительные показываются между двумя информационными окнами.

Одним из видов навязчивой рекламы является автоматическое размножение окон интернет-обозревателя, в каждом из которых загружается определенная веб-страница.

Некоторые рекламные модули выводят на экран рекламу, которую невозможно убрать с помощью кнопок Назад либо Закрыть, поскольку эти кнопки оказываются заблокированными. В данном случае приходится либо закрывать окно с рекламой нажатием комбинации клавиш Alt+F4, либо снимать соответствующую задачу в окне Диспетчера задач.

Неприятной особенностью многих Adware является то, что реклама на экране может появляться даже при отсутствии действующего подключения к Интернету. В подобных случаях Adware проникает в компьютер из внешнего носителя или из Интернета, и активизируется в соответствии с заложенным в него расписанием (например, при каждой загрузке операционной системы, или при каждом запуске Интернет-обозревателя, и т. д.). Иногда ситуация осложняется тем, что убрать рекламное окно с экрана вы не сможете, и пользователь вынужден ждать, пока оно не исчезнет само (обычно терпеть приходится несколько минут). Бывает, что в рекламном окне присутствует счетчик, на котором отсчитывается время до конца демонстрации, а рядом находится текст с предложением отправить СМС-сообщение на указанный номер, чтобы получить ключ для удаления этого Adware. Причем где-нибудь в углу мельчайшими, едва заметными буквами будет дополнение, что для получения ключа надо отправить не одно, а три (пять, десять и т. д.) СМС-сообщений. Стоит ли говорить, что даже после этого ключ для удаления рекламы никто не вышлет!

В подобных ситуациях стоит не отправлять мошенникам СМС, а выйти в Интернет и найти противоядие там. Как правило, достаточно ввести в поисковике запрос с кратким описанием проблемы (например, Как убрать с экрана рекламу секс-шопа, и т. п.) – и в

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

результатах поиска наверняка можно будет найти ответ. В частности, автор этих строк нашел вариант решения подобной проблемы на http://otvet.mail.ru – пользователь, уже столкнувшийся с этой проблемой, прямо указал, где в компьютере «прописался» рекламный модуль. После удаления соответствующих файлов проблема была решена.

**Нейтрализация и удаление рекламных модулей**

Иногда можно попытаться самостоятельно найти и обезвредить рекламный модуль – для этого можно использовать примерно те же методы, что и для поиска SpyWare. Однако это не всегда эффективно, поэтому проще решить проблему с помощью специализированного программного обеспечения.

Но учтите, что Adware (как, собственно, и Spyware), трудно обнаружить и уничтожить с помощью антивирусных программ. Несмотря на то, что некоторые разработчики антивирусного софта включают в свои продукты функции для борьбы с рекламными модулями, целесообразнее использовать для этого специально разработанные утилиты, которые во множестве представлены в Интернете.

Например, многофункциональная программа Ad-aware, разработчиком которой является немецкая компания Lavasoft, представляет собой мощную утилиту для обнаружения и удаления различного рода вредоносных программ, и в том числе – рекламных модулей. Следует отметить, что в настоящее время она является одной из самых популярных программ подобного рода. Достоинство программы – то, что у нее имеется бесплатная версия; единственное ограничение, которое присутствует в бесплатной версии – защита компьютера в режиме мониторинга. Немаловажным является и то, что программа поддерживает русский язык.

В процессе сканирования Ad-aware проверяет содержимое оперативной памяти, системного реестра, а также настройки и содержимое Internet Explorer.

Утилита отличается простым, эргономичным и дружественным интерфейсом, что делает ее доступной даже начинающим пользователям.

Основное предназначение программы Spybot Search & Destroy – поиск и уничтожение с компьютера шпионских и рекламных модулей. Кроме этого, в ней реализована возможность очистки временных файлов Интернета и cookies, а также удаления информации о предыдущем использовании компьютера. Программа распространяется бесплатно и, помимо русского, поддерживает еще около 30 языков.

В Spybot Search & Destroy реализован механизм гибкой настройки параметров сканирования. В частности, можно установить выборочное сканирование – например, искать только рекламные модули Adware, а шпионские модули и прочие вредоносные программы – игнорировать. Кроме этого, средства программы позволяют запомнить текущее состояние настроек системы и в последующем выполнить откат к одному из предыдущих состояний (для устранения последствия пребывания вредоносных программ).

Особо следует отметить возможность программы отслеживать загружаемые из Интернета файлы, что позволяет выявить вредоносные модули еще до проникновения их в компьютер.

Программа NoAdware помогает избавиться не только от рекламных модулей, но и еще

от целого ряда вредоносных программ. К достоинствам программы можно отнести ее быстродействие и простоту в использовании; к недостаткам – отсутствие русскоязычного интерфейса (правда, в Интернете можно найти к ней русификатор), а также то, что иногда она обнаруживает не все Adware. К тому же новая версия утилиты не выходила уже пару лет. В процессе сканирования осуществляется проверка системного реестра и локальных дисков компьютера. При необходимости можно выборочно проверить только те объекты, которые вызывают подозрение. В программе реализована возможность ручного либо автоматического обновления сигнатурных баз.

Программа Нетчарт Фильтр (http://netchart.ru) предназначена для блокировки рекламы и всплывающих окон. Ее хватает, чтобы полностью блокировать большую часть порнорекламы и другой рекламы сайтов сомнительного содержания. Примечательно, то, что фильтр не требует настройки, а его база данных автоматически и регулярно обновляется. Программа препятствует самопроизвольному открытию сайтов, позволяет уменьшить входящий трафик, тем самым снизив расходы на Интернет, не позволяет вирусам и злоумышленникам завладеть вашей персональной информацией.

Программа HtFilter (http://www.tmeter.ru) представляет собой программ-фильтр, который ограждает пользователя от ненужных ему веб-запросов. В итге баннерная реклама, счетчики, ненужные логотипы отсеиваются и не отображаются на вашем компьютере, что в итоге существенно экономит Интернет-трафик и уменьшает время загрузки веб-контента. Удобно то, что программа HtFilter может работает с любым типом браузера, поддерживает любой менеджер закачки файлов. К тому же не требуется никакой предварительной настройки как браузеров, так менеджеров закачек. Утилита может выявлять программы, производящие запросы без ведома пользователя, работает в невидимом для операционной системы режиме, ведет журнал всех запросов, исходящих с пользовательского компьютера.

С помощью программы ATGuard (http://www.atguard.com) вы сможете вырезать ненужную рекламу, блокировать всплывающие окна и отслеживает сетевые подключения. Если вдруг на ваш компьютер будет произведена вирусная атака из глобальной сети, то программа не только выдаст сообщение об этом, но и предложит вариант устранения этой неприятности. Аналогично программа поступит и в тех случаях, когда какая-либо программа будет производить попытку выйти в Интернет. ATGuard может избирательно блокировать потенциально опасные сценарии JavaScript и ActiveX, а также ведет подробную статистику и журнал активности.

## Спам и методы избавления от него

Трудно найти в настоящее время пользователя, который бы не был наслышан о проблеме спама. Что же представляет собой спам, откуда он берется, как его распознать и как можно от него защититься?

### Что такое спам?

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Спам представляет собой один из видов навязчивой рекламы, который распространяется по электронной почте. Справедливости ради нужно отметить, что, вообще-то, примерно 95 % любой рекламы – это назойливая, надоедливая, раздражающая и бесполезная реклама. Характерной особенностью спама является то, что он проникает в личную сферу деятельности человека – в электронную почту, и не просто проникает, а специально придуман и разработан именно для этого, поэтому отгородиться от него достаточно сложно. От телевизионной рекламы можно избавиться, переключившись на другой канал, в газете ее можно просто игнорировать, но если реклама попала в почтовый ящик – скорее всего, с ней придется ознакомиться хотя бы мельком, зачастую лишь для того, чтобы убедиться, что это не какое-то важное почтовое сообщение. А если пользователь открыл спамерское письмо – значит, спамер уже достиг своей цели.

В настоящее время размеры распространяемого спама превысили все разумные пределы. По разным оценкам, от 80 % до 95 % мировой электронной почты составляет спам.

Откуда же берется спам? Рассылкой спама занимаются конкретные люди, именуемые спамерами. За определенное вознаграждение они рассылают информацию, которую предоставил заказчик (эта информация носит рекламный характер), по миллионам электронных адресов. В качестве заказчиков спама выступают продавцы товаров, работ, услуг, в последнее время – даже политические деятели, продвигающие свои идеи.

Откуда же спамеры берут такое количество электронных адресов? На этот вопрос есть несколько ответов, и по мере их рассмотрения мы будем давать рекомендации – каким образом можно сберечь свой электронный адрес от попадания к спамерам.

Во-первых, даже начинающий спамер включит в свои базы данных наиболее популярные электронные адреса. К наиболее популярным и распространенным относятся те адреса, в которых в качестве логина используются распространенные имена: sasha, masha, petr, lena и т. д. и т. п., и которые открыты на известных Интернет-порталах: www.yandex.ru, www.mail.ru, www.rambler.ru и т. д. Для примера станем на место спамера и прикинем, сколько электронных адресов можно получить только из одного имени – sasha.

Итак, вначале будем отталкиваться от популярных почтовых сервисов и получим следующие электронные адреса: sasha@yandex.ru, sasha@mail.ru, sasha@rambler.ru, sasha@inbox.ru, sasha@narod.ru. Наверное, для примера достаточно, хотя подобным образом можно легко собрать еще пару десятков адресов. Теперь к каждому имени добавим 2010 год – например, sasha2010@mail.ru, sasha2010@mail.ru и т. д. Без боязни ошибиться, можно аналогичным образом включить в базу электронные адреса с номерами годов 2000–2009, например: sasha2000@mail.ru, sasha2007@mail.ru, sasha2009@yandex.ru и т. д. Несложно подсчитать, что, проявив определенную фантазию, на основании только одного имени sasha можно придумать несколько сотен электронных адресов. Кроме этого, большинство имен могут принимать разные формы. Например, если мы создали электронные адреса с именем sasha, то несложно придумать аналогичные адреса и с именем alexander – alexander@mail.ru, alexander2008@yandex.ru, alexander2005@mail.ru, и т. д.

Итак, первая рекомендация, которая поможет защитить свой почтовый ящик от спамеров: к выбору логина (имени почтового ящика) следует подойти творчески, избегая простых и очевидных вариантов.

Во-вторых, в поисках новых электронных адресов спамеры регулярно просматривают соответствующие Интернет-ресурсы: бесплатные доски объявлений, различного рода

форумы, чаты, и т. д. Разумеется, они это практически никогда не делают вручную, а в основном с помощью специальных программ-сканеров (такую программу запускают в Интернет, и через некоторое время она собирает приличную базу данных электронных адресов, взятых из открытых источников). Исходя их этого – вторая рекомендация: не следует оставлять свой электронный адрес в различных Интернет-ресурсах в открытом виде. При подаче объявлений следует использовать опцию Скрыть адрес от спамеров; на разных досках объявлений эта опция может называться по-разному, но суть везде одинакова: при публикации объявления для связи с его подателем будет указан не конкретный электронный адрес, а ссылка вроде Написать письмо либо что-то подобное. В этом случае программы-сканеры не обнаружат электронный адрес, а для связи с подателем объявления достаточно будет щелкнуть мышью на этой ссылке. Если же подобная возможность отсутствует, а адрес оставить все равно нужно, можно прибегнуть к такой хитрости: вместо символа @ вставить другой символ либо просто слово собака, например, sasha%mail.ru или petrСобакаmail.ru. В настоящее время все понимают, что адрес представлен в таком виде с целью защиты от спамеров, и путаницы не возникнет.

В-третьих, спамер всегда рад получить любой ответ на свое послание. Это является подтверждением того, что данный почтовый ящик действителен – а подобная информация всегда ценится у спамеров. Поэтому – следующая рекомендация: даже если вам очень хочется ответить на спамерское письмо «парой ласковых», не стоит этого делать – ваш почтовый ящик после этого будет забит спамом постоянно.

Каким же образом можно распознать спамерское письмо в общем списке электронной корреспонденции?

Очень часто у спамерских писем вместо обратного адреса отображается бессмысленный набор символов либо заведомо нереальный адрес (например, из несуществующей доменной зоны). Кроме этого, в поле Тема может быть все, что угодно, кроме того, что ожидает увидеть получатель письма – например, рекламный текст, либо бессмысленный набор символов, либо слова вроде Срочно, Важно и т. п. Кроме этого, спамерское письмо может быть замаскировано под ответное почтовое сообщение (текст в поле Тема начинается с Re: или Re(1), или Re(4) и т. д.).

В настоящее время антиспамовая защита, применяемая в популярных почтовых сервисах (в первую очередь здесь следует отметить www.yandex.ru, www.mail.ru и www.rambler.ru), имеет достаточно высокий уровень. Причем пользователь может сам определить – удалять сразу подозрительные письма или помещать их в папку Рассылки либо Спам (необходимые действия выполняются на почтовом сервере, в режиме настройки своего почтового ящика). При этом очистка папок Рассылки либо Спам от накопившегося мусора выполняется одним щелчком мыши, что довольно удобно.

**Программы, позволяющие избавиться от спама**

Рассмотрим несколько небольших, но эффективных утилит, которые специально разработаны и созданы для избавления от спама.

**E-mail Remover**

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Программа E-mail Remover распространяется бесплатно; скачать ее можно в Интернете по ссылке http://www.antispam.ru/files/e-remover/setup24.exe. Интерфейс E-mail Remover англоязычный, однако это не является существенным недостатком, поскольку порядок работы с утилитой прост и интуитивно понятен.

Чтобы установить программу, запустите инсталляционный файл и следуйте указаниям Мастера установки.

Интерфейс программы E-mail Remover представлен на рис. 2.7.

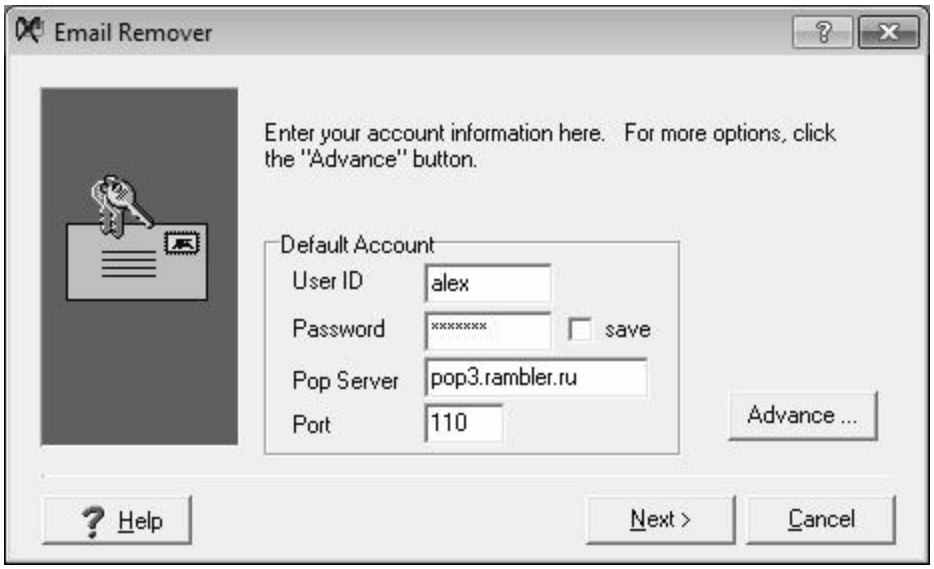



Рис. 2.7. Программа E-mail Remover

В данном окне в полях User ID и Password следует с клавиатуры ввести соответственно имя пользователя и пароль, используемые для доступа к почтовому ящику. Если установить расположенный справа флажок Save, то программа запомнит введенные данные, и впоследствии их не нужно будет каждый раз набирать после запуска программы.

В поле Pop Server с клавиатуры вводится адрес pop-сервера, а в поле Port – номер порта. По умолчанию в поле Port установлено значение 110, и в большинстве случаев данное значение является оптимальным.

После заполнения всех перечисленных параметров нужно подключиться нажать кнопку Next (предварительно подключившись к Интернету) – в результате программа начнет соединение с ящиком на почтовом сервере. Через некоторое время на экране откроется окно с перечнем почтовых сообщений, которые находятся в данный момент в почтовом ящике. В данном окне следует пометить ненужные сообщения (спам), после чего удалить их нажатием кнопки Next. При этом программа выдаст дополнительный запрос на подтверждение операции удаления.

С помощью кнопки Advance осуществляется переход в режим настройки дополнительных параметров работы программы. В частности, здесь можно сформировать список из нескольких почтовых ящиков, с которыми будет работать программа, и указать ящик, который должен использоваться по умолчанию.

**Easy Antispammer**

Здесь мы познакомимся с еще одной утилитой, предназначенной для борьбы со спамом, которая называется Easy Antispammer. Данная программа является бесплатной; ее можно скачать в Интернете по ссылке http://www.cyborghome.ru/download/antispammer/EasyAntispammer.zip.

Программа не требует инсталляции, и сразу после запуска исполняемого файла открывается ее главный интерфейс, который показан на рис. 2.8.

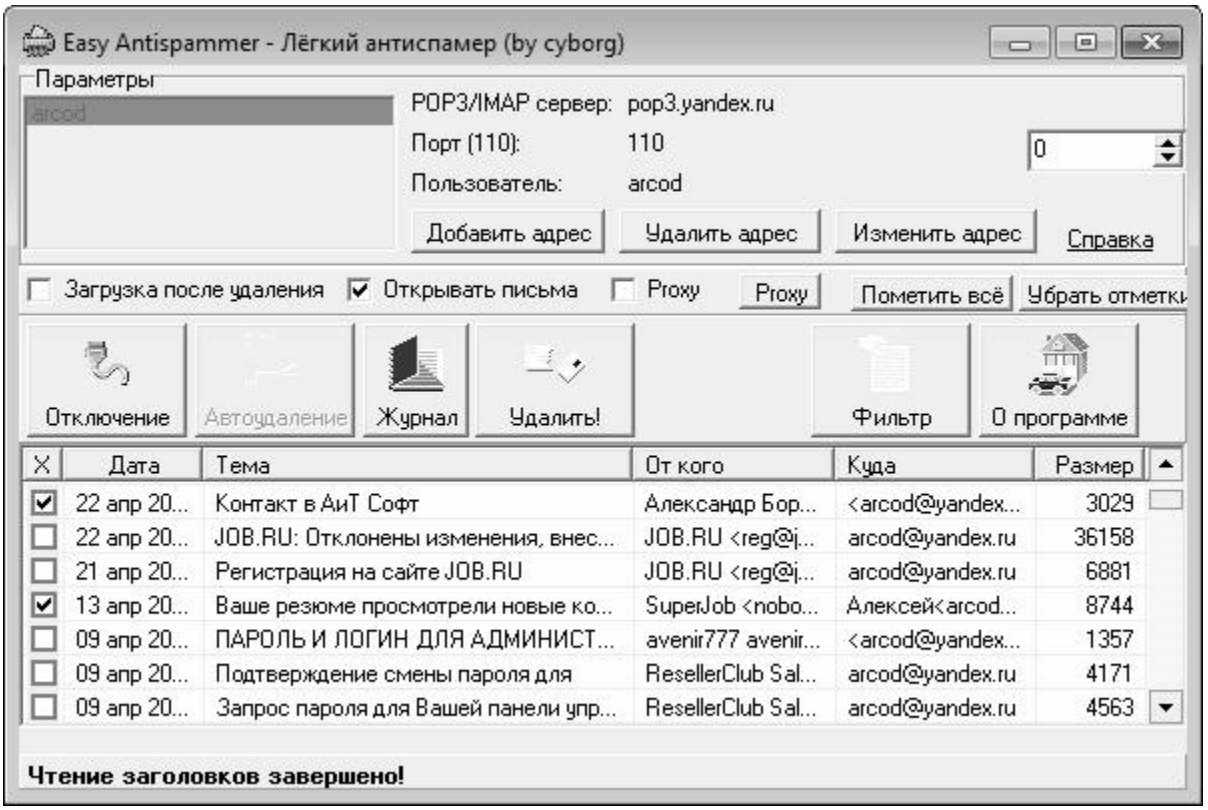



Рис. 2.8. Программа Easy Antispammer

В первую очередь необходимо указать основные параметры почтового ящика (либо – нескольких почтовых ящиков), с которыми будет работать программа. Для этого нужно в главном окне (см. рис. 2.8) нажать кнопку Добавить адрес – в результате на экране откроется окно, изображенное на рис. 2.9.

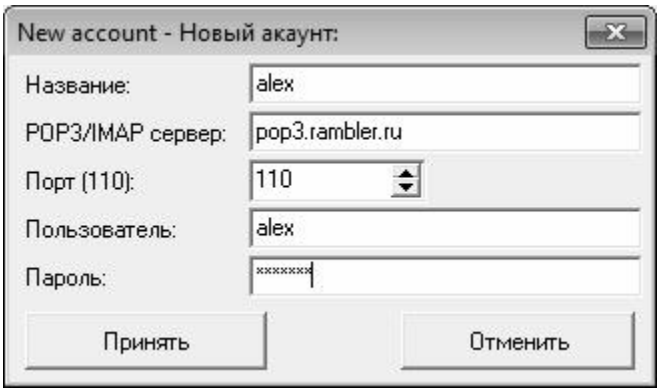



Рис. 2.9. Добавление адреса для обработки почты

В соответствующих полях данного окна последовательно указывается следующая

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

информация: имя создаваемого соединения (произвольное значение, предназначенное для идентификации данного соединения в списке аккаунтов), адрес POP3 либо IMAP сервера, номер порта (по умолчанию используется порт 110), а также имя пользователя и пароль, используемые для доступа к почтовому ящику. После заполнения всех перечисленных параметров в данном окне нужно нажать кнопку Принять – в результате созданный аккаунт отобразится в списке аккаунтов, который находится в левом углу главного окна программы (см. рис. 2.9). При необходимости впоследствии можно изменить параметры любого аккаунта – для перехода в соответствующий режим нужно выделить его в списке курсором и нажать кнопку Изменить адрес. С помощью кнопки Удалить адрес осуществляется удаление из списка выделенного курсором аккаунта. При этом следует соблюдать осторожность, поскольку программа не выдает дополнительный запрос на подтверждение операции удаления.

Чтобы соединиться с почтовым ящиком и просмотреть его содержимое, нужно выделить щелчком мыши требуемый аккаунт и нажать кнопку Соединение. После установления соединения в нижней части окна отобразится список почтовых сообщений, находящихся в почтовом ящике. Для каждой позиции списка в соответствующих колонках отображается дата почтового сообщения, его тема, наименование отправителя и получателя, а также размер.

Для удаления ненужных сообщений следует пометить их флажками (флажки устанавливаются в крайней слева колонке, которая называется X, на рис. 2.8 помечено две записи), и нажать кнопку Удалить.

Если в почтовом ящике находится слишком много почтовых сообщений, то можно ограничить число одновременно загружаемых сообщений. Для этого нужно с клавиатуры либо с помощью кнопок счетчика указать требуемое значение в поле, которое находится в правом верхнем углу главного окна программы. Например, если в почтовом ящике находится 200 сообщений, то целесообразно не загружать сразу все заголовки, а делать это постепенно – например, загружать и просматривать по 30 или 50 заголовков.

### AntispamSniper для The Bat!

AntispamSniper для The Bat! (http://www.antispamsniper.com) – это специальная надстройка для почтовых клиентов The Bat! и Voyager, которая обеспечивает практически полную защиту от спама и фишинга пользовательского почтового ящика. В этой программе реализована комбинация нескольких методов автоматической классификации почты, что дает великолепное качество фильтрации нежелательной почты при минимальном количестве ошибок. В надстройку встроен механизм проверки заголовков, что позволяет удалять большинство таких писем прямо на сервере, не загружая все в свою систему. Осуществляется поддержка почтовых протоколов POP3 и IMAP. Кроме этого используется статистический обучаемый алгоритм для классификации сообщений. Обучаясь на практике, он выделяет отличительные черты писем из разных классов и эффективно использует полученных данные для анализа последующей корреспонденции. В итоге во время обучения алгоритм совершенствуется, улучшается качество классификации с каждым новым письмом. Дополнительно к самообучающемуся алгоритму в программе существуют так называемые «черный» и «белый» списки,

антифишинговый фильтр, существует фильтрация спама по IP-адресу отправителя.

**SpamPal**

SpamPal (http://www.spampal.org) – это еще одна программа для борьбы с нежелательной почтовой корреспонденцией. Программа работает со всеми почтовыми протоколами, такими как SMTP, POP3 и IMAP4, и совместима практически с любым почтовым клиентом. Принципрограммы прост: она удаляет письма, пришедшие с адресов, которые занесены в регулярно обновляемый список международных спамеров. Кроме этого пользователь может воспользоваться своими собственными «черным» и «белым» списками. Программа поддерживает свое функциональное расширение с помощью особых надстроек, которые предназначены для выявления и удаления конкретных типов спама, например, порнографического или фишингового содержания. Кроме этого программа поддерживает добавление возможности применения в правилах фильтрации регулярных выражений и подключение новых методов определения спама.

**Брандмауэр Windows 7**

Помимо различных антивирусных и антишпионских программ существует достаточно надежное средство, позволяющее защитить свой компьютер от несанкционированного доступа извне. Это средство называется брандмауэр.

Брандмауэр (он может называться также сетевой экран, файрвол, шлюз безопасности и др.) – это своеобразный буфер, находящийся между локальным компьютером и Интернетом. Его смысл заключается в том, чтобы блокировать всяческие попытки проникновения как из Интернета в компьютер, так и из компьютера в Интернет различных программ, команд, заданий и т. д.

Может возникнуть вопрос: понятно, когда брандмауэр блокирует несанкционированный доступ из Интернета в компьютер, но зачем же блокировать выход из компьютера в Интернет? А затем, чтобы, например, троян либо иной шпион, проникший в компьютер до установки либо включения брандмауэра, не имел возможности выполнять полученное задание (рассылать спам с зараженного компьютера, отсылать информацию о компьютере и пользователе и т. п.). При этом разрешается выход в Интернет только тем приложениям, которые укажет пользователь (Internet Explorer, Outlook Express и т. п.). Следует, однако, отметить, что не все брандмауэры могут контролировать исходящий трафик.

В операционной системе Windows 7 имеется встроенный брандмауэр подключения к Интернету. По умолчанию он включен, и без особой надобности отключать его настоятельно не рекомендуется.

**Включение, выключение и настройка брандмауэра**

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Чтобы открыть брандмауэр Windows 7, следует в Панели управления выбрать категорию Сеть и Интернет, в этой категории щелкнуть на ссылке Центр управления сетями и общим доступом, а в открывшемся окне – щелкнуть на ссылке Брандмауэр Windows, которая находится в левом нижнем углу. В результате на экране отобразится окно, изображенное на рис. 2.10.

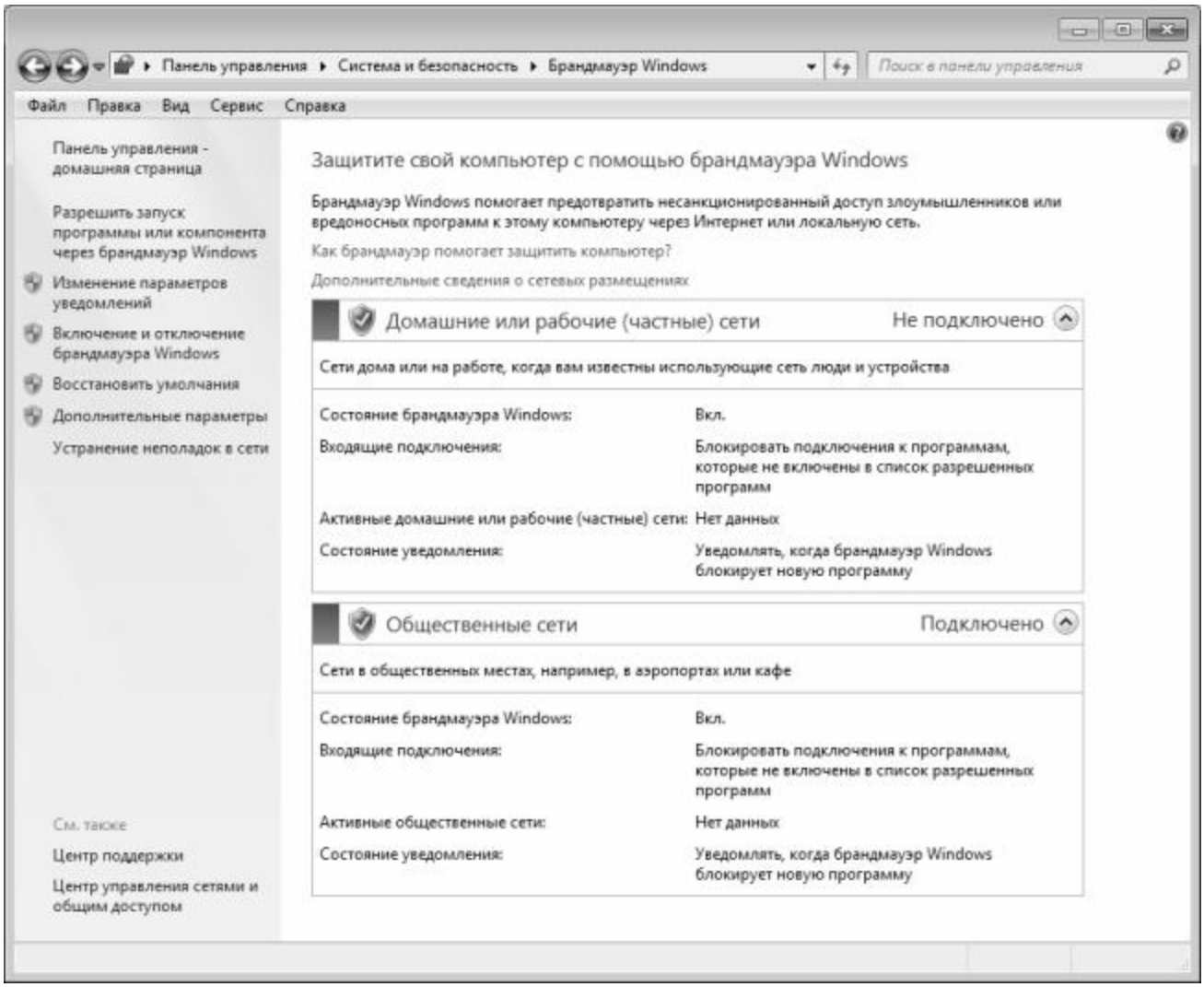



Рис. 2.10. Брандмауэр Windows 7

В данном окне представлена информация о текущем состоянии брандмауэра Windows. На рисунке видно, что брандмауэр включен, все подключения к программам, не внесенным в список разрешенных, буду блокироваться, и о каждом таком блокировании на экране будет отображаться соответствующее информационное сообщение. Отметим, что перечисленные сведения показываются отдельно для домашних, и отдельно – для общественных сетей.

Отметим, что менять параметры брандмауэра Windows 7, которые предложены в системе по умолчанию, без серьезных причин не рекомендуется. Особенно это касается малоопытных пользователей: неквалифицированное редактирование параметров брандмауэра может привести к тому, что компьютер окажется полностью незащищенным от внешних угроз (это касается и всей хранящейся в нем информации). Если все же вы

хотите изменить параметры брандмауэра – щелкните на ссылке Включение и отключение брандмауэра Windows, которая находится в левой части окна (см. рис. 2.10). При этом на экране отобразится окно, которое показано на рис. 2.11.

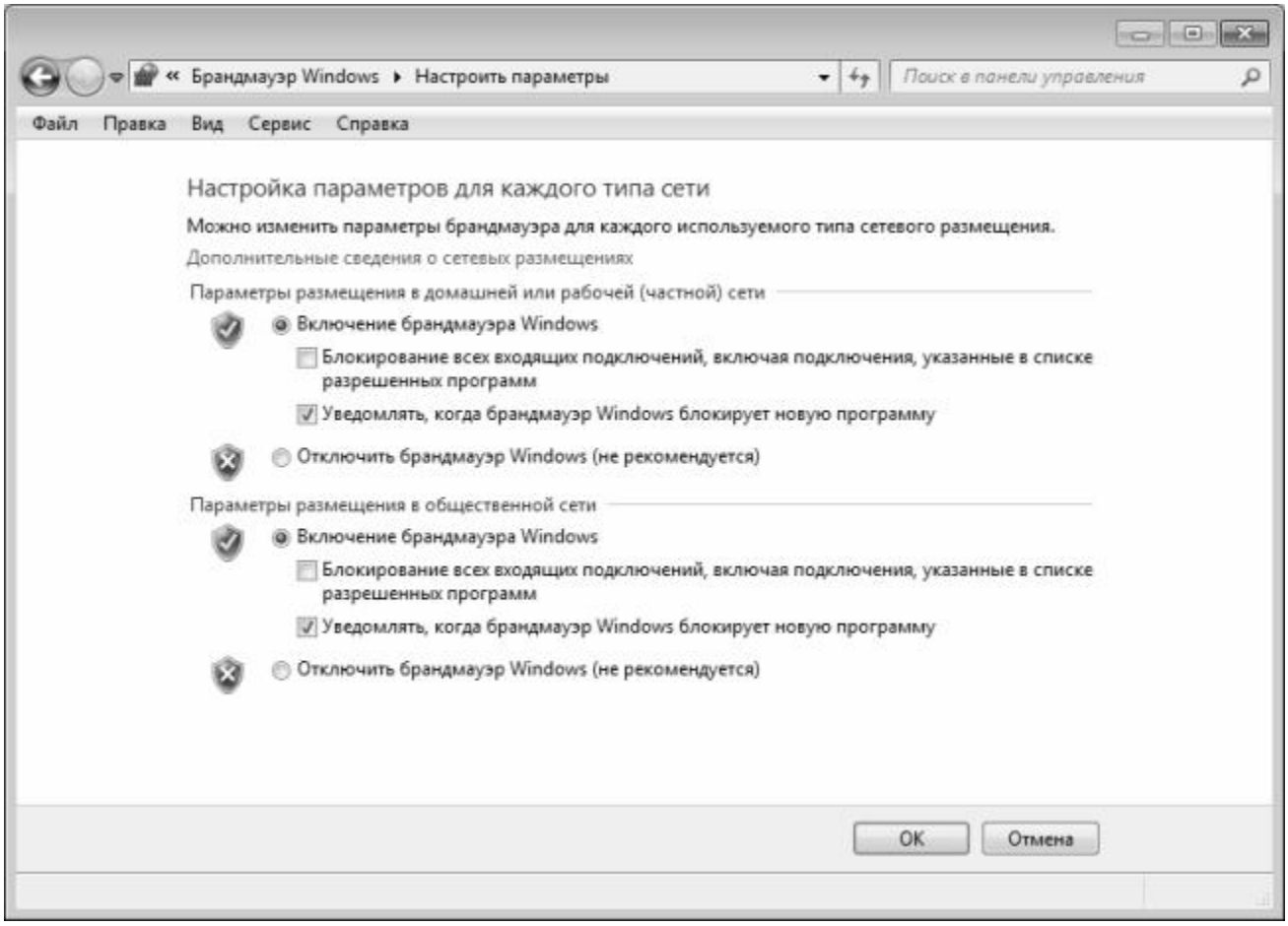



Рис. 2.11. Просмотр и редактирование параметров брандмауэра Windows 7

На данном рисунке показаны значения параметров, которые используются в системе по умолчанию. Как мы уже отмечали ранее, параметры настраиваются отдельно для домашних, и отдельно – для общественных сетей. Если переключатель установлен в положение Включение брандмауэра Windows – значит, защита включена, и компьютер защищен от внешних угроз.

При включенном брандмауэре становятся доступными флажки, позволяющие настроить некоторые режимы работы брандмауэра. При установке флажка Блокирование всех входящих подключений, включая подключения, указанные в списке разрешенных программ брандмауэр Windows будет блокировать все без исключения входящие подключения, в том числе и программы, которые указаны как надежные и проверенные. Если вы хотите, чтобы на экране появлялось информационное сообщение о каждом блокировании новой программы, установите флажок Уведомлять, когда брандмауэр Windows блокирует новую программу.

По умолчанию флажок Блокирование всех входящих подключений, включая подключения, указанные в списке разрешенных программ установлен, а флажок Уведомлять, когда брандмауэр Windows блокирует новую программу – снят.

Если перевести переключатель в положение Отключить брандмауэр Windows (не

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

рекомендуется) – брандмауэр полностью отключается, и компьютер остается без защиты. Как мы уже отмечали ранее, отключение брандмауэра без серьезных причин не рекомендуется. Такими серьезными причинами могут, в частности, являться конфликт брандмауэра с сетевым экраном стороннего разработчика, установленного (или – устанавливаемого) на компьютер, либо его несовместимость с каким-либо программным обеспечением.

Чтобы настройки брандмауэра Windows вступили в силу, нажмите кнопку ОК. Для выхода из данного режима без сохранения выполненных изменений нажмите кнопку Отмена.

**Как разрешить приложению работать через брандмауэр Windows**

Брандмауэр Windows 7 по умолчанию блокирует работу большинства установленных на компьютере приложений. Собственно, во многом благодаря именно этому и достигается высокий уровень безопасности компьютера: если вредоносная программа попытается запуститься на исполнение – она немедленно будет блокирована, и сможет продолжить работу только после соответствующего разрешения пользователя.

Однако такой режим работы брандмауэра не всегда является оптимальным, поскольку он не различает, какая программа запускается на исполнение – вредоносная или обычная. В частности, при загрузке операционной системы брандмауэр наверняка заблокирует большинство приложений, находящихся в каталоге автозагрузки. Соответственно, возникает вопрос: можно ли, не отключая брандмауэр, пользоваться программами, которые он блокирует, и если да – как этот сделать?

Для решения данной проблемы в брандмауэре Windows 7 реализована возможность формирования списка исключений. В этот список добавляются программы, которые не должны блокироваться брандмауэром. Например, если у вас установлена и помещена в каталог автозагрузки программа ICQ, то для того, чтобы она запускалась одновременно с загрузкой операционной системы, ее необходимо добавить в список исключений брандмауэра Windows. В противном случае она будет блокироваться при загрузке.

Стоит отметить, что при каждом добавлении новой программы в список исключений безопасность компьютера снижается. Иначе говоря, чем больше список исключений, тем больше возможностей появляется у хакеров и прочих злоумышленников, а также у вредоносных программ для запуска «червей», получения доступа к содержимому компьютера или использования его для распространения вредоносного программного обеспечения на другие компьютеры, а также в других противоправных целях.

Чтобы минимизировать возможные риски, добавляйте программу в список исключений только тогда, когда это действительно необходимо. Как только необходимость в этом отпала – сразу удаляйте программу из списка исключений. Ну и, конечно, никогда не разрешайте неизвестным программам проходить через брандмауэр.

Чтобы перейти в режим работы со списком исключений, нужно в левой части окна брандмауэра Windows (см. рис. 2.10) щелкнуть на ссылке Разрешить запуск программы или компонента через брандмауэр Windows. В результате на экране отобразится окно, изображенное на рис. 2.12.

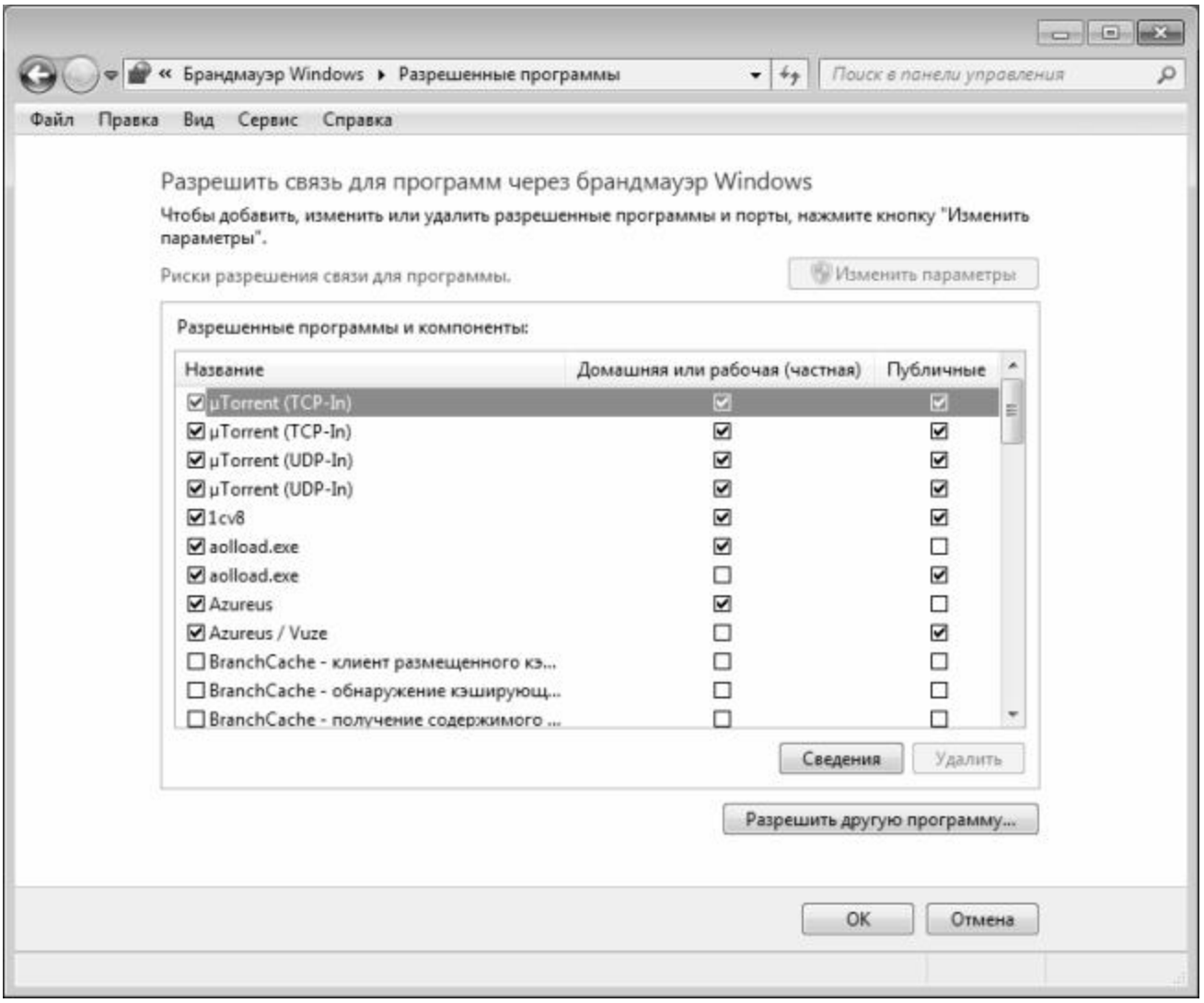



Рис. 2.12. Формирование списка исключений

По умолчанию в данном окне уже содержится определенный перечень программ, которые будут игнорироваться брандмауэром. Чтобы добавить в список исключений другую программу, нажмите кнопку Разрешить другую программу. При нажатии данной кнопки на экране отобразится окно со списком установленных на компьютере программ. Чтобы добавить приложение в список исключений, выделите его в списке щелчком мыши и нажмите кнопку Добавить. Если вы не обнаружили в списке требуемую программу (в частности, это могут быть программы, которые не требуют инсталляции) – можно попробовать найти ее самостоятельно. Для этого нажмите кнопку Обзор, и в открывшемся окне укажите путь к исполняемому файлу требуемого приложения, после чего нажмите ОК.

С помощью кнопки Типы сетевых размещений можно сразу указать, к каким типам сетевых размещений необходимо отнести выбранное приложение (то есть для домашней, рабочей или публичной сети). При нажатии кнопки на экране открывается окно, в котором с помощью соответствующих флажков выбираются типы сетевых размещений. Отметим, что эти сведения впоследствии можно изменить непосредственно в окне списка исключений.

После добавления программы в список исключений нужно установить флажок, который

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

расположен слева от ее названия – только в этом случае брандмауэр будет разрешать этой программе работать. Если же данный флажок снять, то программа останется в списке исключений, но при этом будет блокироваться. Другими словами, с помощью данного флажка вы можете включать/выключать блокировку для каждой программы, внесенной в список исключений.

С помощью флажков Домашняя или рабочая (частная) и Публичная указываются типы сетевых размещений, к которым следует отнести данную программу. Эти параметры также редактируются под кнопкой Типы сетевых размещений и под кнопкой Сведения.

Чтобы удалить программу из списка исключений, выделите ее щелчком мыши и нажмите кнопку Удалить. При этом система выдаст дополнительный запрос на подтверждение операции удаления.

Все настройки, выполненные в окне списка исключений, вступают в силу после нажатия кнопки ОК. Чтобы выйти из данного режима без сохранения изменений, нажмите кнопку Отмена.

## Глава 3. Анонимность работы в Интернете

Многие пользователи Интернета наверняка неоднократно задавали себе вопрос: а можно ли каким-либо образом обеспечить анонимность работы в Интернете? Ведь это позволяет получить целый ряд преимуществ: например, можно посещать любые ресурсы, и никто не вычислит пользователя по IP-адресу; кроме этого, можно получить доступ к веб-ресурсам, которые закрыты для обычного доступа (например, те же www.odnoklassniki.ru, www.vkontakte.ru и другие подобные ресурсы часто блокируются системными администраторами). Да и вообще – очевидно, что лучше не оставлять за собой никаких следов в Сети – ими могут воспользоваться те же шантажисты и прочие злоумышленники. Далее мы рассмотрим некоторые варианты обеспечения анонимности при работе в Интернете.

### Удаление следов своего пребывания в Интернете при работе через Internet Explorer

Многие наверняка сталкивались с такой ситуацией: на работе к компьютеру имеют доступ несколько сотрудников. Может ли пользователь после работы в Интернете сделать так, чтобы о посещенных им ресурсах не узнал никто из других пользователей данного компьютера? Особенно это актуально, если к данному компьютеру имеет доступ также и начальство…

Рассмотрим, каким образом можно решить эту проблему при использовании интернет-обозревателя Internet Explorer.

Чтобы перейти в режим удаления следов своего пребывания в Интернете, следует выполнить команду главного меню Сервис ▸ Свойства обозревателя и в открывшемся окне перейти на вкладку Общие. На данной вкладке нужно нажать кнопку Удалить – в результате откроется окно, изображенное на рис. 3.1.

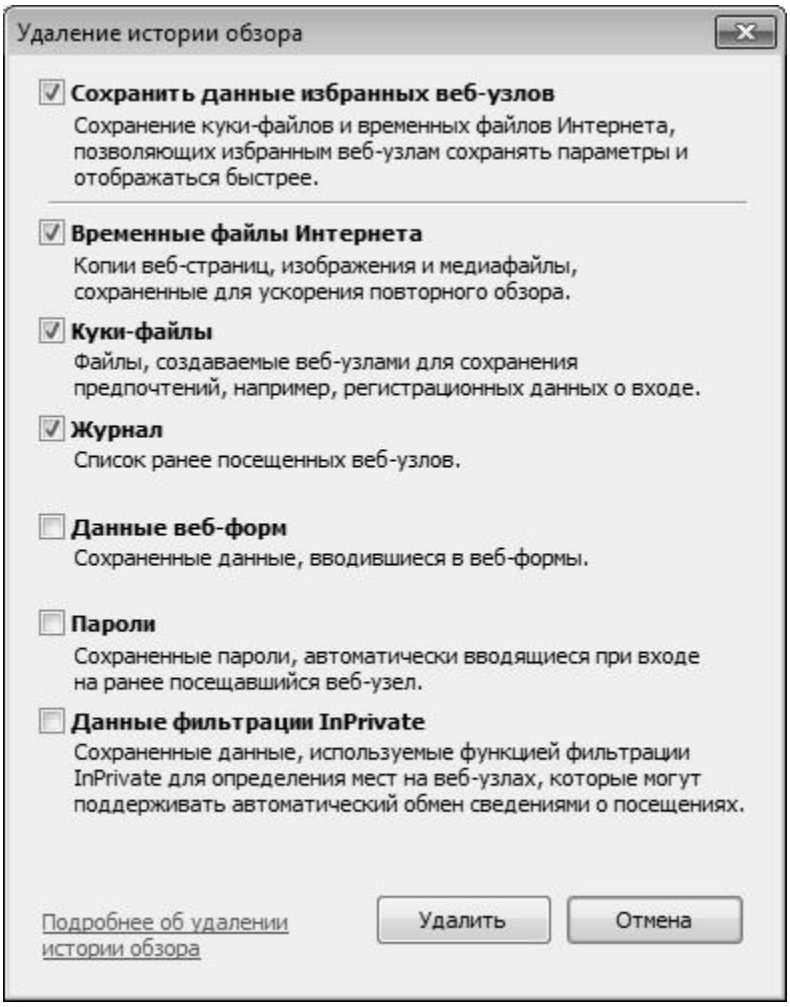



Рис. 3.1. Удаление следов работы в Интернете (Internet Explorer)

Из параметров, расположенных на данной вкладке, нас в первую очередь интересуют кнопки Куки-файлы, Временные файлы Интернета и Журнал. Их изменение вступает в силу после нажатия в данном окне кнопки Удалить.

При установленном флажке Куки-файлы осуществляется быстрое удаление с локального диска всех файлов cookie. Это файлы, создаваемые веб-узлом и содержащие некоторую информацию о пользователе, которая применяется при посещении веб-узла.

Флажок Временные файлы Интернета предназначен для быстрого удаления всех файлов из временной папки Интернета. По умолчанию папка с временными файлами Интернета располагается по пути C: UsersИмя пользователяAppDataLocalMicrosoftWindowsTemporary Internet Files. Однако при необходимости этот путь можно изменить: для этого нужно на вкладке Общие нажать кнопку Параметры, затем в открывшемся окне – кнопку Переместить, после чего в появившемся окне Обзор папок выбрать щелчком мыши требуемую папку и нажать ОК.

Почему желательно удалить содержимое папки с временными файлами? Потому, что посторонний пользователь, заглянув в эту папку, может увидеть там все, что вы видели в Интернете (графические объекты и иконки с www.odnoklassniki.ru и прочих посещенных вами ресурсов, и др.). Кстати, для быстрого открытия данной папки можно воспользоваться кнопкой Показать файлы (она находится в окне, которое открывается после нажатия на вкладке Общие кнопки Параметры).

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Если прогулка по Интернету выполнялась только с помощью ссылок, поисковиков и т. п., то задачу удаления основного «компромата» мы выполнили. Но если какие-то адреса набирались в адресной строке Internet Explorer, то они там сохранились, и их легко можно увидеть, открыв раскрывающийся список адресной строки. Для очистки раскрывающегося списка адресной строки нужно установить флажок Журнал (см. рис. 3.1). Но учтите, что при нажатии на данную кнопку из адресной строки будут удалены все имеющиеся там адреса, поэтому предварительно рекомендуется изучить данный список и отдельно сохранить нужные адреса.

**Удаление следов своего пребывания в Интернете при работе через Mozilla Firefox**

В обозревателе Mozilla Firefox также имеется штатный механизм для удаления следов пребывания вы Интернете. Для перехода в соответствующий режим нужно выполнить команду главного меню Инструменты ▸ Стереть недавнюю историю (эта команда вызывается также нажатием комбинации клавиш Ctrl+Shift+Delete) – в результате на экране откроется окно, изображенное на рис. 3.2.

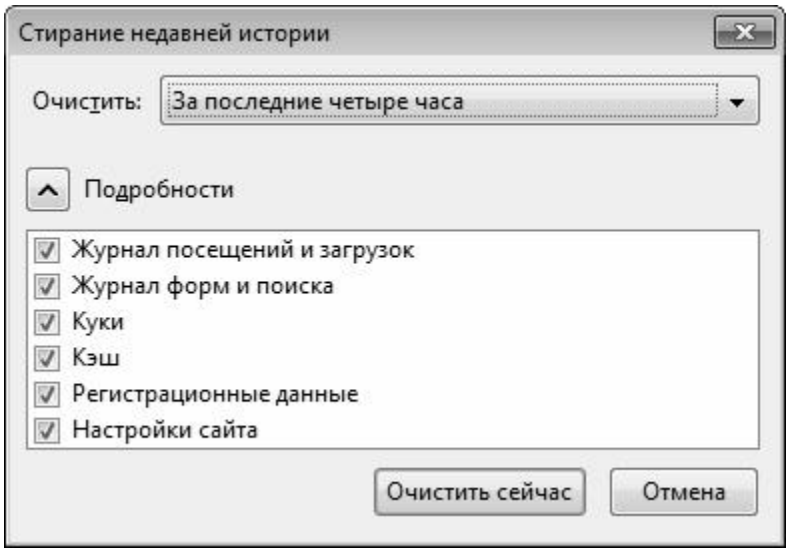



Рис. 3.2. Удаление следов работы в Интернете (Mozilla Firefox)

В данном окне в поле Очистить из раскрывающегося списка нужно выбрать период времени, историю которого вы намерены удалить. Возможен выбор одного из перечисленных ниже вариантов.

♦ За последний час, За последние два часа и За последние четыре часа – при выборе этих значений будет удалена история работы в Интернете соответственно за последний час, два часа и четыре часа.

♦ За сегодня – в данном случае будет очищена история работы в Интернете за сегодняшний день.

♦ Все – при выборе данного значения будет удалена целиком вся история работы в Интернете, за все время использования программы.

С помощью расположенных ниже флажков (управление их отображением осуществляется с помощью кнопки Подробности) можно выбрать данные, которые должны быть удалены при очистке истории работы в Интернете. По умолчанию

установлены все флажки.

Очистка истории в соответствии с установленными параметрами будет выполнена после нажатия кнопки Очистить сейчас (при этом окно будет автоматически закрыто). С помощью кнопки Отмена осуществляется выход из данного режима без удаления истории. Отметим, что процесс удаления истории может занять определенное время, особенно при удалении большого количества данных или при работе на маломощном компьютере.

## Как работать в Интернете незаметно для других

Многие новички ошибочно полагают, что работа в Интернете обеспечивает полную анонимность. При этом они рассуждают примерно так: я сижу дома, меня никто не видит и не слышит, поэтому никто не может знать, когда и что я делал в Интернете.

Но в реальности это далеко не так. При желании можно не только узнать, что и когда вы делали в Интернете, но и без особого труда определить содержимое вашего жесткого диска. Причем сделать это может даже человек, находящийся на другом краю земного шара.

Не вдаваясь в подробности, поясним: каждый компьютер сразу после выхода в Интернет получает свой индивидуальный числовой идентификатор, который называется IP-адрес. По IP-адресу можно вычислить, когда и с какого места (например, из вашей квартиры, из офиса и т. п.) был осуществлен выход в Интернет, какие ресурсы посещались, что скачивалось, пересылалось и т. д. Эти сведения хранятся у Интернет-провайдера, где их могут получить заинтересованные лица.

Поэтому многие пользователи Интернета крайне заинтересованы в том, чтобы сохранить свою анонимность при работе в Интернете и сделать свой компьютер невидимым в Сети. Наиболее популярный способ, позволяющий скрыть IP-адрес при работе в Интернете – это использование прокси-сервера.

## Обеспечение анонимности с помощью прокси-сервера

Прокси-сервер – это промежуточный компьютер между компьютером пользователя и Интернетом. Иначе говоря – это своего рода посредник, промежуточное звено. Анонимность при использовании прокси-сервера достигается за счет того, что вместо реального IP-адреса компьютера, с которого пользователь вышел в Интернет, подставляется совершенно другой IP-адрес. Это позволяет, помимо прочего, посещать веб-ресурсы, зайти на которые без использования прокси-сервера невозможно. Кроме этого, использование прокси-сервера часто позволяет значительно увеличить скорость работы в Интернете (но иногда возможен и противоположный эффект – все зависит от конкретного прокси-сервера).

Каким же образом осуществляется подключение через прокси-сервер? Вначале необходимо найти его адрес и номер порта. Для начала можно поинтересоваться у знакомых – может, у кого-то есть адрес и порт реально действующего прокси-сервера. Если нет – то достаточно войти в Интернет, набрать в любом поисковике «действующий прокси-сервер» либо что-то в этом роде и проанализировать результаты поиска. Следует

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

учитывать, что поисковик, вероятнее всего, выдаст большое количество списков с адресами и номерами портов прокси-серверов, но большая часть из них будет нерабочими. Процесс определения рабочего прокси-сервера можно выполнять вручную (это долго и нудно), а можно – с помощью специальных утилит, которые можно найти в Интернете. Порядок использования большинства таких утилит прост: в программу загружается список портов и адресов, и через некоторое время она выдает перечень тех из них, которые являются действующими.

Чтобы выйти в Интернет через прокси-сервер, необходимо выполнить соответствующие настройки интернет-обозревателя. Рассмотрим настройку выхода в Интернет через прокси-сервер на примере интернет-обозревателя Internet Explorer 8.

В окне Свойства обозревателя, открываемом с помощью команды главного меню Сервис ▸ Свойства обозревателя, следует перейти на вкладку Подключения, выделить на ней щелчком мыши используемое подключение и нажать кнопку Настройка. В результате на экране отобразится окно, которое показано на рис. 3.3.

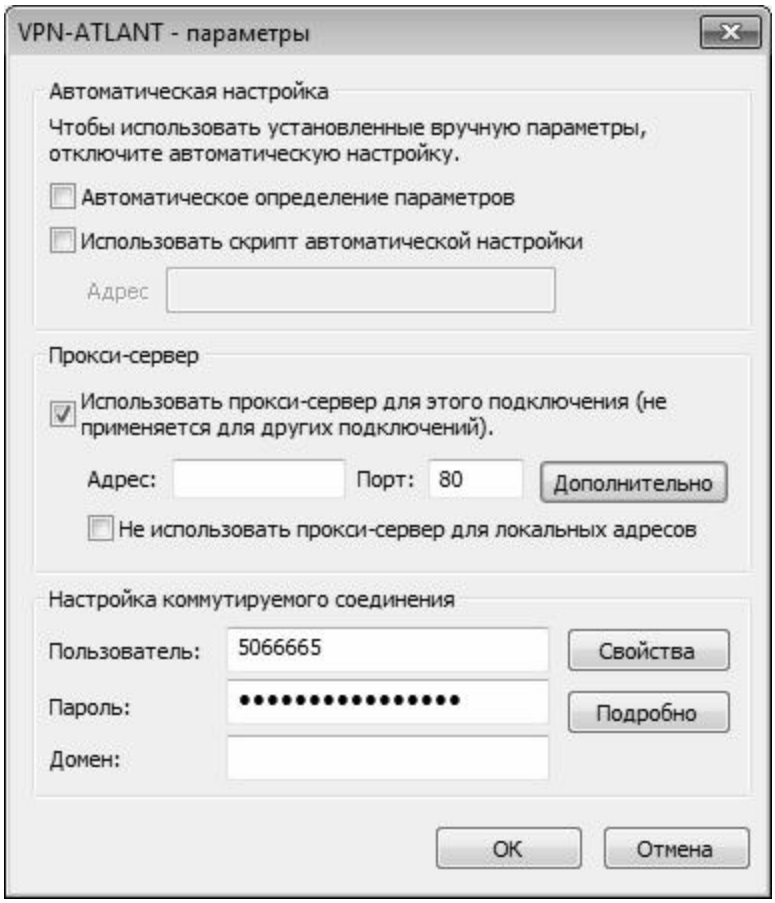



Рис. 3.3. Включение режима использования прокси-сервера

Чтобы включить режим использования прокси-сервера, нужно в данном окне в выделенной области Прокси-сервер установить флажок Использовать прокси-сервер для этого подключения (не применяется для других подключений). После этого станут доступными для редактирования поля Адрес и Порт, в которых с клавиатуры вводятся соответственно IP-адрес используемого прокси-сервера и номер порта. Учтите, что выполненные настройки будут действительны только для того подключения, которое

было выбрано в окне свойств обозревателя на вкладке Подключения.

**Анонимайзер**

Наряду с прокси-серверами, в настоящее время широкое распространение получили анонимайзеры. Анонимайзер – это, по сути, разновидность прокси-сервера. Основное отличие состоит в том, что для использования анонимайзера не нужно выполнять никаких дополнительных настроек. Как правило, анонимайзер не имеет номера порта, представляет собой обычную веб-страницу и имеет стандартный веб-адрес. Например, один из популярных русскоязычных анонимайзеров расположен по адресу http://www.anonymizer.ru.

Порядок использования анонимайзера предельно прост. Каждый анонимайзер имеет свою адресную строку, в которую следует ввести требуемый адрес и нажать расположенную рядом кнопку (она может называться Перейти, Go и т. п.). В результате будет выполнен переход на соответствующую страницу (сайт). Рекомендуется обратить внимание на содержимое адресной строки интернет-обозревателя – хорошо знакомый адрес будет выглядеть весьма непривычно.

На некоторых анонимайзерах предусмотрено выполнение ряда настроек (но это необязательно). Как правило, параметры настройки представляют собой флажки либо переключатели. С их помощью можно включать/выключать разрешение скриптов, рекламы, рисунков и др.

Отметим, что действующий анонимайзер найти проще, чем действующий прокси-сервер.

**Отправка анонимной электронной корреспонденции**

При отправке электронной корреспонденции может возникать необходимость в соблюдении анонимности. Причины для этого могут быть самые разные: желание разыграть коллег по работе либо членов семьи, анонимно сообщить руководству о каких-либо событиях, и т. п. Здесь мы расскажем о том, как это делается.

Если потребность в создании анонимного сообщения – разовая, то наиболее простой способ отправки анонимного письма – это открыть почтовый ящик «одноразового» использования. Иначе говоря, нужно просто зайти на любой почтовый сервис (например, www.mail.ru) и открыть на вымышленное имя самый обычный почтовый ящик. Затем нужно отправить с него почтовое сообщение и сразу же после этого либо забыть о существовании этого ящика, либо просто удалить его.

Но этот метод приемлем, если анонимное почтовое сообщение отправляется не слишком продвинутому в компьютерном отношении пользователю. Однако более опытный человек без труда сможет определить IP-адрес компьютера, с которого выполнялась отправка почтового сообщения. Для этого необходимо почтовой программой принять данное письмо с сервера на компьютер, после чего просмотреть его исходный текст (у разных почтовых клиентов для этого предусмотрены свои механизмы).

Еще один способ анонимной отправки электронной корреспонденции заключается в

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

использовании специальных утилит. В данном случае почтовое сообщение можно отправить от вымышленных имени и адреса отправителя. Подобные программы широко представлены в Интернете; чтобы найти их и скачать, достаточно набрать в любом поисковике текст вроде Программы анонимной отправки почты либо что-то подобное.

Еще один удобный способ заключается в том, что для нужно зайти на специальный сайт, заполнить соответствующую форму и нажать кнопку Отправить (либо Send, либо ОК – в зависимости от конкретного сайта). Такие сайты во множестве представлены в Интернете. Для поиска таких ресурсов достаточно в любом поисковике набрать текст типа Анонимная отправка почты либо Сайты анонимной отправки почты, либо нечто подобное. Один из таких сайтов (причем русскоязычный) расположен по адресу http://bogomol.net/incom/. На данном сайте для отправки анонимного почтового сообщения предлагается заполнить специальную форму. В ней указывается электронный адрес получателя почтового сообщения, тема анонимного сообщения и произвольный адрес отправителя почтового сообщения (это может быть что угодно – хоть бессмысленный набор символов); введенное здесь значение увидит получатель почтового сообщения в поле От. Также указывается произвольное имя отправителя, а для ввода текста письма предназначено поле Текст. Также нужно ввести защитный числовой код (captcha), предложенный системой.

Все поля данной формы заполняются с клавиатуры. При желании вы можете отправить прикрепить к письму вложение (но такую услугу предоставляют не все сервисы анонимной отправки писем). Для отправки анонимного почтового сообщения следует нажать кнопку Отправить.

Примерно по такой же схеме (возможны несущественные отклонения) осуществляется отправка анонимных электронных сообщений и с других подобных сайтов. Следует учитывать, что электронная почта, анонимно отправляемая с подобных сайтов, может приходить с задержкой (в процессе тестирования были отмечены случаи, когда анонимная почта приходила с задержкой в два дня).

**Как вычислить IP-адрес отправителя почтового сообщения?**

С помощью почтовых клиентов можно вычислить IP-адрес отправителя электронного сообщения. Для этого необходимо с помощью почтовой программы принять письмо с сервера на компьютер, после чего просмотреть его исходный текст.

У каждого почтового клиента применяется своя методика для просмотра исходного текста почтового сообщения. Чтобы просмотреть исходный текст в программе The Bat, следует выделить письмо щелчком мыши и выполнить команду главного меню Специальное ▸ Исходный текст письма либо нажать клавишу F9. Этой же командой можно воспользоваться также в режиме просмотра почтового сообщения. В результате на экране откроется окно с исходным текстом письма, в заголовке которого можно увидеть IP-адрес отправителя (рис. 3.4).

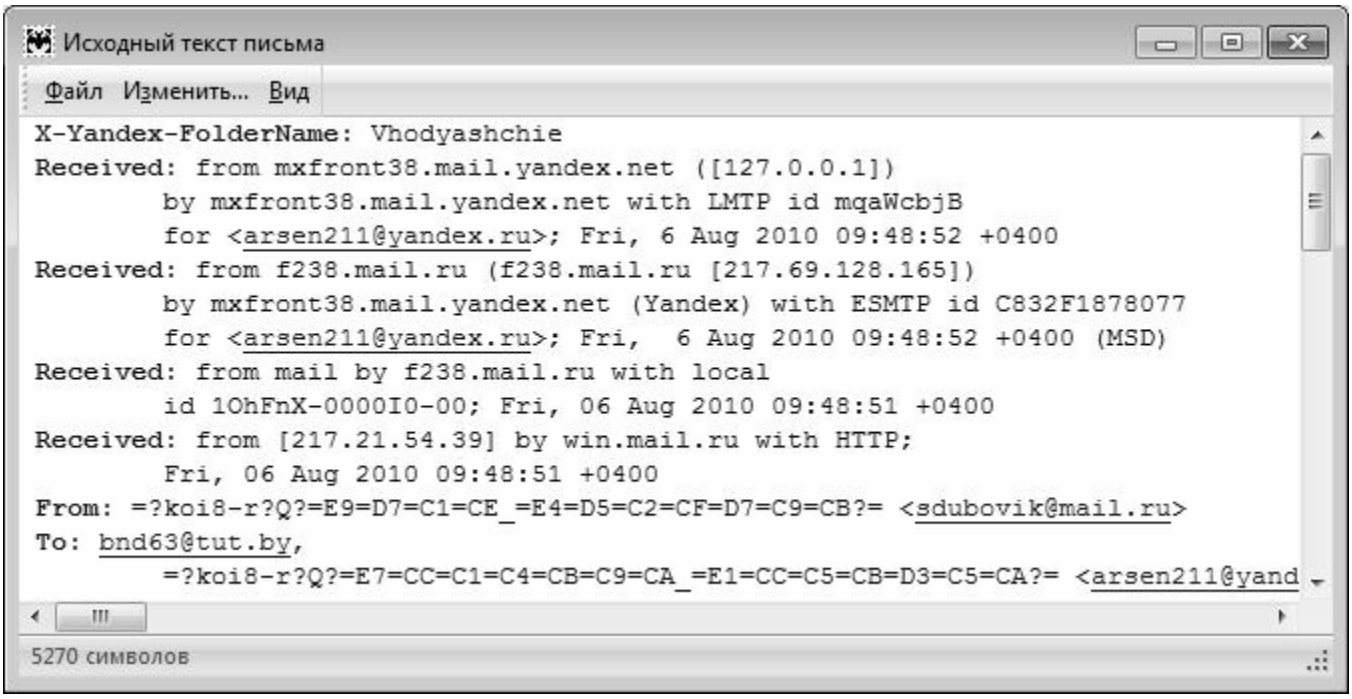



Рис. 3.4. Просмотр исходного кода письма в программе The Bat

Для просмотра исходного текста почтового сообщения в программе Windows Live Mail, нужно щелкнуть на нем правой кнопкой мыши и в открывшемся контекстном меню выбрать команду Свойства. В результате на экране откроется окно, в котором нужно перейти на вкладку Сведения – здесь будет показан исходный текст заголовка почтового сообщения (рис. 3.5).

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

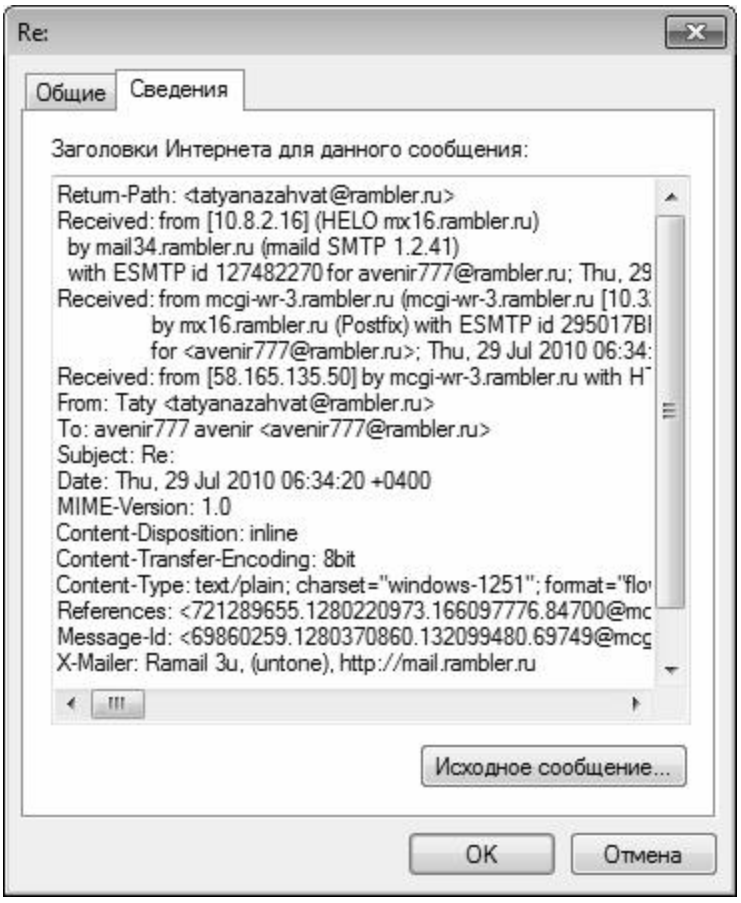



Рис. 3.5. Просмотр исходного текста заголовка письма в программе Windows Live Mail

Если необходимо просмотреть полный исходный текст письма, следует на данной вкладке нажать кнопку Исходное сообщение.

В программе Outlook Express просмотр исходного кода письма осуществляется аналогичным образом – с той разницей, что команда Свойства вызывается также из меню Файл, а в окне свойств нужно открыть вкладку Подробно (аналог вкладки Сведения в Windows Live Mail, см. рис. 3.5).

## Глава 4. Локальная сеть под контролем

Если выход в Интернет осуществляется через локальную сеть, то для обеспечения безопасной работы очень важно выполнить ее грамотную настройку, производить ее обслуживание, а при необходимости – диагностировать и устранять сетевые неполадки. В противном случае компьютер может стать весьма уязвимым для опасностей извне (в частности, те же сетевые черви способны распространяться почти молниеносно). О том, как обеспечить безопасную работу локальной сети в системе Windows 7, мы и расскажем в данной главе.

### Центр управления сетями и общим доступом

Для настройки, просмотра и редактирования параметров локальной сети нужно перейти в Центр управления сетями и общим доступом. Именно здесь содержатся почти все основные инструменты, необходимые для настройки и администрирования локальных сетей.

Центр управления сетями и общим доступом (рис. 4.1) находится в категории Сеть и Интернет Панели управления.

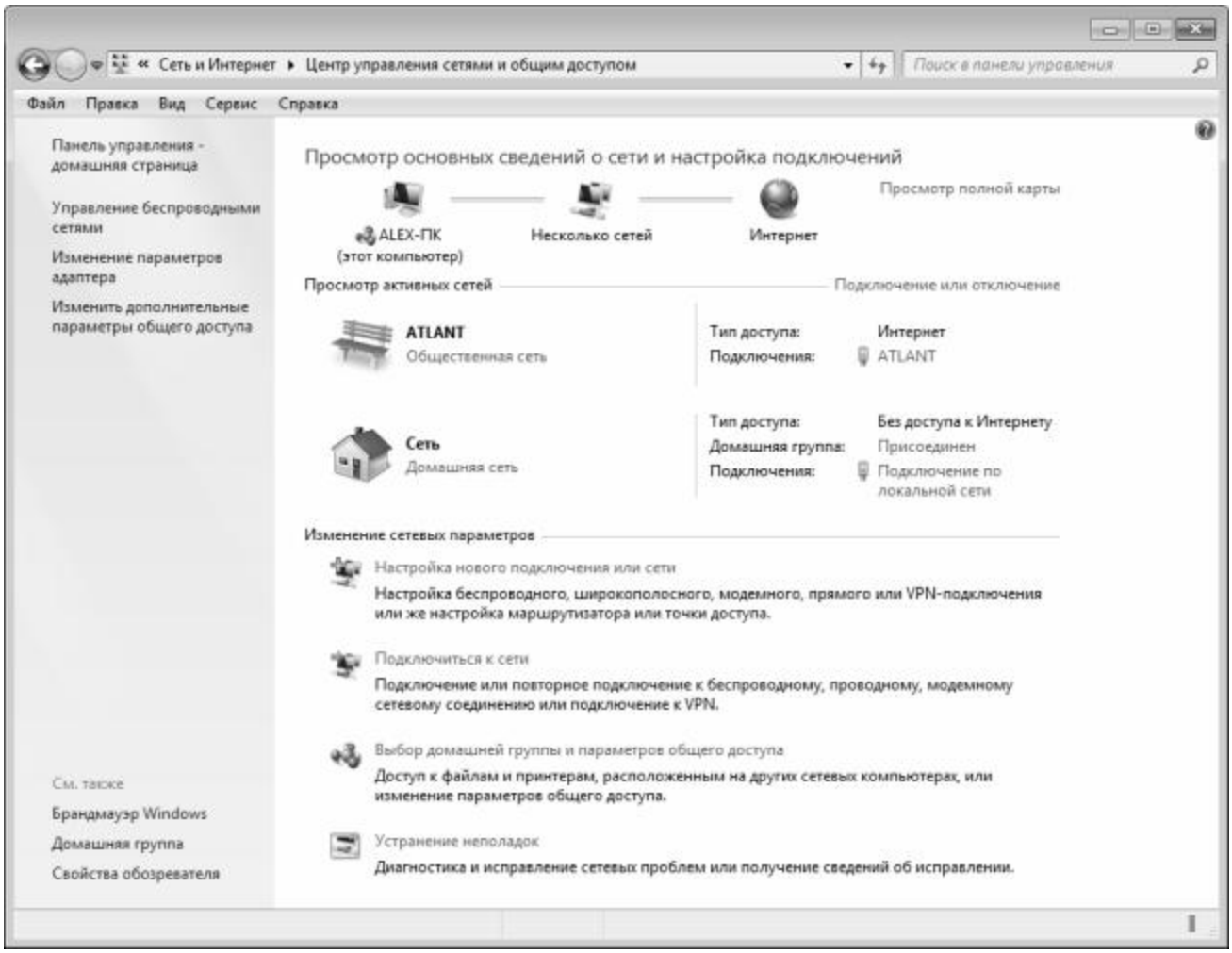



Рис. 4.1. Центр управления сетями и общим доступом

В данном режиме осуществляется создание новых и редактирование имеющихся подключений, переход в режим настройки параметров адаптера и общего доступа, а также выполнение ряда иных функций. Здесь вы можете просмотреть информацию о текущем состоянии сети в режиме реального времени. Также вы можете определить, подключен ли данный компьютер к локальной сети или Интернету, и если подключен – узнать способ подключения и уровень доступа к компьютерам и сетевым устройствам. Эти сведения необходимы как для настройки сети, так и для устранения проблем с безопасностью и подключением.

**Как правильно настроить локальную сеть?**

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Характерной особенностью операционной системы Windows 7 является то, что процесс создания локальных сетей в ней максимально автоматизирован. В результате пользователь выполняет лишь необходимый минимум действий, а все остальное (поиск сети, настройка основных сетевых параметров и др.) выполняется в автоматическом режиме.

Одна из самых распространенных у рядовых пользователей проблем – это объединение двух компьютеров в локальную сеть. Например, таким способом часто объединяются домашние компьютеры. В системе Windows 7 реализована возможность настройки как проводных, так и беспроводных сетевых подключений.

**Создание проводной сети**

Первое, что нужно сделать перед настройкой сети – это убедиться, что на обоих компьютерах имеются сетевые карты, и к ним установлены драйвера.

Если оба компьютера работают под управлением операционной системы Windows 7, то создание сети будет практически полностью автоматизировано. Вам нужно лишь соединить компьютеры кабелем, и проверить, чтобы название рабочей группы у них было одинаковым.

ПРИМЕЧАНИЕ

По умолчанию в операционной системе Windows 7 рабочей группе присваивается название WORKGROUP. Если вы его не меняли ни на одном из компьютеров – то они готовы для объединения в сеть.

Также проверьте, чтобы в настройках сетевых экранов и прочих средств безопасности не была заблокирована возможность работы в локальной сети.

После этого система приступит к настройке сети. Как правило, много времени это не займет, и в области уведомлений панели задач появится характерный значок, свидетельствующий об обнаружении другого компьютера и появлении локальной сети.

Если сеть по каким-то причинам не распозналась – перезагрузите компьютеры. Если и это не помогло – проверьте, включено ли в настройках сетевое обнаружение. Для этого в левой части окна Центра управления сетями и общим доступом (см. рис. 4.1) щелкните на ссылке Изменить дополнительные параметры общего доступа – в результате на экране отобразится окно, которое показано на рис. 4.2.

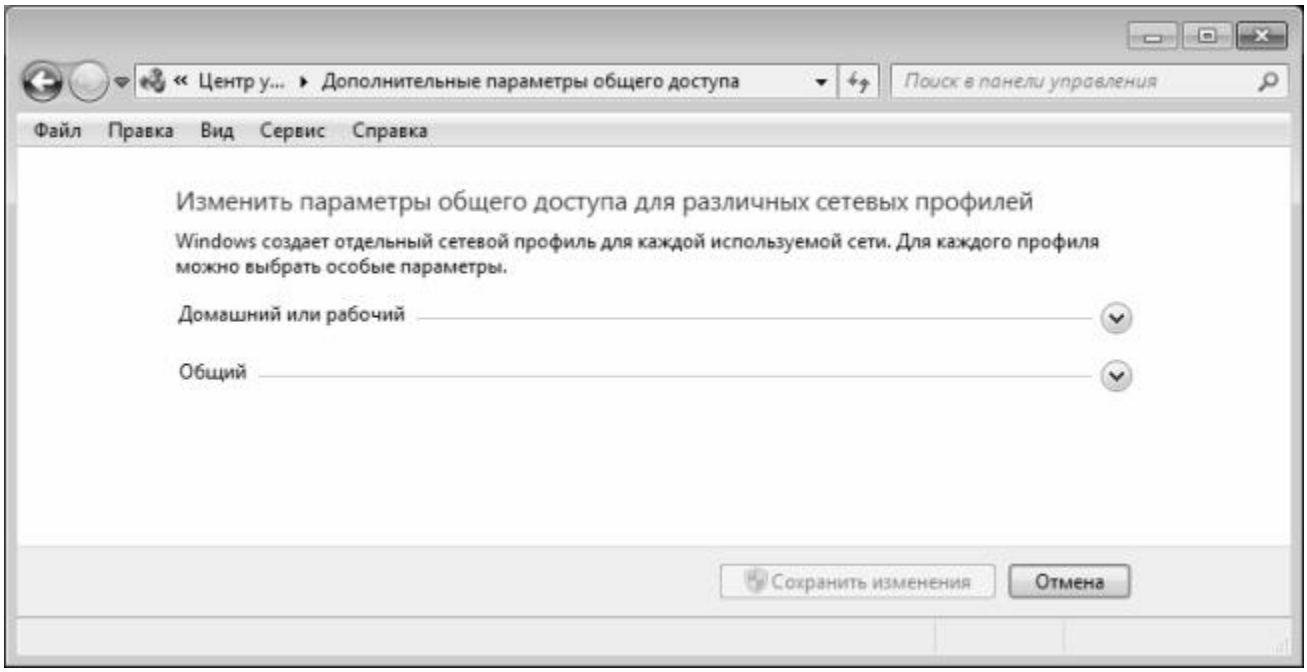
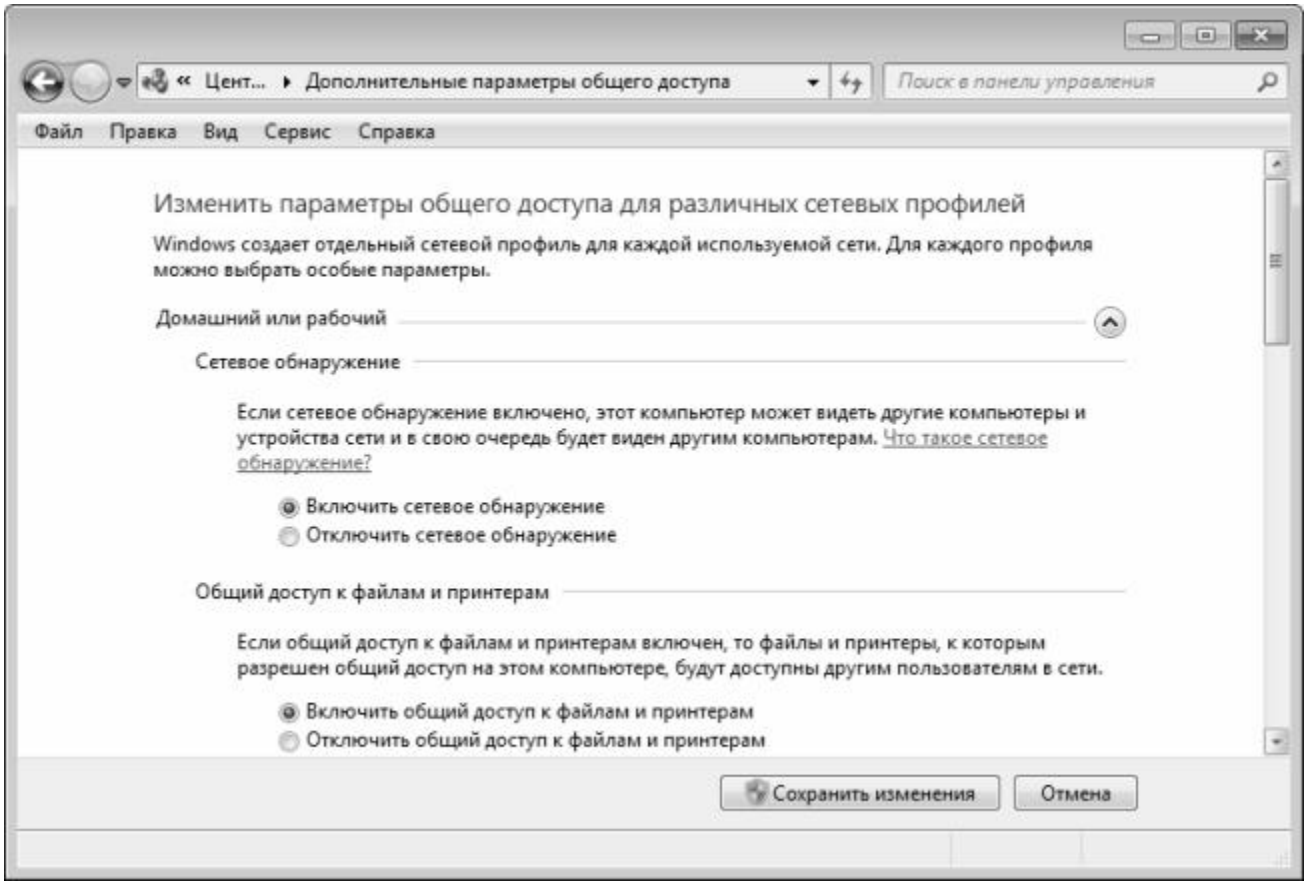



Рис. 4.2. Настройка параметров общего доступа

В данном окне с помощью расположенной справа стрелочки откройте требуемый сетевой профиль, и установите переключатель в положение Включить сетевое обнаружение, после чего нажмите кнопку Сохранить изменения. На рис. 4.3 показана эта настройка для профиля Домашний или рабочий.




Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Рис. 4.3. Включение сетевого обнаружения

Если и после этого сеть не распозналась – проверьте параметры настройки сетевого доступа к дискам, файлам и папкам на обоих компьютерах.

Если подключаемый компьютер работает под управлением операционной системы Windows Vista, то настройка проводной сети осуществляется аналогичным образом.

Если же подключаемый компьютер работает под управлением операционной системы Windows XP, то здесь нужно выполнить некоторые дополнительные действия. Войдите на компьютер под учетной записью администратора, и проверьте имя рабочей группы, к которой относится данный компьютер. Если оно отличается от имени рабочей группы второго компьютера (напомним, что в Windows 7 по умолчанию используется имя WORKGROUP) – приведите его в соответствие. После этого перезагрузите компьютер, откройте папку Сетевое окружение, затем в левой панели открывшегося окна щелкните на ссылке Отобразить компьютеры рабочей группы – в результате появится значок второго компьютера, для подключения к которому достаточно дважды щелкнуть на этом значке мышью.

**Создание беспроводной сети**

Чтобы настроить между двумя компьютерами беспроводную сеть, нужно воспользоваться встроенным в систему Мастером беспроводной сети.

ВНИМАНИЕ

Чтобы объединение компьютеров в беспроводную сеть стало возможным, они должны находиться на расстоянии не более 10 м друг от друга.

В окне Центра управления сетями и общим доступом (см. рис. 4.1) щелкните на ссылке Настройка нового подключения или сети, и в открывшемся окне щелчком мыши выберите пункт Настройка беспроводной сети компьютер-компьютер (рис. 4.4).

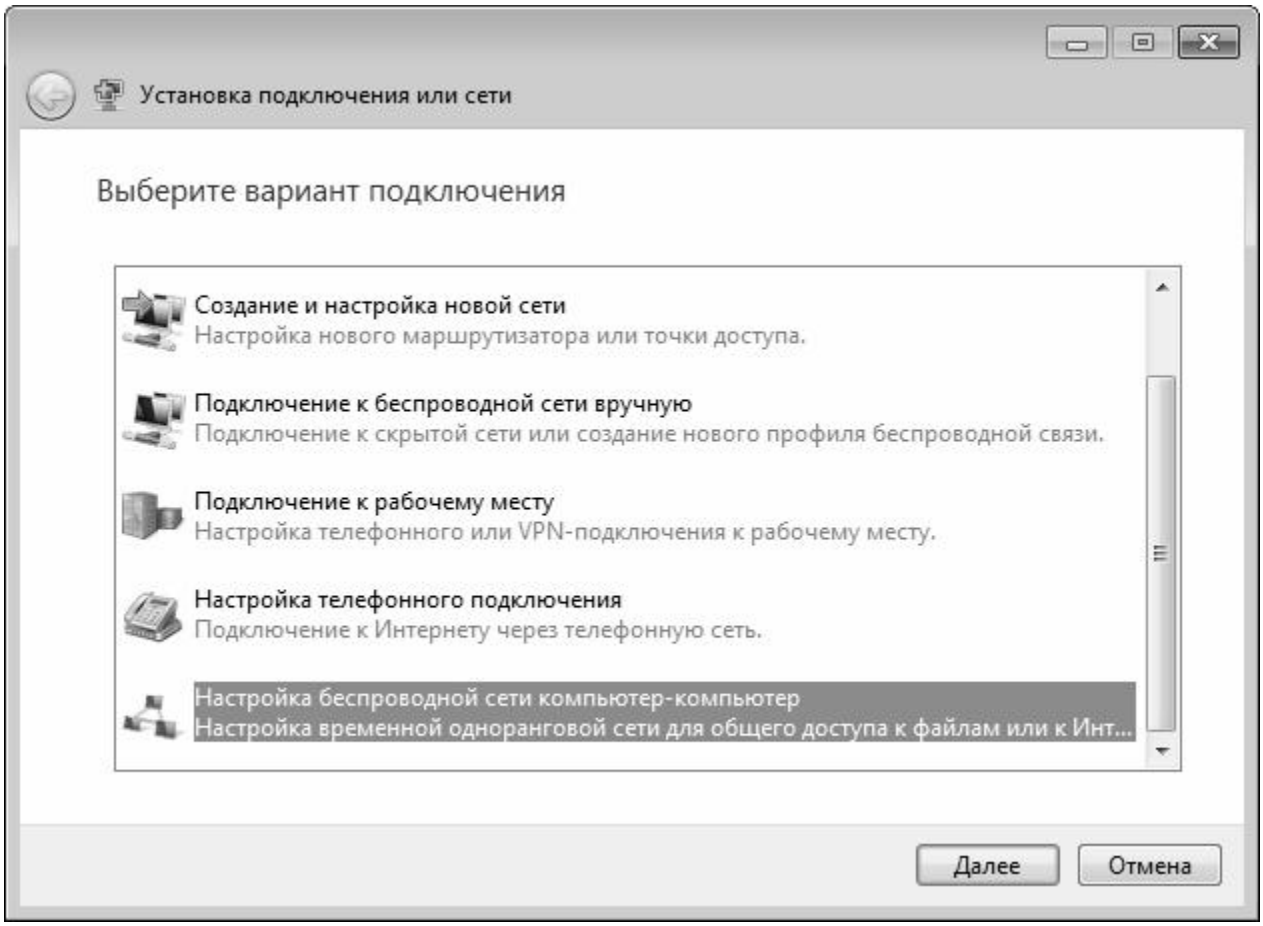



Рис. 4.4. Создание беспроводной сети «компьютер-компьютер»

После нажатия в данном окне кнопки Далее на экране откроется окно, в котором будет приведено краткое описание беспроводных сетей, созданных в Windows 7 (рис. 4.5).

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

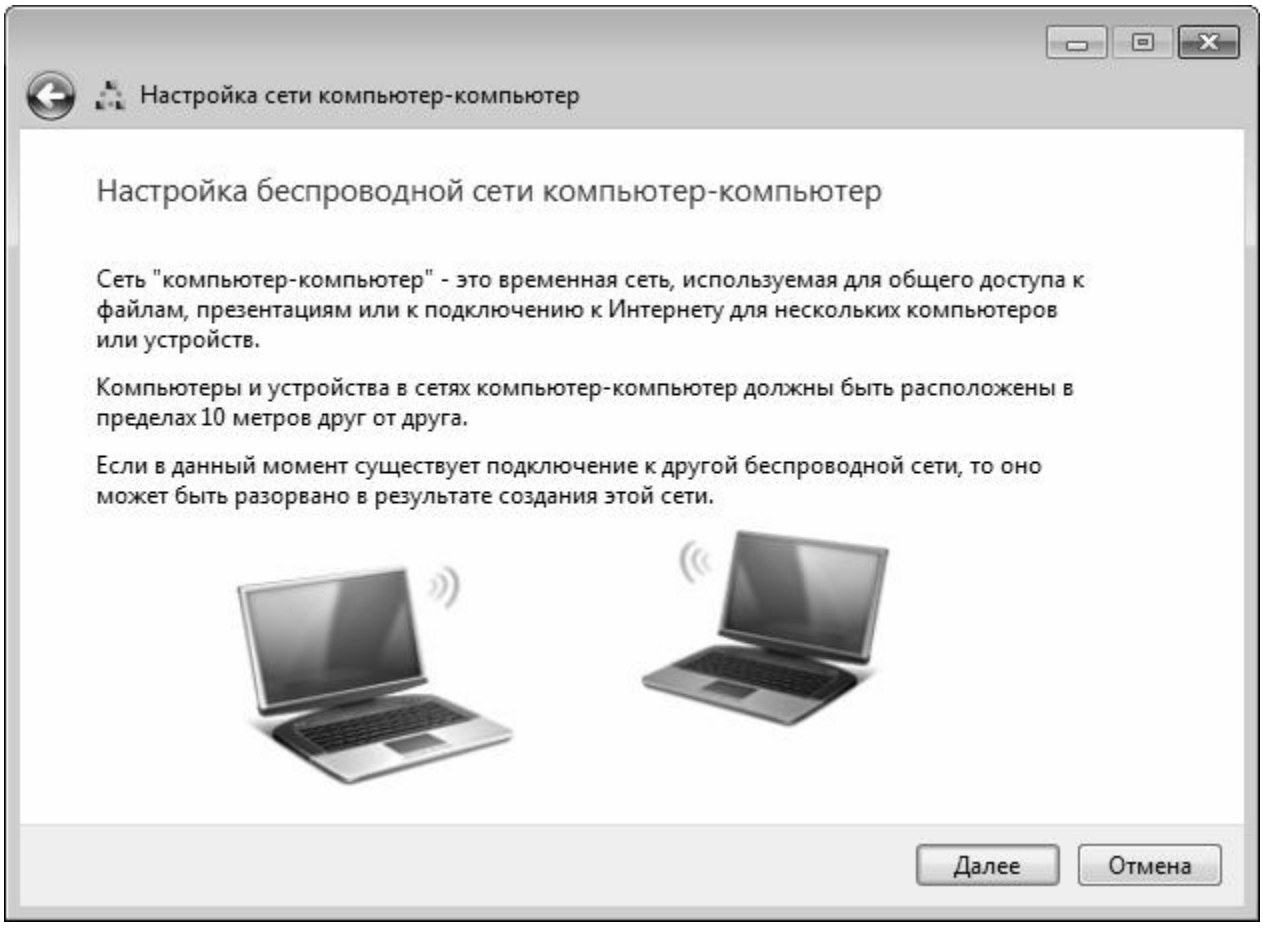



Рис. 4.5. Краткие сведения о беспроводных сетях

Чтобы перейти к следующему этапу настройки сети, нажмите кнопку Далее. В результате окно Мастера примет вид, как показано на рис. 4.6.

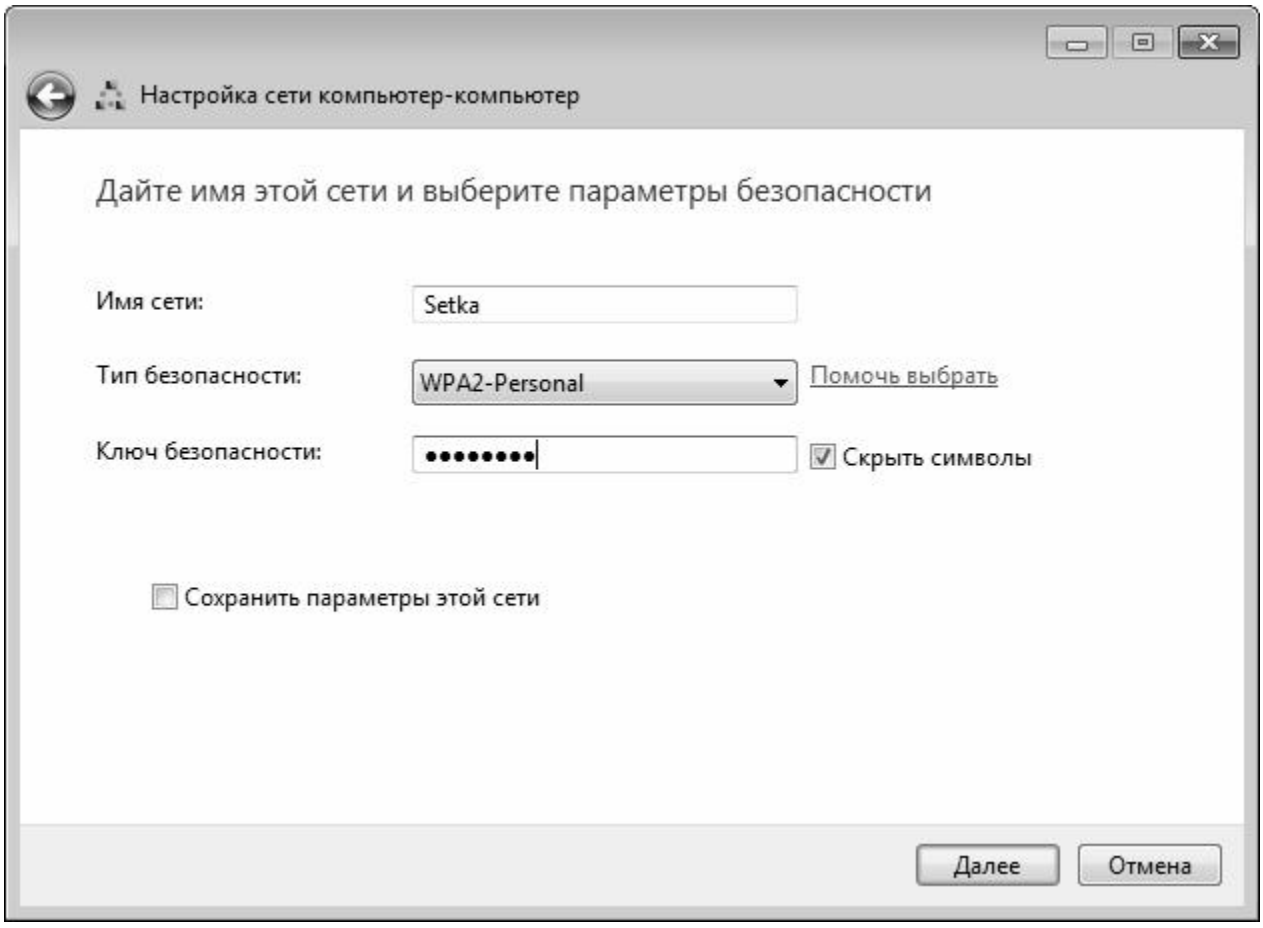



Рис. 4.6. Ввод параметров беспроводной сети

В соответствующих полях данного окна нужно с клавиатуры ввести имя создаваемой сети и ключ безопасности (иначе говоря, пароль). Учтите, что при вводе пароля учитывается регистр символов (прописные и строчные).

Если в данном окне установить флажок Сохранить параметры этой сети, то сеть будет сохранена в системе. В этом случае даже после отключения от нее она все равно будет присутствовать в списке подключений (рис. 4.8), и ее можно будет использовать повторно. Если же данный флажок снят, то после отключения от сети она автоматически будет удалена, и впоследствии ее придется настраивать заново.

После нажатия в данном окне кнопки Далее система приступит к созданию беспроводной сети в соответствии с установленными параметрами. Если процесс завершился успешно, то на экране отобразится соответствующее информационное сообщение (рис. 4.7).

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

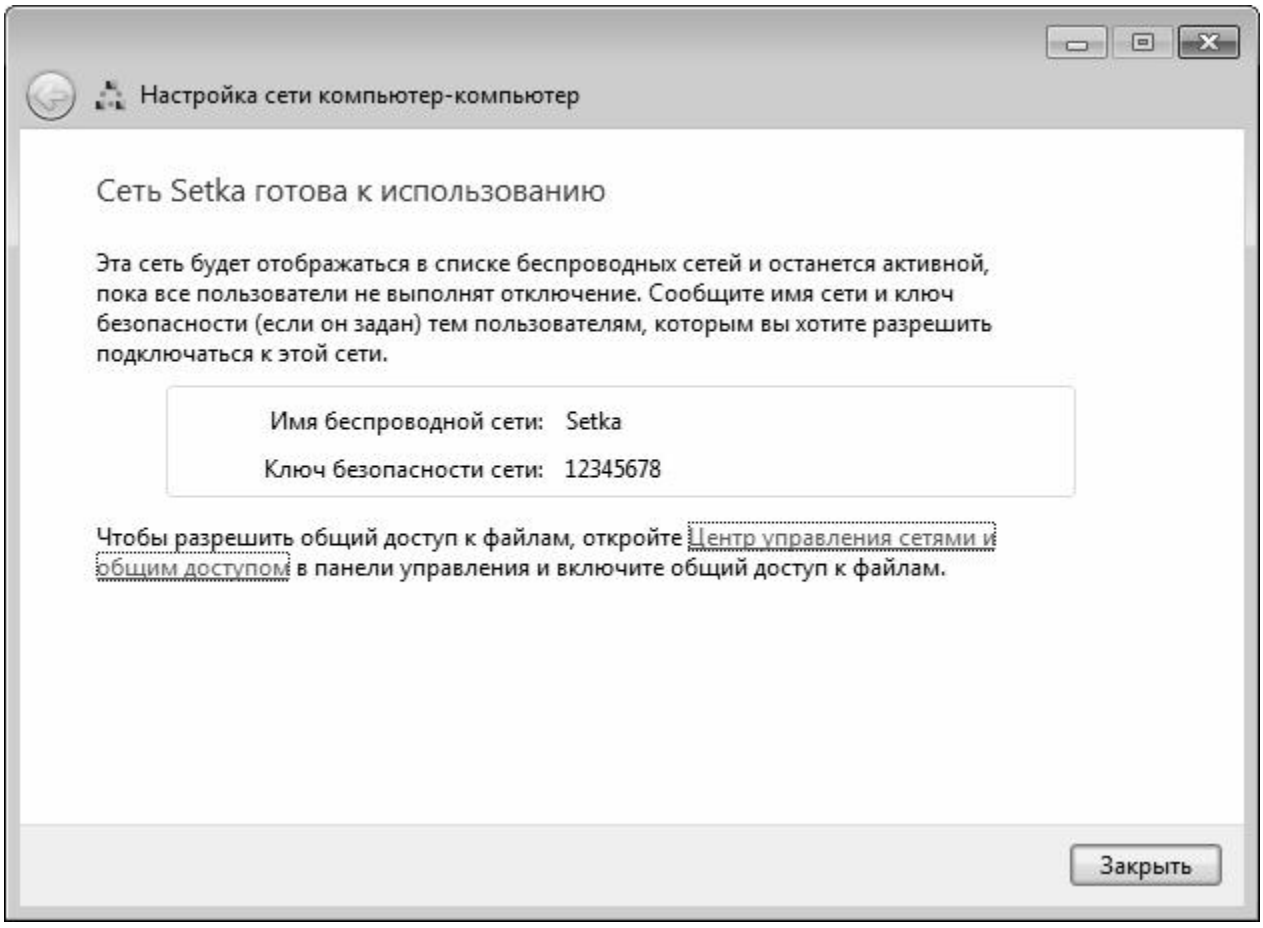



Рис. 4.7. Сообщение об успешном создании беспроводной сети

После нажатия в данном окне кнопки Закрыть созданная беспроводная сеть появится в списке подключений (рис. 4.8).

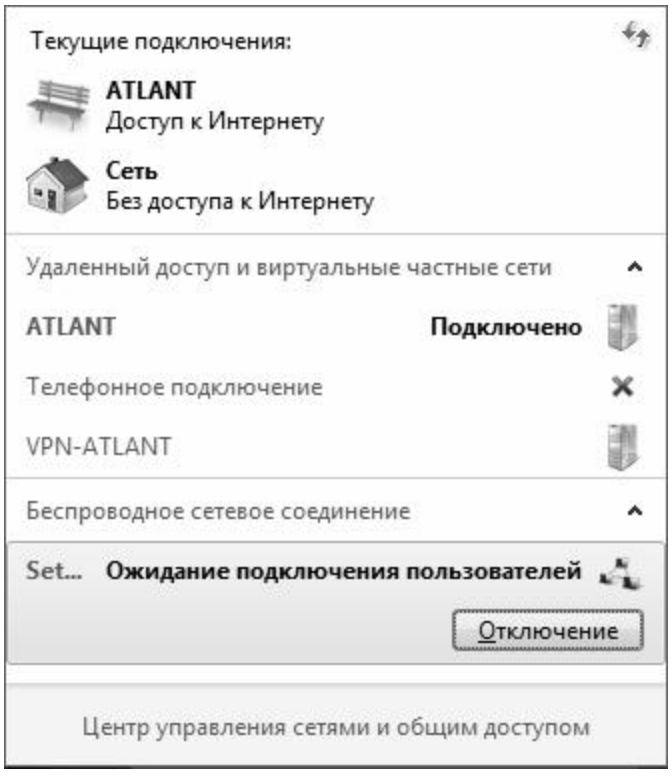


Рис. 4.8. Беспроводная сеть в списке подключений

Чтобы отключиться от беспроводной сети, используйте в данном окне кнопку Отключение.

**Список компьютеров и устройств, подключенных к локальной сети**

Как известно, локальная сеть далеко не всегда ограничивается двумя компьютерами: она может включать в себя множество компьютеров и устройств (принтеров и др.). Следовательно, иногда возникает необходимость подключения то к одному, то к другому сетевому компьютеру или устройству.

Чтобы просмотреть полный список компьютеров и устройств, доступ которым разрешен данному пользователю, выберите в Панели управления категорию Сеть и Интернет, и в открывшемся окне щелкните на ссылке Просмотр сетевых компьютеров и устройств. В результате на экране отобразится окно, изображенное на рис. 4.9.

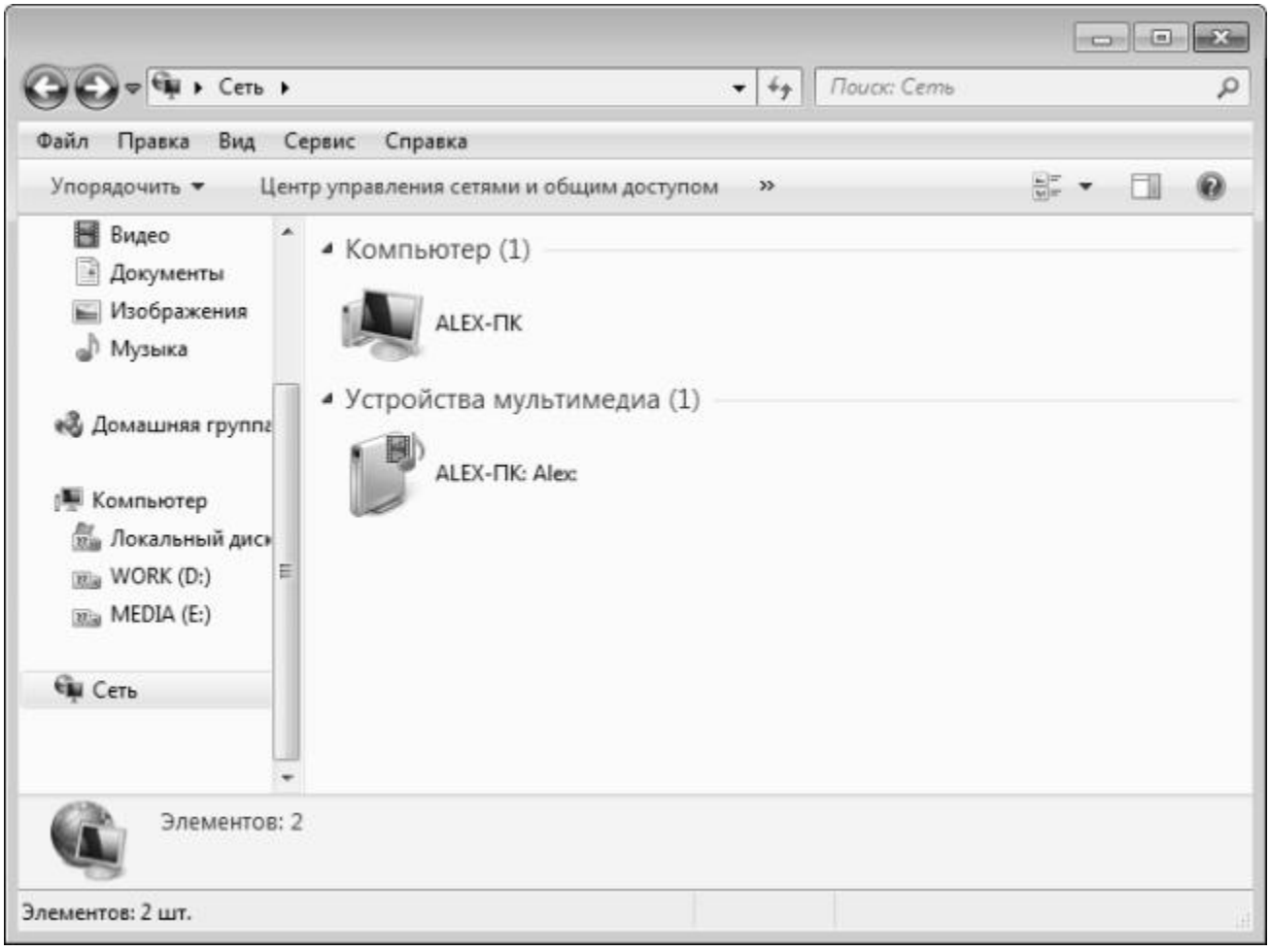



Рис. 4.9. Подключенные к сети компьютеры и устройства

В данном окне содержится перечень всех устройств и компьютеров, доступных по локальной сети. Чтобы подключиться к тому или иному компьютеру, щелкните на нем

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

правой кнопкой мыши и в открывшемся контекстном меню выберите команду Открыть или Открыть в новом окне.

### Выбор сетевого размещения

При первом подключении к локальной сети система попросит пользователя указать сетевое размещение, которому будет отнесено данное подключение. В соответствие с выбранным размещением будут приведены настройки брандмауэра Windows 7, а также прочие параметры безопасности системы.

В Windows 7 предусмотрено использование четырех типов сетевых размещений, которые перечислены ниже.

♦ Домашняя сеть. Данное размещение предназначено для работы в домашних сетях или в сетях, компьютерам которых можно доверять без ограничений. Как правило, компьютеры домашней сети относятся к домашней группе (о том, что представляет собой домашняя группа, будет рассказано в следующем разделе). Режим обнаружения сети, о котором мы говорили ранее (см. рис. 4.3), автоматически включен для домашних сетей.

♦ Сеть предприятия. Этот тип сетевого размещения рекомендуется для работы в локальной сети небольшого офиса или иного подобного рабочего места. Для такой сети также по умолчанию включен механизм сетевого обнаружения, но присоединиться к домашней группе участник рабочей сети не сможет.

♦ Общественная сеть. Данное размещение следует использовать для сетей с низким уровнем доверия. Такое подключение рекомендуется использовать при подключении в общественных местах (Интернет-кафе, вокзал, аэропорт, и т. п.). При работе в условиях общественной сети компьютер становится недоступным для других пользователей, а система автоматически выставляет более строгие параметры безопасности. Механизм сетевого обнаружения в таких сетях по умолчанию выключен, а подсоединение к домашней группе – невозможно.

♦ Домен. Этот тип сетевого размещения применяется в доменных сетях (например, на рабочих станциях в учреждениях и организациях). Такое размещение полностью подконтрольно системному администратору, и пользователь самостоятельно не может выбрать его или изменить.

С точки зрения безопасности из перечисленных сетевых размещений наиболее предпочтительным является общественная сеть.

Чтобы изменить тип сетевого размещения, щелкните в окне Центра управления сетями и общим доступом (см. рис. 4.1) на ссылке, соответствующей текущему названию сетевого размещения (Домашняя сеть, Сеть предприятия или Общественная сеть), и в открывшемся окне укажите требуемый тип размещения.

### Домашняя группа

Домашняя группа – это новый механизм, реализованный в системе Windows 7. Смысл его состоит в том, чтобы предоставить общий доступ к файлам и папкам, а также устройствам всем пользователям, включенным в домашнюю группу. Например, можно

объединить в домашнюю группу все компьютеры домашней сети, или все компьютеры пользователей, которые доверяют друг другу. Отметим, что даже в рамках домашней группы при необходимости можно ограничить доступ к некоторым файлам и папкам. Кроме этого, домашнюю группу можно защитить паролем.

### Создание и настройка домашней группы

Домашняя группа создается автоматически при установке операционной системы. Поскольку в предыдущих версиях Windows данный механизм отсутствовал, объединить в домашнюю группу можно только компьютеры, работающие под управлением Windows 7. Также следует учитывать, что использование домашней группы возможно только при выборе сетевого размещения «Домашняя сеть» (подробнее об этом см. предыдущий раздел).

ПРИМЕЧАНИЕ

Пользователи систем «Windows 7 начальная» и «Windows 7 домашняя» не могут создать домашнюю группу, но могут к ней присоединиться.

Если в компьютере отсутствует домашняя группа (например, ее покинули все пользователи), то ее можно создать. Для этого в категории Сеть и Интернет панели управления щелкните на ссылке Домашняя группа – в результате на экране отобразится окно, которое показано на рис. 4.10.

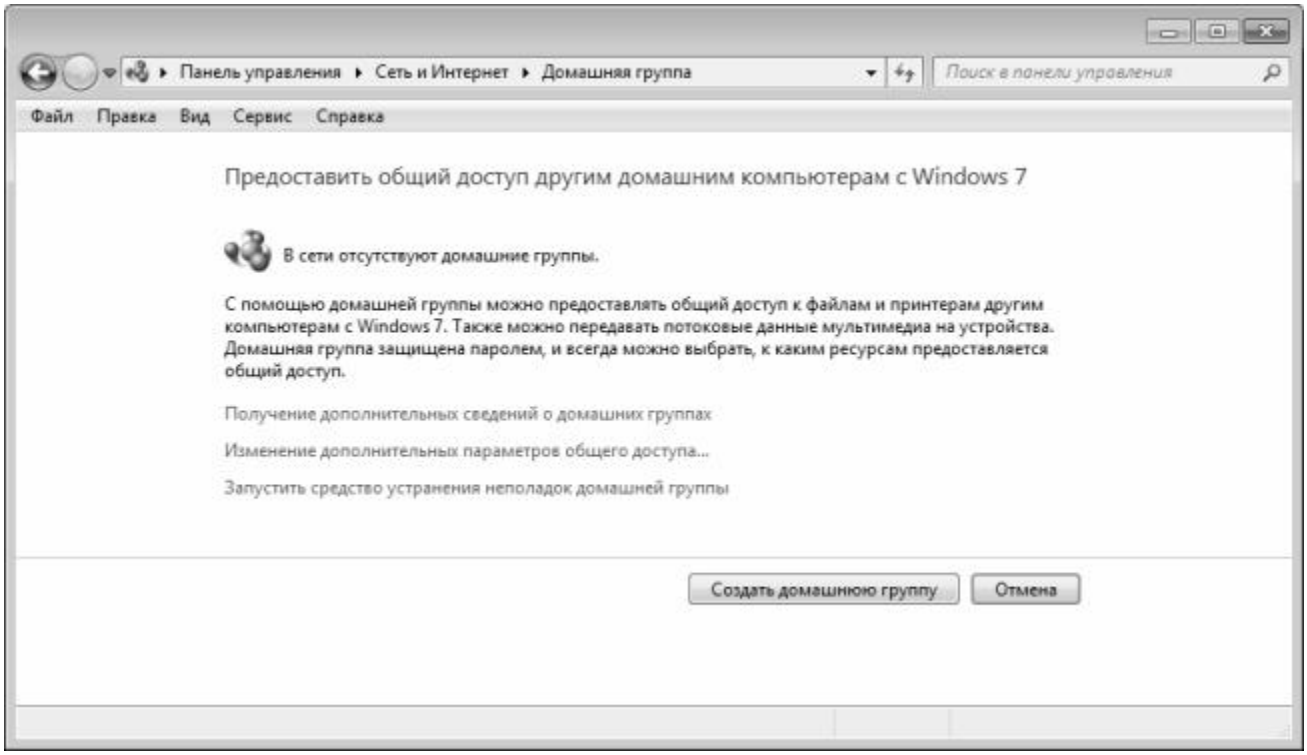



Рис. 4.10. Создание домашней группы

В данном окне нужно нажать кнопку Создать домашнюю группу – в результате будет

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

выполнен переход к параметрам настройки домашней группы (рис. 4.11).

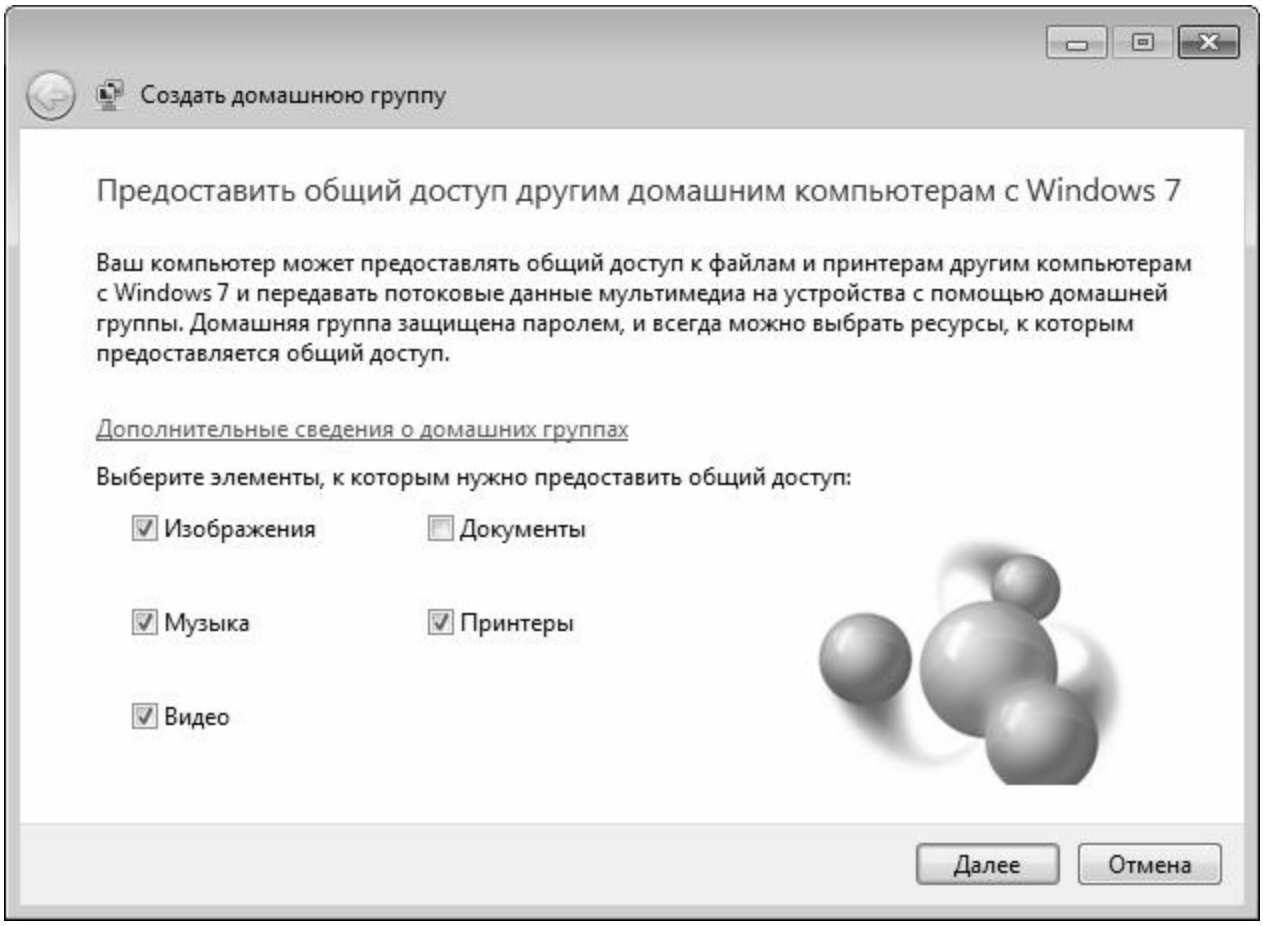



Рис. 4.11. Настройка параметров домашней группы

В данном окне путем установки соответствующих флажков нужно указать элементы, к которым будут иметь доступ все участники домашней группы. После нажатия в данном окне кнопки Далее система предложит запомнить автоматически сгенерированный пароль домашней группы (рис. 4.12).

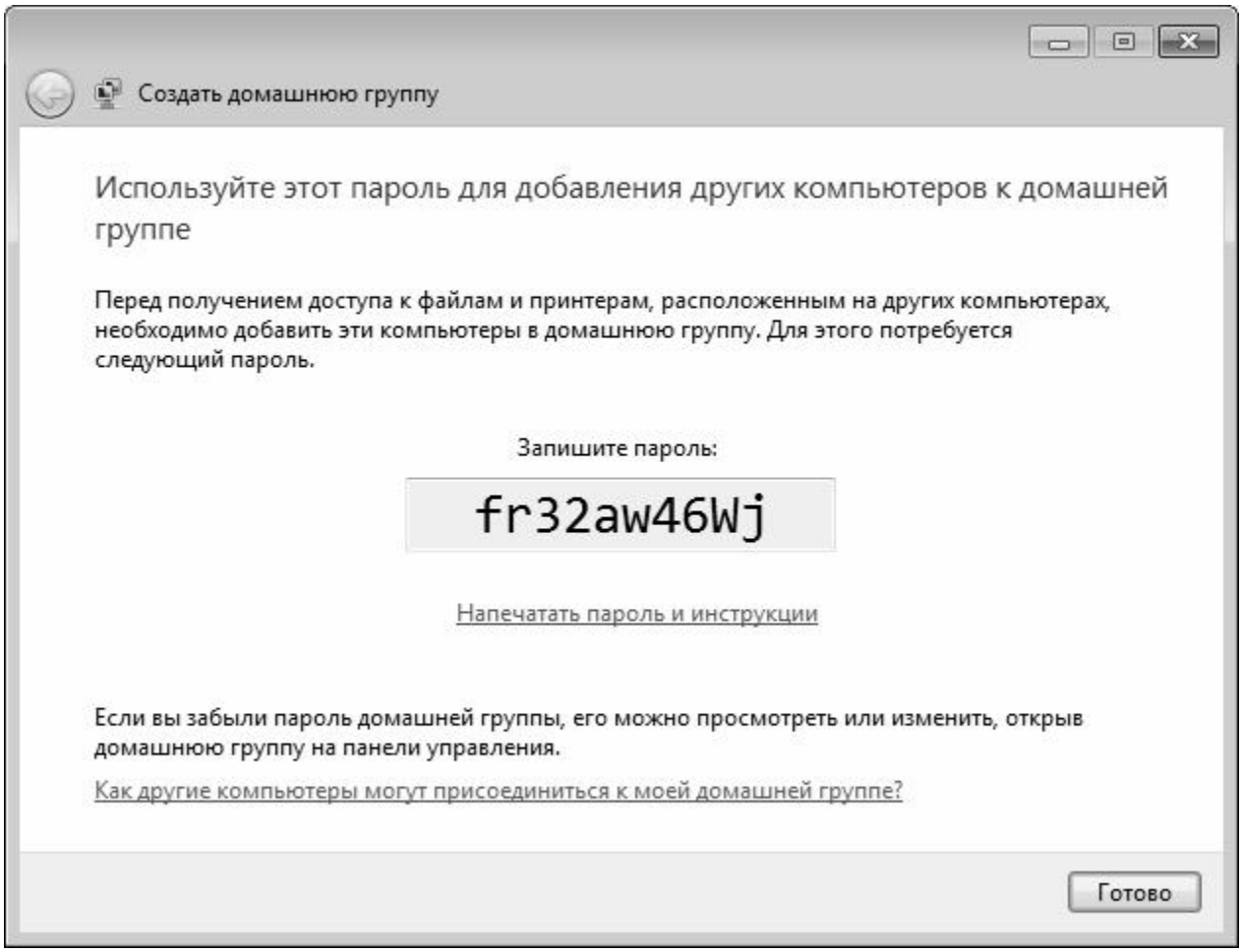



Рис. 4.12. Пароль домашней группы

Этот пароль должны будут указывать другие участники домашней группы для получения доступа к файлам, папкам и устройствам домашней группы.

Чтобы завершить процесс создания домашней группы, нажмите в данном окне кнопку Готово. В результате на экране откроется окно, изображенное на рис. 4.13.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

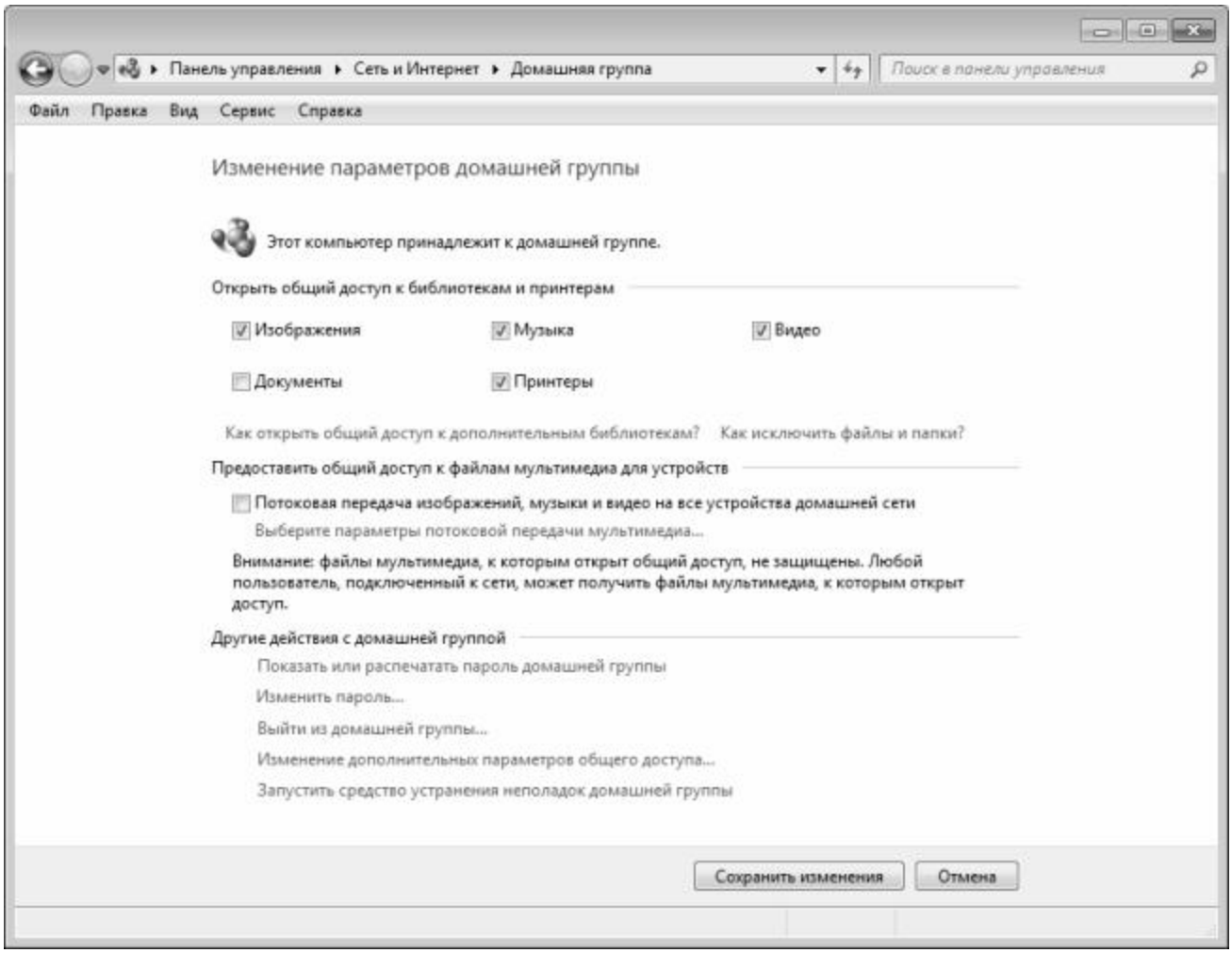



Рис. 4.13. Параметры домашней группы

В данном окне вы можете отредактировать указанные ранее параметры домашней группы. Это окно можно вызвать в любой момент, щелкнув в категории Сеть и Интернет панели управления на ссылке Выбор параметров домашней группы и общего доступа к данным. Если вы забыли или потеряли пароль доступа к домашней группе, щелкните в данном окне на ссылке Показать или распечатать пароль домашней группы, а если вы хотите его изменить – воспользуйтесь ссылкой Изменить пароль.

Вы можете в любой момент выйти из домашней группы – для этого нужно щелкнуть на ссылке Выйти из домашней группы.

Помните, что при присоединении компьютера к домашней группе все созданные в нем учетные записи автоматически становятся членами домашней группы.

### Поиск и устранение неполадок домашней группы

Иногда бывают ситуации, когда в силу каких-то обстоятельств использование домашней группы становится невозможным, либо данный механизм работает нестабильно. Для решения подобных проблем рекомендуется воспользоваться штатным средством устранения неполадок домашней группы. Для этого в окне настройки параметров (см. рис. 4.13) щелкните на ссылке Запустить средство устранения неполадок домашней

группы – в результате на экране откроется окно, изображенное на рис. 4.14.

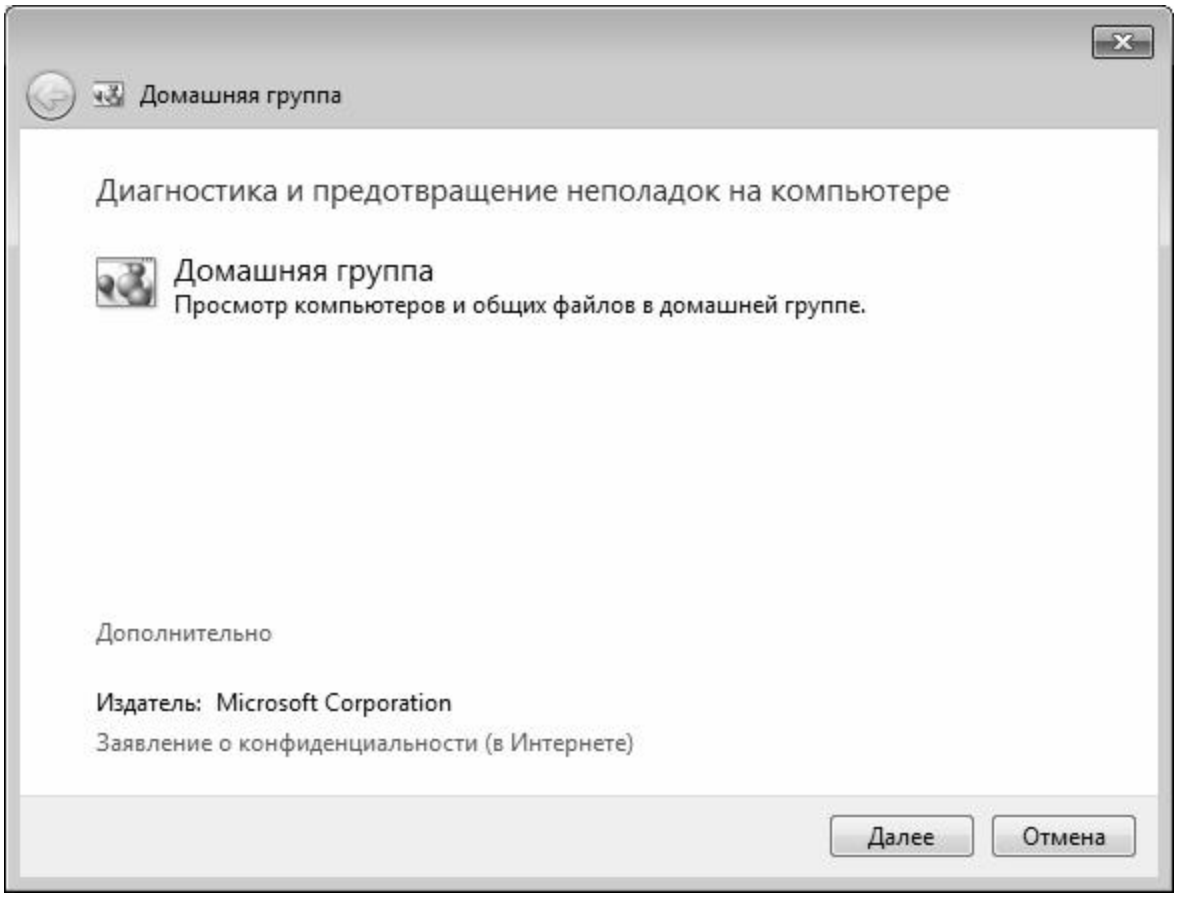



Рис. 4.14. Средство устранения неполадок домашней группы

После нажатия в данном окне кнопки Далее система начнет проверку. Возможные проблемы могут быть обусловлены, например, неполадками в локальной сети (более подробно об этом см. следующий раздел), или какими-то иными причинами. Порядок дальнейших действий зависит от типа обнаруженных неполадок, и в любом случае он большой сложности не представляет, поскольку все необходимые операции выполняются в пошаговом режиме и сопровождаются соответствующими подсказками.

Результаты диагностики выводятся в окне, изображенном на рис. 4.15.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

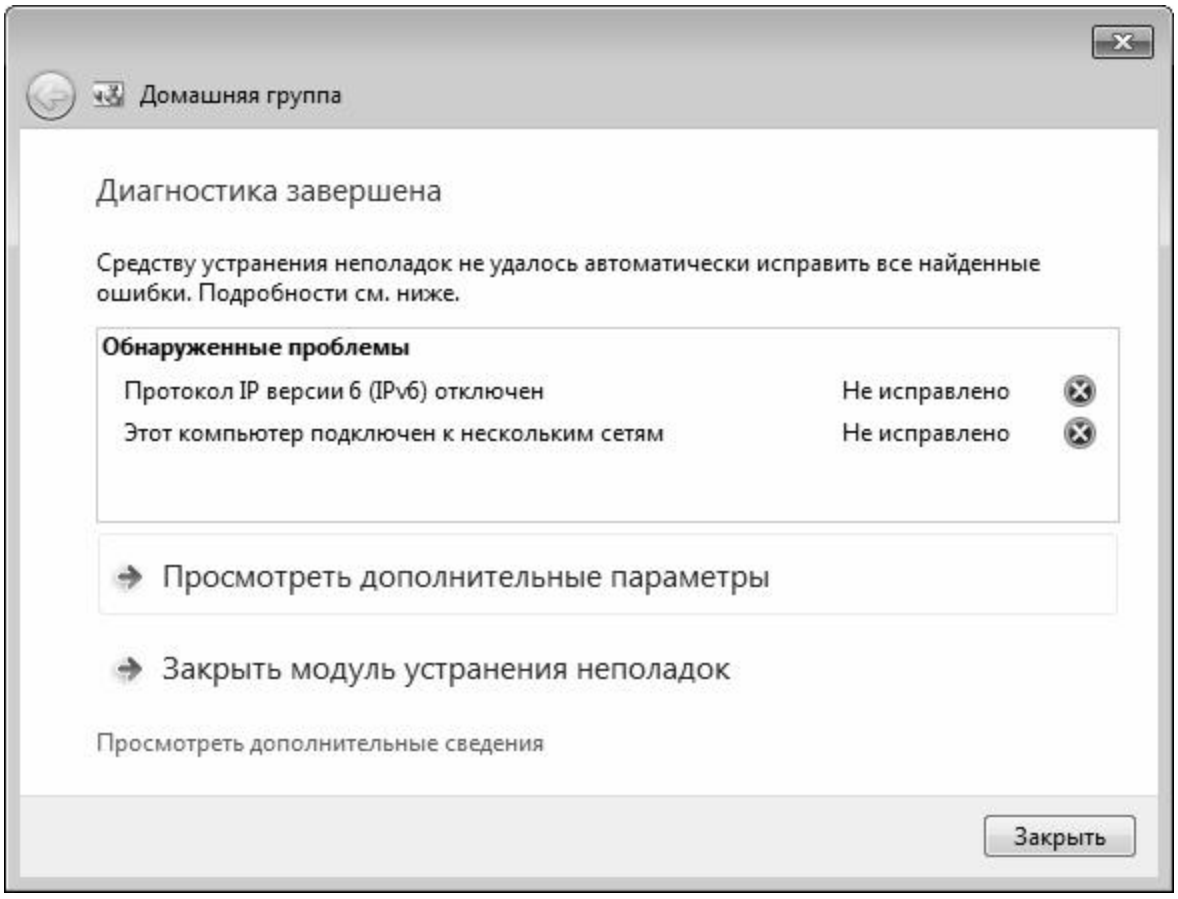



Рис. 4.15. Результат диагностики

В данном окне представлен перечень неполадок, которые могут являться причиной возникновения проблем с домашней группой. После устранения этих неполадок домашняя группа должна работать в нормальном режиме.

**Диагностика и устранение сетевых неполадок**

Локальная сеть представляет собой механизм, функционирование которого зависит от целого ряда внешних факторов: стабильность электропитания, количество и качество установленного на компьютерах программного обеспечения, аппаратное обеспечение компьютеров, защищенность от внешних угроз, и т. д. Каждый их этих факторов может стать причиной нестабильной работы или вообще неработоспособности локальной сети.

Для диагностики и устранения подобных сбоев в системе Windows 7 предусмотрен довольно эффективный штатный механизм устранения сетевых неполадок. Чтобы его запустить, щелкните в окне Центра управления сетями и общим доступом на ссылке Устранение неполадок (см. рис. 4.1). В результате на экране отобразится окно, изображенное на рис. 4.16.

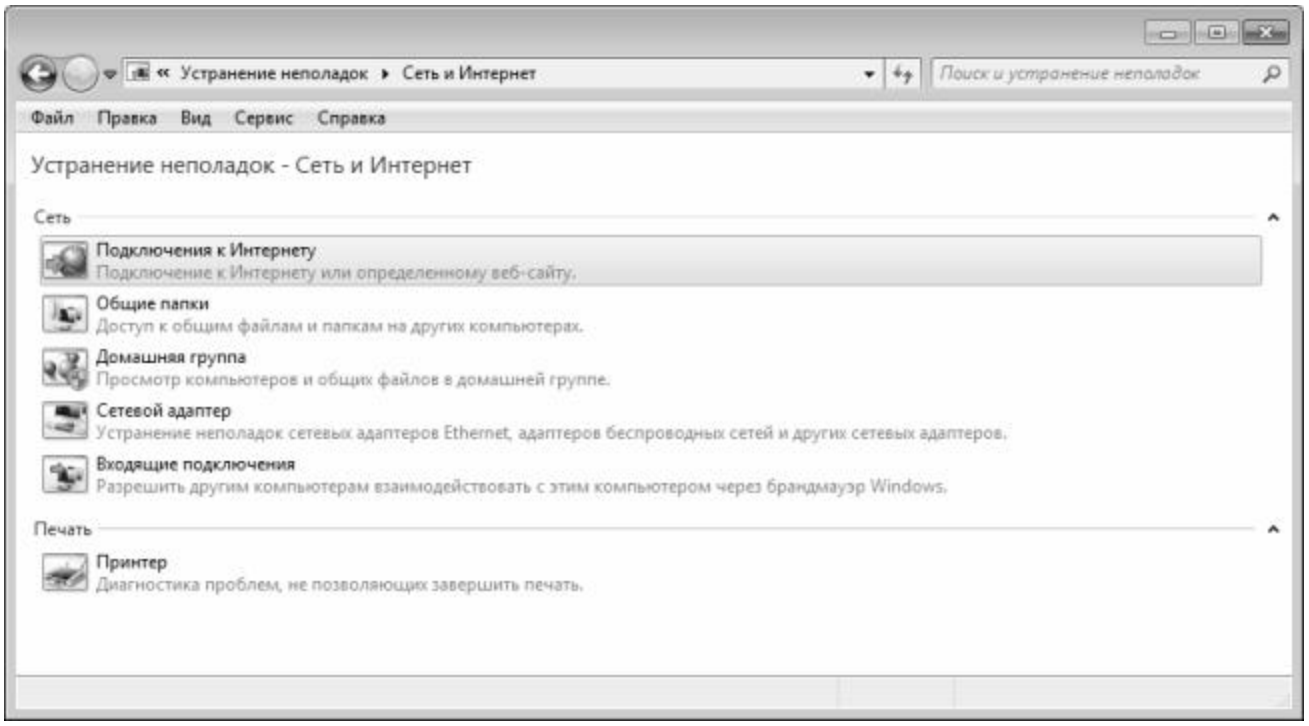



Рис. 4.16. Устранение сетевых неполадок

В данном окне нужно выбрать режим диагностики и устранения неполадок, поскольку дальнейшие действия будут зависеть от выбранного режима.

Если у вас возникли проблемы с подключением к Интернету, выберите в данном окне пункт Подключение к Интернету. На следующем этапе система попросит указать, какого рода проблемы у вас возникли: с выходом в Интернет в целом, или с подключением к конкретной веб-странице. В первом случае будет выполнено тестовое подключение к сайту www.microsoft.com, и в случае обнаружения проблем на экране появится их описание и рекомендации по устранению. Во втором случае нужно будет указать адрес проблемной веб-страницы, и система выяснит причину, по которой не удается открыть данный ресурс.

Аналогичным образом выполняется диагностика и устранение проблем с подключением к общим папкам (нужно будет указать сетевое размещение проблемной папки). Если возникновение сетевых неполадок обусловлено проблемами с сетевым адаптером, выберите в данном окне пункт Сетевой адаптер и следуйте появляющимся на экране указаниям. Все действия выполняются в пошаговом режиме, и, как правило, процесс диагностики и устранения неполадок не вызывает затруднений у пользователей.

При возникновении проблем с входящими подключениями (то есть когда данный компьютер недоступен для других участников сети) щелкните мышью на позиции Входящие подключения. Помимо прочего, Мастер диагностики и устранения неполадок проверит, не обусловлено ли возникновение проблем защитными настройками брандмауэра.

Что касается проблем с домашней группой, то порядок их устранения рассмотрен в предыдущем разделе.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

## Глава 5. Если случилось непоправимое. Как восстановить работоспособность зараженного или испорченного хакерами и вирусами компьютера

Несмотря на многообразие антивирусных средств и достаточно высокую степень их надежности, все равно ни один антивирус не гарантирует стопроцентной защиты компьютера от инфицирования. Здесь мы расскажем о том, какими способами можно восстановить работу зараженного компьютера.

### Компьютер не работает. Что делать?

Если выяснилось, что компьютер поражен вирусом, самое главное – не паниковать и не предпринимать никаких необдуманных действий и «резких движений» (удалять файлы, перезагружать компьютер, и т. п.). Помните, что в большинстве случаев удается выйти из подобных ситуаций без особых потерь, но только тогда, когда все действия были четко продуманы. В любом случае, заражение вирусом – это не самое страшное, что может случиться с компьютером.

Одна из самых неприятных ситуаций – когда отказывается загружаться компьютер либо операционная система. Причиной того, что компьютер не загружается вообще, может быть повреждение вирусом BIOS. В данном случае новичкам рекомендуется самостоятельно не экспериментировать, а обратиться за помощью к профессионалам. В подобных случаях зачастую приходится выполнять перезапись микросхемы BIOS, а эта операция требует немалого опыта и умения.

Если же вирус не вывел из строя BIOS, а лишь несколько подкорректировал параметры его настройки, что стало причиной появления проблем с загрузкой компьютера, то лучше всего в данном случае восстановить настройки BIOS, используемые по умолчанию. Для этого нужно войти в BIOS (для этого в большинстве случаев нужно сразу после включения компьютера нажать и удерживать клавишу Delete, но на ноутбуках могут использоваться другие клавиши – например, F2), и выполнить соответствующую команду. Название этой команды зависит от версии BIOS, но в любом случае ее найти несложно (она может называться, например, Fail-Safe Defaults или Load BIOS Defaults).

Но чаще бывает так, что компьютер загружается нормально, а вот Windows – нет. Первое, что нужно попробовать в такой ситуации – это загрузить систему в одном из дополнительных режимов (для выбора режима загрузки нужно, находясь в интерфейсе загрузочного меню, нажать клавишу F8). В результате на экране откроется меню выбора режима загрузки.

Первый режим, который рекомендуется выбрать – это режим загрузки последней удачной конфигурации. Сущность его состоит в том, что при загрузке Windows будут задействованы те ее параметры и настройки, которые применялись при последнем удачном запуске.

Если эта попытка оказалась безуспешной, выберите для загрузки режим отладки либо безопасный режим. Эти режимы позволяют загрузить Windows с определенными ограничениями ее функциональности.

ПРИМЕЧАНИЕ

Если все попытки запустить Windows оказались неудачными – ищите неисправность в аппаратной части компьютера, либо переустанавливайте Windows. И в первом, и во втором случае новичкам рекомендуется не действовать самостоятельно, а обратиться за помощью к специалистам.

Если же Windows все же удалось запустить в одном из нестандартных режимов, попробуйте выполнить перечисленные ниже действия.

♦ Просканируйте компьютер хорошей антивирусной программой с актуальными сигнатурными базами.

♦ Выполните восстановление Windows (Пуск ▸ Все программы ▸ Стандартные ▸ Служебные ▸ Восстановление системы). Эта функциональность предназначена для возврата Windows к одному из предыдущих состояний. Иногда это устраняет последствия деятельности вирусов и прочего вредоносного ПО.

♦ Выполните резервное копирование хранящейся в компьютере информации на внешний носитель или на сетевой диск (особенно, если сканирование антивирусом не принесло результатов) – ведь неизвестно, как поведет себя Windows при следующей загрузке.

Обычно при заражении вирусами проблема устраняется после проверки компьютера хорошей антивирусной программой. Отметим, что некоторые антивирусы умеют «откатывать» Windows к «довирусному» состоянию.

Если Windows категорически не желает загружаться ни в одном из режимов и очевидно, что без ее переустановки (а возможно – и без форматирования жесткого диска) не обойтись, то нужно постараться сохранить имеющиеся в компьютере данные. Попробуйте загрузиться в режиме MS-DOS с загрузочного диска, и перенести данные на внешние носители (флеш-накопитель, компакт-диск, сетевой диск и др.).

**Диагностика жесткого диска с помощью Hard Drive Inspector**

Здесь мы расскажем о том, каким образом можно проверить состояние жесткого диска и узнать, не нужно ли срочно предпринять какие-либо действия по предотвращению его порчи либо для спасения хранящейся на нем информации.

Одним из наиболее распространенных и удобных продуктов, предназначенных для диагностики состояния жесткого диска, является программа Hard Drive Inspector от компании AltrixSoft (сайт разработчика – www.altrixsoft.com). Данная утилита является условно-бесплатной, ее демонстрационную версию, которая функционирует в течение 14 дней с момента инсталляции, можно скачать на сайте разработчика.

Устанавливается программа стандартным образом – для этого нужно запустить инсталляционный файл и выполнять рекомендации мастера установки. По окончании инсталляции в меню Пуск будет создана программная группа Hard Drive Inspector.

Утилита довольно проста и удобна в работе, обладает понятным интерфейсом и, что немаловажно – поддерживает русский язык, чем выгодно отличается от многих аналогичных продуктов (выбор языка осуществляется на стадии установки программы, но впоследствии его можно изменить в настройках).

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

**Общий принцип работы программы**

После установки программа осуществляет постоянный мониторинг технических условий эксплуатации используемых в компьютере дисков. Во многих случаях она способна заблаговременно уведомить пользователя о приближающейся поломке жесткого диска, которая может произойти в ближайшем будущем. Это дает возможность пользователю своевременно скопировать всю имеющуюся информацию в другое место и заменить ненадежный диск, избежав тем самым потерю данных.

Принцип работы программы базируется на использовании технологии S.M.A.R.T., которая была специально разработана и создана для своевременного распознавания грядущих поломок жестких дисков. Поддерживающие данную технологию жесткие диски включают в себя интеллектуальные процедуры самодиагностики и могут информировать о своем нынешнем состоянии. Данные диагностические сведения выводятся в виде коллекции атрибутов. В данном случае атрибутом считается конкретная характеристика жесткого диска, применяемая для анализа его надежности, работоспособности и производительности. Например, S.M.A.R.T.– атрибутами являются характеристики Seek Error Rate (Частота ошибок позиционирования) и Spin-Up Time (Время раскрутки шпинделя диска). Стоит отметить, что перечень применяемых атрибутов индивидуален для каждого производителя, а в некоторых случаях – даже для разных модификаций дисков от одного изготовителя. Тем не менее, преимущественная часть ключевых атрибутов для всех жестких дисков имеет один и тот же смысл.

Все атрибуты имеют текущее значение, которым является любое число из диапазона от 1 до 100, 200 или 253 (отметим, что общих стандартов для верхних границ значений атрибута не предусмотрено; данный показатель может иметь различие даже для разных атрибутов одного и того же жесткого диска). Текущее значение со временем со временем может изменяться (обычно в сторону уменьшения), демонстрируя тем самым отрицательную динамику параметров жесткого диска, характеризуемых данным атрибутом.

Помимо текущего значения, каждый атрибут имеет критическое значение, установленное предприятием-изготовителем. Если текущее значение какого-нибудь атрибута становится равным критическому или, что еще хуже – меньше его, тогда жесткий диск считается ненадежным. В частности, снижение атрибута Spin-Up Time (Время раскрутки шпинделя диска) меньше критического значения обычно свидетельствует о том, что механическая часть диска сильно изношена и диск больше не в состоянии поддерживать скорость вращения, установленную предприятием изготовителем.

Стоит отметить, что программу Hard Drive Inspector компания AltrixSoft выпускает в двух вариантах: для стационарных компьютеров (версия Professional, которая рассматривается в данной книге), и для ноутбуков (версия for Notebooks). Отметим, что в версии for Notebooks реализована вся функциональность версии Professional, но при этом в ней учитывается специфика мониторинга жестких дисков ноутбуков. Необходимость создания версии для ноутбуков вызвана тем, что эти компьютеры имеют следующие характерные особенности:

♦ Жесткий диск ноутбука часто и помногу испытывает существенные механические вибрации (это происходит при транспортировке ноутбука), причем даже в работающем

состоянии переносной компьютер не всегда неподвижен (например, многие любят работать в поезде или в автобусе). Подобные вибрации всячески способствуют преждевременному износу механической части жесткого диска.

♦ Свое влияние оказывает и нестабильность электропитания. Даже если ноутбук имеет хороший блок питания в режиме энергопотребления от электросети, при работе от аккумулятора винчестер может не получать достаточной для бесперебойной работы мощности. В данном случае он не состоянии обеспечивать постоянную скорость вращения пластин, что может привести к возникновению bad-блоков.

♦ В ноутбуках система охлаждения является менее эффективной, в отличие от стационарных компьютеров. Это приводит к тому, что многие элементы ноутбука (и жесткий диск – в том числе) работают в условиях, приближенных к максимально допустимым температурным значениям.

Однако внешне порядок работы с версиями Professional и for Notebooks практически не отличается.

**Настройка программы и подготовка ее к работе**

Программа начинает проводить диагностику жесткого диска и выдавать пользователю соответствующую информацию его состоянии сразу после запуска. Однако иногда бывает полезно просмотреть и, при необходимости – отредактировать параметры ее настройки. Кстати, в отличие от многих аналогов Hard Drive Inspector обладает довольно гибкой настройкой, что позволяет легко адаптировать ее к потребностям конкретного пользователя.

Чтобы перейти к настройкам программы, нужно в инструментальной панели нажать кнопку Настройки. В результате на экране отобразится окно настройки параметров, которое показано на рис. 5.1.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

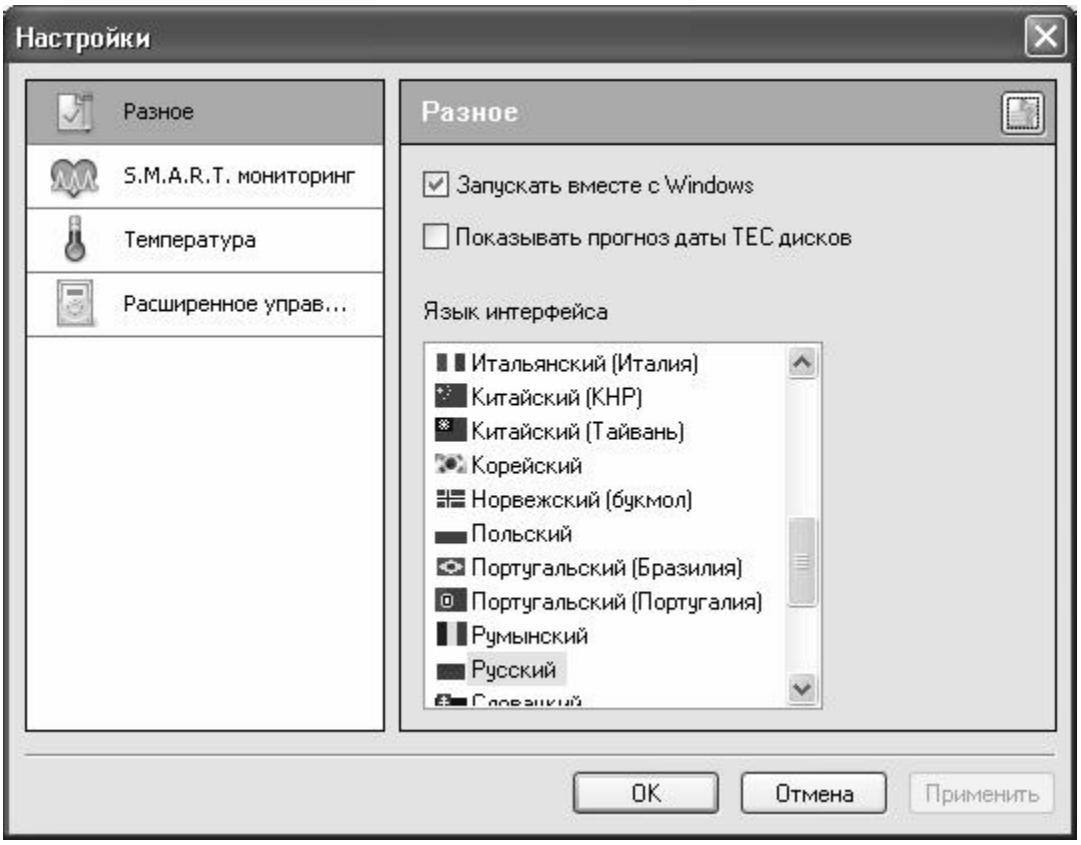



Рис. 5.1. Настройка программы, раздел Разное

Режим настройки содержит четыре раздела, перечень которых представлен в левой части окна. Выбор требуемого раздела осуществляется щелчком мыши – при этом в правой части отобразятся входящие в его состав параметры.

В разделе Разное содержатся параметры общего характера. Если установлен флажок Запускать вместе с Windows, то программа будет автоматически запускаться одновременно с загрузкой операционной системы. Чтобы убрать Hard Drive Inspector из каталога автозагрузки, снимите этот флажок. При этом не стоит забывать, что если программа не запустилась с загрузкой системы – то и диагностика выполняться не будет до тех пор, пока пользователь ее не запустит с помощью соответствующей команды меню Пуск.

Если в данном разделе установить флажок Показывать прогноз даты ТЕС дисков, то программа будет автоматически рассчитывать прогнозную дату предполагаемого выхода жесткого диска из строя (или когда он окажется в критическом состоянии). Стоит отметить, что данный прогноз является довольно приблизительным и условным, поэтому его не стоит рассматривать в качестве надежного источника информации. По большому счету, он является лишь дополнением к основным диагностическим данным, отображающимся в главном окне программы в разделе Основная информация (более подробно с этим режимом работы мы познакомимся ниже).

В поле Языки интерфейса представлен перечень языков, поддерживаемых программой. Как мы уже отмечали ранее, требуемый язык выбирается в начале инсталляции, однако в настройках программы его при необходимости можно изменить. Для этого следует выделить требуемую позицию щелчком мыши и нажать кнопку Применить или ОК.

Содержимое раздела S.M.A.R.T. мониторинг показано на рис. 5.2.

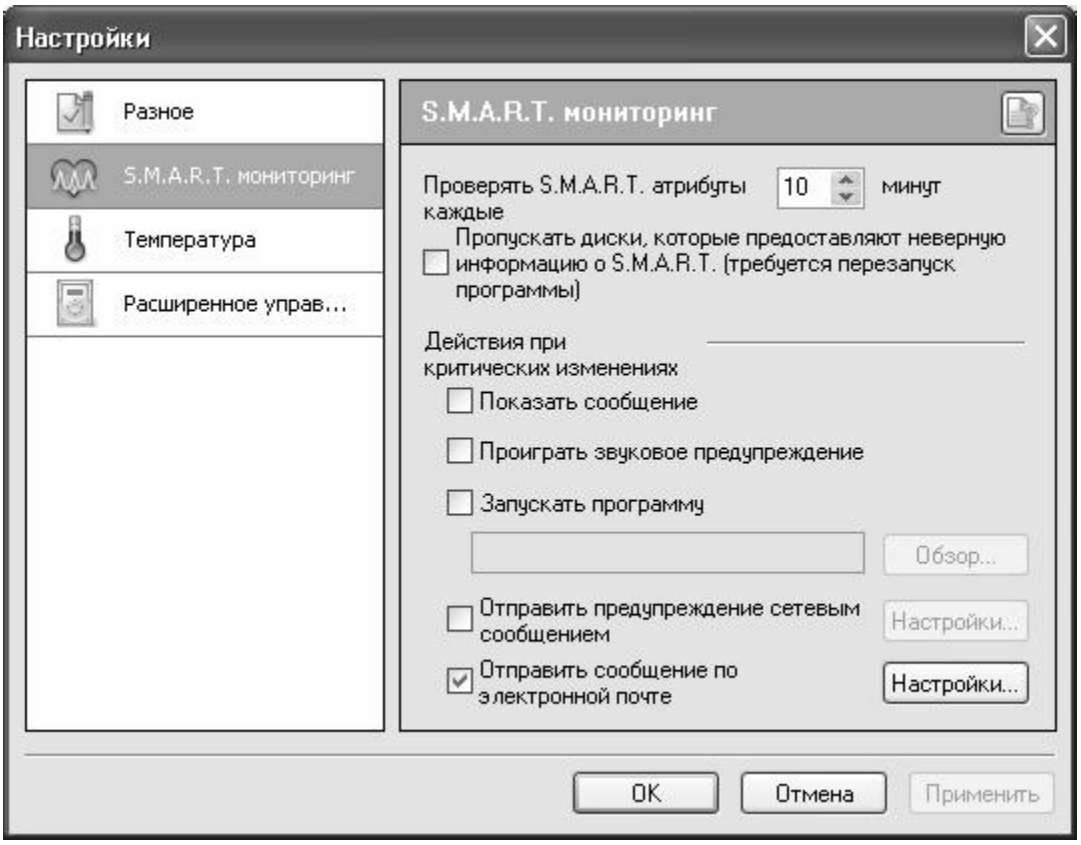



Рис. 5.2. Настройка программы, раздел S.M.A.R.T. мониторинг

С помощью параметра Проверять S.M.A.R.T. атрибуты каждые указывается интервал времени в минутах, через который должна осуществляться автоматическая проверка состояния диска на основе S.M.A.R.T.-технологии. Чем этот интервал меньше – тем больше вероятность того, что неисправность будет распознана своевременно и пользователь успеет предпринять необходимые меры для сохранения важной информации. Однако не стоит забывать и тот факт, что при слишком частых проверках работоспособность и быстродействие компьютера могут снизиться, поскольку часть ресурсов расходоваться на тестирование жесткого диска. По умолчанию данному параметру установлено значение 10, и в большинстве случаев оно является оптимальным.

С помощью группы параметров Действия при критических изменениях можно определить действия программы, которые она должна предпринять в случае, когда состояние жесткого диска приблизится к критическому. Если установлен флажок Показать сообщение, то в подобной ситуации на экране отобразится соответствующее информационное сообщение. Чтобы включить звуковое оповещение о приближающейся опасности, следует установить флажок Проиграть звуковое оповещение. Этот параметр особенно удобно использовать в случае, когда пользователь отлучается от работающего компьютера: ведь появившееся на экране информационное сообщение он увидеть не сможет.

С помощью параметра Запускать программу можно указать приложение или команду, которые должны автоматически выполняться при возникновении критической ситуации. В частности, этот параметр позволяет сделать так, что при появлении опасности начнется автоматическое резервное копирование данных в надежное место. Установите флажок Запускать программу – в результате станет доступным расположенное ниже поле, а также находящаяся справа от него кнопка Обзор. При нажатии данной кнопки на экране

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

отобразится окно, в котором нужно указать путь к исполняемому файлу требуемого приложения и нажать кнопку Открыть. Выбранный путь отобразится в поле под флажком Запускать программу.

Если установлен флажок Отправить предупреждение сетевым сообщением, то при возникновении критической ситуации программа автоматически направит соответствующее предупреждение на удаленный компьютер с помощью стандартной команды net send. Чтобы указать этот компьютер, нажмите кнопку расположенную справа кнопку Настройки (она становится доступной только при установленном флажке Отправить предупреждение сетевым сообщением), затем в открывшемся окне с клавиатуры введите имя (адрес) компьютера и нажмите кнопку ОК или клавишу Enter.

Аналогичным образом можно выполнить настройку отправки сообщения о приближении критической ситуации по электронной почте. Для этого нужно установить флажок Отправить сообщение по электронной почте и нажать расположенную справа кнопку Настройки (она становится доступной только при установленном данном флажке). В результате выполненных действий на экране откроется окно, изображенное на рис. 5.3.

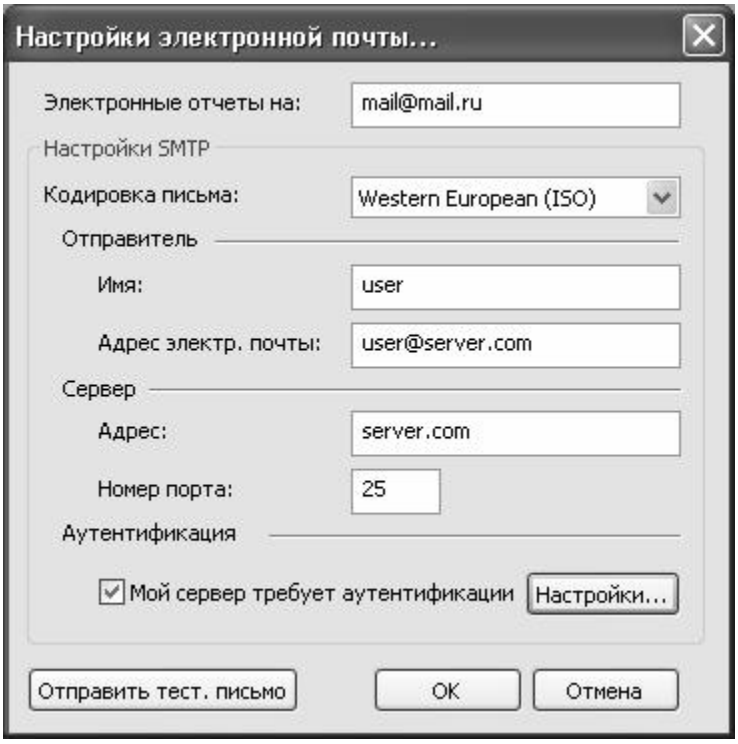



Рис. 5.3. Настройка параметров отправки сообщения по электронной почте

В данном окне осуществляется настройка параметров отправки сообщения. В поле Электронные отчеты на следует с клавиатуры ввести адрес электронной почты, на который должно отправляться информационное сообщение. Отметим, что в случае ввода некорректного адреса программа выдаст соответствующее предупреждение.

В области настроек Настройки SMTP указываются необходимые сведения об учетной записи почтового ящика, который будет использоваться программой для соединения с почтовым сервером. Как правило, здесь применяются те же самые настройки, которые определены для исходящей почты используемой почтовой программы (Microsoft Outlook, Outlook Express, The Bat, и др.). Если настройка этих параметров вызывает у вас затруднения, то проконсультируйтесь у сетевого администратора или у интернет-

провайдера.

В поле Кодировка письма из раскрывающегося списка следует выбрать кодировку символов, которая используется для отправки почтовых сообщений. Как правило, значение, предложенное по умолчанию, является оптимальным.

В поле Имя с клавиатуры вводится значение, которое будет в полученном почтовом сообщении отображаться в поле От (попросту говоря, имя отправителя). Здесь можно ввести название программы – Hard Drive Inspector, или значение, кратко отражающее суть почтового сообщения – например, Внимание, проблемы с жестким диском, и т. п. Это позволит быстро обратить внимание на данное почтовое сообщение и сразу выделить его среди прочей электронной корреспонденции.

В поле Адрес электр. почты следует ввести адрес электронного почтового ящика, с которого будет отправлено сообщение и проблемах с жестким диском.

В области Сервер указываются параметры SMTP-сервера исходящих почтовых сообщений. В поле Адрес вводится его адрес, а в поле Порт – номер порта SMTP-сервера (в большинстве случаев здесь нужно ввести значение 25, и именно его программа предлагает использовать по умолчанию).

Если используемый вами SMTP-сервер для отправки электронных почтовых сообщений требует авторизации, то установите флажок Мой сервер требует аутентификации и нажмите расположенную справа кнопку Настройки. После этого в открывшемся окне с клавиатуры введите логин, пароль, из раскрывающегося списка выберите метод аутентификации (обычно оптимальным является значение, предложенное по умолчанию) и нажмите кнопку ОК.

Чтобы выполненные настройки электронной почты вступили в силу, нажмите в окне Настройки электронной почты кнопку ОК.

Одним из важнейших показателей работоспособности жесткого диска является его температура. Ведь его чрезмерное нагревание может стать причиной снижения производительности и надежности, а также заметно сократить срок службы диска. К примеру, максимально допустимая рабочая температура жестких дисков серии Western Digital's Caviar составляет 55 градусов по Цельсию (131 по Фаренгейту), однако ее снижение до 45 градусов по Цельсию (113 по Фаренгейту) способно повысить их надежность в два раза.

Если используемый на компьютере жесткий диск оборудован встроенным датчиком температуры, то программа Hard Drive Inspector может отслеживать его температуру. Настройка соответствующих параметров осуществляется в разделе Температура, содержимое которого показано на рис. 5.4.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

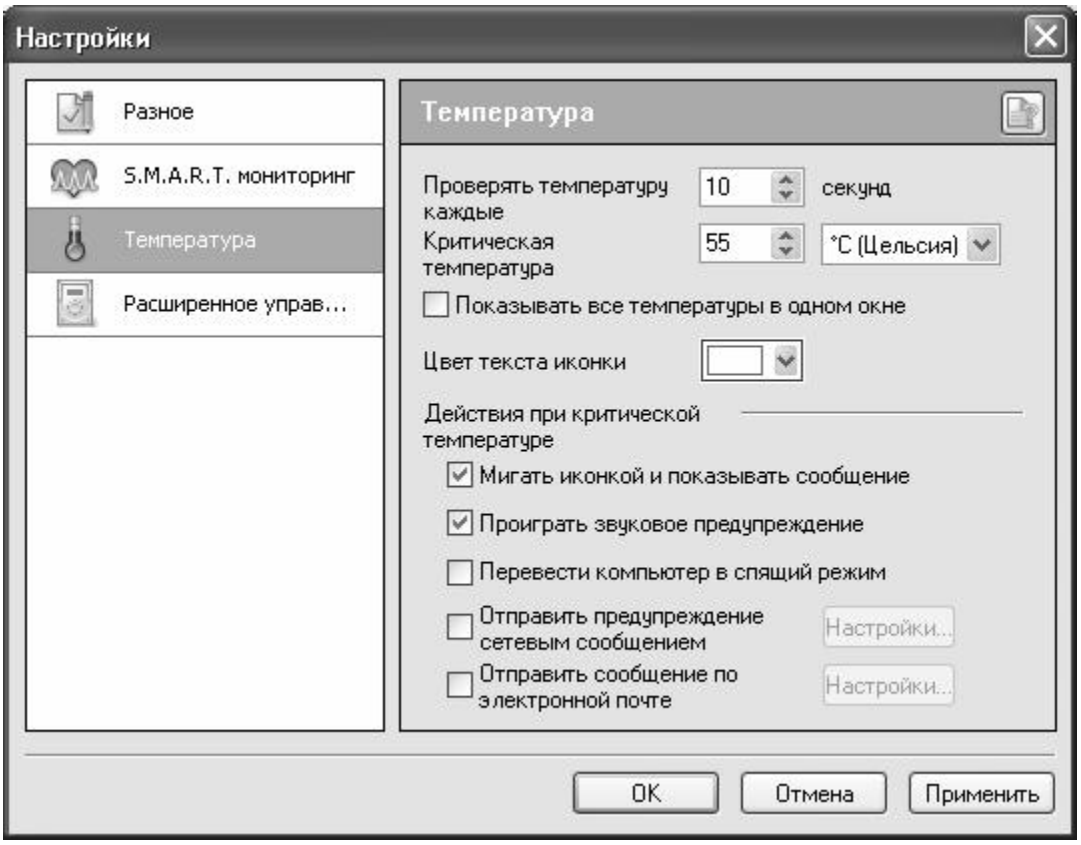



Рис. 5.4. Настройка параметров слежения за температурой

В поле Проверять температуру каждые с клавиатуры либо с помощью кнопок счетчика можно указать интервал времени, через который программа должна выполнять автоматическую проверку температуры жесткого диска. Данный показатель выражается в секундах, и он не может быть меньше 10 секунд (именно это значение предлагается в программе по умолчанию).

С помощью параметра Критическая температура следует указать максимально допустимое значение температуры для данного жесткого диска. Этот параметр включает в себя два поля: в первом из них нужно указать конкретное температурное значение, а во втором из раскрывающегося списка выбрать единицу измерения (по Цельсию или по Фаренгейту). При каждом перевыборе единицы измерения числовой показатель температуры изменится автоматически. Другими словами, если в первом поле указано значение 55, а во втором – *C (Цельсия), то после выбора во втором поле значения *F (Фаренгейта) числовой показатель автоматически примет значение 131.

Когда температура жестокого диска достигнет указанного здесь значения, то программа автоматически начнет предпринимать действия, указанные в области настроек Действия при критической температуре. Отметим, что максимально допустимая температура жесткого диска определяется его заводом-изготовителем. Для большинства современных жестких дисков она составляет 55 градусов по Цельсию или 131 градус – по Фаренгейту.

Если установлен флажок Показывать все температуры в одном окне, то для всех используемых жестких дисков информация о температуре будет выводиться в одном всплывающем окне. При снятом данном флажке температура каждого диска будет показана в отдельной иконке. При этом цвет иконки выбирается из расположенного ниже раскрывающегося списка (поле Цвет текста иконки). Очевидно, что использование данного параметра имеет смысл только в том случае, если на компьютере эксплуатируется

несколько жестких дисков.

В области настроек Действия при критической температуре пользователь определяет действия программы, которые она должна будет предпринять, когда температура жесткого диска превысит максимально допустимое значение (которое указано выше, с помощью параметра Критическая температура). Если установить флажок Мигать иконкой и показывать сообщение, то о возникшей ситуации пользователь будет информирован с помощью мигающей иконки и появившегося на экране информационного сообщения. Можно сделать так, что при превышении температурой максимально допустимого значения компьютер будет автоматически переведен в спящий режим с одновременной остановкой всех жестких дисков – для этого достаточно установить флажок Перевести компьютер в спящий режим.

Что касается параметров Проиграть звуковое предупреждение, Отправить предупреждение сетевым сообщением и Отправить сообщение по электронной почте, то они настраиваются таким же образом, как и в разделе S.M.A.R.T. мониторинг, описание которого приведено выше.

В некоторых современных жестких дисках реализована поддержка современных возможностей для управления шумом и энергопотреблением. Программа Hard Drive Inspector предоставляет механизм управления этими возможностями для каждого используемого на компьютере жесткого диска. Необходимые действия выполняются в настройках программы в разделе Расширенное управление, содержимое которого показано на рис. 5.5.

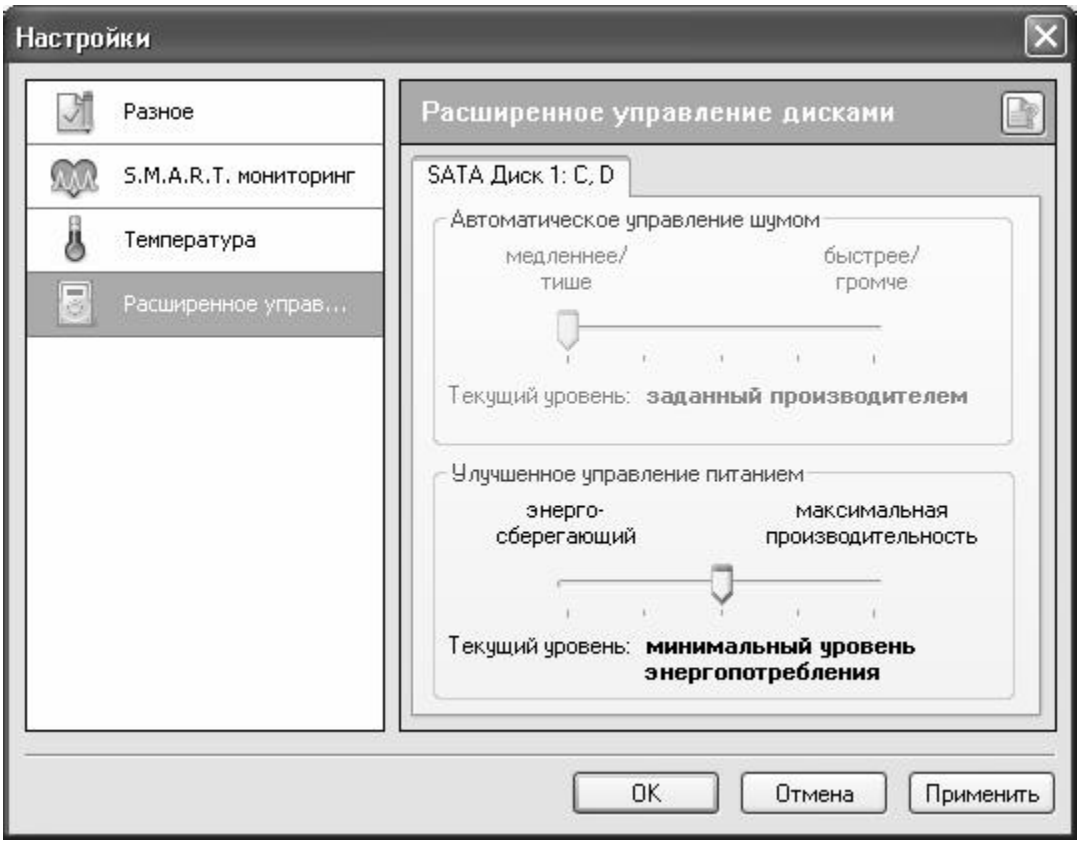



Рис. 5.5. Настройка параметров, раздел Расширенное управление

Технология автоматического управления шумом создана и разработана для снижения уровня шума, издаваемого жесткими дисками, за счет незначительного падения

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

производительности. Обычно в жестких дисках данный механизм по умолчанию отключен, однако вы можете включить его в разделе Расширенное управление. Для этого в области настроек Автоматическое управление шумом следует перетащить ползунок в требуемое положение. При этом в информационной строке Текущий уровень отобразится краткое описание выбранного положения (по умолчанию здесь отображается значение заданный производителем).

Механизм улучшенного управления питанием позволяет уменьшить потребление электроэнергии жестким диском за счет незначительного снижения его производительности. Для этого в области настроек Улучшенное управление питанием следует перетащить ползунок в требуемое положение. При этом в информационной строке Текущий уровень отобразится краткое описание выбранного положения (по умолчанию здесь отображается значение минимальный уровень энергопотребления).

Все настройки, выполненные в разделах окна Настройки, вступают в силу после нажатия кнопки ОК (с одновременным закрытием окна) либо Применить (окно останется открытым). С помощью кнопки Отмена осуществляется выход из данного режима без сохранения выполненных изменений. Перечисленные кнопки доступны во всех разделах окна.

**Проведение диагностики**

Как мы уже отмечали выше, диагностика жесткого диска программой Hard Drive Recovery начинается сразу же после ее запуска. Интерфейс программы в режиме диагностики показан на рис. 5.6.

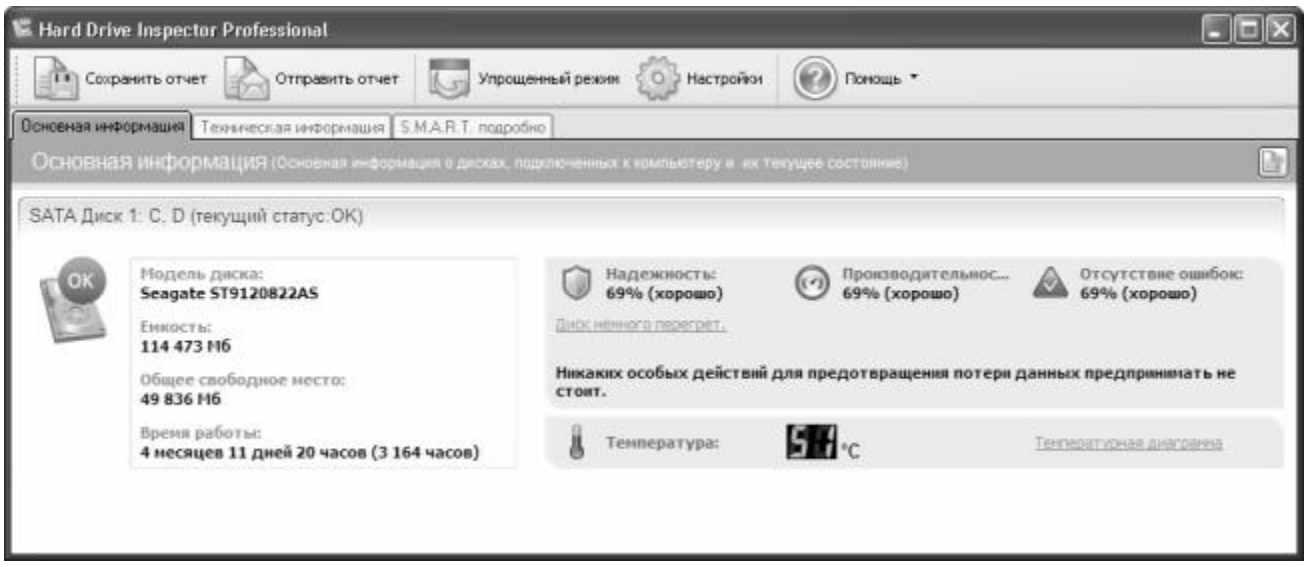



Рис. 5.6. Диагностика жесткого диска в программе Hard Drive Recovery

В верхней части окна программы расположена инструментальная панель, кнопки которой предназначены для активизации соответствующих функций программы, перехода в режим настройки, переключения режимов отображения данных, а также вызова справочной информации.

С помощью кнопки Сохранять отчет вы можете сохранить отчет о состоянии жесткого

диска в отдельном файле формата TXT или HTML (последний вариант предлагается по умолчанию). При нажатии данной кнопки на экране отображается окно Сохранить отчет как, в котором нужно указать путь для сохранения, имя файла отчета и его тип, после чего нажать кнопку Сохранить. Эту возможность удобно использовать, например, при обнаружении неполадок в работе жесткого диска – это может намного упростить поиск причины неисправности. Даже если вам непонятна содержащаяся в отчете информация, она может оказаться весьма ценной для специалиста, к которому вы решите обратиться за помощью.

С помощью кнопки Отправить отчет вы можете отправить отчет о состоянии жесткого диска по электронной почте. При нажатии данной кнопки программа выдаст запрос относительно настройки отправки электронных почтовых сообщений через SMPT-сервер. При утвердительном ответе на данный запрос на экране отобразится окно Настройки электронной почты (см. рис. 5.3), описание которого приведено выше. Если настройка отправки электронной корреспонденции уже была выполнена ранее, то на данный запрос следует ответить отрицательно, и письмо с отчетом будет отправлено незамедлительно. Помните, что для этого необходимо наличие действующего подключения к Интернету.

При нажатии кнопки Упрощенный режим в окне программы будет отображаться только основная информация, которая на рис. 5.6 представлена на вкладке Основная информация. Что касается вкладок Техническая информация и S.M.A.R.T. подробно, то они будут скрыты. После нажатия данной кнопки она примет название Расширенный режим – теперь с ее помощью можно будет вновь включить отображение всех вкладок.

С кнопкой Настройки мы уже познакомились ранее, а с помощью кнопки Помощь осуществляется вызов справочной информации.

Все основные сведения, которых достаточно для того чтобы принять решение о дальнейших действиях, отображаются на вкладке Основная информация (см. рис. 5.6). Слева вверху находится индикатор, который информирует пользователя о текущем состоянии жесткого диска. Этот индикатор может принимать одно из четырех состояний.

♦ Слово OK на зеленом фоне (такой индикатор отображается на рис. 5.6) – диск находится в нормальном состоянии, поводов для беспокойства нет.

♦ Восклицательный знак на желтом фоне – диск работоспособен и пока еще надежен, однако некоторые его важные параметры вызывают опасения.

♦ Восклицательный знак на красном фоне – такой индикатор свидетельствует о неудовлетворительном состоянии жесткого диска. В данном случае настоятельно рекомендуется как можно быстрее сохранить всю информацию с него на другой носитель и больше не пользоваться этим диском.

♦ Вопросительный знак на желтом фоне – данное состояние индикатора говорит о том, что Hard Drive Inspector не может выполнить диагностику жесткого диска. Данная ситуация может иметь две причины: либо данный жесткий диск не поддерживает технологию S.M.A.R.T., либо используется незарегистрированная версия программы.

Чуть правее индикатора состояния жесткого диска отображается информация о его основных технических характеристиках: модель, емкости, наличие свободного места, время работы в часах (днях). Последний из перечисленных параметров обычно используется для того, чтобы определить интенсивность эксплуатации жесткого диска. Отметим, что в некоторых случаях вместо времени работы отображается вопросительный знак. Это свидетельствует о том, что в данный момент программа еще не определила, как долго эксплуатируется жесткий диск. Обычно это происходит потому, что ей требуется

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

определенное время, чтобы определить, какие единицы измерения времени работы используются заводом-изготовителем данного устройства. В зависимости от модели жесткого диска программе на это требуется от 2 минут до 2 часов.

Справа вверху содержится три индикатора: Надежность, Производительность и Отсутствие ошибок. Они показывают количественную и качественную оценки соответствующих характеристик устройства. Количественная оценка выражается в процентах, а качественная выражается словами хорошо, удовлетворительно или плохо. Если отображается слово хорошо – повода для беспокойства нет, в случае оценки удовлетворительно жесткий диск работоспособен, но некоторые его характеристики вызывают опасения. Если же отображается оценка плохо, то следует как можно быстрее сохранить данные с этого жесткого диска в надежное место и больше им не пользоваться (по крайней мере, до устранения неисправности). И количественные, и качественные оценки состояния жесткого диска рассчитываются программой на основании анализа его ключевых показателей.

Под индикаторами оценок отображается строка, содержащая краткое описание текущего состояния жесткого диска. На рис. 6.6 в ней содержится информация Диск немного перегрет. Чуть ниже находится строка рекомендаций; здесь программа советует, какие действия в сложившейся ситуации следует предпринять для предотвращения потерь данных. Как видно на рис. 6.6, несмотря на то что диск немного перегрет, это не является поводом для беспокойства (в строке рекомендаций отображается текст Никаких особых действий для предотвращения потери данных предпринимать не стоит).

В поле Температура показывается температура жесткого диска в соответствии с последним измерением. Напомним, что периодичность измерения температуры указывается в настройках программы, в разделе Температура (см. рис. 5.4). Справа от данного поля расположена ссылка Температурная диаграмма. Если на ней щелкнуть мышью, то на экране отобразится окно, в котором выводится график динамики температуры. По горизонтальной оси указывается временной масштаб, который указывается с помощью расположенного внизу окна ползунка (возможные варианты – 10 секунд, 1 минута, 10 минут, 1 час). По вертикальной оси отражаются температурные показатели, причем критический уровень обозначен красной чертой. Но учтите, что программа выводит информацию о температуре и строит температурные диаграммы только для тех жестких дисков, которые имеют температурный датчик.

Если в настройках программы в разделе Разное (см. рис. 5.1) установлен флажок Показывать прогноз даты ТЕС дисков, то на вкладке Основная информация под сведениями о температуре будет отображаться прогнозная дата, при наступлении которой жесткий диск окажется в критическом состоянии. Как мы уже отмечали ранее, данный параметр является приблизительным, поэтому его нужно сопоставлять с индикатором состояния диска и индикаторами его оценки.

## Восстановление удаленных и «ремонт» поврежденных хакерами и вирусами файлов с помощью EasyRecovery Pro

С утратой или порчей вирусами и хакерами хранящихся в компьютере файлов и папок

сталкивались многие пользователи. В данном разделе мы расскажем, как самостоятельно реанимировать поврежденные данные с помощью специально предназначенной для этого программы, которая называется EasyRecovery Pro.

Этот продукт создан зарубежными разработчиками – ее автором является компания Kroll Ontrack (сайт программы – www.ontrackdatarecovery.com). Демо-версию программы можно скачать на ее домашней странице, к скачиванию предлагается дистрибутив объемом около 40 Мб.

Чтобы установить программу на компьютер, запустите инсталляционный файл и далее следуйте указаниям мастера установки.

EasyRecovery Pro обладает очень удобным и интуитивно понятным пользовательским интерфейсом, что позволяет эксплуатировать ее даже малоопытным пользователям. Также отметим, что программа является многоязычной, и в числе прочих она поддерживает русский язык.

### Общие правила работы с программой

После запуска программы на экране отображается ее пользовательский интерфейс, который представлен на рис. 5.7.

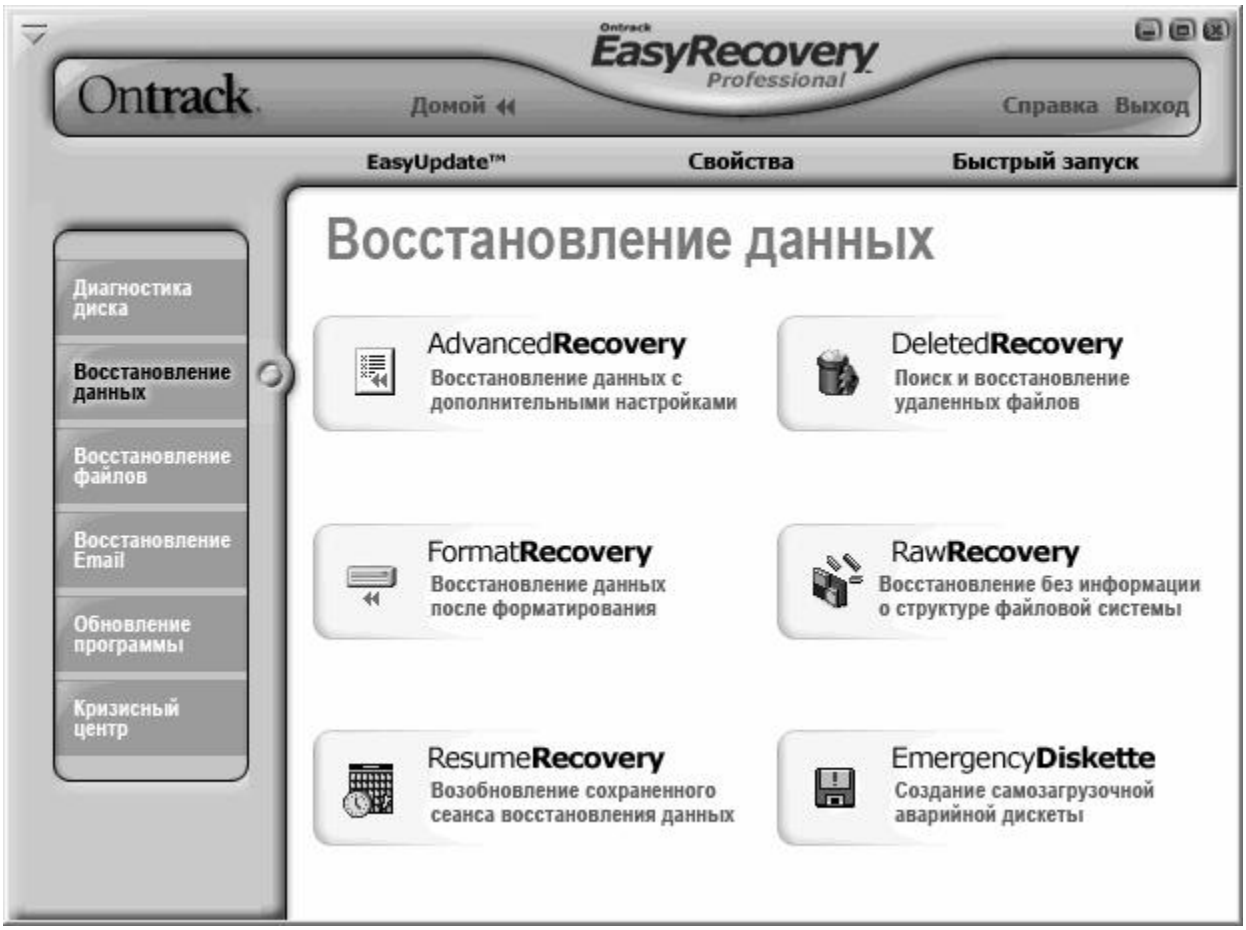



Рис. 5.7. Интерфейс программы EasyRecovery Pro

В левой части интерфейса содержится перечень разделов программы. Чтобы выбрать

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

требуемый раздел, достаточно щелкнуть на нем мышью. В центральной части интерфейса показано содержимое текущего раздела (то есть перечень доступных в нем режимов работы); чтобы выбрать требуемый режим, щелкните на нем мышью. Отметим, что возле названия каждого режима имеется его краткое описание, что существенно облегчает выбор, особенно на начальных этапах работы с программой.

В верхней части окна программы содержится несколько ссылок. Ссылка Домой предназначена для включения стартового интерфейса программы. С помощью ссылки EasyUpdate осуществляется переход в режим обновления программы. Отметим, что для этого необходимо наличие действующего подключения к Интернету.

Ссылка Справка предназначена для вызова справочной информации, а ссылка Выход – для завершения работы и выхода из программы.

С помощью ссылки Свойства осуществляется переход в режим настройки параметров программы. Более подробное его описание приводится в следующем разделе.

Ссылка Быстрый запуск предназначена для перехода в режим настройки панели быстрого запуска, а также открывает эту панель, если она ранее была настроена. Панель быстрого запуска позволяет быстро перейти в тот или иной режим работы программы, поэтому в нее можно включить команды, соответствующие наиболее востребованным режимам работы.

**Подготовка к восстановлению данных**

Перед тем как приступить к эксплуатации программы, рекомендуется просмотреть и, при необходимости – отредактировать параметры ее настройки. Несмотря на то, что в большинстве случаев предложенные по умолчанию параметры являются оптимальными, иногда все же приходится внести в настройки программы некоторые корректировки.

Как мы уже отметили чуть выше, для перехода в режим настройки параметров программы предназначена ссылка Свойства, расположенная вверху интерфейса. При щелчке на ней мышью на экране отображается окно, которое показано на рис. 5.8.

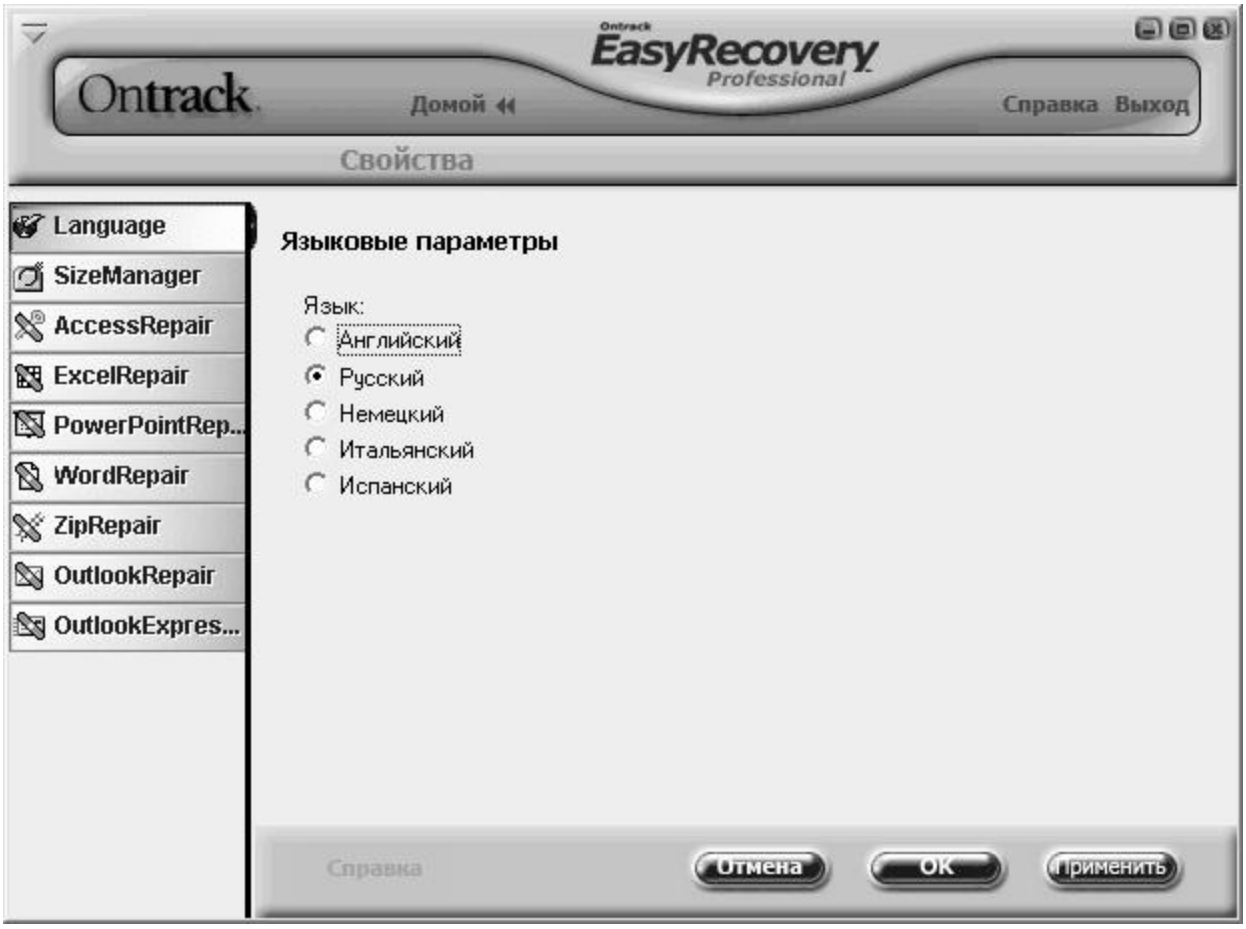



Рис. 5.8. Настройка параметров программы, раздел Language

В левой части данного окна содержится перечень разделов настройки, а в правой отображается содержимое текущего раздела. Кратко рассмотрим содержимое каждого раздела.

В разделе Language осуществляется выбор языка интерфейса. Для этого достаточно установить переключатель в соответствующее положение и нажать кнопку OK.

В разделе Size Manager можно выполнить настройку автоматической проверки дисков, а также их отображения. С помощью кнопок Проверка дисков и Отображение дисков выбирается соответствующий режим настройки. Порядок работы в каждом из них одинаков: нужно флажками отметить диски и нажать кнопку OK. В разделе Установка цветов можно настроить цветовое оформление помеченных папок, а также диаграмм.

В разделах Access Repair, Excel Repair, PowerPoint Repair, Word Repair и Zip Repair содержится параметр Папка восстановленных файлов. В ней указывается путь к каталогу, в который программа будет автоматически помещать все восстановленные объекты. По умолчанию предлагается следующий путь: C: Program FilesOntrackEasyRecovery ProfessionalRepaired, однако при необходимости вы можете его изменить. Для этого нужно нажать расположенную справа кнопку Обзор, и в открывшемся окне Обзор папок указать требуемый путь.

В разделе Outlook Repair можно выполнить настройку восстановления файлов программы Microsoft Outlook. Помимо уже знакомого нам параметра Папка восстановленных файлов, в данном разделе содержится также переключатель Выбор сообщений, область настроек Размер восстановленного файла, а также флажок Полное сканирование.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

С помощью переключателя Выбор сообщений нужно указать, сообщения какого типа программа должна восстанавливать. Возможен выбор одного из трех вариантов:

♦ Восстанавливать только текущие сообщения – в данном случае будут проигнорированы все сообщения, кроме текущих.

♦ Восстанавливать только удаленные сообщения – при выборе данного значения программа восстановит лишь удаленные сообщения. Этот режим удобно использовать, например, если какие-то сообщения были удалены ошибочно.

♦ Восстанавливать оба типа сообщений – в данном случае программа будет восстанавливать и текущие, и удаленные сообщения.

В области настроек Размер восстановленного файла можно задать ограничение по размеру восстанавливаемых объектов. По умолчанию переключатель установлен в положение Неограниченный – в этом случае размер восстанавливаемых файлов приниматься во внимание не будет. Если же установить переключатель в положение Макс. размер восстановленного файла, то открывается для редактирования расположенное ниже поле, в котором с клавиатуры либо с помощью кнопок счетчика можно указать максимально допустимый размер восстановленного файла (данный параметр выражается в мегабайтах).

Что касается раздела Outlook Express Repair, то здесь можно настроить восстановление файлов известной почтовой программы Outlook Express. В данном разделе содержатся уже известные нам параметры: поле Папка восстановленных файлов и переключатель Выбор сообщений, с которыми мы уже познакомились выше.

Все изменения, выполненные в режиме настройки параметров программы, вступают в силу только после нажатия кнопки Применить либо ОК (в последнем случае настройки вступят в силу с одновременным закрытием окна). С помощью кнопки Отмена осуществляется выход из данного режима без сохранения выполненных изменений.

**Проведение предварительной диагностики**

Возможности программы EasyRecovery Pro предусматривают выполнение диагностики диска по разным направлениям. Обнаруженные неполадки зачастую позволяют обнаружить причину потери или порчи важной информации и определить оптимальные варианты ее восстановления. Но даже если к настоящему времени ваш компьютер функционирует исправно – выполнить диагностику не помешает: это позволит своевременно устранить неполадки и предотвратить тем самым порчу или потерю данных.

Диагностика выполняется в разделе Диагностика диска, содержимое которого показано на рис. 5.9.

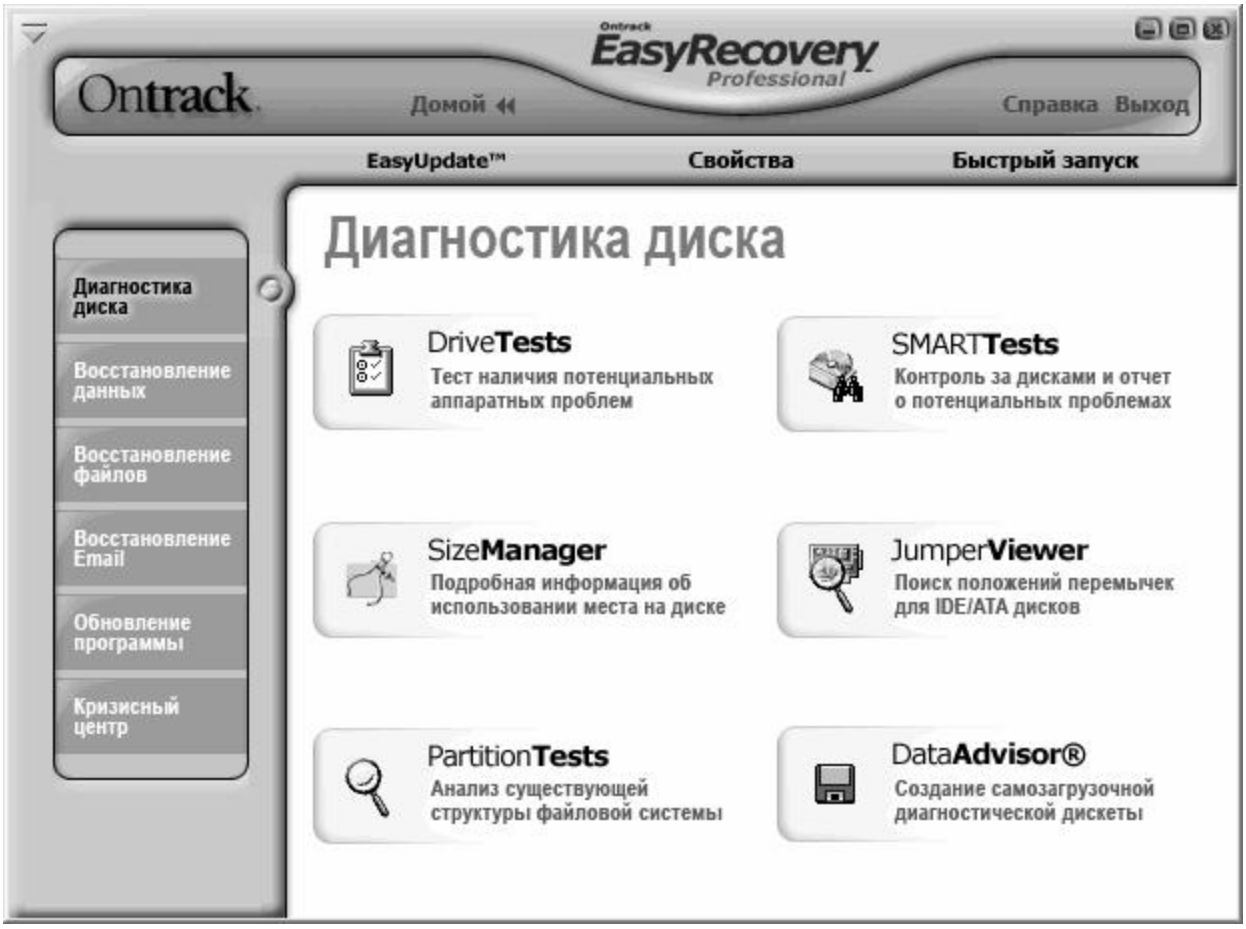



Рис. 5.9. Диагностика диска

Рассмотрим все варианты диагностики, которые предлагает программа EasyRecovery Pro.

Тест наличия потенциальных аппаратных проблем позволяет на ранней стадии диагностировать различного рода неполадки. Чтобы провести данный тест, щелкните мышью на соответствующем значке в центральной части интерфейса. В левой части открывшегося окна отобразится модель и емкость используемого на данном компьютере жесткого диска. Если на компьютере установлено несколько жестких дисков, то все они также будут представлены в списке, равно как и сменные носители информации.

Диски, которые необходимо диагностировать, следует выбрать путем установки соответствующих флажков. При выборе нескольких дисков они будут протестированы последовательно.

Для перехода к следующему этапу диагностики нажмите кнопку Далее (она становится доступной только после того, как для проверки выбран хотя бы один диск). Затем в открывшемся окне с помощью переключателя следует выбрать подходящий тест. Если вы желаете выполнить проверку за минимальное время, установите переключатель в положение Быстрая диагностика. В данном случае программа проверит наличие физических проблем на жестком диске примерно за полторы минуты, при этом достоверность полученных данных составит 90 %.

Если же необходимо провести тщательную проверку жесткого диска, установите переключатель в положение Полная диагностика. В данном случае программа проверит жесткий диск на наличие физических проблем, нечитаемых секторов, и т. д. Но в этом случае будьте готовы к тому, что диагностика может занять много времени.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

После выбора теста нажмите кнопку Далее, чтобы инициировать процесс тестирования. Когда тестирование будет завершено, в окне отобразится информация о его результатах. Ее можно сохранить в отдельном файле: для этого нужно нажать кнопку Сохранить, и в открывшемся окне указать путь для сохранение и имя файла отчета.

После нажатия кнопки Готово вновь откроется содержимое раздела Диагностика диска (см. рис. 5.9).

Один из наиболее интересных тестов – это диагностика на предмет того, как используется место на жестком диске компьютера. После щелчка мыши на соответствующем значке начнется процесс тестирования, информация о ходе которого будет отображаться на экране. При необходимости вы можете прекратить тестирование досрочно, нажав в данном окне кнопку Стоп. После того как процесс будет завершен, эта кнопка будет называться Готово. Чтобы посмотреть, каким образом используется место на дисках, следует щелчком мыши развернуть соответствующую позицию (рис. 5.10).

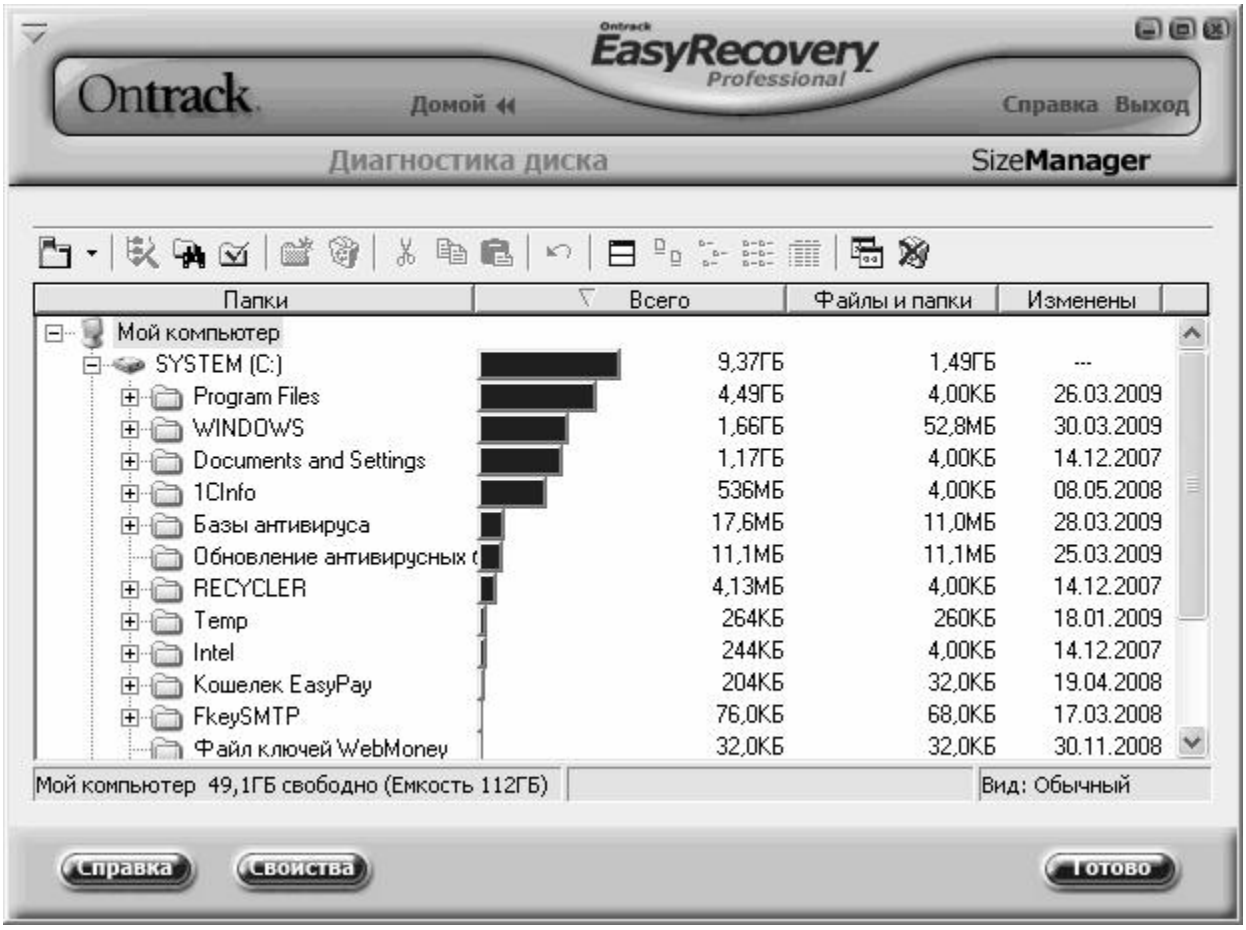



Рис. 5.10. Результаты тестирования

В верхней части данного окна находится инструментальная панель, кнопки которой предназначены для выполнения определенных действий с результатами диагностики либо для выбора режимов работы. Названия кнопок инструментальной панели отображаются в виде всплывающих подсказок при подведении к ним указателя мыши. Отметим, что доступность кнопок может определяться текущим режимом работы, в частности – месторасположением курсора. Кратко рассмотрим назначение наиболее востребованных из них.

С помощью кнопки Проверить диск можно запустить процесс повторной проверки

выбранного диска. Это бывает полезно, например, когда полное сканирование не принесло желаемых результатов, но позволило определить, что для ответа на имеющийся вопрос нужно повторно просканировать не весь жесткий диск, а какой-то его раздел. При нажатии данной кнопки на экране отобразится окно, в котором нужно будет подтвердить выполнение данной операции.

Кнопка Поиск папок предназначена для перехода в режим поиска требуемого каталога. При нажатии данной кнопки на экране отображается окно, которое включает в себя четыре раздела (Поиск, Размер папки, Имя папки и Дата/время папки). Здесь осуществляется настройка параметров поиска. Раздел Поиск предназначен для выбора диапазона поиска и параметров отображения (для этого достаточно установить соответствующий переключатель в требуемое положение).

В разделе Размер папки можно задать ограничения по размеру и содержимому папок, которые должны включаться в область поиска. Если переключатель Размер установлен в положение Игнорировать размер папки, то в процессе поиска размер каталогов приниматься во внимание не будет. Если же данный переключатель установить в положение Папки со следующими размерами, то становятся доступными для редактирования расположенные ниже параметры, предназначенные для тонкой настройки поиска по размерам. В поле детали из раскрывающегося списка можно выбрать тип объекта, на который распространяются указанные настройки (возможные варианты – Всего, Файлы и папки и Подпапки). После этого из расположенного ниже раскрывающегося списка следует выбрать условие сравнения (Равен, Между, и др.), максимально допустимый объем (вводится с клавиатуры или с помощью кнопок счетчика) и единицу измерения (Мб, Гб, Кб или Байт).

В разделе Имя папки можно задать ограничение по имени отыскиваемого объекта (например, когда известен фрагмент этого имени). Это позволит значительно сократить время поиска, особенно при работе с большими объемами информации или на маломощном компьютере. Если переключатель Имя установлен в положение Игнорировать имя папки, то в процессе поиска имя папки не будет приниматься во внимание. Если же выбрать значение Папки с совпадающими именами, то ниже открывается для редактирования поле, в котором с клавиатуры либо из раскрывающегося списка можно задать критерий поиска.

В разделе Дата/Время папки можно задать ограничение по дате и времени доступности, изменения или создания объекта. Если переключатель Дата установлен в положение Игнорировать дату и время папки, то параметры времени при поиске будут игнорироваться. Если же выбрано значение Папки, которые были или Папки, которые не были (в последнем случае применяется обратный фильтр), то открываются для редактирования расположенные ниже параметры – переключатель без названия и два поля, объединенные под названием В течение.

Переключатель может принимать одно из трех положений: Доступны, Изменены или Созданы. Первое положение определяет доступность объекта в течение указанного ниже интервала времени, второй – его последнее изменение, третий – его создание. В полях В течение указывается продолжительность времени, а также его единица измерения (часы, дни, и др.).

Чтобы начать поиск в соответствии с установленными параметрами, нажмите в данном окне кнопку ОК. С помощью кнопки Отмена осуществляется выход из данного режима без выполнения поиска.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Вернемся в окно результатов тестирования (см. рис. 5.10). Если необходимо быстро пометить несколько папок, которые удовлетворяют некоторым общим условиям, нажмите в инструментальной панели кнопку Пометить папки, затем в открывшемся окне определите критерии, в соответствии с которыми будут помечены папки, и нажмите кнопку ОК.

Чтобы создать новую папку, нажмите в инструментальной панели кнопку Создать, после чего в открывшемся окне введите ее имя, а также укажите путь для сохранения.

Для удаления объекта из списка выделите его щелчком мыши и нажмите в инструментальной панели кнопку Удалить. При этом программа выдаст дополнительный запрос на подтверждение данной операции.

Кнопка Панель файлов предназначена для управления отображением файловой панели. Если эта кнопка нажата, то в нижней части окна будет представлена файловая панель. В ней будет отображаться содержимое папки, на которой в верхней части окна установлен курсор.

С помощью кнопки Установка и удаление программ можно перейти в соответствующий режим работы Windows, который также вызывается с помощью специально предназначенного апплета Панели управления.

Для быстрой очистки Корзины используйте в инструментальной панели кнопку Очистить корзину.

Чтобы проконтролировать текущее состояние дисков компьютера и получить отчет о возможных проблемах (SMART-тестирование), щелкните в центральной части интерфейса (см. рис. 5.9) на значке Контроль за дисками и отчет о потенциальных проблемах. После непродолжительного сканирования системы на экране отобразится перечень дисков. Чтобы выбрать диск для проверки, отметьте его флажком. После нажатия в данном окне кнопки Далее (она становится доступной только после выбора хотя бы одного диска) на экране отобразится интерфейс выбора теста. Чтобы выбрать подходящий в данном случае тест, установите переключатель в соответствующее положение. При выборе значения Вывод состояния SMART будет выполнена проверка всех отмеченных на предыдущей стадии дисков, в результате которой пользователь получит информацию обо всех имеющихся SMART-тревогах.

Если вы ограничены по времени и вам нужно сделать быструю проверку, установите переключатель в положение Запуск короткого SMART теста. В данном случае сканирование каждого выбранного диска займет не более одной-двух минут (на маломощных компьютерах, возможно, потребуется больше времени).

Наиболее же тщательная проверка будет проведена в том случае, если установить переключатель в положение Запуск расширенного SMART теста. В данном случае программа выполнит расширенный SMART тест и представит соответствующий отчет. Отметим, что такое тестирование потребует определенного времени: в частности, сканирование только одного диска занимает в среднем около 20 минут.

После выбора режима тестирования нажмите кнопку Далее. Через некоторое время на экране отобразятся результаты проверки.

Еще один интересный вид диагностики, который реализован в программе EasyRecovery Pro – это проведение анализа существующей структуры файловой системы. Дело в том, что диск может не иметь никаких физических повреждений, но вирус мог внести изменения в его структуру. При проведении данной проверки осуществляется расширенное сканирование структуры файловой системы, по результатам которого

программа автоматически генерирует соответствующий отчет.

В процессе анализа структуры файловой системы программа проверяет целостность данных разделов FAT и NTFS. Что касается продолжительности проверки, то она во многом определяется объемом проверяемого раздела, а также количеством находящихся в нем объектов.

Чтобы выполнить данное тестирование, щелкните в разделе Диагностика диска (см. рис. 5.18) на значке Анализ существующей структуры файловой системы – в результате на экране отобразится окно, в котором будет представлен список разделов (томов) жесткого диска данного компьютера. Для каждой позиции списка в соответствующих колонках отображается название тома, его файловая система, а также объем в гигабайтах. Чтобы выбрать для проверки раздел жесткого диска, нужно пометить его соответствующим флажком. Запуск тестирования осуществляется нажатием кнопки Далее (эта кнопка становится доступной только после того, как установлен флажок возле хотя бы одного раздела).

По окончании тестирования, как уже отмечалось выше, программа сформирует соответствующий отчет.

Как и при проведении некоторых других проверок, программа выдает не просто отчет, а дополняет его соответствующими рекомендациями относительно того, как действовать в данном конкретном случае. Чтобы сохранить этот отчет в отдельном файле, нажмите кнопку Сохранить, после чего в открывшемся окне укажите путь для сохранения и имя файла отчета. Завершается работа в данном режиме нажатием кнопки Готово. Если же необходимо выполнить проверку остальных разделов жесткого диска, нажмите кнопку Назад, выберите требуемый раздел и нажмите Далее.

**Восстановление удаленных файлов**

Чтобы приступить к восстановлению данных, нужно выбрать в левой части окна программы соответствующий раздел, содержимое которого показано на рис. 5.11.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

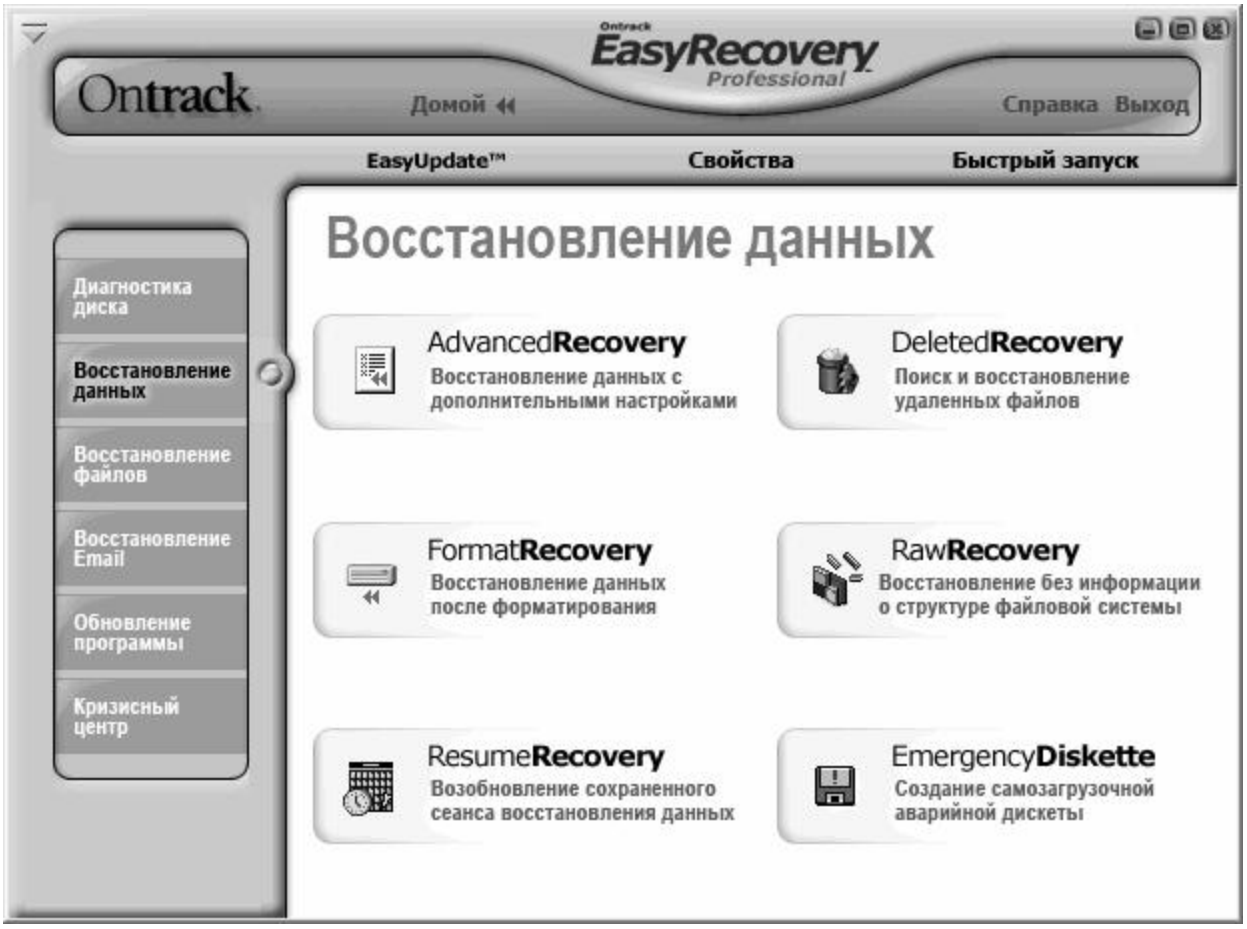



Рис. 5.11. Раздел Восстановление данных

Как видно на рисунке, в данном разделе имеется шесть вариантов восстановления данных. Одним из наиболее востребованных является режим Поиск и восстановление удаленных файлов, переход в который осуществляется с помощью соответствующей ссылки. В левой части открывшегося окна появится перечень разделов жесткого диска. Чтобы выбрать раздел для поиска удаленных данных, достаточно щелкнуть на нем мышью.

Возможности программы предусматривают в данном режиме два вида сканирования: быстрое и полное. По умолчанию предлагается выполнить быстрое сканирование: в данном случае для поиска удаленных файлов и папок используется существующая файловая структура.

Если вирус удалил пару файлов, и вы ничего не копировали в тот раздел, где они были расположены, то в большинстве случаев восстановить их можно с помощью быстрого сканирования. Если же вирус удалил объемный каталог, содержащий подпапки и файлы – то, по всей вероятности, придется прибегнуть к полному сканированию. Как нетрудно догадаться, полное сканирование займет на порядок больше времени, чем частичное.

Если вам известно имя файла, который требуется восстановить, или его расширение – вы можете установить фильтр на сканирование. Для этого в поле Фильтр файлов введите соответствующий шаблон, а в расположенном ниже раскрывающемся списке выберите тип файла. Отметим, что по завершении сканирования результаты, включаемые в отчет, также будут отобраны в соответствии с условиями установленного ранее фильтра.

Чтобы начать процесс сканирования в соответствии с установленными параметрами, нажмите кнопку Далее. При этом на экране отобразится окно, в котором будет

демонстрироваться информация о ходе.

После того как сканирование завершится, на экране отобразится окно с результатами сканирования. В левой части данного окна будет представлен иерархический перечень восстановленных каталогов в соответствии с существующей в данном разделе файловой структурой. Что касается восстановленных файлов, то их список для той папки, которая отмечена флажком, отображается в правой части окна.

При необходимости вы можете установить фильтр на отображаемые данные. Эту возможность особенно удобно использовать при работе с большими объемами информации. Для перехода в режим настройки параметров фильтра нажмите кнопку Фильтр, после чего в открывшемся окне путем установки соответствующих флажков отметьте свойства, которым должны соответствовать отображаемые в окне данные. В поле Файлы с именем можно ввести шаблон имени, а в расположенном ниже поле из раскрывающегося списка выбрать тип файлов, которые должны отображаться в списке.

Если в поле Файлы с датой выбрано любое значение, кроме Пропущено, то справа открывается поле, в котором можно указать условие фильтра (в данном случае это будет дата). Аналогичным образом в поле Файлы с размером (КБ) можно установить фильтр на данные в зависимости от размера файла (данный параметр выражается в килобайтах).

Чтобы применить настроенный фильтр, нажмите в данном окне кнопку ОК. Если впоследствии потребуется его отключить, снимите в окне результатов сканирования флажок Использовать фильтр.

Чтобы выбрать объекты для восстановления, отметьте их флажками, после чего нажмите кнопку Далее. В результате на экране откроется окно настройки параметров восстановления, которое показано на рис. 5.12.


Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Рис. 5.12. Настройка параметров восстановления

Возможности программы предусматривают сохранение восстановленных объектов не только на локальный диск, но и на удаленный FTP-сервер: для выбора подходящего режима установите переключатель в соответствующее положение. При сохранении на локальный диск нажмите расположенную справа кнопку Обзор и в открывшемся окне укажите каталог для сохранения. Если же вы предполагаете сохранить данные на FTP-сервер, нажмите кнопку Опции FTP и в открывшемся окне укажите имя ftp-сервера, пароль доступа, иные необходимые данные.

Восстановленные данные при необходимости можно сразу заархивировать и поместить в указанное место уже в виде zip-архива. Для этого установите флажок Создать Zip, и в расположенном справа поле с клавиатуры либо с помощью кнопок счетчика укажите максимально допустимый объем zip-файла в мегабайтах.

В программе реализована возможность автоматического генерирования отчета о ходе восстановления удаленных объектов. Для этого нужно установить флажок Генерация отчета восстановления, нажать расположенную справа кнопку Обзор и в открывшемся окне указать путь для сохранения отчета и имя файла отчета (эти данные должны отобразиться в поле Адресат).

Чтобы запустить процесс восстановления в соответствии с установленными параметрами, нажмите кнопку Далее. Через определенное время (как правило, его требуется немного) на экране отобразится информация о завершении восстановления. Эти же сведения содержатся в отчете, если ранее был включен режим его формирования.

Чтобы завершить работу в данном режиме и вернуться в главное окно программы, нажмите кнопку Готово.

Режим восстановления данных с дополнительными настройками отличается тем, что вы можете выполнить тонкую настройку параметров восстановления. Для перехода в данный режим щелкните в разделе Восстановление данных (см. рис. 5.11) на значке Восстановление данных с дополнительными настройками – в результате откроется окно, которое показано на рис. 5.13.

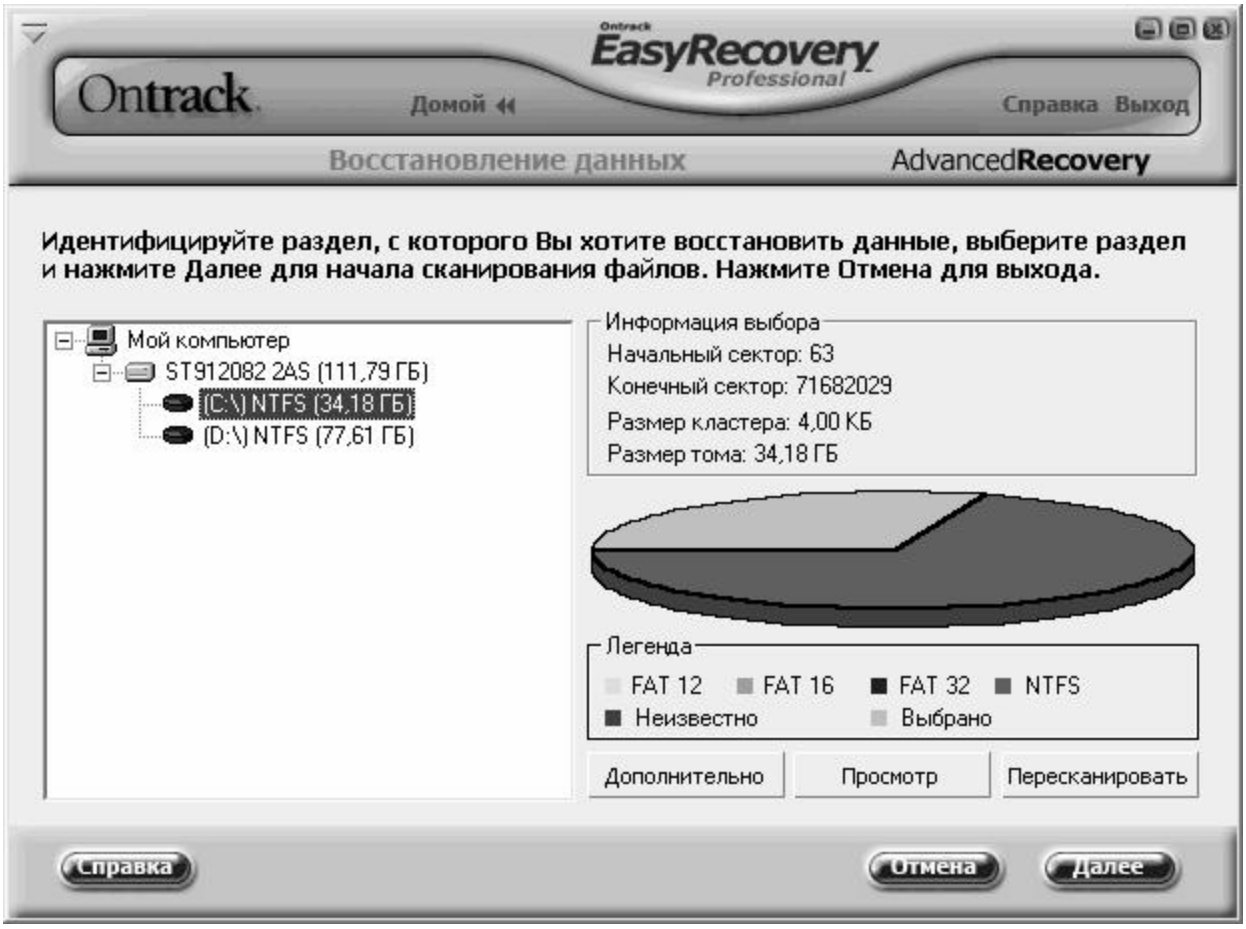



Рис. 5.13. Восстановление данных с дополнительными настройками

В левой части данного окна представлен список разделов жесткого диска. Выбор раздела для восстановления данных осуществляется щелчком мыши.

В правой части показана диаграмма, иллюстрирующая состояние жесткого диска. Для разных файловых систем на ней используются разные цвета (например, для NTFS – розовый цвет); кроме этого, серым цветом выделен объем, соответствующий выбранному в левой части окна разделу.

Под диаграммой находятся кнопки Дополнительно, Просмотр и Пересканировать. С помощью кнопки Просмотр вы можете просмотреть информацию о диске. Кнопка Пересканировать предназначена для повторного сканирования выбранного диска. Что касается кнопки Дополнительно, то она предназначена для перехода в режим настройки дополнительных параметров восстановления. При нажатии данной кнопки на экране открывается окно, которое показано на рис. 5.14.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

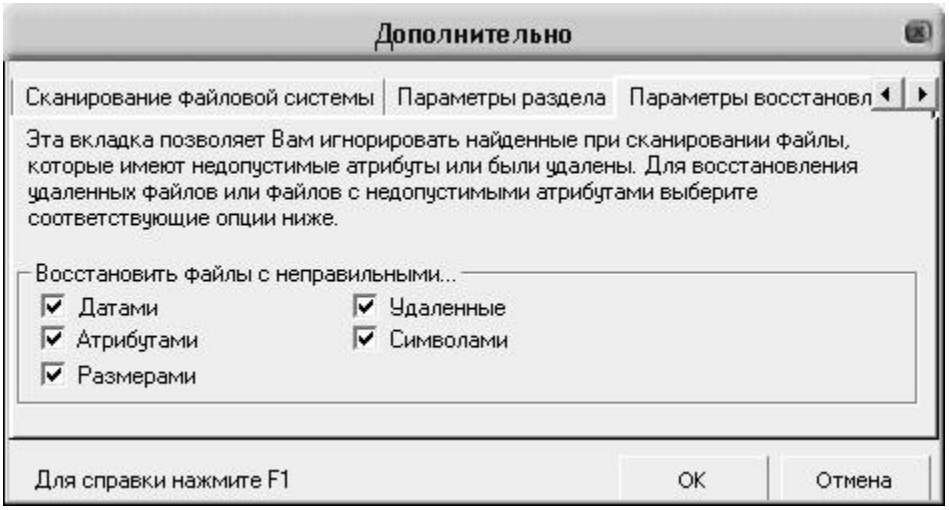



Рис. 5.14. Настройка восстановления, вкладка Параметры восстановления

Данное окно включает в себя несколько вкладок. Ввиду небольшого размера окна они не все видны, поэтому для выбора вкладки можно использовать кнопки с черными треугольниками, находящиеся в правом верхнем углу окна.

На вкладке Параметры восстановления (см. рис. 5.14) можно указать, каким свойствам и атрибутам должны соответствовать восстанавливаемые файла. Для этого в группе флажков Восстановить файлы с неправильными установите требуемые флажки из перечисленных ниже:

- ♦ Датами;
- ♦ Атрибутами;
- ♦ Размерами;
- ♦ Удаленные;
- ♦ Символами.

На вкладке Параметры раздела содержится раскрывающийся список, в котором можно выбрать одно из двух значений.

♦ Использовать MFT – это значение следует выбрать в случае, если требуется восстановить данные из поврежденных разделов. В данном случае для сканирования будет использована текущая таблица MFT.

♦ Игнорировать MFT – этот вариант является оптимальным, например, если вы случайно переформатировали раздел. В данном случае все структуры файловой системы проигнорируются, и будет просто выполнено сканирование данных файлов.

По умолчанию на данной вкладке предлагается использовать значение Использовать MFT.

На вкладке Сканирование файловой системы в поле Файловая система из раскрывающегося списка нужно выбрать тип файловой системы, используемой в данном разделе (NTFS, FAT32, RAW и др.). После этого с помощью переключателя указывается метод анализа. Если переключатель установлен в положение Простой, то программа произведет анализ стартовой информации в начале указанного раздела. При выборе значения Глубокий будет выполнен анализ всего раздела и восстановление стартовой информации. В последнем случае становится доступной кнопка Дополнительно, с помощью которой осуществляется переход в режим настройки параметров глубокого сканирования.

Чтобы выполненные настройки вступили в силу, нажмите в данном окне кнопку ОК.

Кнопка Отмена предназначена для выхода из данного режима без сохранения выполненных изменений.

Чтобы начать сканирование, нажмите кнопку Далее (см. рис. 5.13). Через некоторое время на экране отобразится окно с результатами сканирования. Далее работа ведется так же, как и в режиме восстановления удаленных объектов, описание которого приведено выше.

Отметим, что в разделе восстановление данных имеется еще несколько режимов работы: Восстановление данных после форматирования, Восстановление без информации о структуре файловой системы, Возобновление сохраненного сеанса восстановления данных и Создание самозагрузочной аварийной дискеты.

Первые два режима предназначены для восстановления данных соответствующими способами, Порядок действий в этих случаях будет во многом таким же, как и в режиме восстановления удаленных объектов, с которым мы познакомились ранее.

Режим Возобновление сохраненного сеанса восстановления данных позволяет вернуться к сохраненному ранее сеансу восстановления данных. Дело в том, что после каждого восстановления программа предлагает сохранить сеанс в отдельном файле, чтобы при необходимости можно было воспользоваться им в дальнейшем. Чтобы вернуться к сохраненному ранее сеансу, нужно щелчком мыши выбрать данный режим, и в открывшемся окне указать путь к файлу сеанса (этот файл имеет расширение *.dat).

В программе EasyRecovery реализована возможность создания аварийных загрузочных дискет или компакт-дисков. Поскольку время дискет уже практически ушло в прошлое (в современных компьютерах зачастую даже отсутствуют дисководы), рассмотрим, каким образом в программе можно создать аварийный загрузочный компакт-диск.

В разделе Восстановление данных щелкнем мышью на ссылке Создание самозагрузочной аварийной дискеты (она находится в правом нижнем углу окна). В открывшемся окне нужно установить переключатель в положение Создать аварийный загрузочный CD-ROM. В данном случае программа создаст аварийный загрузочный компакт-диск, используя для этого имеющееся на компьютере программное обеспечение, предназначенное для записи компакт-дисков.

ВНИМАНИЕ

Учтите, что создание аварийного загрузочного компакт-диска требует специального программного обеспечения. В операционных системах Windows 95, 98, Me, NT и 2000 встроенное программное обеспечение, предназначенное для записи компакт-дисков, отсутствует. В операционной системе Windows XP SP2 такое программное обеспечение имеется, но оно не может создавать загрузочные компакт-диски.

После нажатия в данном окне кнопки Далее будет выполнен переход к следующему этапу создания загрузочного диска. Вставьте диск в CD-привод и запустите программу, предназначенную для записи компакт-дисков, после чего выполняйте указания для создания нового диска из файла образа ISO9660.

Укажите путь к размещению файла образа ERBootEnglish.iso в каталог, где установлена программа EasyRecovery. По умолчанию данный путь выглядит следующим образом: C: Program FilesOntrackEasyRecovery. Далее выберите файл образа ERBootEnglish.iso, после чего завершите создание загрузочного компакт-диска.

Загрузка с созданного компакт-диска осуществляется следующим образом: нужно

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

включить компьютер, с которого необходимо запустить EasyRecovery, вставить в CD-привод созданный загрузочный компакт-диск, и перезагрузить компьютер таким образом, чтобы он загрузился с этого диска. Возможно, для этого придется внести соответствующие изменения в настройки BIOS.

**«Ремонт» поврежденных файлов**

Раздел Восстановление файлов, выбор которого осуществляется щелчком мыши на соответствующей позиции в левой части основного окна программы, предназначен для восстановления поврежденных файлов следующих форматов: Access, Excel, Power Point, Word и ZIP. Содержимое данного раздела показано на рис. 5.15.

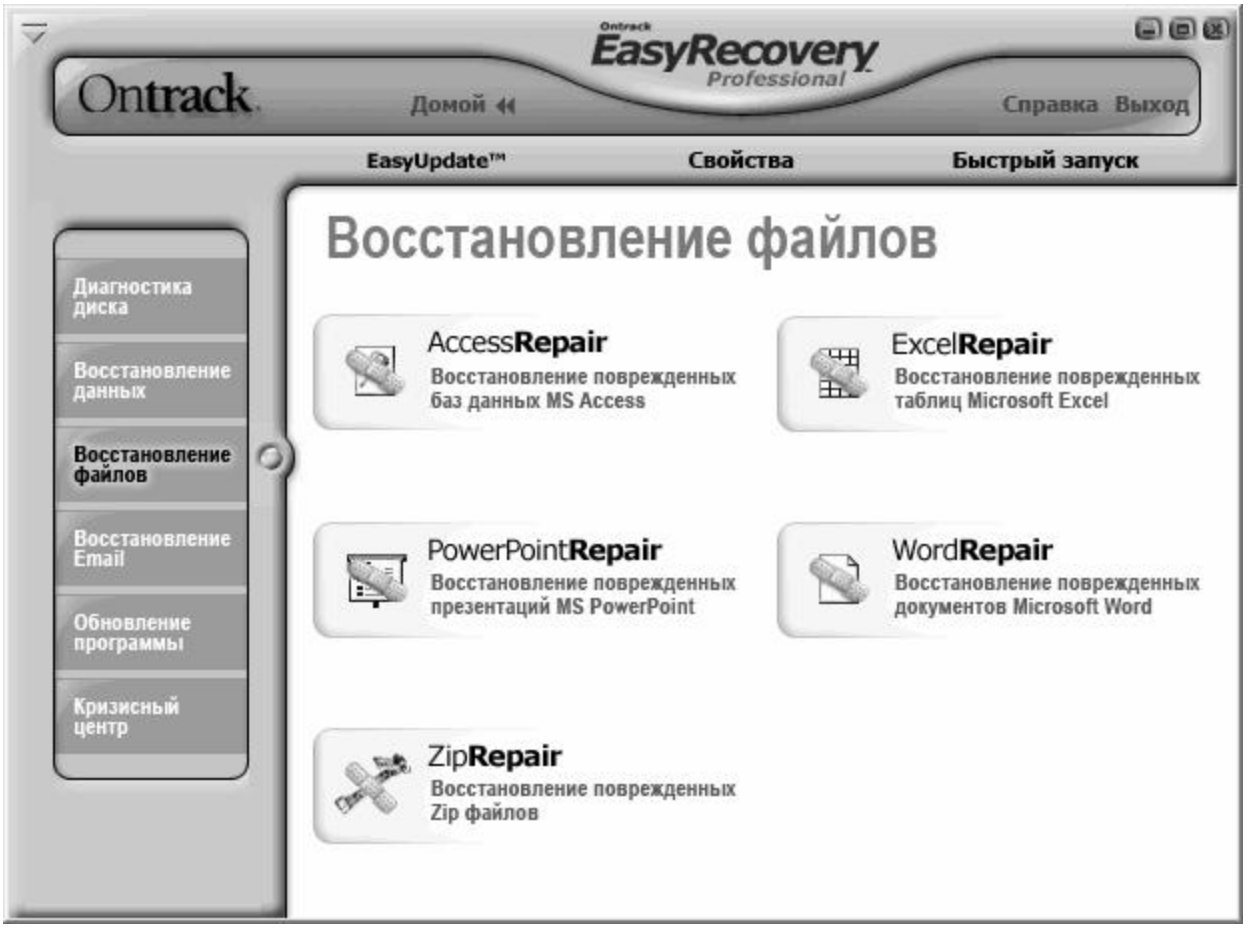



Рис. 5.15. Раздел восстановления поврежденных файлов

Поскольку порядок восстановления поврежденных файлов всех перечисленных форматов во многом идентичен, мы не будем останавливаться на каждом из них, а рассмотрим порядок работы на примере восстановления файлов одного из самых распространенных форматов – MS Excel.

Для перехода в режим восстановления файлов, созданных и сохраненных в текстовом редакторе Excel, щелкните на ссылке Восстановление поврежденных документов Microsoft Excel. В результате на экране откроется окно, изображенное на рис. 5.16.

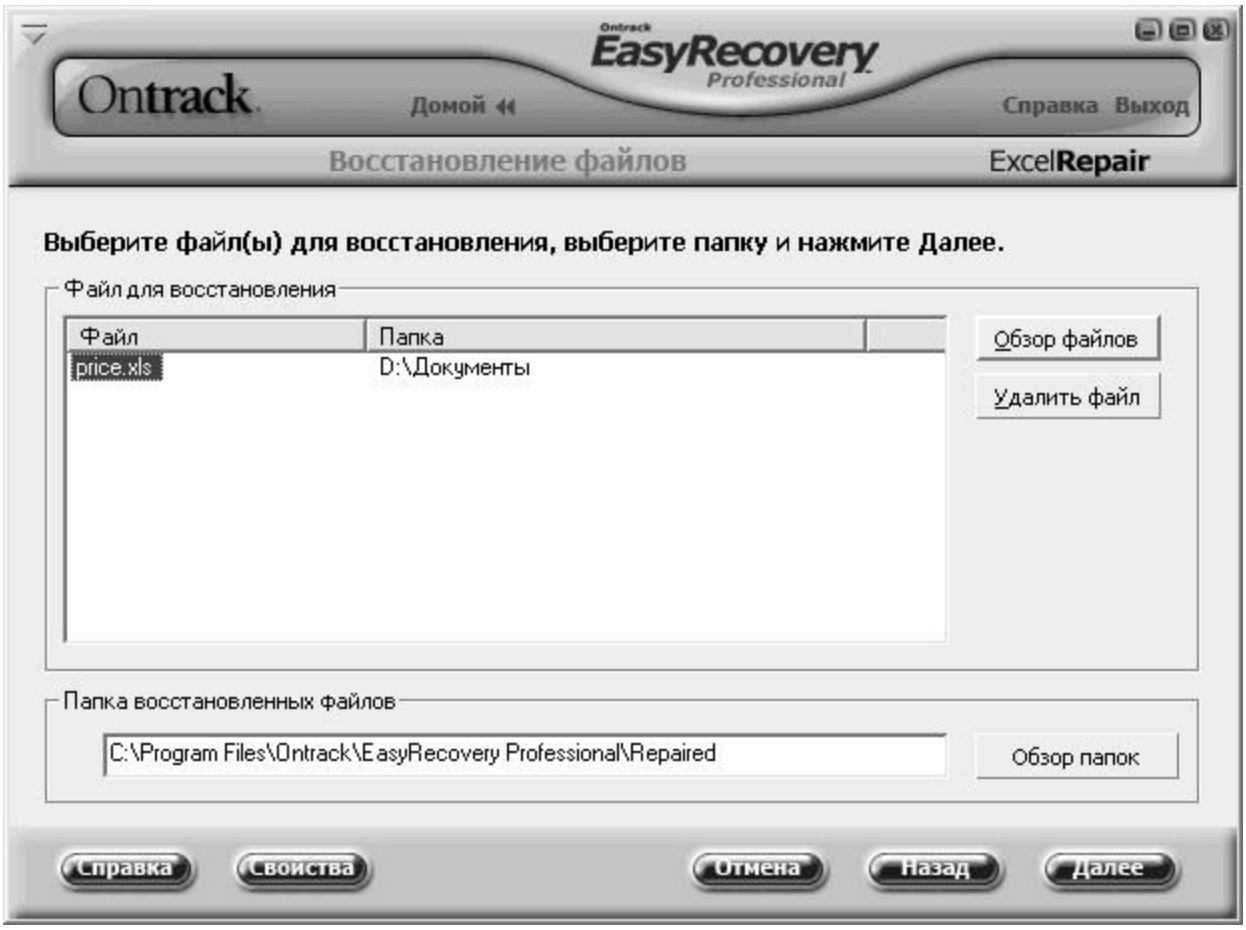



Рис. 5.16. Настройка параметров восстановления

В данном окне осуществляется настройка параметров восстановления. Стоит отметить, что возможности программы предусматривают восстановление сразу нескольких файлов, перечень которых формируется в поле Файл для восстановления. Чтобы добавить поврежденный файл в этот список, нужно нажать расположенную справа кнопку Обзор файлов. В результате на экране откроется окно Открыть, в котором по обычным правилам Windows следует выбрать требуемый файл и нажать кнопку Открыть.

При необходимости можно удалить файл из списка объектов, подлежащих восстановлению. Для этого нужно выделить его щелчком мыши и нажать кнопку Удалить файл, расположенную справа от списка. При этом следует соблюдать осторожность, поскольку программа не выдает дополнительный запрос на подтверждение операции удаления.

В нижней части окна отображается путь к папке, в которую будут помещены восстановленные объекты. По умолчанию предлагается следующий путь: C: Program FilesOntrackEasyRecovery ProfessionalRepaired. Чтобы изменить это значение, нажмите расположенную справа кнопку Обзор папок, и в открывшемся окне выберите подходящий каталог. Кстати, сделать это можно и в режиме настройки программы, для перехода в который предназначена кнопка Свойства, расположенная внизу окна.

ВНИМАНИЕ

Учтите, что восстановление файлов невозможно, если в это время запущено приложение, предназначенное для работы с этими файлами. Иначе говоря, если вы восстанавливаете файл Excel – закройте все открытые окна Excel, если восстанавливаете

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

файл Word – закройте программу Word, и т. д.

Чтобы начать процесс восстановления, нажмите кнопку Далее, расположенную слева внизу окна. При этом на экране отобразится информация о ходе процесса восстановления.

Если восстановление прошло успешно, то через некоторое время на экране отобразится соответствующее информационное сообщение. После нажатия в данном окне кнопки ОК можно запустить программу Microsoft Excel, чтобы убедиться в том, что поврежденный файл восстановлен.

Программа EasyRecovery формирует небольшой отчет по результатам восстановления. Этот отчет можно сохранить в отдельном файле. Для этого нужно нажать кнопку Сохранить, и в открывшемся окне указать путь для сохранения и имя файла отчета (отметим, что этот файл будет иметь расширение *.rtf). Чтобы вывести полученный отчет на печать, нажмите кнопку Печать, расположенную слева от кнопки Сохранить.

Аналогичным образом выполняется восстановление поврежденных файлов, созданных в программах Microsoft Outlook и Outlook Express. Это осуществляется в разделе Восстановление Email. В данном разделе нужно щелчком мыши выбрать требуемый режим и дальше действовать так, как и при восстановлении файла Excel.

## Глава 6. Как злоумышленники вымогают деньги с помощью программных средств

Начиная с этой главы, мы начнем рассказывать о том, как мошенники и проходимцы всех мастей воруют, вымогают и выманивают деньги у доверчивых пользователей Интернета. В частности, существует категория злоумышленников, которые обладают очень неплохими знаниями в сфере IT-технологий. Это позволяет им практически безнаказанно заниматься мошенничеством, вымогательством, шантажом и прочими подобными вещами. В этой главе мы расскажем о том, как мошенники выманивают деньги с помощью специальных программных средств.

### DOS-атака на сайт

Многие наверняка знакомо такое понятие, как DOS-атака. Сущность заключается в том, что какой-либо веб-ресурс подвергается мощной программной «бомбежке», в результате чего сайт или начинает очень сильно «тормозить», или попросту «падает». Долгие годы этот метод использовался преимущественно для того, чтобы вывести из строя сайты конкурентов, или просто отомстить той или иной организации.

Однако с недавних пор этот технический прием стал активно использоваться мошенниками. Алгоритм их действий прост: на сайт-жертву организуется мощная DOS-атака. После того как сайт успешно «ляжет», злоумышленники связываются с его владельцем или администрацией, и диктуют свои условия: мол, платите такую-то сумму денег – и сайт «оживет». Чтобы «подтолкнуть» жертву к принятию «правильного» решения, мошенники могут добавить, что в случае оплаты они гарантируют сайту защиту

от подобных атак в будущем. В случае отказа атаки будут продолжаться, причем их мощность будет с каждым разом увеличиваться.

Стоит ли говорить, что после перечисления денег мошенникам никакая защита сайту от DOS-атак обеспечиваться не будет! Более того – выманив деньги один раз и «почуяв слабину», мошенники наверняка повторят свои действия.

В подобных ситуациях настоятельно рекомендуется не идти на поводу у мошенников, а объединить свои действия с владельцем хостинга и обратиться с соответствующим заявлением в правоохранительные органы.

**Предложение купить антивирусную программу якобы для удаления вирусов с компьютера**

Вот еще один распространенный способ мошенничества. Начинается все с того, что пользователь Интернета получает сообщение об инфицировании его компьютера вредоносным ПО. Это сообщение может отобразиться, например, в виде всплывающего окна. Причем оно может выглядеть устрашающе – с соответствующим визуальным и звуковым оформлением (резкие цвета и рисунки, неприятные скрежещущие звуки, и т. п.). Это делается для того, чтобы у пользователя не осталось сомнений в заражении его компьютера мощным вредоносным программным обеспечением. При этом сообщение об инфицировании может оформляться от имени программного продукта, предлагаемого мошенниками – например, «Программа такая-то бесплатно проверила ваш компьютер и обнаружила у вас вирус, и чтобы избавиться от него, перейдите по ссылке». Если вы перейдете по этой ссылке – попадете на страницу, где вам будет предложено купить надежное антивирусное средство, гарантирующее не только избавление от обнаруженного вируса, но и надежную защиту от любых заражений в будущем.

Ну а дальше возможны варианты. Иногда мошенники, получив деньги, просто перестают отвечать на любые обращения и исчезают. Иногда они действительно присылают какую-то программу или архив – но пользоваться такой «покупкой» категорически не рекомендуется. Как показывает практика, вы получите не «надежный недорогой антивирус», а трояна или SpyWare, который «поселится» в вашем компьютере и будет, во-первых, информировать злоумышленника обо всех выполняемых на компьютере действиях, а во-вторых – предоставлять ему доступ к хранящимся на вашем компьютере файлам, папкам и приложениям. Помимо прочего, мошенник сможет получить доступ к вашим электронным кошелькам.

В некоторых случаях злоумышленники предлагают загрузить «антивирус» бесплатно. В этом случае сомневаться не приходится – вы получите либо троян, либо программу-шпиона.

Поэтому, если вы получили непонятно от кого сообщение об инфицировании компьютера – не следуйте рекомендациям мошенников, а просканируйте компьютер хорошей антивирусной программой с новейшими сигнатурными базами.

**Предложение купить Internet Explorer**

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Суть обмана, о котором мы сейчас расскажем, заключается в том, что при очередном запуске Internet Explorer пользователь замечает, что он автоматически попадает на страницу компании Microsoft. На этой странице отображается информационное сообщение о том, что теперь обозреватель Internet Explorer является платным, и за него нужно заплатить с помощью СМС-сообщения – в противном случае использование программы невозможно. Стоимость одного сообщения – всего 30 рублей (сумма может быть и другая).

На самом деле в компьютер пользователя была внедрена специальная вредоносная программа, которая автоматически переправляла Internet Explorer на подложную страницу, являющуюся точной копией страницы компании Microsoft. Вообще о том, что это подвох, можно было бы догадаться и сразу: вряд ли столь солидная и уважаемая компания, как Microsoft, будет собирать деньги с пользователей своих программных продуктов с помощью СМС-сообщений.

Кстати, если на сайте написано, что стоимость одного СМС составляет 30 рублей – будьте готовы к тому, что с вашего счета после отправки сообщения снимут рублей 100–150.

Устранить проблему можно самостоятельно без отправки СМС и прочих контактов с мошенниками. Для этого в свойствах Internet Explorer (переход в данный режим осуществляется с помощью команды главного меню обозревателя Сервис ▸ Параметры) откройте вкладку Дополнительно, и нажмите в ней кнопку Сброс (рис. 6.1).

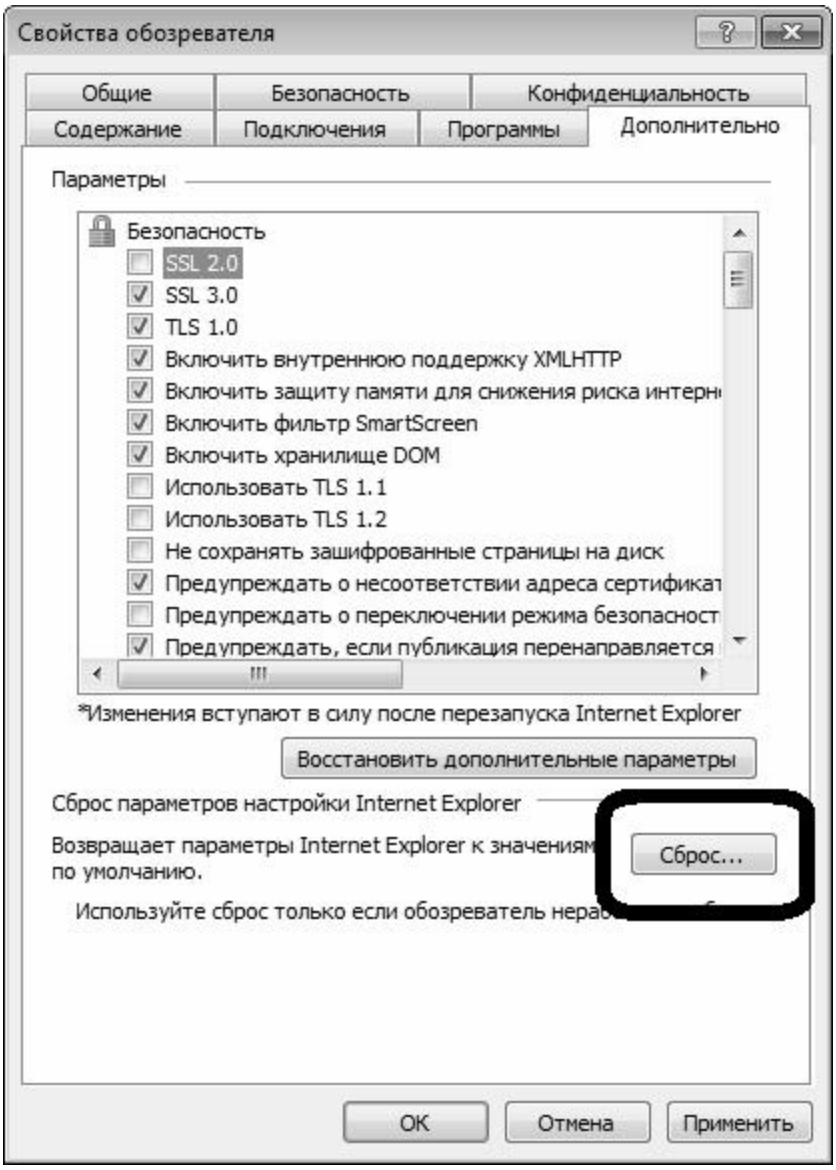



Рис. 6.1. Возврат к настройкам по умолчанию

Тем самым вы вернетесь к настройкам Internet Explorer, используемым по умолчанию.

После этого перейдите на вкладку Программы, и откройте список надстроек обозревателя (рис. 6.2).

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

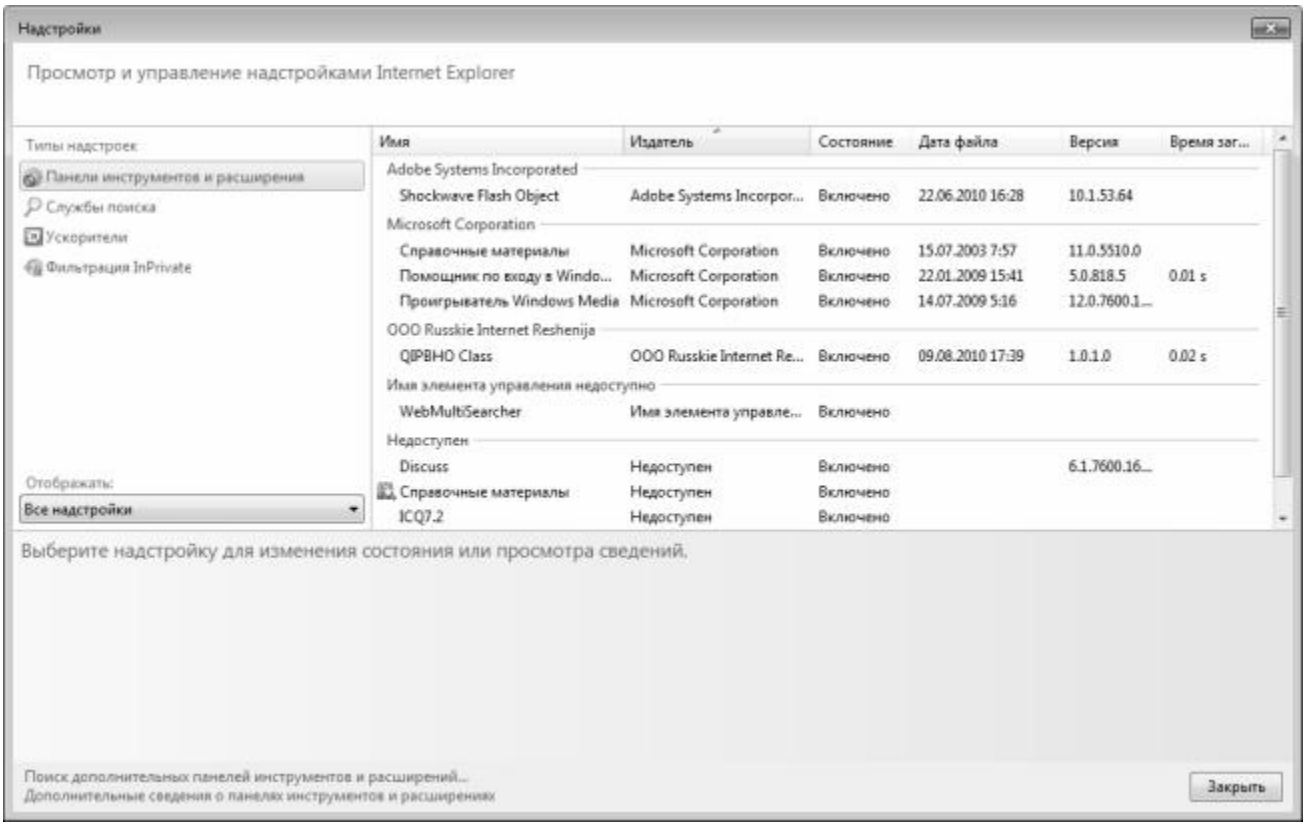



Рис. 6.2. Список надстроек в Internet Explorer

В этом списке отключите все имеющиеся надстройки. Затем закройте обозреватель, запустите его вновь и откройте какую-либо страницу, после чего вновь вызовите список надстроек. Посмотрите, какая надстройка включилась самостоятельно, найдите соответствующий ей файл и удалите его.

А вообще при всем уважении к компании Microsoft стоит отметить, что обозреватель Internet Explorer не отличается высокой степенью безопасности и надежной защитой от проникновения извне. Во многом это обусловлено не конструктивными или иными недостатками программы, а тем, что данный продукт изучен злоумышленниками лучше, чем имеющиеся аналоги.

### Устранение рекламы за СМС

Одним из наиболее неприятных и изощренных видов мошенничества является удаление с экрана навязчивой рекламы за СМС.

В один прекрасный день пользователь замечает, что на экране монитора появляется рекламное окно. Это может произойти в любой момент – например, при загрузке компьютера, при активизации какой-либо функции, или просто без привязки к действиям пользователя. Причем рекламное окно появляется независимо от наличия действующего подключения к Интернету.

Характерной особенностью данной аферы является то, что такое окно может иметь явно неприличный характер. Например, подобным образом часто рекламируются интернет-магазины, торгующие товарами сексуально-эротического ассортимента (попросту говоря,

секс-шопы). Причем эта реклама не просто навязчивая – ее так просто удалить с экрана вы не сможете: окно не закрывается (или при попытке закрытия вы автоматически будете перенаправлены на сайт секс-шопа), через Диспетчер задач его также отключить невозможно. Оно исчезает обычно само, но – лишь по истечении немалого промежутка времени (это может быть, например, 100 секунд, или 3 минуты). В течение этого времени вы будете вынуждены наблюдать рекламу эротических и порнографических материалов. Стоит ли говорить, насколько вредной является такая реклама, если к компьютеру имеют доступ несовершеннолетние!

Рекламный модуль проникает в компьютер в виде трояна незаметно для пользователя, а иногда – при невольном его содействии (посещение зараженного сайта, распаковка непроверенного зараженного архива, и т. п.). Для избавления от него мошенники требуют отправить СМС-сообщение на указанный номер – эта информация отображается на видном месте в рекламном окне. Но даже если вы отправите СМС – не обольщайтесь, ибо не факт, что вам сразу вышлют инструкции по удалению рекламы. Во-первых, после получения денег вы перестанете представлять для мошенников всякий интерес, а во-вторых – одного СМС может быть недостаточно. Часто в подобных рекламных окнах мельчайшим шрифтом где-нибудь внизу или в углу написано, что для удаления рекламы требуется отправить три (пять, десять и т. д.) СМС.

Но не спешите делиться с мошенниками своими деньгами – решить проблему можно и самостоятельно. Обычно в таких случаях помогает Интернет – для этого нужно в любом поисковике кратко описать проблему (например, Как удалить рекламу с экрана, и т. п.), и ознакомиться с результатами. Можно задать вопрос на специализированных сервисах – например, http://otvety.google.ru, http://otvet.mail.ru и т. п., или поискать ответ среди задаваемых ранее вопросов. Например, автор этой книги успешно решил подобную проблему, найдя подходящий ответ на http://otvet.mail.ru: опытный пользователь подсказал, какой файл и где именно нужно удалить, чтобы избавиться от рекламы.

### Фишинг

Вид мошенничества, который мы рассмотрим в данном разделе, используется для кражи данных кредитных карт (номера кредитной карты, пароля, пин-кода и т. д.) с целью последующего присвоения чужих денежных средств.

Первые попытки фишинга были зафиксированы в конце 90-х годов прошлого столетия, и с тех пор популярность этого вида мошенничества постоянно растет. Каким же образом мошенники могут заполучить данные чужой кредитной карты?

Самый распространенный способ заключается в следующем. Пользователь получает электронное письмо от лица, например, своего банка с просьбой (а точнее – с требованием) срочно перейти по указанной в письме ссылке и подтвердить свои регистрационные данные. Ссылка приводит пользователя на поддельный сайт, который является точной копией сайта банка. Разумеется, ничего не подозревающий пользователь спокойно вводит свои конфиденциальные данные в форму на этом сайте, и в этот же момент эти данные попадают к злоумышленникам.

Необходимо учитывать, что здесь возможны различные варианты. Например, мошенники могут потребовать ввести регистрационные данные либо для их подтверждения, либо для подтверждения якобы полученного крупного денежного

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

перевода, и др.

Каким же образом можно распознать, что полученное от имени банка письмо – фальшивка?

В большинстве случаев подобные письма могут иметь следующие признаки:

♦ к пользователю обращаются не лично по имени и фамилии, а общим приветствием – вроде «Уважаемый клиент»;

♦ в письме обязательно будет присутствовать гиперссылка на сайт и предложение туда перейти;

♦ требования подтвердить свои конфиденциальные данные весьма настойчивы;

♦ в письме возможно наличие угроз (закрыть счет, прекратить сотрудничество и т. п.) в случае отказа от выполнения требований;

♦ не исключено наличие в письме грамматических и иных ошибок.

Также для заманивания пользователя на фальшивый сайт может использоваться внедренная в его компьютер вредоносная программа. Ее задача заключается в том, чтобы автоматически перенаправить пользователя на фальшивый сайт, как только он наберет в интернет-обозревателе определенный веб-адрес (как правило – адрес своего банка). Ну а дальше – обычная схема: ввод конфиденциальных данных в предложенную форму, после чего они попадут в руки мошенников.

Иногда для фишинга используются специальные клавиатурные шпионы (подробно о таких вредоносных программах рассказывается выше). Их отличие от обычных клавиатурных шпионов (кейлоггеров) заключается в том, что они активизируются только после входа пользователя на определенный сайт (например – сайт банка). В результате все выполненные на этом сайте действия (в том числе и ввод данных кредитной карты) становятся известны злоумышленникам.

**Удаленное шифрование данных с последующим вымогательством денег за расшифровку**

В отличие от перечисленных выше схем выманивания денежных средств через Интернет, которые больше напоминают элементарный «развод» или «кидалово», описываемый в этом разделе способ интернет-мошенничества относится к разряду «продвинутых» и требует от злоумышленника определенной квалификации.

Речь идет об удаленном шифровании данных. Смысл этого способа заключается в том, что злоумышленник, получив доступ к удаленному компьютеру, шифрует в нем определенные файлы, документы и т. п. таким образом, что пользователь не может их самостоятельно расшифровать. Через определенное время пользователь зараженного компьютера получает электронное письмо с требованием перевести определенную сумму денег (это может быть и 100, и 10000 долларов, и любая другая сумма) по указанным реквизитам – за это ему будет выслан ключ для расшифровки информации. Разумеется, пользователь в большинстве случаев готов отдать требуемую сумму, лишь бы вернуть свои данные.

Этот прием в настоящее время набирает все большую популярность. Следует отметить, что злоумышленники сейчас предпочитают шифровать данные не у какого-то домашнего пользователя (хотя такие случаи тоже нередки), а на корпоративных компьютерах и

серверах – ведь домашний пользователь при всем желании не сможет заплатить столько же, сколько какая-нибудь даже небольшого размера фирма.

При возникновении подобной ситуации можно считать удачей, если злоумышленник требует перевести деньги банковским переводом – в этом случае его относительно легко вычислить (разумеется, обратившись своевременно в соответствующие органы). Но если в качестве платежных реквизитов указывается кошелек WebMoney, Яндекс. Деньги либо аналогичной интернет-системы, то здесь шансы обнаружить злоумышленника невелики. В данном случае хорошо, если после получения денег он не поленится выслать ключ для расшифровки данных.

Можно сказать, что удаленное шифрование данных является одним из самых изощренных и опасных видов интернет-мошенничества.

**Мошенничество под прикрытием азартных игр**

Часто злоумышленники, промышляющие выманиванием и воровством электронных денег, действуют под прикрытием интернет-казино и прочих подобных виртуальных заведений. Рассмотрим несколько примеров.

Самый примитивный способ «развода» на деньги – организация фальшивых интернет-казино. Мошенники «рисуют» красивый сайт с привлекательным дизайном, яркими картинками и баннерами, и т. д. Всем желающим предлагается принять участие в игре, «вероятность выигрыша в которой составляет 70 %» (процент может быть разный – в зависимости от наглости мошенников).

Самое интересное заключается в том, что никакой игры в таком казино на самом деле не ведется. Хотя выглядеть все может очень прилично: игроки делают ставки, и т. д. но на самом деле деньги сразу попадают в кошельки злоумышленников, а незадачливый игрок получает сообщение «Сожалеем, Вы не выиграли, но Вам обязательно повезет в следующий раз» или нечто в этом роде.

Существует и иной вид мошенничества – когда за участие в игре предлагается пройти платную регистрацию. Это, конечно, уже верх цинизма – игрок готов играть и оставлять деньги в казино, а ему предлагают еще и платно зарегистрироваться за это! После оплаты регистрации жертве предлагается какое-то время подождать – мол, на электронный адрес придет письмо с инструкциями об «активации статуса игрока» (или нечто подобное). Стоит ли говорить, что никаких писем мошенники не присылают!

Отметим, что злоумышленники в подобных ситуациях могут прикрываться названиями или адресами настоящих интернет-казино, в которых игра ведется по-честному. Например, в рекламном объявлении может быть сказано примерно следующее: мол, игра ведется по этому адресу, но регистрация игроков нашего казино осуществляется на другом сайте, для перехода на который используйте эту ссылку. Поскольку злоумышленники прикрываются настоящим, честным казино, то даже если вы захотите проверить это казино (например, можно почитать отзывы о нем игроков в Интернете, ознакомиться с черными списками и т. п.) – у вас может не возникнуть никаких подозрений. Перейдя по ссылке, вы регистрируетесь на постороннем сайте, отправляете мошенникам деньги – и после этого они попросту забывают о вашем существовании.

Помните: если вам предлагают платную регистрацию за право играть в казино – это, скорее всего, самый обыкновенный «лохотрон».

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

В последние годы на многих досках бесплатных объявлений и прочих рекламно-информационных ресурсах можно встретить объявления вроде этого:

Добрый день! Вы наверняка слышали про интернет-казино, а также о том, что в них выиграть практически невозможно. Так вот: до последнего времени это было действительно так. Но с недавних пор все кардинально изменилось! В результате многолетних и регулярных игр в интернет-казино, расположенном по адресу (дается ссылка на сайт казино), мне удалось обнаружить дыру в скрипте (прореху в системе безопасности, программный сбой и т. п.), в результате чего можно не только выиграть, но и вывести из казино кучу денег! Зачем я об этом рассказываю? Дело в том, что недавно я выиграл в этом казино крупную сумму, но мне ее не выплатили. Как любой нормальный человек, я на них очень разозлился, но сейчас я знаю, как им отомстить, а потому с радостью делюсь со всеми своим изобретением! С помощью известного мне приема я уже вывел не только свой выигрыш, но даже намного больше денег! Перейдите по ссылке, чтобы узнать подробности!

Если вы перейдете по предложенной ссылке, то, скорее всего, попадете на сайт процветающего казино, где вам предложат поиграть. А секрет заключается в том, что вы перешли по реферальной ссылке человека, который впоследствии будет денежное вознаграждение в виде процентов от всех ваших проигрышей в этом казино. Попросту говоря, это один из способов заманивания в казино новых игроков, причем так могут действовать не только рефералы, но и владельцы подобных ресурсов.

И помните: если бы действительно можно было так просто выводить из казино деньги – неужели с вами кто-то стал бы делиться секретом? Конечно же, нет, и все деньги успешно вывели бы и без вашей помощи.

А вот еще один распространенный способ. Вы получаете электронное письмо, СМС-сообщение или сообщение ICQ, в котором говорится, что вы выиграли в лотерею огромный приз – 100 000 долларов. Вообще суммы могут называться разные – и сотни тысяч, и миллионы долларов, но смысл от этого не меняется: вы имеете шанс почти моментально стать сказочно богатым человеком.

Но для этого необходимо выполнить одно условие, а именно – перевести небольшую сумму денег за «регистрацию», «активацию счета», «услуги по перечислению денег» и т. п. Могут попросить выслать 10, 20, 50, 500 долларов или любую другую сумму, которая может выражаться в виде процента от «выигрыша».

После перевода денег по указанным реквизитам о вас просто забудут, и на ваши обращения никто отвечать не будет. Распознать подобное мошенничество несложно – оно обычно «шито белыми нитками» и сразу становится понятно, что вас пытаются «развести». Особенно, если вы не принимали участия ни в каких лотереях и розыгрышах.

Как показывает практика, большинство подобных писем составлено на английском языке, причем нередко – с большим количеством ошибок.

## Глава 7. Хищение денег из платежных интернет-систем

Постоянно растут суммы денег, вращающихся в среде электронных платежных интернет-систем (WebMoney, Яндекс. Деньги, и др.), и было бы удивительно, если бы мошенники оставили эту сферу без своего внимания. Рассмотрим несколько распространенных и эффективных способов, которыми оперируют злоумышленники.

### «Генератор карт» платежной системы

Распространенный способ «развода» доверчивых обывателей на деньги состоит в том, что вам предлагается купить так называемый WebMoney-генератор – программу, которая автоматически генерирует коды карт WebMoney. Стоимость такой «программы» у мошенников составляет от 10 долларов США до «плюс бесконечности», а главное ее «достоинство» якобы состоит в том, что с помощью генерирования кода можно быстро пополнить собственный кошелек суммой 100 долларов США.

Первый вопрос, который должен возникнуть при появлении такого предложения – почему же такая волшебная программа стоит так дешево, и зачем кому-то делиться таким замечательным изобретением, а не использовать его только для себя? Если вы зададите мошенникам такой вопрос, то либо не получите ответа, либо вам ответят в том духе, что, мол, возможности программы ограничены, и более чем на 100 долларов один и тот же кошелек вы пополнить не сможете. Ответ явно неубедительный, однако многие будущие жертвы «развода» об этом не задумываются, и охотно перечисляют мошенникам деньги.

Что будет дальше – догадаться несложно: либо на ваши вопросы и письма перестанут отвечать, либо пришлют дистрибутив со шпионским модулем или троянской программой, который позволит мошеннику получить удаленный доступ к вашему компьютеру. Помните, что создать подобный WebMoney-генератор невозможно в принципе – во многом потому, что коды WebMoney-карт генерируются случайным образом.

### Обман при проведении операций конверсии

Одним из самых удобных интернет-сервисов являются электронные (виртуальные) обменные пункты, в которых можно обменять одну электронную валюту на другую. Например, вы хотите заплатить за телефон, но у вас в кошельке имеются только доллары, а мобильный оператор принимает оплату исключительно в рублях. В этом случае можно воспользоваться услугами многочисленных виртуальных обменников: процесс обмена занимает не более пары минут, курс вполне приемлемый, и все это можно сделать, не выходя из дома.

Найти электронный обменный пункт просто – нужно лишь набрать в любом поисковике соответствующий запрос. Выбор валют в виртуальных обменниках, как правило, хороший: здесь можно найти не только доллары или евро, но и, например, валюты стран СНГ. На сайте электронного обменного пункта вам предложат указать кошелек, с которого вы отдадите одну валюту, и кошелек, на который будет зачислена другая валюта.

И все было бы хорошо, если бы в этой сфере не вели активную деятельность мошенники. Под маской виртуальных обменников они обманывают доверчивых людей, причем зачастую это выглядит донельзя примитивно: вы перечисляете мошенникам

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

деньги – и на этом все заканчивается.

Если вы являетесь обладателем WM-кошелька, то для обмена валют лучше использовать собственный сервис WebMoney.

Если же вы решили воспользоваться услугами сторонних обменных пунктов – будьте внимательны и осторожны. Надо отдать злоумышленникам должное – они умеют сделать сайт, который может не вызвать подозрений даже у опытных пользователей, регулярно пользующихся услугами электронных обменных пунктов. По крайней мере, внешне все может выглядеть вполне прилично. Чтобы минимизировать возможность обмана, помните о нижесказанном.

♦ У любого честного обменного пункта имеется лимит на сумму обмена по каждой валюте. Это зависит от того, сколько электронных денег имеется в обменном пункте. Например, если в наличии есть 1000 долларов США, 100 000 российских рублей и 2000 евро, то и менять валюту можно только в этих пределах (то есть больше 1 000 долларов вы купить в данный момент не сможете). Бывает и так, что какой-то валюты нет в наличии, или ее совсем немного. Информация о максимальной сумме обмена всегда имеется на сайте обменного пункта. Если же такой информации нет – скорее всего, вы имеете дело с мошенниками (у них все просто – чем больше пришлют денег, тем лучше).

♦ Фальшивые обменные пункты почти всегда размещаются на бесплатных хостинговых площадках. Иногда они пользуются платным хостингом, но всегда – дешевым, причем оплачивают его ненадолго (поскольку понимают, что длительное время такой ресурс не просуществует – его просто заблокируют).

♦ Если по каким-то причинам вы не хотите пользоваться обменным автоматом платежной системы – обращайтесь к услугам только тех электронных обменных пунктов, в которых вы уверены (например, неоднократно работали с ними ранее). Если вы впервые меняете деньги – обратитесь к более опытным знакомым, чтобы они порекомендовали вам надежный виртуальный обменник.

♦ Если вы человек неопытный, а рекомендаций попросить не у кого – можете посмотреть содержимое черных списков обменников. Найти такие списки можно с помощью любого поисковика. Можно также просто ввести адрес электронного обменного пункта, вызвавшего у вас подозрения, в поисковую систему, и ознакомиться с результатами поиска.

♦ Если вы проверили обменный пункт «со всех сторон», но сомнения у вас остались – либо откажитесь от него, либо попробуйте обменять незначительную сумму. Если все прошло успешно – отправьте сумму побольше. В любом случае крупные суммы менять за один раз не рекомендуется, даже если вы пользуетесь проверенным и вроде бы надежным обменником.

Ни в коем случае не переводите деньги на обмен, если у вас имеются какие-то сомнения относительно честности электронного обменного пункта. Помните, что в случае обмана вернуть перечисленные мошенникам деньги невозможно.

Прикрываясь обменом валют, мошенники могут действовать и более изощренно. Справедливости ради отметим, что им очень помогает жадность и алчность пользователей, желающих быстро обогатиться, не прилагая для этого никаких усилий.

Итак, первое, что делает мошенник – это регистрирует доменное имя и заказывает хостинг (либо бесплатный, либо предельно дешевый). После этого он создает англоязычный сайт привлекательного дизайна, солидно оформленный и вообще вызывающий доверие. Как правило, он копирует дизайн и оформление известных

зарубежных виртуальных обменников. Сайт оформляется от имени серьезной зарубежной организации, которая на протяжении многих лет якобы осуществляет активную деятельность в сфере финансов. На этом сайте предлагается обменять валюту в направлении USD E-Gold – WMZ, причем зачастую это единственное направление, в котором работает «серьезная и солидная финансовая компания». Для правдоподобности здесь могут предлагаться и другие направления обмена валют, но все они будут «временно недоступны» (в данном случае это явный признак того, что сайт является мошенническим!).

После этого мошенник заводит русскоязычную веб-страничку (как правило, на бесплатном хостинге), с минимумом дизайна и практически без всякого оформления. На этой странице он красочно описывает новый метод быстрого обогащения, суть которого состоит в следующем: нужно обменять имеющиеся WMZ на USD E-Gold в любом обменнике (для примера обычно приводятся известные электронные обменные пункты, тот же RoboXchange), после чего на «сайте одной зарубежной компании» (здесь он дает ссылку на свой англоязычный «обменник») их можно обменять обратно по очень выгодному курсу. Повторяя эти операции, якобы можно постепенно наращивать свой капитал, в результате чего он многократно увеличится.

Стоит ли говорить, что все деньги, перечисленные доверчивыми жертвами для обмена, оседают в кармане преступника!

Ссылку на эту русскоязычную страницу злоумышленник помещает на досках бесплатных объявлений, рассылает со спамовыми письмами, вообщем – всячески «раскручивает» и «оптимизирует» свой проект. Ну а после этого ему остается лишь сидеть перед компьютером и периодически проверять свой электронный кошелек, на который будут приходить деньги от доверчивых любителей халявы.

Иногда на подобных мошеннических ресурсах устанавливается минимальная сумма обмена. Это своего рода защита от бдительных посетителей. Ведь многие люди очень осторожно пользуются неизвестными обменниками (и это правильно!), и для пробы посылают для обмена небольшие суммы (один-два доллара). Чтобы исключить подобное, мошенник сразу указывает, что операции с суммами меньше, например, 10 или 20 долларов не проводятся.

**Предложения несанкционированного доступа к чужим кошелькам**

В Интернете можно встретить огромное количество предложений о взломе чужих электронных кошельков. Все подобные «предложения» можно разделить на три основные категории.

♦ WM-генераторы, автоматические переводчики денег, и т. п. Предлагая подобные «продукты», мошенники могут пояснять, что они используют «дырку» в системе защиты WebMoney или протоколе WebMoney Keeper (программы, которая устанавливается на компьютер пользователя для работы с деньгами WebMoney). Стоит ли говорить, что от подобных предложений нужно держаться подальше! Ибо в конечном итоге результат окажется таким же, как рассказано чуть выше.

♦ Различного рода «кряки», программы-взломщики и т. п. Их предлагают за деньги, стоимость подобных «продуктов» варьируется примерно от 10 долларов США до «плюс бесконечности» – здесь все зависит от фантазии и наглости мошенника. Вам скажут, что

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

эта программа подбирает пароль, или умеет обходить файл ключей, вообщем – могут «плести» все, что взбредет в голову злоумышленнику. В реальности же после перечисления денег вы либо ничего не получите, либо получите файл с трояном или программой шпионом, который моментально «срисует» идентификационные данные вашего кошелька (идентификатор, пароль, файлы доступа), и передаст эти сведения хозяину. Некоторые трояны умеют не просто воровать учетные данные, но и одновременно менять пароль. В этом случае троян идентифицируется в кошельке под вашим именем с использованием ваших данных, и тут же меняет пароль, после чего сообщает хозяину новый пароль, в результате чего вы моментально теряете доступ к своему кошельку. Кстати, подобные продукты могут предлагать и бесплатно – в этом случае «лохи» ведутся на приманку практически без сомнений.

♦ Специальные сайты для взлома WebMoney, вход на которые может быть как платным, так и бесплатным. Подобные ресурсы предлагают два вида «услуг». В первом случае при посещении сайта на компьютер пользователя автоматически устанавливается программное обеспечение, позволяющее взламывать кошельки. Отметим, что программное обеспечение если и будет установлено – то лишь с целью кражи идентификационных данных вашего WM-кошелька. Во втором случае предлагается заполнить определенную форму на сайте. В ней просят указать: номер кошелька, который вы хотите взломать, а также номер кошелька, на который вы хотите получить похищенные средства, а также (внимание!) – идентификатор и пароль вашего кошелька, путь к файлу ключей и код доступа к файлу ключей. Спрашивается – зачем эти сведения для обычного перевода денег с одного кошелька на другой?

Кстати, платный сайт такого рода может оказаться «меньшим злом», чем бесплатный. Дело в том, что мошенники иногда ограничиваются взиманием денег за вход: возьмут с вас 5-10-20 долларов – и на этом все может закончиться. Если же это ресурс бесплатный – не сомневайтесь, что в компьютер непременно проникнет троян, который моментально «сольет» все ваши конфиденциальные данные своему хозяину. Хотя такое не исключено и на платных сайтах.

К программам для «взлома» электронных кошельков может прилагаться инструкция, в которой подробно рассказывается, куда распаковать архив и как запустить «взломщика». Чтобы не быть голословными, ниже мы приводим текст такой инструкции, причем самые характерные места выделены жирным шрифтом.

Установите на компьютер WebMoney Keeper Classic, скачав ее с сайта www.webmoney.ru. Пополните нужный кошелек (3 WMZ или 78 WMR) на нужную сумму. Распакуйте архив WMCrack.rar в любую папку и запустите WMCrack.exe. При этом сам WebMoney Keeper Classic должен быть закрыт. Прежде чем использовать WMCrack, Вам необходимо настроить программу. Для настройки WMCrack нажмите кнопку «Настройки программы» в окошке «кряка» (смотрите скриншот). В открывшемся окне введите данные Вашего кошелька: WMID – идентификатор Вашего кошелька; введите R-кошелек и Z-кошелек; пароль – пароль от Вашего кошелька; файл ключа *.kwm – файл ключей; файл кошелька *.pwm – файл кошельков (он находится в папке вместе с файлом *.kwm или в папке C: Documents and SettingsПользовательApplication DataWebMoney); Пароль доступа – пароль восстановления ключей из резервной копии, Вы его указывали при регистрации; Почта – Ваш электронный адрес, на который Вы регистрировали Ваш кошелёк. Эта почта применяется для отчета, который придет после взлома. Убедитесь в правильности

введенных данных («кряк» не может проверять корректность данных) и нажмите «Сохранить». Приступайте к взлому Webmoney. Все наши сайты блокируют, из-за нелегального использования, мы создали ещё пару сайтов, которые опять же заблокировали. Текущий сайт – это уже четвёртый сайт, который также ждёт блокирование. Вы уже, наверное, задумались, – почему мы вам отдаем этот «кряк» бесплатно потому что, осенью 2009 года у нашей компании был взломан электронный кошелек и сумма на нём была очень большая, мы много раз писали письма в поддержку webmoney, но кто взломал наш кошелек – никто нам на этот вопрос не смог ответить. Поэтому мы создали WMCrack, чтобы мстить Webmoney.

Орфография и стиль написания инструкции сохранены. Как говорится, no comments.

Вообщем, все предлагаемые в Интернете средства для взлома электронных кошельков объединяет то, что ни одно из них не способно взломать ни один кошелек. И учтите: если бы было так легко взломать электронный кошелек – этим бы занимались все, кому не лень, и в течение максимум нескольких дней вся система WebMoney была бы полностью опустошена.

**Фальшивые обращения от службы технической поддержки платежной системы**

Сущность способа, о котором сейчас пойдет речь, состоит в том, что пользователь WebMoney или другой платежной системы получает электронное письмо якобы от службы технической поддержки. В нем сообщается, что необходимо подтвердить свои учетные данные, и предлагается выслать их по указанному адресу. При этом могут потребовать указать не только идентификатор и пароль, но также путь к файлу ключей и код доступа к файлу ключей. Как только вы отправите эти сведения – они немедленно попадут к злоумышленникам.

А вот еще один вариант подобной аферы. В данном случае от имени службы технической поддержки у жертвы требуют перевести определенную сумму по указанным реквизитам. В качестве обоснования могут привести все, что угодно: подтверждение работоспособности кошелька, залоговая сумма в счет гарантий порядочности, платное обновление WM Keeper (без которого программа якобы не будет работать, и доступ к кошельку заблокируется, и т. п.).

ВНИМАНИЕ

Помните: ни одна служба технической поддержки никогда не требует у пользователей системы прислать или подтвердить свои регистрационные данные, либо, тем более – переводить куда-то деньги. Если вы все же сомневаетесь – просто позвоните в службу технической поддержки по телефонам, имеющимся на сайте www.webmoney.ru, или свяжитесь с техподдержкой по электронной почте.

В письме может содержаться ссылка с требованием перейти по ней, и ввести данные на открывшейся странице. Иногда эта страница является полной копией страницы сайта www.webmoney.ru, на которой пользователи системы указывают свои регистрационные данные. Поэтому будьте внимательны, и не ленитесь лишний раз проверить адрес, который отображается в адресной строке вашего интернет-обозревателя.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Подобные письма могут иметь ряд характерных признаков, с помощью которых можно распознать аферистов. В частности – мошенники к вам обращаются не по имени-отчеству или нику, а абстрактно – например, «Уважаемый пользователь системы WebMoney», или что-то в этом роде. Это неудивительно – ведь пока еще они не знают ваших регистрационных данных. Также учтите, что в своих требованиях мошенники могут быть настойчивыми, причем не исключены даже угрозы (мол, не оплатите платную активацию или не пришлете регистрационные данные – потеряете доступ к кошельку, и т. п.).

**«Ошибка» в электронном кошельке**

Вот еще один распространенный, даже банальный способ мошенничества. «Приманка» обычно забрасывается с помощью спамерского письма либо объявления, которое размещается на досках бесплатных объявлений (таких досок в Интернете имеется великое множество). Содержимое письма или объявления примерно такое:

Добрый день! Я долгое время работал в службе техподдержки (отделе разработки и др.) компании WebMoney (или – Яндекс. Деньги, и др.). Недавно меня незаслуженно уволили. Но перед увольнением я сумел украсть секрет: есть такой кошелек (или – несколько кошельков), на который, если перевести сумму денег, то она вернется отправителю увеличенная в три раза (пять раз, десять раз – возможны варианты) максимум через три дня. Вот его номер: №№№. Спешите увеличить свой капитал! Время ограничено! Удачи!

Стоит ли объяснять, что это всего-навсего наглый и примитивный обман, и никаких «волшебных» кошельков нет и в помине? На эту удочку иногда попадаются пользователи, которые недавно установили себе платежную интернет-систему, не уяснили толком себе ее возможности, и поэтому верят в подобные небылицы.

Кроме этого, подобные кошельки отслеживаются соответствующими службами WebMoney и других платежных систем, и оперативно уничтожаются вместе со всем содержимым.

Отдельно следует упомянуть о программах, которые якобы позволяют получить доступ (путем взлома паролей, ключей и т. п.) к чужим кошелькам WebMoney и других платежных систем. Большое количество таких программ продается в Интернете, и объединяет их то, что в настоящее время ни одна из них не способна взломать чужой кошелек.

**«Автоматический инкассатор»**

Одним из распространенных мошеннических способов является продажа так называемых «автоматических инкассаторов» – программ, которые якобы умеют собирать деньги из чужих электронных кошельков и доставлять их в указанный кошелек.

Характерной особенностью является то, что стоимость такой программы намного меньше, чем она якобы может собрать денег всего за один день. Иначе говоря, лишь за пару часов она окупится, и вы будете получать прибыль! Обычно стоимость таких «программ» злоумышленники оценивают примерно в 10–20 долларов США, при этом

гарантируя, что за один день программа соберет с чужих кошельков минимум 80-100 долларов.

Помните: во-первых, ни один подобный «автоматический инкассатор» не способен похищать деньги с чужих кошельков (это в принципе исключено самой конструкцией системы электронных платежей, независимо от того, какую систему вы используете – WebMoney, Яндекс. Деньги или др.). Во-вторых, если после перечисления денег мошенник вам ничего не пришлет – это еще далеко не самый худший вариант, поскольку за ваши деньги вам могут прислать вирус, троян, SpyWare и вообще что угодно, только не «автоматический сборщик денег».

Для рекламы «автоматических сборщиков» злоумышленники специально создают сайты – ведь продукт вызывает намного больше доверия, если у него есть свой сайт. Учтите, что такие сайты могут располагаться на хороших платных хостингах, иметь привлекательный дизайн и грамотно составленный контент. На сайте может работать форум или иметься гостевая книга – правда, ни один критический пост вы опубликовать не сможете, поскольку будет действовать жесткая модерация (по умолчанию возможность «прямой речи» просто блокируется). Некоторые особо «продвинутые» мошенники идут дальше: они специально создают в Интернете подделки на свой же сайт, и на своем сайте дают ссылки на эти подделки с предупреждением – мол, берегитесь, там мошенники, они подделали мой сайт и прикрываются моим честным именем!

Помните: никаких автоматических сборщиков денег с чужих электронных кошельков не бывает, и не может быть в принципе.

**Кража персональных данных с последующим выманиванием денег**

Одним из наиболее изощренных методов мошенничества является кража персональных данных с последующим выманиванием денег. При этом деньги могут выманиваться как у вас, так и ничего не подозревающих ваших знакомых.

Главная задача мошенника – получить доступ к вашему электронному почтовому ящику, ICQ или иным инструментам для общения в Интернете. Обычно это делается путем подбора пароля, поскольку очень многие пользователи совершенно безответственно относятся к паролю и используют в его качестве легко угадываемый набор символов. Также для этого могут использоваться SpyWare (о них шла речь выше) и прочие технические, программные, психологические и иные средства.

После того как мошенник получил доступ, например, к вашему ICQ, он всем найденным в адресной книге контактам рассылает от вашего имени просьбу прислать определенную сумму денег на указанный электронный кошелек. Эту просьбу он может обосновывать чем угодно, например – внезапными неприятностями (попадание в дорожно-транспортное происшествие, болезнь или смерть близкого человека, пожар, ограбление, квартирная кража и т. д.). Иногда злоумышленник просит просто одолжить немного денег «до получки».

Разумеется, большинство людей удовлетворят просьбу хорошего знакомого (друга, родственника, ребенка) и переведет сумму по указанным реквизитам, не подозревая, что деньги попадут к мошенникам. В конечном итоге рассчитываться по долгам приходится жертве, у которой были украдены персональные данные.

Иногда злоумышленники действуют иначе: они просто предлагают жертве вернуть

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

доступ к своим аккаунтам (почтовым ящикам, ICQ и др.) за деньги. В случае отказа могут последовать угрозы: мол, по всем имеющимся адресам мы разошлем сообщения такого характера, что с тобой никто иметь дела не будет: семья отвернется, с работы уволят и т. д. Но даже если вы согласитесь заплатить злоумышленникам требуемую сумму – нет никакой гарантии, что они действительно вернут вам доступ к вашим аккаунтам.

На основании вышеизложенного делаем два вывода. Во-первых, нужно пользоваться хорошими надежными паролями, чтобы исключить вероятность их подбора или взлома. А во-вторых – если вы получаете от знакомого человек электронное письмо, сообщение ICQ и т. п. с просьбой оказать финансовую помощь – не спешите переводить деньги по указанным реквизитам, поскольку эта просьба может исходить от мошенника. В подобной ситуации рекомендуется связаться с этим знакомым по телефону или иным альтернативным способом, чтобы уточнить – действительно ли просьба о финансовой помощи исходит от него.

### Финансовые интернет-пирамиды

Схема финансовых пирамид многим знакома из реальной жизни – еще на слуху печально известные различного рода АО МММ, «Хопер-Инвест», «Русский дом Селенга» и т. п. Аналогичный механизм успешно используется в настоящее время многими интернет-мошенниками.

Обычно предложение поучаствовать в финансовой пирамиде приходит в виде спамерского письма; кроме этого, реклама подобных мероприятий часто встречается в Интернете. Пользователю предлагается внести определенный взнос под умопомрачительные проценты и ждать баснословных барышей. При этом никаких гарантий на руки вообще не выдается (кстати, МММ и ему подобные хоть акции на руки выдавали…). Хотя на словах, конечно, сообщается, что сохранность вклада и получение процентов по нему гарантируется всеми, кем только можно (хоть правительством, хоть Папой Римским).

Как ни странно, в наше время еще находятся люди, готовые перечислить свои денежки неизвестно кому под честное слово для участия в сомнительном проекте, поэтому данный вид мошенничества все еще достаточно распространен.

## Глава 8. Разные мошеннические приемы и методы

В этой главе мы рассмотрим и проанализируем ряд мошеннических приемов и методов, относящихся к разным направлениям и тематикам.

### Составление гороскопов «под заказ»

Узнать свое будущее в той или иной степени интересно большинству обывателей. Кто-то для этого учится расшифровывать сны, кто-то ходит к гадалкам, а с появлением

Интернета появилась возможность находить и изучать самые разнообразные гороскопы и предсказания.

Подавляющее большинство имеющихся в Интернете гороскопов находятся в свободном доступе и открыты для просмотра всеми желающими. По большому счету, это логично, поскольку ценность и актуальность подобных гороскопов весьма сомнительна: в большинстве случаев они представляют собой ничего не значащий набор общих фраз.

В связи с этим в Интернете объявилось великое множество мошенников, готовых «за небольшую плату» составить индивидуальный гороскоп или предсказание будущего всем желающим. Эти мошенники не имеют никакого понятия об астрологии и прочих подобных науках, зато очень неплохо научились выискивать подходящие гороскоп в Интернете и адаптировать их к конкретному пользователю. Относительная достоверность их предсказаний объясняется рядом факторов.

Например, перед составлением гороскопа мошенник просит клиента предоставить некоторую информацию о себе. Если клиент, предположим, в ближайшем будущем оканчивает институт – в гороскопе появится информация о том, что его скоро ждет «интересная работа». Если у человека тяжело болеет старенькая бабушка – ему предскажут «временные трудности, после которых наступит облегчение, возможно получение внепланового дохода». Расшифровать логику мошенника нетрудно: временные трудности – это уход за больным и его смерть, облегчение – когда со временем уйдет боль утраты, и в то же время ни за кем не надо ухаживать, а внеплановый доход – оставшаяся от бабушки квартира или иное наследство.

Также информацию о клиенте мошенник может получить из социальных сетей (ведь клиент ему сообщит ФИО, адрес и иные данные, по которым его легко можно найти в социальной сети). Например, в социальной сети можно узнать, что человек недавно женился (следовательно – предсказать ему скорое появление наследников), и т. д.

Так что не стоит слишком сильно доверять различного рода предсказателям и составителям гороскопов, оказывающим свои услуги за деньги – их методы работы банальны и не содержат никакой мистики.

**Предложения стать участником «реалити-шоу» или иного привлекательного проекта**

Несколько лет назад в Рунете появился относительно новый вид интернет-мошенничества, сущность которого заключалась в приглашении всех желающих поучаствовать в новом реалити-шоу.

Схема мошенничества базируется на распространении в Интернете рекламных объявлений, в которых сообщается, что на одном из федеральных телевизионных каналов открывается новое реалити-шоу, участвовать в котором могут все желающие. Вернее, все желающие могут подавать заявки, а к участию допускаются только те, кто прошел предварительный отбор. Всем участникам такого шоу гарантируется огромная популярность, известность и успех (или крупные выигрыши вроде квартиры или машины), и эта информация неудержимо толкает наивных обывателей в сети мошенников.

Вначале на сайте будущего реалити-шоу предлагается оформить соответствующую заявку для предварительного рассмотрения кандидатуры. Обычно такая заявка имеет

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

шаблонный вид, в ней указывается набор стандартных данных – пол, возраст, рол занятий, образование, фотография, семейное положение и т. д. Если человек допускается к участию в реалити-шоу (кто бы сомневался!) – ему предлагается перечислить по указанным реквизитам определенную сумму денег в качестве уплаты за «регистрацию участников», «компенсацию накладных расходов» и т. п. Основания для перечисления денег могут приводиться разные, и, как правило, подчеркивается, что реалити-шоу будет проходить в другом городе, что, несомненно, связано с дополнительными расходами.

О том, что происходит дальше, догадаться нетрудно: после перечисления денег мошенники перестают отвечать на электронные письма. Кстати, если в объявлении о наборе участников в реалити-шоу отсутствуют контактные данные организаторов (кроме электронного адреса) – это однозначно «лохотрон». Иногда мошенники после получения могут сообщить, что, мол, условия конкурса изменились, и вы теперь нам не подходите, а деньги мы вернуть не можем, поскольку вы в любом случае были зарегистрированы. Но это редкость – обычно они исчезают вместе с деньгами.

Помните, что организаторы настоящих реалити-шоу никогда не проводят набор участников через Интернет. Все организационные подробности озвучиваются через эфир телеканала, на котором предполагается выпуск шоу. Что касается отбора кандидатов, то он не ограничивается рассмотрением каких-то поверхностных шаблонных анкет, а проходит в несколько этапов. Конечно, анкетирование потенциальных участников тоже проводится – но это только первый этап, за которым обычно следует личное собеседование и видеосъемка. В некоторых реалити-шоу на этапе анкетирования или личного собеседования необходимо представить свое портфолио. При этом все этапы отбора проводятся совершенно бесплатно.

Характерной особенностью данного мошеннического приема является то, что по закону злоумышленников очень трудно привлечь к ответственности. Это обусловлено тем, что в соответствии с действующим законодательством обращаться по факту мошенничества в правоохранительные органы имеет смысл только после той даты, на которую была назначена съемка. Иначе говоря – только после того, как обман фактически был совершен. До этой даты факт мошенничества недоказуем. Этот юридический нонсенс предоставляет злоумышленникам достаточно времени для того, чтобы позаботиться о своей безопасности и успешно замести следы.

**Опасность, исходящая из социальных сетей**

Социальные сети пользуются популярностью не просто у обывателей, но и у мошенников. Во многом это обусловлено тем, что подавляющее большинство пользователей таких сетей не имеют почти никакого представления об опасности, которая может исходить из Интернета. Многие из них вообще имеют компьютер только для общения в социальных сетях. Жертвами мошенников становятся в первую очередь именно такие беспечные граждане.

Известно, что в социальных сетях каждый пользователь может оставлять о себе самые разнообразные данные: возраст, место работы или учебы, оконченная школа или факультет института, хобби и др. Кроме этого, в списке гостей содержится информация о круге общения данного человека. Этих сведений предприимчивым злоумышленникам бывает вполне достаточно для того, чтобы успешно «разводить» людей на деньги.

Вот характерный пример. Человеку присылают СМС-сообщение примерно следующего содержания: «Папа, я попал в неприятность, нахожусь в милиции. Передай брату Антону, чтобы искал адвоката, скажи однокласснику Сергею, чтобы временно уехал за город, а Света (жена) пусть приготовит мне передачу. Но в первую очередь положи, пожалуйста, на этот номер деньги: мой телефон в милиции забрали, но в камере есть нелегально телефон, мне дали с него позвонить, но нужно положить на него деньги. Сразу после пополнения баланса я сообщу подробности. Очень жду».

Не правда ли, эмоциональное сообщение? Отметим, что иногда мошенники не СМС отправляют, а звонят человеку и эмоционально, сбивчиво, а потому – очень правдиво говорят примерно то же самое (якобы их попросил связаться с родственниками попавший в неприятность человек). При этом ситуации могут обыгрываться самые разные: попадание в милицию, дорожно-транспортное происшествие, попадание в больницу, и т. д.

Успешность данной аферы в определяющей степени зависит от умения мошенника ошеломить человека, сбить его с толку и вынудить его немедленно, на эмоциях пополнить баланс указанного телефона (иначе говоря, заставить человека сделать что-то прежде, чем подумать). И в этом ему очень помогают реальные данные о человеке, полученные из социальных сетей. Именно там он узнает, что у этого человека есть брат Антон, одноклассник Сергей и жена Света. Причем брат Антон работает юристом (следовательно – у него, по идее, должны иметься связи в адвокатской среде), одноклассник Сергей имеет криминальное прошлое (значит, у него могут быть причины скрываться от милиции), а жена Света очень любит мужа и, конечно же, приготовит ему передачу в камеру.

Но это еще не все. Зачастую мошенники не гнушаются «проиллюстрировать» свои послания. И если мобильный телефон жертвы поддерживает передачу фотографий – то в подтверждение СМС он может получить фотографию своего родственника, сидящего в камере в окружении бритых уголовников. Как нетрудно догадаться, эта фотография также берется из персональной странички человека в социальной сети, после чего соответствующим образом обрабатывается в Фотошопе или другом графическом редакторе. Если же мошенники обыгрывают ситуацию, например, с попаданием близкого человека в дорожно-транспортное происшествие – они могут прислать фотографию, где этот человек лежит окровавленный под машиной, и т. п.

Надо отдать злоумышленникам должное – они отлично понимают, на какие «болевые точки» человека нужно надавить, чтобы он, немедленно бросив все, побежал пополнять баланс неизвестного ему телефонного счета.

Чтобы не стать жертвой подобного «развода», нужно в подобной ситуации, прежде всего, связаться со своим «попавшим в беду» родственником и выяснить, действительно ли это так. Иногда для этого бывает достаточно просто позвонить ему на мобильный телефон или связаться по ICQ.

И еще: без особой надобности не выкладывайте в социальных сетях слишком много информации о себе: фотографии (особенно своих детей!), круг общения, род занятий, и т. п. Иначе ваши шансы стать жертвой мошенников многократно увеличиваются.

**Предложение защитить доменное имя веб-ресурса**

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Предположим, вы являетесь владельцем сайта, расположенного по адресу www.resurs.com. Это сайт вашей компании или вашего бизнеса, имеющий постоянных посетителей и, образно говоря, давно и прочно занимающий свое место. В определенный момент вы получаете по электронной почте письмо, автором которого является некая служба мониторинга доменных имен. В этом письме вам сообщается, что есть злоумышленники, которые хотят зарегистрировать очень похожее доменное имя – например, www.resurs.org, причем точно известно, что они будут осуществлять мошенническую деятельность.

Следовательно, тень от их неблаговидной деятельности может пасть и на вполне благополучный сайт www.resurs.com. Это может привести к потере доверия со стороны постоянных клиентов, а в некоторых случаях даже к неприятностям с правоохранительными органами. Поэтому настоятельно рекомендуется предотвратить регистрацию такого доменного имени, тем более что стоить это будет всего 50 долларов США (сумма может быть разной – и 20, и 100 долларов).

Как нетрудно догадаться, в данном случае мошенником является тот, кто предлагает защиту от злоумышленников. Прием простой, если не сказать – примитивный, но, как ни странно, на него попадаются владельцы даже уважаемых и известных веб-ресурсов.

**Мошенничество с доверительным управлением финансами на валютных и фондовых рынках**

Все гениальное просто, и это крылатое выражение находит свое подтверждение в том, как мошенники обманывают доверчивых игроков на валютном рынке Forex, а также на фондовых рынках, где ведется торговля ценными бумагами.

На валютном рынке Forex предлагается такая услуга, как размещение временно свободных денежных средств под доверительное управление. Суть операции состоит в том, что трейдер (биржевой игрок) распоряжается деньгами инвестора (заключает сделки, и т. д.) по своему усмотрению. Иначе говоря, инвестор разрешает трейдеру пользоваться своими средствами на бирже как угодно, лишь бы это приносило прибыль.

Если в результате биржевой игры действительно удается получить доход – клиент отдает трейдеру предварительно оговоренную часть (например, 30 % или 50 % прибыли). Если же биржевая игра получилась неудачной и принесла убытки, то стороны сразу определяют его максимально допустимый размер (обычно где-то треть от суммы вклада), при достижении которого игра должна прекратиться. В данном случае все потери ложатся полностью на инвестора, трейдер ничем не рискует – таковы правила, о которых инвестор знает заранее.

Этот нюанс и позволил появиться гениально простому, и в то же время – очень эффективному способу мошенничества. Трейдер через Интернет находит двух инвесторов, располагающих временно свободным капиталом, убеждает их в своем высоком профессионализме и уверяет, что распорядится деньгами лучше, чем кто-то другой. Получив средства в доверительное управление, трейдер-мошенник выбирает позицию и на одном счете открывает ее вверх, а на другом – вниз (иначе говоря, играет одновременно на повышение и на понижение курса). В результате у одного инвестора образуется доход, а у другого – убыток такого же размера.

Когда убытки инвестора, которому не повезло, достигают оговоренной заранее суммы –

трейдер сворачивает деятельность на его счете. Инвестор забирает свои оставшиеся деньги – но трейдер-то при этом ничего не теряет! Зато со счета другого инвестора, где получился доход, мошенник законно получает причитающуюся часть прибыли.

Аналогичным образом мошенники действуют не только на валютном, но и на фондовых рынках, на которых ведутся торги ценными бумагами.

**Взимание денег за продвижение и «раскрутку» веб-ресурсов**

Каждый владелец сайта желает, чтобы у него было много посетителей. Посещаемый ресурс способен привлекать клиентов, приносить прибыль, способствовать появлению выгодных деловых партнеров, дальнейшему развитию бизнеса, и т. д.

Учет числа посещений ведется с помощью специальных счетчиков. Сегодня абсолютно бесплатно можно получить счетчики, например, на следующих сервисах: www.hotlog.ru (это один из самых популярных статистических ресурсов), www.mail.ru или www.bigmir.net.

А вообще можно набрать в любом поисковике запрос «счетчик посещений» – и вам будет предложено множество ссылок, по которым вы найдете счетчики на любой вкус.

В настоящее время развелось немало мошенников, которые делают вид, что занимаются продвижением сайтов. В реальности они лишь пускают пыль в глаза, однако их «услуги» по «раскрутке и оптимизации сайта» стоят недешево.

ВНИМАНИЕ

Многие мошенники подкупают тем, что за свои услуги они могут не требовать предоплаты.

В общем случае обман происходит примерно следующим образом. Человек вводит в поисковую систему запрос «услуги по продвижению сайтов», и в предложенном списке выбирает какую-нибудь организацию.

Связавшись с ней, он объясняет ситуацию (мол, такой-то сайт нужно раскрутить, и т. п.), после чего стороны оговаривают стоимость услуг и сроки окончания работ.

Мошенники могут предложить клиенту, чтобы он наблюдал за тем, как растет число посетителей его сайта. Человек реально видит: вчера было столько-то посещений, сегодня их стало намного больше, а на следующий день счетчик вообще показал цифры, о которых и мечтать не приходилось, и т. д. Когда наступает срок сдачи работ, заказчик с чистой совестью рассчитывается с «исполнителями», поскольку результат налицо.

Сразу после расчета ситуация кардинально меняется. Человек видит, что число посещений вновь резко снизилось, более того – вернулось практически на начальный уровень. Следовательно, деньги за раскрутку и продвижение сайта были потрачены зря.

А секрет состоит в том, что никто и не занимался оптимизацией, продвижением и раскруткой веб-ресурса. Вся «работа» мошенников заключалась в том, чтобы с помощью нехитрых манипуляций искусственно «накрутить» показания счетчика. Как только они получили деньги от заказчика – они прекратили его «накручивать», следовательно – данные о посещаемости вернулись на прежний уровень.

ПРИМЕЧАНИЕ

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Сегодня в Интернете можно найти утилиты, предназначенные как раз для искусственной накрутки установленных на веб-ресурсах счетчиков. Если вас устроит такая «псевдопосещаемость» – вы можете накрутить показания счетчиков и самостоятельно, и вовсе не обязательно обращаться для этого к мошенникам.

Если вы намереваетесь заказать раскрутку и продвижение сайта у профессионалов – постарайтесь найти их по рекомендации людей, которым вы доверяете. В крайнем случае, если такой возможности нет, хотя бы не поленитесь навести об организации, к которой вы хотите обратиться, справки в Интернете.

### «Нигерийский спам»

«Нигерийский спам» – это схема выманивания денег, при которой пользователь получает письмо примерно следующего содержания:

Я, такой-то, недавно работал секретарем Саддама Хусейна (варианты – «черным» кассиром Ясира Арафата, финансовым работником Бориса Березовского, в последние годы очень популярны такие письма от «бухгалтеров», «финансовых директоров» и т. п. компании «ЮКОС»), и мне удалось завладеть суммой 50 млн. долларов США (разумеется, суммы фигурируют самые разные). Но самостоятельно я их снять не могу (в силу каких-то причин), и мне нужна помощь постороннего лица. Вы можете мне помочь. Для этого вам нужно открыть счет в зарубежном банке, на который будут перечислены денежные средства. Вам за это причитается 5 % (или 1 %, или 20 %) от суммы.

Затем пользователю предлагается перечислить некоторую сумму денег для покрытия «накладных расходов». Само собой, после перечисления «накладных расходов» никакая «помощь» от пользователя уже не требуется…

Причем в подобном письме история возникновения денег может быть разной – не только «мне удалось завладеть деньгами бывшего шефа», но и, например, «помогите спасти часть капиталов (эдак миллионов 500 долларов) бывшему олигарху, попавшему в беду… для этого откройте счет… причитается вознаграждение… накладные расходы небольшие…».

Почему этот вид мошенничества получил название «нигерийский спам»? Дело в том, что в первых таких письмах, которые рассылались по всему миру, фигурировало имя бывшего нигерийского диктатора Сани Абачи (якобы люди, имеющие доступ к его счетам, не могли снять деньги без посторонней помощи). В настоящее время в этих письмах можно встретить имена любых известных людей (чаще всего попавших в неприятность – например, преследуемых официальными властями, или вообще умерших), но первоначальное название так и осталось.

## Глава 9. Сомнительные предложения о работе и легком заработке

В этой главе мы расскажем о схемах, которыми пользуются интернет-злоумышленники

для обмана соискателей работы и приработка.

**Предложение купить «бизнес-комплекс»**

Одним из распространенных видов интернет-мошенничества является предложение купить некие «бизнес-пакеты», в которых содержатся все необходимые инструкции для открытия и успешного развития своего прибыльного бизнеса. Расчет злоумышленников строится на том, что вести собственный бизнес, не выходя из дома, и получать умопомрачительные барыши хочет каждый.

Отличительной чертой многих подобных объявлений является то, что мошенник всячески подчеркивает эксклюзивность и уникальность предлагаемого «комплекса» или «бизнес-пакета», по сравнению с которым все остальные аналоги – полная чепуха. При этом больше никаких подробностей не сообщается, за исключением того, что «вложения окупятся очень быстро, и вы станете сказочно богаты». Да, насчет вложений: обычно за подобное мошенники просят от 10 долларов и выше (могут называться цены и 50, и 100 долларов).

При этом зачастую продажей одного «бизнес-пакета» или «комплекса» афера не ограничивается. После первого приобретения выясняется, что это лишь первая часть «программы успеха», и чтобы получить вторую (без которой, разумеется, ничего не получится), нужно перечислить еще определенную сумму денег (как правило – больше, чем за первую часть). После второй может последовать третья, и так далее – до того момента, как жертва, наконец, «прозреет» и поймет, что ее попросту немилосердно обманывают.

Иногда мошенники предлагают купить сразу несколько «комплексов». При этом они говорят, что, мол, даже один «комплекс» принесет вам успех, но если вы приобретете два таких «бизнес-пакета» – ваши доходы вырастут в 10 раз, а если три – в 100 раз. При этом один пакет предлагается по цене, предположим, 50 долларов, два пакета – по цене 70 долларов, а 3 пакета – по цене 90 долларов (вроде как создается иллюзия того, что несколько пакетов покупать выгоднее, чем один).

После того как вы перечислите деньги, никакого интереса для злоумышленника вы представлять больше не будете. Впрочем, он может действительно вышлет вам какие-то «комплексы» или «бизнес-пакеты» – как правило, это текстовые файлы, иногда «сдобренные» графиками и диаграммами. Но не обольщайтесь, поскольку никакой ценной информации в них содержаться не будет (суть многостраничного документа может сводиться к тому, что «кто не работает – тот не ест»).

**Участие в реферальных программах**

Еще один популярный вид интернет-мошенничества состоит в том, что соискателю предлагается зарабатывать деньги путем перехода по ссылкам и посещения определенных веб-ресурсов. Подобных объявлений в Интернете сейчас множество, их можно встретить и на сайтах, посвященных трудоустройству, и на досках бесплатных объявлений. Внешне все выглядит пристойно, но на практике оборачивается полным «пшиком».

Вначале нужно зарегистрироваться в системе и завести себе электронный кошелек

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

(чаще всего требуется WebMoney). За каждый переход по ссылке работнику начисляются либо деньги, либо бонусы, которые в конечном итоге конвертируются в деньги. Доход зачисляется на счет участника системы, откуда он может вывести деньги на свой кошелек.

Но не рассчитывайте на легкий заработок: за каждый переход начисляется мизерная сумма – обычно от одной до нескольких копеек. Таким образом, за день кропотливой и нудной работы вы заработаете максимум несколько рублей (несмотря на то, что вам ранее могли пообещать доход в размере и 300, и 500, и 1000 рублей в день). И учтите, что одними щелчками на ссылках дело может не ограничиться – в некоторых случаях для получения бонуса необходимо ответить на какой-либо несложный вопрос.

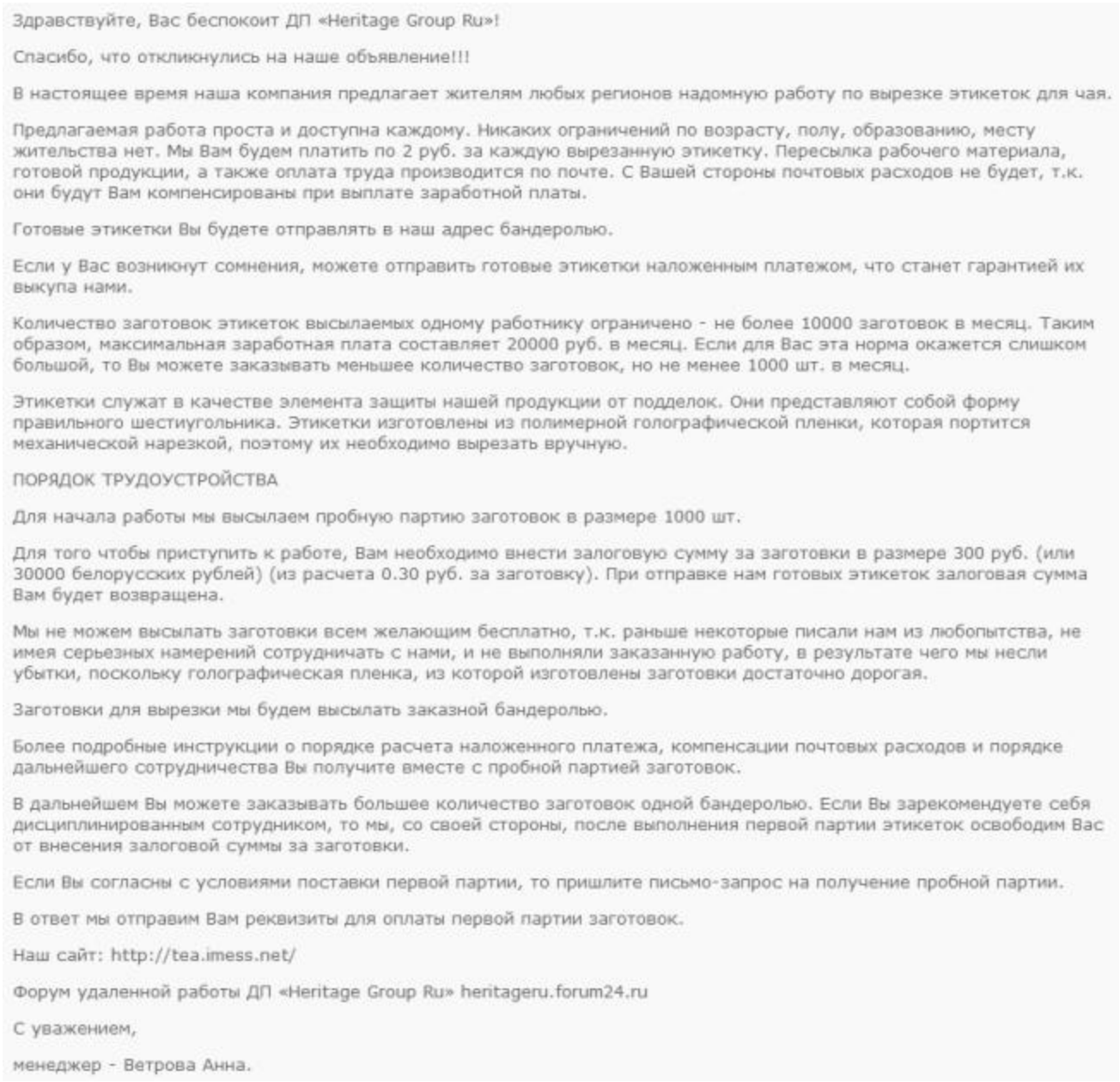
Но и это еще не все. У каждого такого сервиса существует правило: вывести деньги из системы на свой электронный кошелек можно только при достижении на счету определенной суммы. Другими словами, пока вы не накопите на счету определенную сумму – вывести деньги вы не сможете. У кого-то этот минимум составляет 10 долларов, у кого-то 20, и т. д. – все зависит от конкретного сервиса. При этом система возьмет с вас комиссию за вывод средств – она обычно составляет около 5 %. Так что если у вас и получится что-то заработать – это, во-первых, будет во много раз меньше того, что вам изначально было обещано, а во-вторых – вывести деньги будет не так просто.

В этой сфере существует немало откровенных мошенников, которые вообще ничего не выплачивают. Иначе говоря, вы можете несколько дней упорно ходить по ссылкам, копить бонусы, а когда на вашем счете накопится достаточная сумма для вывода средств – он или обнулится, или при попытке вывода отобразится сообщение об ошибке.

И еще. В Интернете можно встретить предложения о продаже специальных программ – сборщиков бонусов. Они якобы избавляют пользователя от необходимости ходить по ссылкам – программа все делает сама, и фактически человек имеет возможность получать деньги, ни прилагая усилий. Учтите, что это обман: почти всегда мошенники продают под видом таких программ какие-нибудь «левые» файлы, но если вам и удастся каким-то чудом приобрести реального сборщика бонусов – вас моментально разоблачат, и ваш аккаунт будет немедленно заблокирован и обнулен.

### Производство этикеток, вырезание ярлыков и т. п

В Интернете можно встретить массу объявлений, которых объединяет следующее: в них удаленным работодателям предлагается делать какую-либо надомную работу, не связанную с компьютером, а результат работы высылать бандеролью или посылкой. Есть и еще одна черта, которая является общей для всех подобных объявлений – это, как вы, наверное, уже догадались, требование выслать определенную сумму денег по указанным реквизитам в качестве «залога», «гарантии порядочности» и т. п. Что касается непосредственно вида деятельности, то это может быть все, что угодно: вырезание наклеек или этикеток, упаковка компакт-дисков, склеивание бумажных журавликов, обработка паром изделий из полиэтилена, перебирание черно-белых шариков (!) и их сортировка, и т. п. На рис. 9.1 показан пример такого объявления, в котором речь идет о вырезании этикеток для чая.



Здравствуйте, Вас беспокоит ДП «Heritage Group Ru»!

Спасибо, что откликнулись на наше объявление!!!

В настоящее время наша компания предлагает жителям любых регионов надомную работу по вырезке этикеток для чая.

Предлагаемая работа проста и доступна каждому. Никаких ограничений по возрасту, полу, образованию, месту жительства нет. Мы Вам будем платить по 2 руб. за каждую вырезанную этикетку. Пересылка рабочего материала, готовой продукции, а также оплата труда производится по почте. С Вашей стороны почтовых расходов не будет, т.к. они будут Вам компенсированы при выплате заработной платы.

Готовые этикетки Вы будете отправлять в наш адрес бандеролью.

Если у Вас возникнут сомнения, можете отправить готовые этикетки наложенным платежом, что станет гарантией их выкупа нами.

Количество заготовок этикеток высылаемых одному работнику ограничено - не более 10000 заготовок в месяц. Таким образом, максимальная заработная плата составляет 20000 руб. в месяц. Если для Вас эта норма окажется слишком большой, то Вы можете заказывать меньшее количество заготовок, но не менее 1000 шт. в месяц.

Этикетки служат в качестве элемента защиты нашей продукции от подделок. Они представляют собой форму правильного шестиугольника. Этикетки изготовлены из полимерной голографической пленки, которая портится механической нарезкой, поэтому их необходимо вырезать вручную.

ПОРЯДОК ТРУДОУСТРОЙСТВА

Для начала работы мы высылаем пробную партию заготовок в размере 1000 шт.

Для того чтобы приступить к работе, Вам необходимо внести залоговую сумму за заготовки в размере 300 руб. (или 30000 белорусских рублей) (из расчета 0.30 руб. за заготовку). При отправке нам готовых этикеток залоговая сумма Вам будет возвращена.

Мы не можем высылать заготовки всем желающим бесплатно, т.к. раньше некоторые писали нам из любопытства, не имея серьезных намерений сотрудничать с нами, и не выполняли заказанную работу, в результате чего мы несли убытки, поскольку голографическая пленка, из которой изготовлены заготовки достаточно дорогая.

Заготовки для вырезки мы будем высылать заказной бандеролью.

Более подробные инструкции о порядке расчета наложенного платежа, компенсации почтовых расходов и порядке дальнейшего сотрудничества Вы получите вместе с пробной партией заготовок.

В дальнейшем Вы можете заказывать большее количество заготовок одной бандеролью. Если Вы зарекомендуете себя дисциплинированным сотрудником, то мы, со своей стороны, после выполнения первой партии этикеток освободим Вас от внесения залоговой суммы за заготовки.

Если Вы согласны с условиями поставки первой партии, то пришлите письмо-запрос на получение пробной партии.

В ответ мы отправим Вам реквизиты для оплаты первой партии заготовок.

Наш сайт: http://tea.imess.net/

Форум удаленной работы ДП «Heritage Group Ru» heritageru.forum24.ru

С уважением,

менеджер - Ветрова Анна.

Рис. 9.1. Мошенники предлагают вырезать этикетки для чая

Поскольку соискателям предлагается перечислить некий залог в размере 300 российских или 30 000 белорусских рублей (что в любом случае составляет примерно 10 долларов США), то уже ясно, что здесь действуют злоумышленники. Тем же, у кого остались какие-то иллюзии, рекомендуем обратить внимание на указанный в объявлении сайт: http://tea.ueuo.com. Он располагается на бесплатном хостинге, и сразу возникает вопрос: почему фирма, которая предлагает простую надомную работу за очень неплохие деньги (20 000 рублей – это около 700 долларов США), не может позволить себе платный хостинг? Неужели для нее 10–15 долларов (за эти деньги можно купить хороший хостинг на год) – такая неподъемная сумма?

А фраза «Этикетки изготовлены из полимерной голографической пленки, которая портится механической нарезкой, поэтому их необходимо вырезать вручную», способна рассмешить даже безнадежных скептиков и зануд.

Что касается «форума удаленной работы», ссылка на который дается в объявлении, то на

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

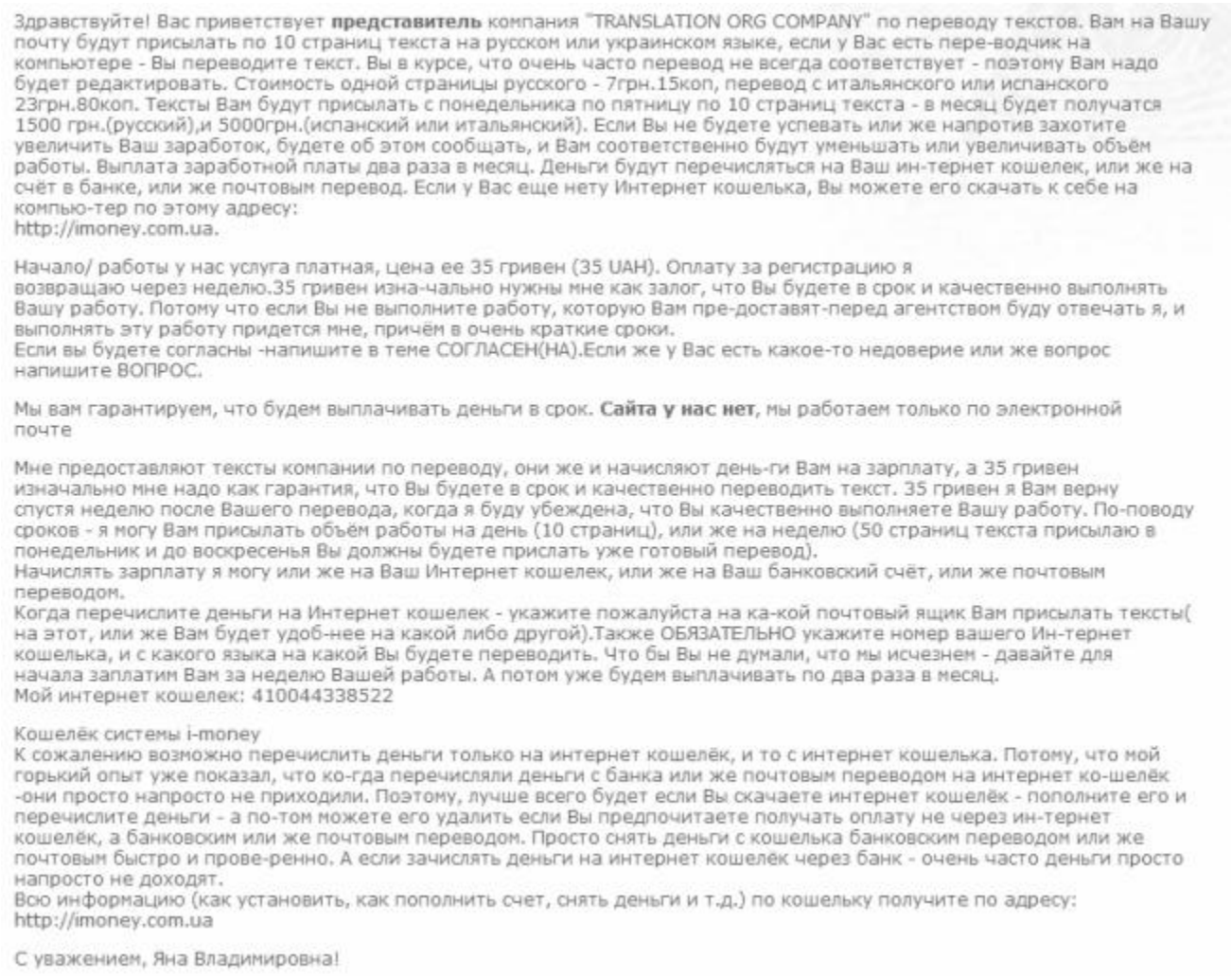
нем имеется несколько тем и разделов, посты в которых составлены в едином стиле (видимо, их сочинял специально нанятый человек). Как нетрудно догадаться, почти все посты в этом форуме примерно такого плана: отличная компания, я уже много денег заработал, присоединяйтесь, и т. п. Для разнообразия вставлено несколько постов якобы от сомневающихся («а не обман ли это», «а у вас действительно можно заработать»), которым тут же «отвечают» якобы опытные работники компании («да, не сомневайтесь», «все честно и справедливо»), и т. д. Ну и для пущей «достоверности» есть несколько постов, предупреждающих о том, что «под вывеской нашей честнейшей фирмы появились мошенники, будьте внимательны».

**«Работа» для переводчиков**

Переводчики-фрилансеры часто становятся жертвами мошенников. Ниже мы приводим конкретный пример объявления, которое дали промышляющие подобным образом злоумышленники.

Здравствуйте!
Вас приветствует компания по переводам «Форум». В связи с расширением и увеличением работ мы проводим дополнительный набор сотрудников для удаленной работы, это выгодно и Вам и нам – Вам тем, что Вы в свободное от работы время можете дополнительно зарабатывать, ну а нам – тем что не надо дополнительного места в офисе.
Условия работы: Вам будет выслан по электронной почте текст в документе WORD. Вам надо будет его перевести, и отправить обратно. Я могу Вам присылать объем работы на день (10 страниц), или же на неделю (50 страниц текста присылаю в понедельник и до воскресенья Вы должны будете прислать уже готовый перевод). График работы Вы устанавливаете себе сами.
Оплата: Перевод текстов с русского на украинский и наоборот (1500грн) в переводчике и соответственно редактирование (на дому). Кто знает испанский или итальянский – зарплата 900 грн. Подробности на e-mail: nabor-text@inbox.ru в теме письма укажите «Работа с текстом».

Автор этой книги не поленился и ради эксперимента написал письмо по указанному адресу. Через некоторое время пришел ответ, который показан на рис. 9.2.



Здравствуйте! Вас приветствует **представитель** компания "TRANSLATION ORG COMPANY" по переводу текстов. Вам на Вашу почту будут присылать по 10 страниц текста на русском или украинском языке, если у Вас есть пере-водчик на компьютере - Вы переводите текст. Вы в курсе, что очень часто перевод не всегда соответствует - поэтому Вам надо будет редактировать. Стоимость одной страницы русского - 7грн.15коп, перевод с итальянского или испанского 23грн.80коп. Тексты Вам будут присылать с понедельника по пятницу по 10 страниц текста - в месяц будет получатся 1500 грн.(русский),и 5000грн.(испанский или итальянский). Если Вы не будете успевать или же напротив захотите увеличить Ваш заработок, будете об этом сообщать, и Вам соответственно будут уменьшать или увеличивать объём работы. Выплата заработной платы два раза в месяц. Деньги будут перечисляться на Ваш ин-тернет кошелек, или же на счёт в банке, или же почтовым перевод. Если у Вас еще нету Интернет кошелька, Вы можете его скачать к себе на компью-тер по этому адресу:
http://imoney.com.ua.

Начало/ работы у нас услуга платная, цена ее 35 гривен (35 UAH). Оплату за регистрацию я возвращаю через неделю.35 гривен изна-чально нужны мне как залог, что Вы будете в срок и качественно выполнять Вашу работу. Потому что если Вы не выполните работу, которую Вам пре-доставят-перед агентством буду отвечать я, и выполнять эту работу придется мне, причём в очень краткие сроки.
Если вы будете согласны -напишите в теме СОГЛАСЕН(НА).Если же у Вас есть какое-то недоверие или же вопрос напишите ВОПРОС.

Мы вам гарантируем, что будем выплачивать деньги в срок. **Сайта у нас нет**, мы работаем только по электронной почте

Мне предоставляют тексты компании по переводу, они же и начисляют день-ги Вам на зарплату, а 35 гривен изначально мне надо как гарантия, что Вы будете в срок и качественно переводить текст. 35 гривен я Вам верну спустя неделю после Вашего перевода, когда я буду убеждена, что Вы качественно выполняете Вашу работу. По-поводу сроков - я могу Вам присылать объём работы на день (10 страниц), или же на неделю (50 страниц текста присылаю в понедельник и до воскресенья Вы должны будете прислать уже готовый перевод).
Начислять зарплату я могу или же на Ваш Интернет кошелек, или же на Ваш банковский счёт, или же почтовым переводом.
Когда перечислите деньги на Интернет кошелек - укажите пожалуйста на ка-кой почтовый ящик Вам присылать тексты( на этот, или же Вам будет удоб-нее на какой либо другой).Также ОБЯЗАТЕЛЬНО укажите номер вашего Ин-тернет кошелька, и с какого языка на какой Вы будете переводить. Что бы Вы не думали, что мы исчезнем - давайте для начала заплатим Вам за неделю Вашей работы. А потом уже будем выплачивать по два раза в месяц.
Мой интернет кошелек: 410044338522

Кошелёк системы i-money
К сожалению возможно перечислить деньги только на интернет кошелёк, и то с интернет кошелька. Потому, что мой горький опыт уже показал, что ко-гда перечисляли деньги с банка или же почтовым переводом на интернет ко-шелёк -они просто напросто не приходили. Поэтому, лучше всего будет если Вы скачаете интернет кошелёк - пополните его и перечислите деньги - а по-том можете его удалить если Вы предпочитаете получать оплату не через ин-тернет кошелёк, а банковским или же почтовым переводом. Просто снять деньги с кошелька банковским переводом или же почтовым быстро и прове-ренно. А если зачислять деньги на интернет кошелёк через банк - очень часто деньги просто напросто не доходят.
Всю информацию (как установить, как пополнить счет, снять деньги и т.д.) по кошельку получите по адресу:
http://imoney.com.ua

С уважением, Яна Владимировна!

Рис. 9.2. Ответ, полученный от мошенников

Как видно на рисунке, в ответе полно грамматических, орфографических и стилистических ошибок, а также явных опечаток (может, и номер кошелька указан с ошибкой?). Ну а тот факт, что «сайта у нас нет, и мы работаем только по электронной почте», у любого здравомыслящего человека может вызвать лишь саркастическую улыбку. А если говорить серьезно, то все очень похоже на то, что данное письмо составлено и отправлено автоответчиком. Получается, что деятельность мошенника состоит из следующих этапов:

♦ размещение в Интернете объявлений о наборе удаленных переводчиков;

♦ настройка автоответчика для автоматической рассылки ответов тем, кто прислал на рассмотрение свои кандидатуры;

♦ получение денег из электронного кошелька, который пополняется за счет обманутых соискателей.

Иначе говоря, мошенник даже не утруждает себя тем, чтобы прочесть письма соискателей, а просто периодически проверяет кошелек и получает деньги.

**«Работа» для наборщиков текстов**

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Сплошь и рядом на сайтах, посвященных трудоустройству, а также на досках бесплатных объявлений можно встретить объявления о наборе удаленных сотрудников для набора отсканированного текста. При этом «работодатель» красочно описывает перспективы, высокие расценки и привлекательные заработки – правда, сам при этом не имеет ни сайта, ни контактного телефона, а электронный ящик у него открыт на бесплатном ресурсе. На рис. 9.3 показан пример такого объявления.

**Описание объявления «Требуется наборщик текстов»**

Требования:
- Знание русского языка, грамотность;
- Знание ПК и офисных программ;
- Доступ в Интернет для поддержки связи с офисом и передачи материала;
- Возраст от 16 лет;
- Место проживания не имеет значения.

Обязанности: Обработка материала любой тематики посредством текстового редактора, это может быть печатный или рукописный отсканированный текст.

Условия: свободный график, сдельная оплата до 30000 рублей в месяц.

Рис. 9.3. Мошенническое объявление о вакансии наборщика текстов

Первая мысль, которая приходит в голову после прочтения подобного объявления: если бы это было реально – половина населения России немедленно бросила бы работу и села набирать тексты по свободному графику за 30 000 рублей (фактически 1 000 долларов) в месяц!

Хотя на первый взгляд такая работа кажется вполне реальной: ведь набор текстов – это конкретный вид деятельности, в отличие от той же обработки почтовой корреспонденции или прочих сомнительных предложений. Но после того как вы отправите письмо с предложением своей кандидатуры, вам предложат перечислить некоторую сумму (это может быть и 50, и 100, и 300 рублей, и др.) в счет гарантии того, что вы действительно выполните порученное задание качественно и в срок, либо в качестве залога за присланные вам компакт-диски с заданием, и т. п.

Очевидно, что подобные обоснования «притянуты за уши» и не имеют под собой никаких оснований. Стоит ли говорить, что после отправки мошенникам денег никакого задания вы не получите! А может – получите, и даже выполните его, и отправите мошенникам – только вот денег за выполненную работу вам никто не заплатит.

Стоит отметить, что в последнее время злоумышленники сделали выводы из предыдущих ошибок и иногда готовы прислать по требованию соискателя реквизиты фирмы (адрес, ИНН, банковские счета), а также контактные телефоны. Это делается для того, чтобы усыпить бдительность потенциальных жертв. Вот только ничего общего с реальностью эти реквизиты иметь не будут: такая фирма либо вообще не существует, либо занимается совсем другими видами деятельности. Поэтому желательно уточнить следующие моменты:

- ♦ действительно ли существует такая фирма;
- ♦ действительно ли она находится по указанному адресу;
- ♦ действительно ли она набирает удаленных сотрудников для набора текста;

♦ действительно ли это ее телефон;

♦ действительно ли по этому телефону отвечает сотрудник данной фирмы (а не кто-то посторонний).

Также всегда полезно дать понять удаленному работодателю, что вы можете подъехать по указанному адресу для личной беседы. Даже если вы живете, например, в Красноярске, а удаленную работу предлагает московский работодатель – попросите адрес фирмы и скажите, что вы хотите побеседовать лично в офисе. Очень может быть, что после этого все дальнейшие вопросы отпадут сами собой…

А вообще помните: отсканированные тексты проще не набирать, а распознавать с помощью специальных программ (например, та же Fine Reader). И если вам предлагают набрать отсканированный рукописный или иной плохо распознаваемый текст – это, возможно, действительно реальная работа, а если текст хорошо распознается специальными программами – то задумайтесь: зачем работодателю платить кому-то за набор текста, если его можно распознать самому быстро, качественно и бесплатно?

**«Работа» с почтовой корреспонденцией**

Способ мошенничества, о котором мы расскажем в данном разделе, имеет давнюю историю. Он зародился лет двадцать назад, и первое время реализовывался не с помощью Интернета, а посредством обычной почты. С развитием же интернет-технологий действовать мошенникам стало намного проще.

Сущность способа состоит в том, что мошенники предлагают людям зарабатывать умопомрачительные деньги путем простой обработки писем. Ниже приводится пример электронного письма, с помощью которого мошенники завлекают потенциальных жертв.

Вы уже готовы зарабатывать от 500$ в неделю изменить свою жизнь? Тогда наше предложение именно для Вас!

Надомная работа по программе «Homemailer's Program» от латвийской почтовой компании «Sayma, Ltd». Заполнение конвертов по схеме 2$ за конверт. По этой программе успешно работают заполнители в странах ближнего и дальнего зарубежья.

С помощью «Homemailer's Program» очень многие люди стали довольно состоятельными людьми и смогли осуществить свои самые заветные желания, значительно улучшить свой социальный статус, им стали доступны не досягаемые ранее блага.

Если и Вы готовы примкнуть к рядам этих людей, то Вам неимоверно повезло, ибо то, что мы Вам предлагаем – это просто удача для Вас!

Простая, приятная работа, которую Вы можете выполнять дома в спокойной обстановке всего несколько часов в день. Но эта простая работа принесёт Вам (при должном старании) 50$ и более в ДЕНЬ!!! Разве это не то, что вы искали всю свою сознательную жизнь?

Не дайте ГОСПОЖЕ УДАЧЕ проскользнуть мимо Вас!

Только тот ничего не добивается, кто ни на что не решается! Примите правильное решение, и Ваша семья будет Вам благодарна всю жизнь!

Приступайте немедленно, и тогда Вы можете застать наше СПЕЦИАЛЬНОЕ ПРЕДЛОЖЕНИЕ, приуроченное ко второй годовщине «Homemailer's Program» на рынке труда Украины, России и всего СНГ!

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Место жительства не имеет абсолютно никакого значения! За дополнительной информацией обращаться на e-mail sayma_ukraine@hotpop.com
РЕШАЙТЕСЬ!

Заметьте: никаких контактных данных, кроме электронного ящика, в письме нет. После того как вы напишете письмо на этот ящик, вам придет ответ, сущность которого состоит в следующем: для начала работы вам следует перевести определенную сумму денег по указанным реквизитам. Стоит ли говорить, что после перечисления денег все сотрудничество с этой конторой бесславно закончится!

В данном конкретном случае мошенники завели себе простенький сайт на дешевом хостинге – чтобы создать иллюзию более-менее солидной конторы. Но последние сомнения в нечистоплотности этих «деятелей» исчезают после знакомства с вывешенными на сайте контактными данными (рис. 9.4).


Рис. 9.4. Контактные данные мошенников

Обратите внимание – центральный офис «солидной почтовой компании» находится в абонентском ящике! После этого только самый наивный человек может еще верить в порядочность злоумышленников.

Кстати, важный момент: даже если мошенники дают ссылку на свой сайт – то этот сайт, как правило, имеет примитивный вид и характеризуется отсутствием всякого дизайна. А услуги хостинга в лучшем случае оплачены на непродолжительный срок, что составляет совсем незначительную сумму (в пределах 5-10 долларов США), или вообще являются бесплатными. Это касается всех интернет-мошенников, предлагающих удаленную работу. Проверить историю сайта (на каком хостинге зарегистрирован, на какой срок оплачен хостинг, и др.) можно с помощью специализированных ресурсов в Интернете.

**Предложение о трудоустройстве за дополнительную плату**

Одна из популярных схем выманивания денег выглядит так: пользователь получает письмо (не обязательно спамерское – это может быть просто отзыв на оставленное резюме), в котором красочно описываются сказочные перспективы – «я был почти нищим,

весь в долгах, но благодаря этой замечательной программе быстро разбогател – теперь у меня много денег, вилла на Канарах, куча машин», и тому подобная чепуха. Причем это описание достаточно длинное – оно может занимать несколько страниц. Короче говоря, пользователя, получившего письмо, вначале «грузят» по полной программе.

Если человек, получивший такое письмо, недостаточно опытный – он его не удалит немедленно, как это надо бы сразу сделать, а дочитает до конца. Вот в конце-то и будет сказано о главном условии подобного «счастья» – нужно всего-навсего перевести по указанным реквизитам (чаще всего – на кошелек WebMoney либо аналогичной платежной системы) некоторую сумму денег (сумма варьируется от 10 долларов США до «плюс бесконечности»). Причем – не просто перевести, а оплатить какой-либо информационный пакет, либо ключ, либо инструкции, либо еще что-нибудь, необходимое для дальнейшей «работы». Нужно сказать, что в большинстве случаев пользователь после оплаты действительно получает по почте какую-то информацию, но никаким положительным образом это на его финансовом благополучии не скажется, поскольку приобретает он бессмысленный набор фраз типа «проявляйте усердие, и удача будет с вами».

Еще один способ выманивания денег заключается в том, что мошенник предлагает «содействие в трудоустройстве». Самый примитивный вариант – это когда предлагается прислать свои данные, а вместе с ними некоторую сумму денег за «услуги по поиску работы» и ждать ответа. Само собой, ждать придется бесконечно.

Более «хитрый» вариант может выглядеть так. Пользователь получает отзыв на свое резюме, которое он разместил в Интернете ранее. В письме сообщается, что его резюме весьма заинтересовало руководство крупной (российской или зарубежной) компании, и будет предложено пройти удаленное тестирование. Для этого нужно будет заполнить либо анкету на сайте, либо ответить на присланные вопросы, либо еще что-то подобное. После этого придет письмо с содержанием типа «поздравляем вас, вы прошли предварительное тестирование, результаты отличные». В этом же письме (а может – в следующем) будет предложено продолжить тестирование, но для получения следующих вопросов (анкет и т. п.) нужно заплатить определенную сумму денег. Вот на этом этапе и нужно немедленно прекратить сотрудничество с «агентством», «работодателем» или как там еще мог представиться мошенник. В принципе, не исключено, что после оплаты пользователь получит еще какие-то тесты, анкеты либо вопросы, но после их заполнения и отправки ответ будет либо «к сожалению, повторное тестирование вы не прошли», либо «вы успешно прошли тестирование, но пока вакансии для вас нет», либо что-то аналогичное. В любом случае, если при поиске работы требуют деньги за содействие, за тестирование, за «бланки анкет» либо за что-то еще, нужно помнить – это мошенничество, и ничто иное.

Следует отметить, что агентства по трудоустройству, само собой, могут потребовать плату за свои услуги, но это ни в коем случае не предоплата (в данном случае «предоплата» и «мошенничество» – это синонимы). Обычно плата за трудоустройство взимается в виде определенного процента с первой зарплаты соискателя, полученной им на новом месте работы, и этот процент строго оговаривается заранее.

### Прочие приемы и методы обмана удаленных работников

Привлекательность удаленной работы очевидна, и это намного облегчает деятельность мошенников разного калибра. Самыми легкими их жертвами становятся те, кто спит и во

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

сне видит себя фрилансером (немало людей, готовых хоть завтра бросить работу – были бы привлекательные заказы от удаленных работодателей). Один из самых распространенных приемов обмана состоит в том, что соискателю предлагается выполнить тестовое задание. Если вы копирайтер – это может быть статья или фрагмент текста, если программист – написание фрагмента программного кода или разработка приложения, если веб-разработчик – создание веб-страницы, и т. д. Причем нередко мошенники прямо заявляют: мол, это задание тестовое, оно не оплачивается, но если вы выполните его качественно – мы возьмем вас на работу, и вот тогда вы будете работать за деньги. Стоит ли говорить, что после выполнения такого задания незадачливый фрилансер либо получает отказ в приеме на работу, либо никто вообще с ним не выходит на связь!

Отметим, что подобный «развод» может прикрываться не только тестовым заданием, но и вполне реальной работой. Ведь часто на подобные предложения откликаются опытные люди, у которых есть образцы работ. В этом случае мошенники отвечают в том духе, что, мол, примеры ваших работ нам понравились, и мы предлагаем вам сразу начать работать за деньги (разрабатывать сайт, создавать программный код, писать статьи и книги, переводить тексты, и т. д.). Только вот денег вам, как вы догадались, никто не заплатит.

Ниже мы приводим несколько примеров, как и с какими целями может использоваться подобные мошеннические приемы.

♦ Создание веб-ресурсов. Каждый обманутый фрилансер из числа веб-разработчиков готовит отдельную страницу в виде «тестового задания», такие же наивные копирайтеры готовят контент для данного сайта, а обманутые веб-дизайнеры разрабатывают дизайн. Получается, что над созданием ресурса работает целая команда людей – незнакомых друг с другом, находящихся в разных городах (а возможно – и странах), и в конечном итоге – обманутых. Мошенники лишь координируют их действия и собирают из готовых фрагментов, подобно конструктору.

♦ Разработка программных продуктов. Каждый соискатель пишет свой фрагмент программного кода, такие же фрилансеры из числа технических писателей документируют продукт, и т. д. Когда все фрагменты будущего продукта готовы – удаленным разработчикам вежливо говорят «спасибо, вы нам не подходите». Или вообще ничего не говорят.

♦ Написание книг. Не секрет, что в России действует многочисленная армия «литературных негров», силами которых создается большинство всей современной российской беллетристики (это касается как художественной, так и нехудожественной литературы). Солидные издательства рассчитываются с удаленными работниками полностью и в срок, но существует немало «деятелей», которые делают неплохой бизнес на «халяве», то есть на неоплаченных текстах. Они могут называть себя по-разному: менеджерами проектов, литературными агентами, и т. д. Обычно такой «менеджер проектов» работает примерно так: приглашает на «тестовое задание»» несколько удаленных авторов, каждый из которых пишет отдельную главу книги, затем удаленный редактор редактирует текст, удаленный верстальщик делает верстку, и т. д. После этого всем фрилансерам дается полный «отлуп», готовая и сверстанная книга в электронном виде продается в издательство, и «менеджер проектов» получает свой гонорар. Пытаться делать что-либо в такой ситуации почти бесполезно, и все ваши попытки доказать, что именно вы являетесь истинным автором книги, будут выглядеть нелепо.

♦ Перевод текстов. Алгоритм примерно такой же: удаленному переводчику предлагается перевести пару страниц «на пробу» (или – на условиях последующей оплаты и постоянного сотрудничества). После того как он сдает работу, с ним на связь никто не выходит, и на его письма никто не отвечает.

♦ Написание статей, журналистских материалов, и т. д. Удаленный автор или журналист присылает работу (или несколько работ) – и на этом связь с ним прекращается.

♦ Написание сценариев для сериалов, фильмов, компьютерных игр. Известны случаи, когда по украденным таким способом сценариям создавались популярные телевизионные сериалы и разрабатывались компьютерные игры, ставшие впоследствии бестселлерами.

Во всех перечисленных примерах расчет мошенников безошибочный: поскольку обманутые люди незнакомы друг с другом, они не могут скоординировать свои действия и объединиться с целью поимки и разоблачения злоумышленников. Да никому и не хочется этим заниматься – проще смириться с тем, что время на работу было потрачено впустую. Если же кто-то все же пожелает каким-то образом добиться правды – это будет очень сложно: электронная переписка доказательством не является, координат «работодателей» нет, их ФИО никто не знает (разумеется, мошенники представляются под вымышленными именами), да и находиться они могут в другой стране. Причем даже если вы вовремя догадаетесь, что вас пытаются банально «развести», и вовремя «соскочите с крючка» – мошенник ровным счетом ничего не потеряет, поскольку легко и быстро найдет вам замену.

Тем не менее, если вы хотите заниматься фрилансерской деятельностью – ставить крест на своих планах не стоит. Достаточно соблюдать несложные меры предосторожности, которые хоть и не дают 100 %-ной защиты от мошенников, но позволяют свести возможный риск к минимуму, и сделать вероятные потери совсем несущественными и не заслуживающими внимания.

Прежде всего, помните: вы должны четко знать, с кем вы намерены иметь дело, и где находится ваш потенциальный работодатель. Например, если вы получили электронное письмо с предложением выполнить работу (неважно, тестовую или нет), и в нем отсутствуют контактные данные отправителя (электронный адрес не в счет) – будьте особо бдительны. Напишите ответное письмо с требованием прислать адрес работодателя и телефон, по которому вы могли бы с ним побеседовать. Как правило, мошенники просто не отвечают на подобные письма, понимая, что этого человека «развести» не получится. Или присылают нелепые отговорки – мол, мы меняем адрес, телефон пока не подключили, и т. п. В любом случае знайте: без контактных данных работодателя (и их последующей проверки – как минимум нужно позвонить) к работе приступать нельзя, поскольку если вам их не дают – это однозначно «лохотрон».

ВНИМАНИЕ

Мошенник может настойчиво требовать от вас подробное развернутое резюме и прочие сведения, но при этом о себе он не скажет ни слова, несмотря на все ваши требования. Желая получить от вас максимум информации, он тем самым стремится обезопасить себя: например, вдруг программный код, который вы ему пришлете, является украденным, или присланный вами текст книги является плагиатом, и т. д. Имея же ваше резюме с образцами работ, он, по крайней мере, будет знать, что вы действительно программист или копирайтер, а не такой же жулик, который на халяву решил подзаработать.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Многие мошенники, предлагающие удаленную работу, сразу спрашивают: можете ли вы подъехать в офис для личной беседы? Такой вопрос должен насторожить: это, скорее всего, «проверка на вшивость». Если вы ответите, что, мол, я не могу приехать, поскольку живу в другом городе – вам тут же с радостью ответят, что «это желательно, но не критично, можете приступать к работе». Злоумышленники будут знать, что вы живете далеко, следовательно – вас можно обманывать без страха и упрека.

СОВЕТ

В подобной ситуации всегда отвечайте: да, я готов приехать в офис – даже если работодатель находится в другом регионе. Если вам назначат встречу – тогда можно извиниться и сказать: мол, извините, я не заметил, что вы находитесь в другом городе. По крайней мере, это будет свидетельствовать о том, что работодатель от вас не прячется.

Получив предложение об удаленной работе, наведите справки о своем потенциальном работодателе. С помощью Интернета это несложно: введите в любой поисковик название фирмы, или ФИО написавшего вам человека, на худой конец – просто электронный адрес, и ознакомьтесь с результатами поиска. В большинстве случаев даже такая элементарная проверка позволяет быстро расставить все точки над «i».

Еще один эффективный способ проверки удаленных работодателей – так называемые «черные списки работодателей», которые во множестве представлены в Интернете. Эти списки формируются по всем сферам, в том числе и по удаленной работе. Если вы сомневаетесь в честности работодателя – возможно, он уже кого-то обманул, и информация о нем есть в «черном списке». Если же вы стали жертвой мошенника – не поленитесь внести в такой список о нем информацию: возможно, кому-то эти сведения помогут избежать обмана. Найти «черный список» просто – для этого достаточно в любом поисковике ввести соответствующий запрос.

ПРИМЕЧАНИЕ

Иногда информация попадает в «черные списки» от конкурентов вполне порядочного работодателя. Однако в большинстве случае содержимому «черных списков» можно доверять.

Ну и, конечно, ни в коем случае не соглашайтесь переводить деньги «за материалы для работы», «услуги по пересылке задания» и т. п. Помните: если в качестве условия приема на работу вас кто-то просит перевести пусть даже немного денег – это обман, и ничто иное.

## Глава 10. Как противостоять интернет-мошенникам

Ранее мы уже неоднократно говорили о том, что каждый пользователь Интернета в состоянии самостоятельно обезопасить себя от посягательств удаленных злоумышленников. В данной главе мы приведем конкретные рекомендации относительно

того, что для этого нужно сделать, и чего делать не стоит.

**Меры ответственности за противоправные действия в области высоких технологий**

Поскольку действия интернет-мошенников прямо подпадают под юрисдикцию Уголовного кодекса РФ, мы приведем статьи УК, в соответствии с которыми злоумышленников можно привлечь к ответственности.

Статья 159 УК РФ. Мошенничество

1. Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, – наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо арестом на срок от двух до четырех месяцев, либо лишением свободы на срок до двух лет.
2. Мошенничество, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, – наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо исправительными работами на срок от одного года до двух лет, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года либо без такового.
3. Мошенничество, совершенное лицом с использованием своего служебного положения, а равно в крупном размере, – наказывается штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок от двух до шести лет со штрафом в размере до десяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного месяца либо без такового и с ограничением свободы на срок до полутора лет либо без такового.
4. Мошенничество, совершенное организованной группой либо в особо крупном размере, – наказывается лишением свободы на срок от пяти до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Статья 272 УК РФ. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273 УК РФ. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

**Профилактические меры безопасности**

Дабы максимально оградить себя от посягательств злоумышленников, соблюдайте меры предосторожности и правила, которые перечислены ниже. О некоторых их них мы уже упоминали ранее, но в данном случае повторение лишним не будет.

♦ Прежде чем выходить в Интернет, установите на компьютер хорошую антивирусную программу. Следите за тем, чтобы антивирусные базы все время были актуальными, и помните, что в мире ежечасно появляется несколько новых вирусов.

♦ Никогда не храните логины, пароли, пин-коды, номера кредитных карт и прочие конфиденциальные сведения в открытом виде – например, в обычном текстовом файле, или на бумажке, прикрепленной к монитору. Как показывает практика, множество афер совершается благодаря тому, что беспечная жертва своевременно не позаботилась о хранении секретных данных в надежном месте.

♦ Если вы подключаетесь к Интернету через телефонную линию, никогда не выключайте динамик модема. Это позволит сразу распознать попытки интернет-мошенников несанкционированно подключить ваш компьютер к тому или иному удаленному веб-ресурсу путем набора заданного телефонного номера (часто это практикуют распространители порнографических сайтов и услуг подобной направленности).

♦ Если вы все же хотите хранить все конфиденциальные данные в одном файле – заархивируйте этот файл и защитите архив надежным паролем (минимум из 16 символов). Рекомендуется использовать для этого архиватор WinRAR – как показывает практика, расшифровать такой пароль практически нереально.

♦ Если вы услышали, что модем начал самопроизвольно набирать какой-то номер без вашего участия – срочно отключитесь от Интернета путем физического отсоединения

кабеля. Затем просканируйте компьютер специальной программой категории Antispyware (антишпионским приложением) – очень может быть, что в компьютер тайно внедрен шпионский модуль автоматического дозвона. В конечном итоге это чревато получением астрономических счетов от телефонной компании.

♦ Не доверяйте посторонним свои учетные данные, а также не предоставляйте право пользования своими электронными кошельками, управления банковскими счетами через Интернет, и т. п. К сожалению, нередко мошенниками становятся именно те, кому вы больше всего доверяете. Кроме этого, даже если доверенное лицо является кристально честным человеком, ваши конфиденциальные данные у него могут просто похитить.

♦ Будьте максимально бдительны и осторожны при посещении неизвестных страниц в Интернете. Сегодня широко распространены шпионы и вирусы, для заражения которыми достаточно просто зайти на определенную веб-страницу.

♦ Электронную корреспонденцию, поступившую от неизвестных и сомнительных отправителей, перед открытием обязательно проверяйте надежной антивирусной программой (с актуальными базами). Несоблюдение этого правила может привести к тому, что ваш компьютер быстро превратится в «шпионское гнездо».

♦ После скачивания из Интернета файлов, архивов и т. п. надо сразу же проверить их антивирусной программой, и только после этого запускать на выполнение, распаковывать и т. д. Помните, что многие вредоносные программы распространяются в виде исполняемых файлов либо архивов.

♦ Если вы пользуетесь операционной системой Windows – регулярно проверяйте ее на предмет безопасности. В частности – своевременно скачивайте с сайта Microsoft и устанавливайте на свой компьютер все последние обновления, касающиеся безопасности (так называемые «заплатки»).

♦ Никогда не отвечайте на запросы и письма, в которых содержится просьба прислать ваши секретные данные (логин, пароль, пин-код и т. п.) по указанному адресу. Этот нехитрый способ (разновидность так называемой «социальной инженерии») позволяет злоумышленникам получить чужие логины, пароли, пин-коды кредитных карт, и иные конфиденциальные сведения.

♦ Если при посещении различных ресурсов в Интернете (форумы, страницы регистрации, и т. д.) требуется оставить о себе некоторые данные, то они должны содержать минимум сведений. В частности, никогда и никому не сообщайте свои паспортные данные, домашний адрес, различные пароли и т. п. Несмотря на то, что владельцы и руководители многих Интернет-ресурсов гарантируют полную конфиденциальность, не будьте наивными: если кому-то надо получить эту информацию, он ее получит, и вполне может использовать для шантажа, вымогательства и т. п.

♦ По окончании работы в Интернете обязательно отсоединяйте кабель от линии соединения с Интернетом. Помните, что в противном случае ваш компьютер будет уязвимым даже в выключенном состоянии.

Помимо перечисленных правил безопасности, при работе в Интернете руководствуйтесь нормами и принципами, которые диктуется здравым смыслом и элементарной осторожностью.

**Характерные признаки, позволяющие с высокой долей вероятности распознать обман**

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Несмотря на то, что мошеннических методов известно немало, многие жулики работают стандартно, по определенному шаблону. Ниже дается перечень типичных признаков, позволяющих вовремя распознать злоумышленников.

♦ В мошенническом предложении непременно будет содержаться просьба перечислить (перевести, заплатить и т. п.) определенную сумму по указанным реквизитам под тем или иным предлогом – в зависимости от того, что именно вам предлагают. Это может быть «плата за регистрацию», «залог как подтверждение порядочности», «инвестиции под высокие проценты», перевод денег на «волшебный кошелек», «аванс под выгодную покупку», «ставка на участие в игре» и т. д. В любом случае, обоснование платежа значения не имеет – важно помнить одно: если в любом поступившем из Интернета предложении, рекламе и т. п. содержится требование или просьба перевести деньги – это однозначно «лохотрон».

♦ Как правило, мошенники просят перечислить деньги на электронный кошелек WebMoney (чаще всего), Яндекс. Деньги или других электронных платежных систем. Это обосновано тем, что при банковском или почтовом переводе злоумышленника можно вычислить, а вот электронные платежные системы гарантируют полную анонимность.

♦ Мошеннические предложения характерны тем, что в них отсутствуют координаты и контактные данные. Максимум, что они предоставляют – электронный почтовый адрес, иногда – сайт. Иначе говоря, ни фирма, ни виртуальное казино, ни интернет-магазин, ни «инвестиционный фонд» своего адреса и сайта не имеют. Даже мобильный телефон (не говоря уже о городском) злоумышленники давать боятся. Если в объявлении все же присутствует какой-то почтовый адрес – это или абонентский ящик (см. рис. 1.1), или фальшивый адрес, который либо вообще не существует, либо в нем находится совершенно посторонняя организация, не имеющая к мошенникам никакого отношения. Учтите, что фальшивый адрес может быть составлен хитро: например, злоумышленники указывают вполне реальную улицу, реальный почтовый индекс, а вот номер дома – вымышленный, причем ненамного отличающийся от реального. В частности, если на данной улице последний номер дома 43, то мошенники могут указать в объявлении несуществующий дом № 44. Такой нехитрый прием зачастую позволяет ввести в заблуждение даже тех жертв, которые неплохо знают данный район. Например, знаете ли вы последний номер дома на улице, где вы живете или работаете? А иногда даже номер дома указывается верно, но к нему добавляется несуществующий корпус или строение.

♦ Письмо с предложением (о работе, об участии в бизнес-проекте, о выгодных покупках, об инвестициях, поиск спутника жизни и пр.) является спамом. Помните – ни одна серьезная организация не будет опускаться до того, чтобы деловые предложения распространять в виде спама. Ей просто это не нужно – по-настоящему выгодные и перспективные проекты навязчивой рекламы не требуют.

♦ Письмо или объявление изобилует большим количеством грамматических, орфографических, стилистических и прочих ошибок. Это может свидетельствовать о том, что его составлял либо полуграмотный, либо безответственный и небрежный человек. Естественно, это в принципе исключает возможность того, что он способен предложить что-то действительно стоящее и заслуживающее внимания. Если же вы получили такое безграмотное письмо в ответ на свое сообщение – вероятнее всего, оно сгенерировано автоответчиком. В этом случае злоумышленник даже не удосуживается почитать, что вы там ему написали, а просто информирует вас о том, сколько и куда нужно перечислить денег (подробно сдабривая эту информацию сказками о «крутизне» фирмы, о будущих

астрономических доходах и т. п.).

♦ В предложении о работе вам обещают поистине сказочные доходы, иногда подтверждая это отсканированными копиями якобы «чеков» с умопомрачительными суммами. При этом работа занимает немного времени, не требует специального образования и подготовки, легка и приятна.

♦ Вам неоднократно подчеркивают преимущества надомной работы, делая акценты на «болевых точках», которые есть у большинства обывателей: мол, зачем работать «на дядю» – лучше на себя; зачем вставать каждое утро по будильнику – спите сколько хотите и работайте по свободному графику; зачем ждать очередной отпуск – ведь намного лучше отдыхать тогда, когда вам хочется, а не когда начальник соизволит отпустить вас; зачем унижаться перед руководством, выпрашивая отгул – лучше самостоятельно планировать свое время и т. п.

♦ Если в мошенническом предложении есть ссылка на веб-сайт компании – то этот сайт будет располагаться на бесплатном хостинге, а если и на платном – то срок аренды хостинга будет минимальным, как и размер оплаты. Иначе говоря, «известная фирма с мировым именем», «успешное онлайн-казино», «интернет-магазин с многомиллионным оборотом», «крупнейший инвестиционный фонд» и прочие «Рога и копыта» не имеют даже 15–20 долларов США, чтобы арендовать более-менее приличную хостинг-площадку. Еще одна характерная особенность состоит в том, что мошеннические сайты, как правило, сделаны наспех, содержат минимум информации, практически не имеют дизайна, и зачастую состоят всего из одной-двух страниц.

♦ Если мошенники предлагают способ заработка, то никаких возрастных, половых, профессиональных и прочих требований к будущим сотрудникам они не предъявляют. Стандартный набор критериев – возраст от 16 до 60 лет (или вообще не ограничен), образование значения не имеет, опыт работы не требуется, специальная подготовка не нужна. При этом мошенники могут делать упор на то, что их предложение будет особенно интересно врачам, учителям, преподавателям, военным и представителям прочих профессий с традиционно невысоким уровнем заработка.

♦ В подтверждение своей «порядочности» мошенники могут предъявлять электронные копии различного рода «сертификатов». Как правило, основные реквизиты на этих «сертификатах» являются неразличимыми. Это может касаться серии и номера документа, даты его выдачи, наименования организации, выдавшей документ, а также печатей и штампов. Но даже если все данные на сертификате хорошо читаются – не обольщайтесь: очень может быть, что организации, якобы выдавшей сертификат, вообще не существует. С особым подозрением следует относиться к сертификатам, которые якобы выданы зарубежными структурами и составлены на иностранном языке: проверить наличие это организации вы не сможете.

Таковы основные признаки, которые могут помочь вам своевременно распознать мошенников. В целом суть большинства из них к тому, что человеку предлагается быстро стать богатым, не прилагая для этого никаких усилий.

**Что нужно помнить при использовании платежных интернет-систем**

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )

Поскольку самой популярной такой системой является WebMoney, мы дадим несколько советов и рекомендаций ее пользователям, соблюдение которых позволит минимизировать риск попадания в сети злоумышленников.

♦ Если с электронными кошельками вы работаете через WebMoney Keeper (эта программа предоставляется пользователям системы бесплатно, скачать ее можно на сайте www.webmoney.ru), то настоятельно рекомендуется использовать последнюю версию программы. Отметим, что в некоторых случаях вы можете вообще не получить доступ к кошелькам, пока не установите последний релиз. Дело в том, что разработчики системы постоянно следят за надежностью системы безопасности, и вовремя вносят необходимые изменения в программу. Если вы будете пользоваться устаревшими версиями WebMoney Keeper – риск стать жертвой мошенников существенно возрастает.

♦ При перечислении денег со своего электронного кошелька используйте систему СМС-подтверждения. В данном случае деньги будут переведены только после того, как вы введете код подтверждения, который система пришлет на указанный вами при регистрации мобильный телефон. Подробнее об этом механизме защиты см. www.webmoney.ru.

♦ В настройках безопасности включите опцию автоматического контроля IP-адреса. Благодаря этому доступ к вашему кошельку будет возможен только с вашего IP-адреса. Но учтите, что если вы будете работать через прокси-сервер, или по каким-то причинам прятать свой IP-адрес с помощью предназначенных для этого утилит – кошелек может не открыться, пока вы не войдете в Сеть под «родным» IP-адресом.

♦ Файлы ключей храните только на внешних носителях. Если они будут находиться на жестком диске, удаленный злоумышленник может легко получить к ним доступ. Оптимальный вариант – записать их на компакт-диск или флеш-накопитель, и подключать такой носитель только при работе с системой WebMoney. Этот нехитрый прием, хоть и не дает стопроцентной защиты от злоумышленников, по крайней мере сводит к минимуму вероятность того, что удаленный мошенник успеет получить доступ к файлам ключей.

♦ Как можно больше увеличьте размер файла ключей – например, до 100 Мб. В этом случае даже если мошенник и найдет у вас эти файлы – выкачать их ему будет очень сложно ввиду большого размера.

♦ По умолчанию файл ключей системы WebMoney имеет расширение *.kwm. Попробуйте изменить его на какое-либо другое – например, *.txt. В сущности, программе WebMoney Keeper без разницы, какое расширение будет у файла ключей, а вот злоумышленника, имеющего доступ к вашему компьютеру, тем самым можно ввести в заблуждение.

### Почему нельзя пользоваться шаблонными паролями

Многие пользователи часто совершают одну и ту же ошибку, пользуясь стандартными, шаблонными паролями. Один из самых характерных примеров – когда пароль совпадает с логином. Подобрать такой пароль элементарно, а дальше злоумышленник будет действовать в зависимости от того, к чему относится данный пароль. Если это кредитная карта или банковский счет, управлять которым можно через Интернет – все деньги с этого счета исчезнут моментально. Если это пароль к электронному почтовому ящику – злоумышленник получает доступ ко всей вашей переписке, в том числе и

конфиденциального и личного характера. Это дает ему практически неограниченные возможности для шантажа и вымогательства, кроме этого – он может писать от вашего имени любые письма всем имеющимся адресатам. Если этот пароль используется для входа в блог – можно ожидать появления в собственном блоге провокационных, оскорбительных и прочих записей. Другими словами, беспечность при выборе пароля может обернуться огромными финансовыми потерями и прочими неприятностями.

Ниже мы приводим перечень наиболее часто встречающихся стандартных паролей. Если в этом списке вы найдете свой пароль – рекомендуется немедленно заменить его, поскольку эти пароли хорошо известны даже начинающим мошенникам.

♦ password
♦ parol
♦ monkey
♦ myspace1
♦ password1
♦ blink182
♦ 123456 (варианты – 1234567, 12345678, 987654321 и другие логичные последовательности цифр)
♦ Qwerty
♦ abc123
♦ letmein

Кроме этого, стандартными являются пароли с названием марки автомобиля, породы собаки, населенного пункта, и т. п. Если вы не хотите дать мошенникам лишнюю возможность для реализации своих преступных замыслов – потрудитесь придумать нестандартный пароль, тем более что это совсем несложно.

**Заключение**

Надеемся, предложенный материал предостережет читателя от попадания в изощренные ловушки промышляющих в Интернете злоумышленников. Теперь вы наверняка сумеете отличить мошенническое предложение о сотрудничестве от настоящего, сохранить в целости свои электронные деньги, бороться со спамом, вирусами, интернет-шпионажем и прочими негативными явлениями, получившими в последние годы самое широкое распространение.

Отредактировал и опубликовал на сайте : PRESSI ( HERSON )