Лабораторная работа №18
Тема: «Обеспечение безопасности системы»

Теоретическая часть

Защита от вторжений. Брандмауэры

Учитывая все возрастающее количество программ, разрабатываемых для атак на ОС, важнейшей проблемой стало обеспечение безопасности компьютера. Прошло время, когда источником вредоносного программного обеспечения были документы на дискетах и приложения к электронным письмам. Сейчас вирусы и «черви» могут проникнуть в компьютер вообще без каких-либо действий пользователя. Инфицированная машина сама может превратиться в источник распространения вирусов.

Поскольку взаимодействие компьютера с внешним миром осуществляется через порты, а их достаточно много (65 536 в 1 BM-совместимом компьютере), то целесообразна идея закрытия (портов) большинства из них, кроме немногих (одного-двух), абсолютно необходимых. Определить, насколько компьютер открыт для внешнего мира, можно с помощью специальных тестов, позволяющих оценить уровень уязвимости компьютера.

Идеальных ОС не существует, в их числе и Windows XP. Поэтому Microsoft выпускает ежемесячные обновления безопасности, а также срочные внеплановые обновления. Веб-сайт Windows Update позволяет познакомиться со всеми обновлениями, критически важными (critical update), и обновлениями механизмов ОС (features updates). Критически важные обновления призваны решать проблемы, связанные с безопасностью, например проблему защиты от различных видов «эксплойта» (exploit - компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему). В Windows XP имеется полезная служба автоматического обновления («Пуск» - ПКМ по значку «Мой компьютер» - «Свойства» - «Автоматическое обновление»; установка расписания для ежедневной автоматической проверки и установки новых обновлений – рис. 1, по умолчанию обновления отключены).

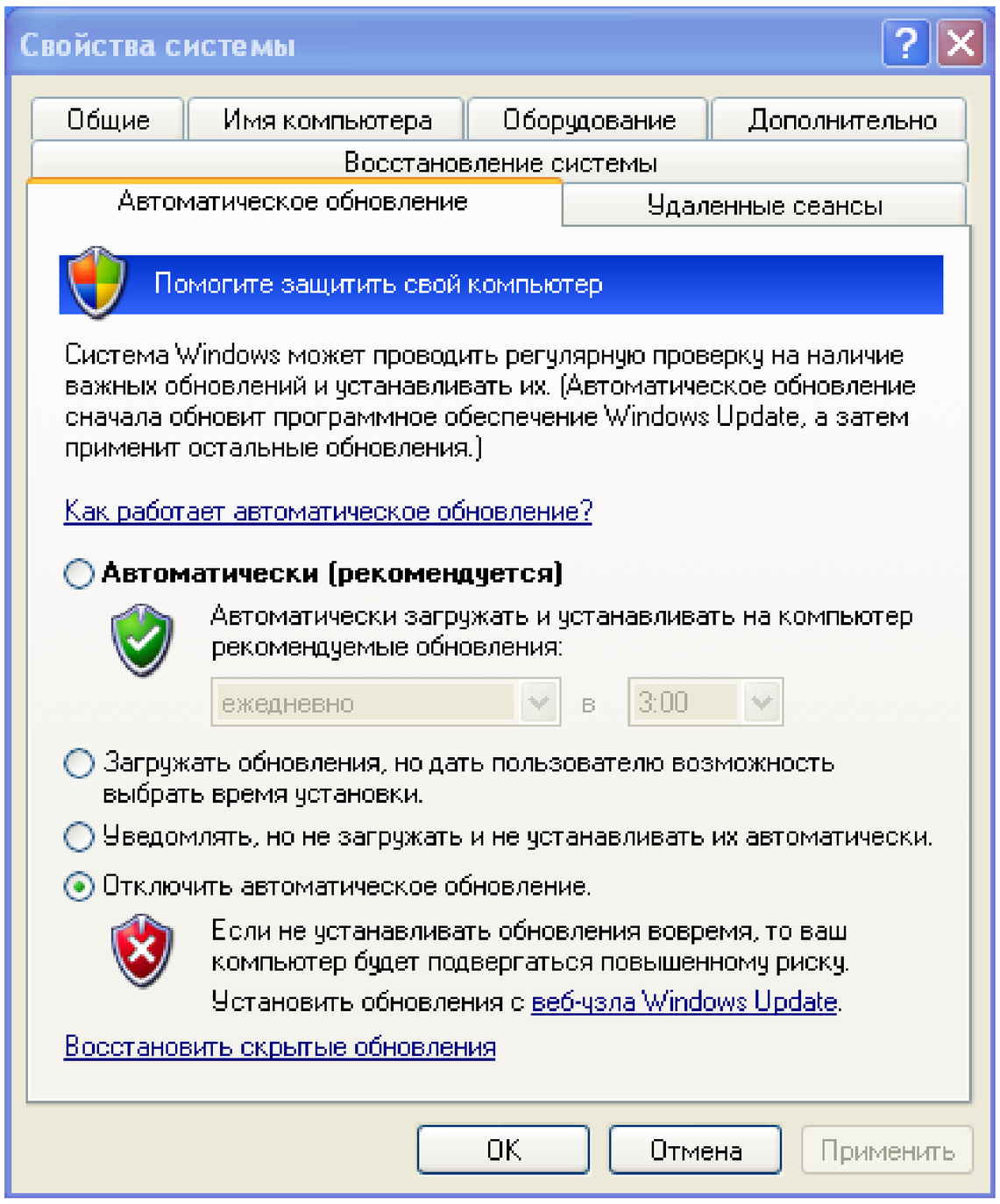

Рис. 1

В Windows XP встроен брандмауэр Internet Connection Firewall (ICF). Брандмауэр – Firewall – программный комплекс, который служит для защиты компьютера от взлома хакерами, а также

всевозможных вирусов и «троянов». Благодаря данной системе повышается степень безопасности работы в сети, и отражаются многие атаки на компьютер за счет фильтрации некоторых информационных пакетов. Брандмаэур отслеживает и блокирует все потенциально опасные подключения, тем самым эффективно защищая личные данные пользователя. Не стоит путать брандмауэр с антивирусными приложениями! Антивирусные приложения необходимы для борьбы с угрозами, которые уже расположены на компьютере или на съемных носителях. Брандмаэур выполняет следующие задачи:

- Отслеживание всех подозрительных соединений – некоторые программы могут отправлять определенные данные в Интернет (Outlook Express; ICQ, MSN – мессенджеры), с этим все нормально. Однако если программа «самовольно» пытается переслать какие-либо данные в сеть Интернет, то это с высокой долей вероятности – вирус/«троян».
- Блокирование всех портов, ненужных для работы, анализ трафика, идущий через открытые порты - компьютер «общается» с Интернетом через порты, задача брандмауэра – защищать эти порты, ведь через них и производятся атаки на компьютер.
- Наблюдение за выполняемыми или запускаемыми программами – если программа запускается в первый раз, то брандмауэр запоминает ее данные. Когда вдруг выясняется, что программа изменилась, брандмауэр должен предупредить об этом пользователя.

Настоятельно не рекомендуется отключать брандмауэр, однако по умолчанию он отключен. Для его использования нужно выполнить два действия:

1) В командной строке «cmd» набираем строку «firewall.cpl» и щелкаем по кнопке «OK»;
2) После открытия диалогового окна (рис. 2) устанавливаем переключатель «Включить» и щелкаем по кнопке «OK».

По умолчанию брандмауэр блокирует все подключения, поэтому его нужно настроить так, чтобы трафик определенных приложений мог проходить через брандмауэр. Настройка заключается в указании программ, трафик которых не должен блокироваться брандмауэром.

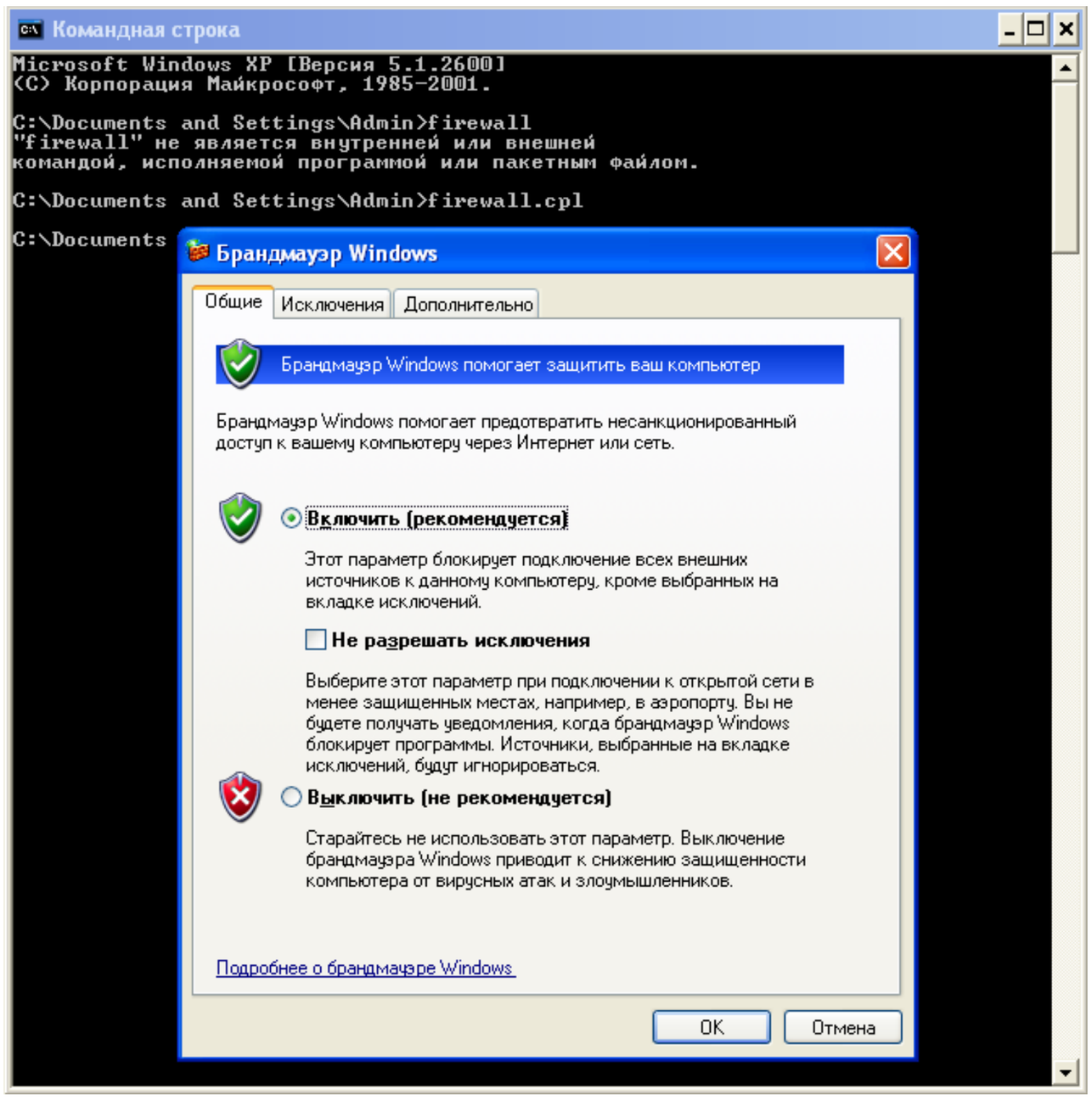

Рис. 2

Для открытия брандмауэра для определенного приложения нужно выполнить следующие шаги:

1) Перейти на вкладку «Исключения» (рис. 3);
2) Просмотреть список всех разрешенных программ (слева от названий таких программ установлен флажок). Целесообразно сбросить флажки для всех программ, которые не предполагается использовать;
3) Если нужно добавить в список исключений новое приложение, которое должно обрабатывать

подключения и данные из внешнего мира, следует щелкнуть на кнопке «Добавить программу»;

4) Из предложенного списка программ выделить название программы, щелкнуть по кнопке «ОК», после чего название программы появится в списке;

5) Установить флажок возле имени добавленного приложения и щелкнуть «ОК» для активизации новых параметров брандмауэра (рис. 3).

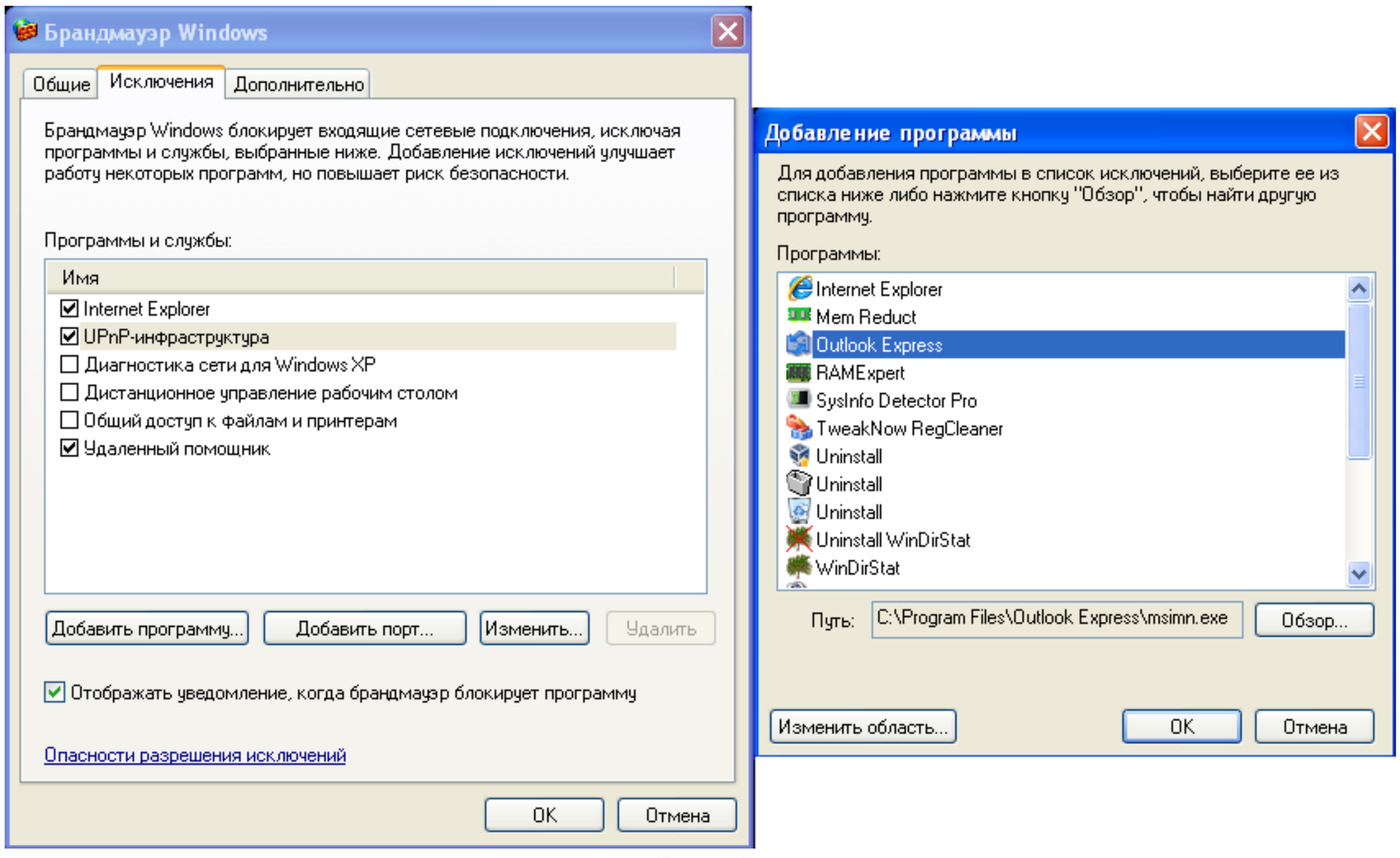

Рис. 3

Брандмауэр Windows позволяет задать режим ответа компьютера в случае посылки ему некоторых стандартных управляющих интернет-сообщений. Например, можно разрешить или запретить команду «ping», которая используется для оценки интервала времени между посылкой данных какому-либо компьютеру и получением от него ответа. Для изменения соответствующего параметра следует перейти на вкладку «Дополнительно» и щелкнуть по кнопке «Параметры» в разделе «Протокол ICMP» (ICMP – протокол управляющих сообщение Интернета). Откроется диалоговое окно «Параметры ICMP» (рис. 4). Если требуется, чтобы компьютер был невидим в Интернете, нужно сбросить все флажки в данном окне.

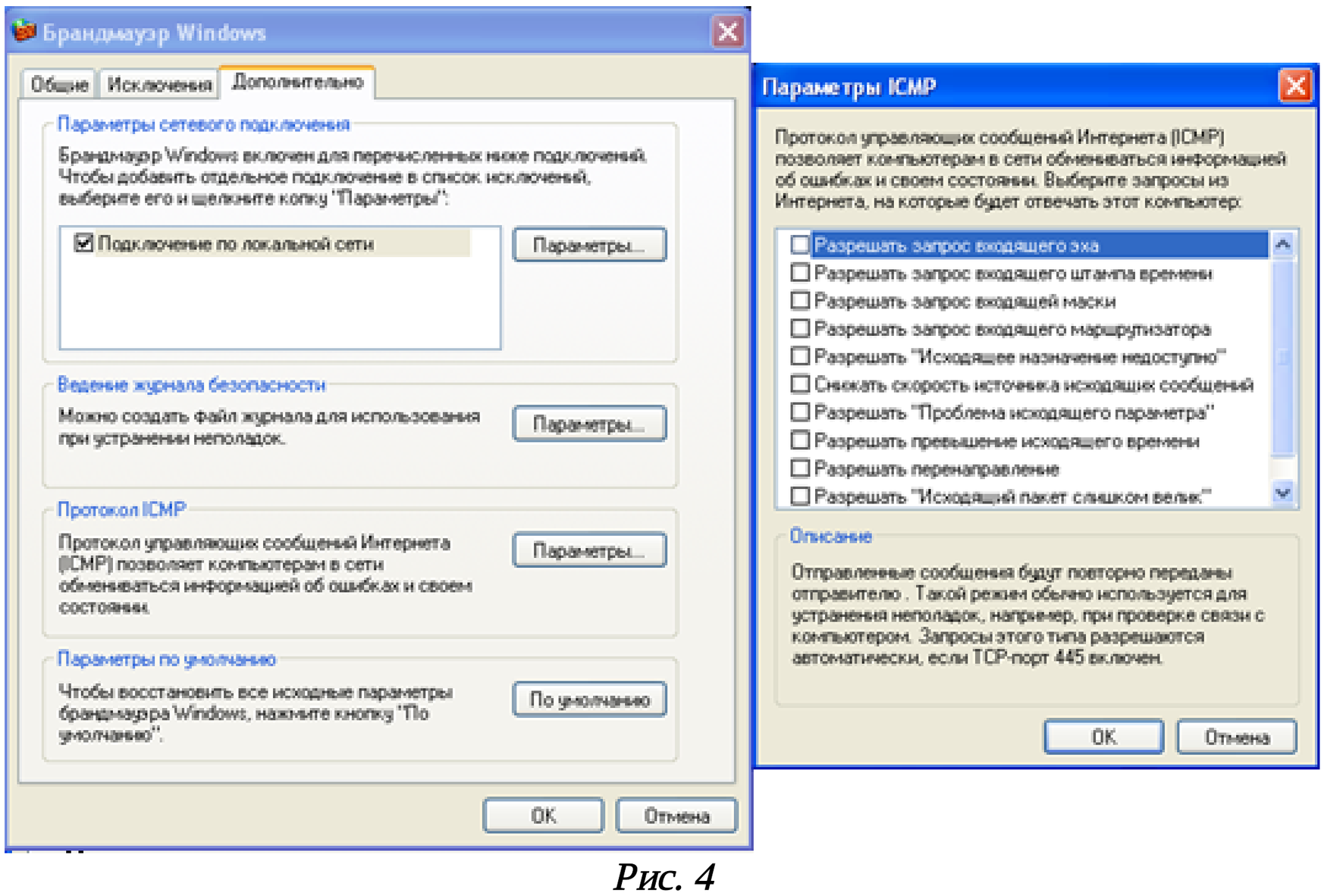

Рис. 4

Брандмауэр Windows XP относится к брандмауэрам одностороннего типа, т.е. может блокировать только входящий трафик. Компания «Zone Labs» разработала двухсторонний брандмауэр ZoneAlarm. Двухсторонний брандмауэр может блокировать не только входящий, но и исходящий трафик, который пытаются отослать приложения с компьютера пользователя. Зачем нужно блокировать исходящий трафик? Например, если пользователь заботится о своей конфиденциальности и не желает, чтобы приложения, установленные на компьютере, связывались с веб-сайтом разработчика для пересылки туда данных, проверки обновлений или лицензий. Кроме того, очень полезной является возможность контролировать, какие приложения получают доступ к Интернету. Особенно эффективен такой брандмауэр в том случае, если пользователь разрешает коллегам иногда работать на своем компьютере. В этом случае недобросовестный коллега, установивший программу «Троянский конь», не получит желаемого результата. Двухсторонние брандмауэры типа ZoneAlarm делают подобные приложения бесполезными, так как подобные вредоносные программы оказываются изолированными и не могут связаться с Интернетом. Помимо ZoneAlarm есть такие брандмауэры, как:

- **TinyWall** – (установил – «отправился по делам») базируется на стандартном брандмауэре Windows. После установки, TinyWall запускается в фоновом режиме с иконкой в системном трее. Все функции программы доступны только из системного трея – никакого интерфейса вида «главного окно» в нем нет. В зависимости от характера программ, можно ограничить брандмауэр только «исходящим» трафиком.

- **AVS Firewall** – имеет дополнительные модули защиты, связанные с реестром. Три уровня защиты: 1) «Выключено» - выключение брандмауэра; 2) «Пользовательский» - позволяет настраивать правила для соединений; 3) «Высокий» - блокирует все соединения. Модуль защиты реестра обеспечивает контроль и безопасность реестра на предмет модификаций, с возможностью настройки конкретных разделов. Устанавливается вместе с браузером AVS Software.

- **Comodo Firewall** – солидный брандмауэр, имеет полнофункциональный пакет безопасности. Предназначен для опытных пользователей и для тех, кто хочет обеспечить себя максимальным уровнем безопасности. Проверяет неизвестные приложения и анализирует «последствия» от приложений, т.е. «как скажется установка этого приложения на операционной системе?». Это мощный брандмауэр с массой гибких настроек, который обеспечивает высокий уровень защиты.

Практическая часть

Настроить брандмауэр Windows XP. Определить список программ, которым разрешено обрабатывать данные, поступающие в компьютер из внешнего окружения.

Отключение неиспользуемых служб

Существуют такие службы, которые можно отключить для повышения защищенности компьютера. «Удаленный рабочий стол в Windows XP» — компонент ОС, позволяющий получить доступ к своему компьютеру в те моменты, когда пользователь находится вдали от своего офиса или дома. Однако если компьютер недостаточно хорошо защищен, удаленный рабочий стол может стать отличным средством для любого злоумышленника, пытающегося проникнуть на чужой компьютер и установить над ним полный контроль. Вся защита удаленного рабочего стола основывается на пароле, который во многих случаях несложно подобрать. В связи с этим, если удаленный рабочий стол не используется, его лучше отключить. Для этого нужно сделать следующее:

❖ Щелкнуть правой кнопкой мыши на значке «Мой компьютер» и выбрать в контекстном меню команду «Свойства»;

❖ В открывшемся окне перейти на вкладку «Удаленные сеансы» (рис. 5), позволяющую задать параметры удаленного доступа;

❖ Сбросить флажки в разделах «Удаленный помощник» и «Дистанционное управление рабочим столом». Щелкнуть по кнопке «ОК» для сохранения изменений.

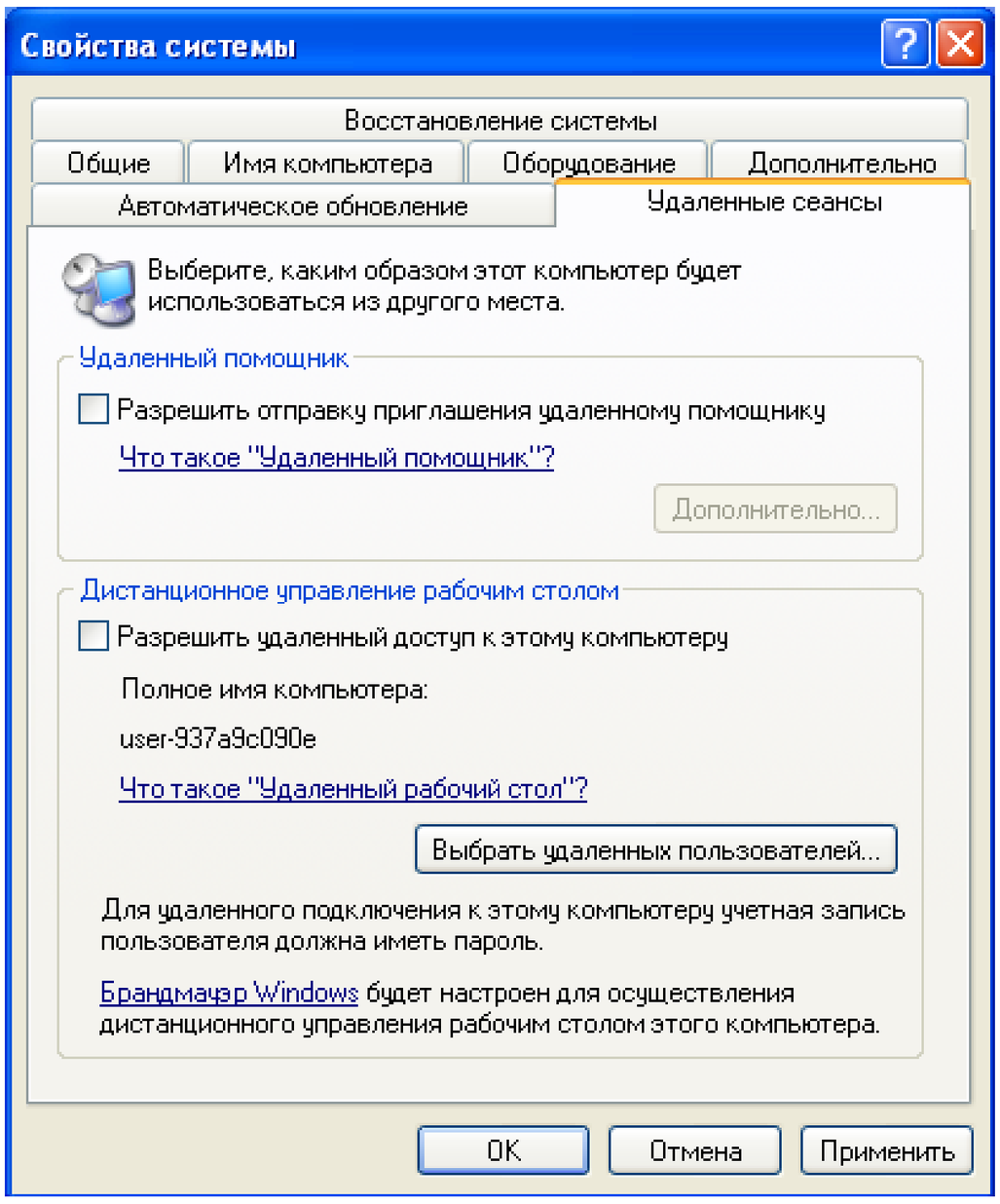

Рис. 5

Отключение службы сообщений.

В последних версиях Windows предусмотрена служба, позволяющая системному администратору посылать сообщения всем компьютерам в локальной сети. Это очень продуктивная служба, если ее правильно использовать. Некоторые пользователи, знающие про эту службу, могут злоупотреблять ею, рассылая сообщения и, хуже того, спам всем пользователям сети. Таким образом, пользователи сети будут получать спам не только через свой почтовый ящик, но и в неожиданно всплывающих диалоговых окнах.

Служба сообщений, как и любая другая программа, имеющая доступ во внешнюю сеть, является потенциальной угрозой безопасности компьютера. Поэтому из соображений безопасности службу сообщений лучше отключить. Для этого следует выполнить команды: «Пуск — Программы — Администрирование — Службы». В открывшемся окне «Службы» выбрать из списка служб строку «Служба сообщений», щелкнуть на ней правой клавишей мыши и выбрать в контекстном меню команду «Свойства» (рис. 6). Далее в раскрывающемся списке «Тип запуска» выбрать пункт «Отключено» и щелкнуть по кнопке «ОК» для сохранения изменений.

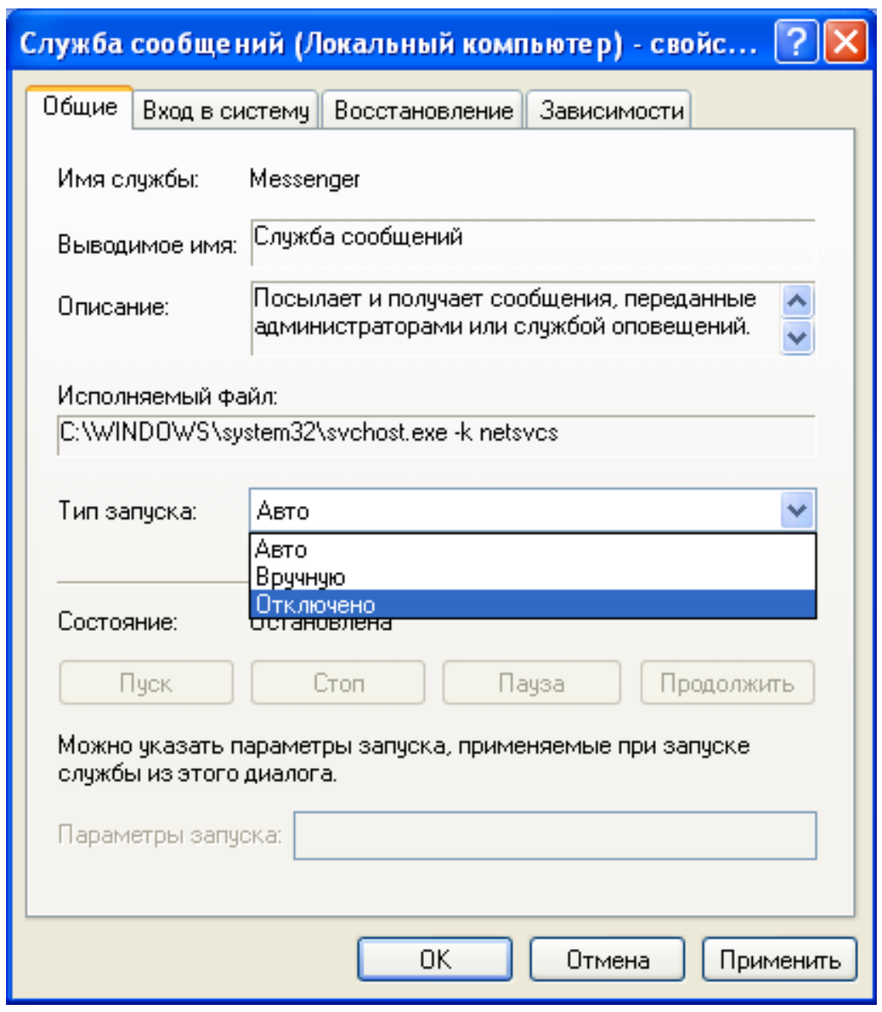

Рис. 6

Отключение поддержки универсальной технологии Plug-and-Play

Универсальная технология Universal Plug-and-Play (UPnP) представляет собой развитие технологии Plug-and-Play. Она позволяет быстро и просто добавлять и контролировать самые различные устройства. Учитывая низкую в настоящее время распространенность устройств UPnP и факт снижения уровня безопасности при использовании службы поддержки таких устройств, ее лучше отключить. Для этого нужно поступить так же, как и при отключении службы сообщений, но в перечне служб выбрать «Узел универсальных РпР-устройств» (рис. 7). Далее в раскрывающемся списке «Тип запуска» выбрать пункт «Отключено» и щелкнуть по кнопке «ОК» для сохранения изменений.

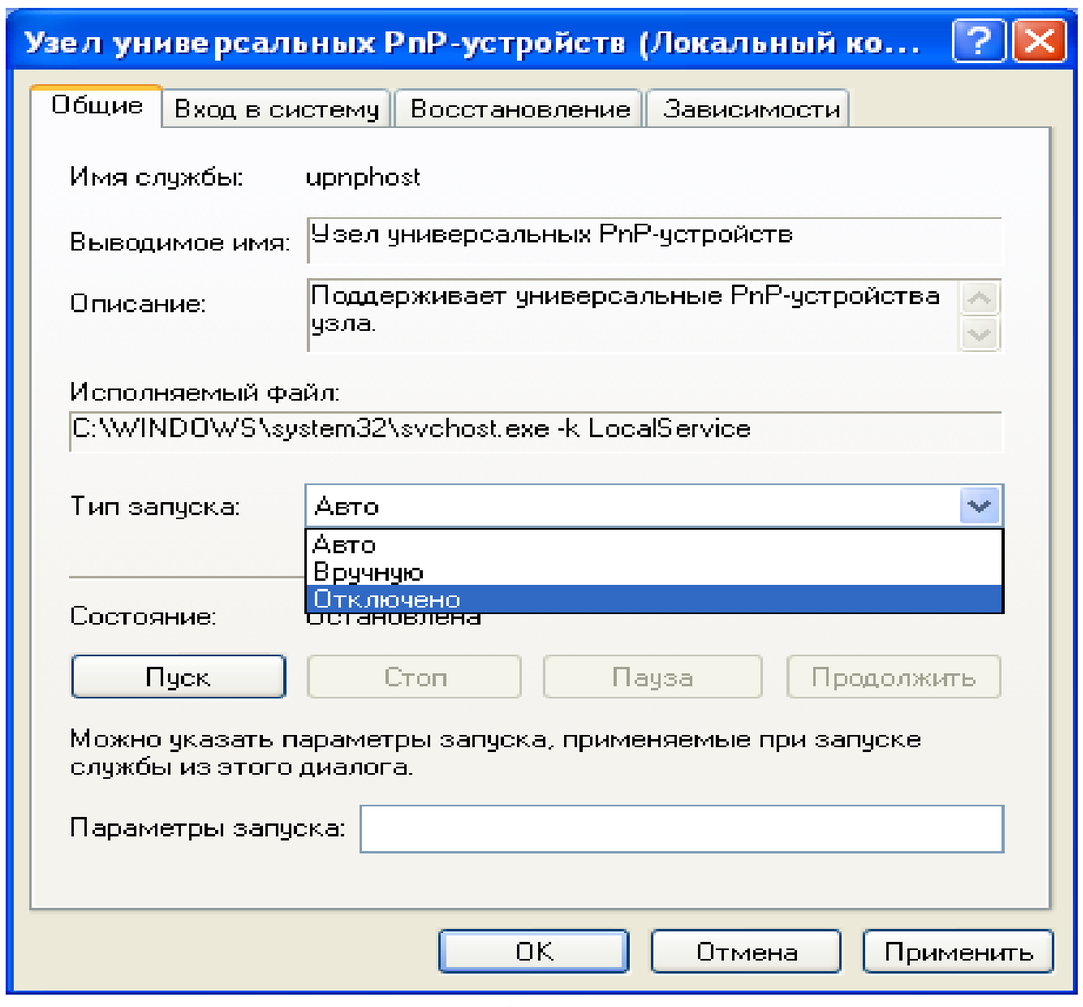

Рис. 7

Отключение удаленного доступа к реестру

В состав Windows XP Professional входит служба «Удаленный реестр», позволяющая пользователям с правами администратора подключаться к реестру компьютера и редактировать его. Чтобы не дать кому-либо дополнительный шанс проникнуть в один из наиболее важных компонентов ОС, лучше отключить эту службу (рис. 8).

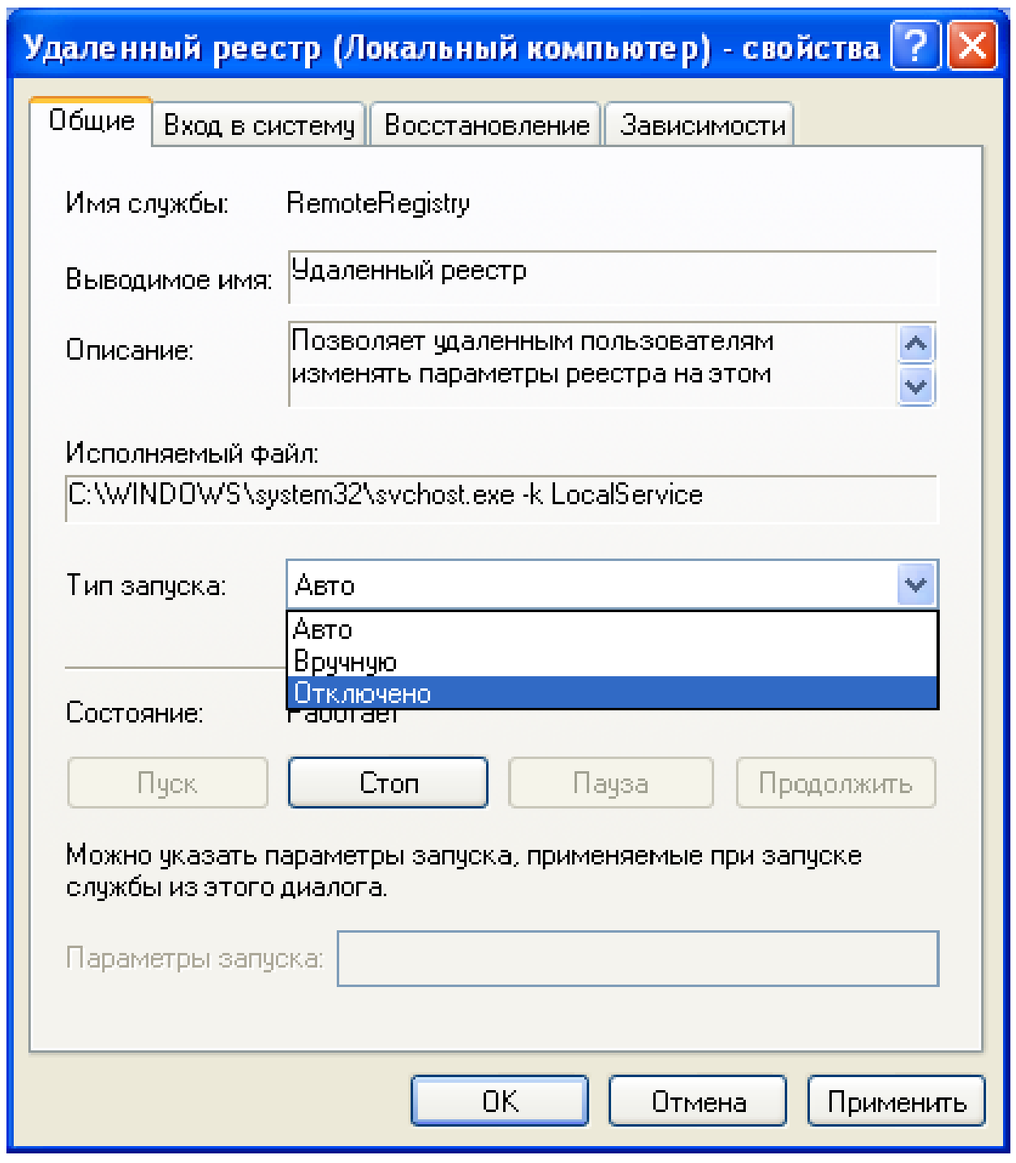

Рис. 8

Отключение поддержки DCOM

Поддерживаемая Windows технология DCOM (Distributed Component Object Model — распределенная объектная модель программных компонентов) предоставляет удобный интерфейс программирования для разработчиков сетевых приложений. Большинство пользователей отключает эту службу (исключение составляют лишь те пользователи, которые пользуются приложениями, реально требующими поддержки DCOM). Однако обычными методами DCOM не отключить.

Компания «Gibson Research» разработала утилиту DCOMbobulator (рис. 9), которая поможет отключить DCOM на компьютере. После ее запуска открывается окно, в котором нужно перейти на вкладку «DCOMbobulator Me!», и щелкнуть по кнопке «Disable DCOM» (рис. 10), а затем по кнопке «Exit» (необходимо перезагрузить компьютер).

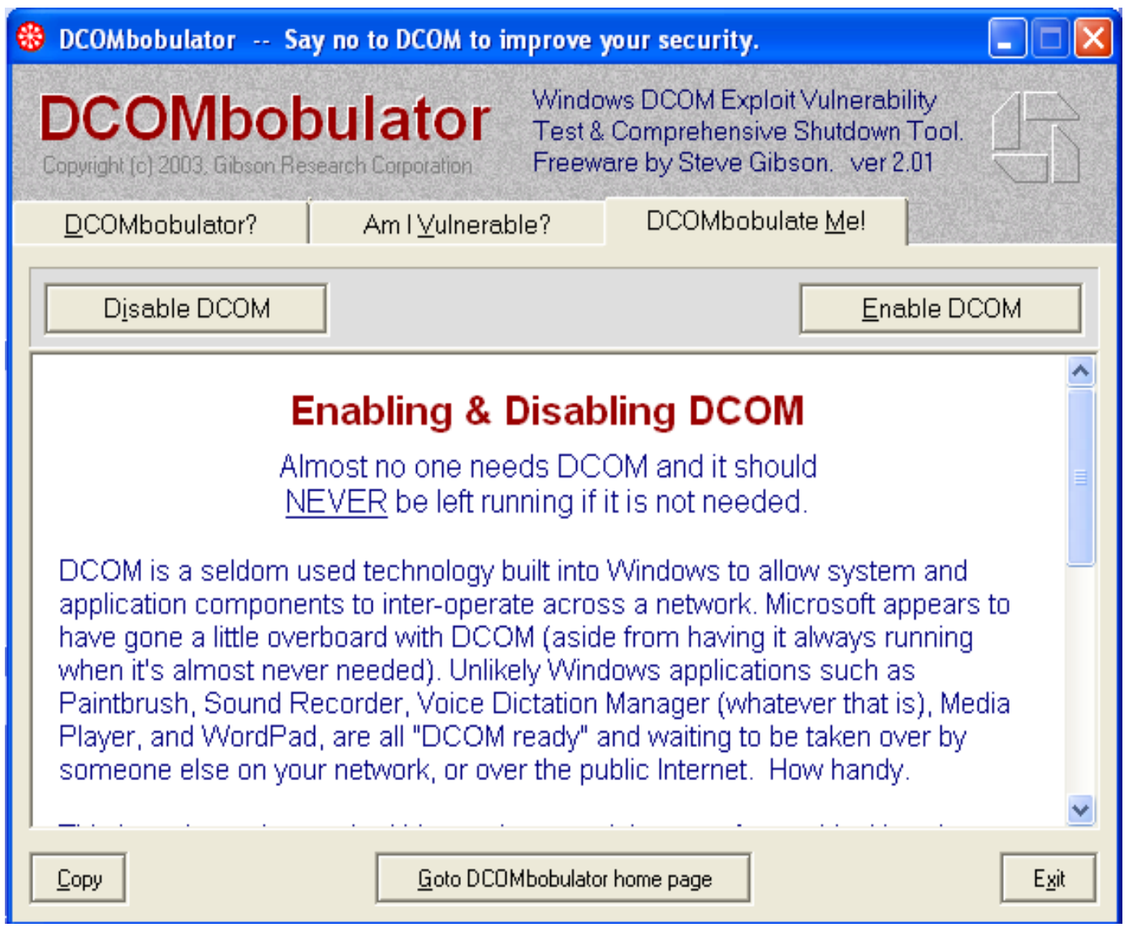

Рис. 9

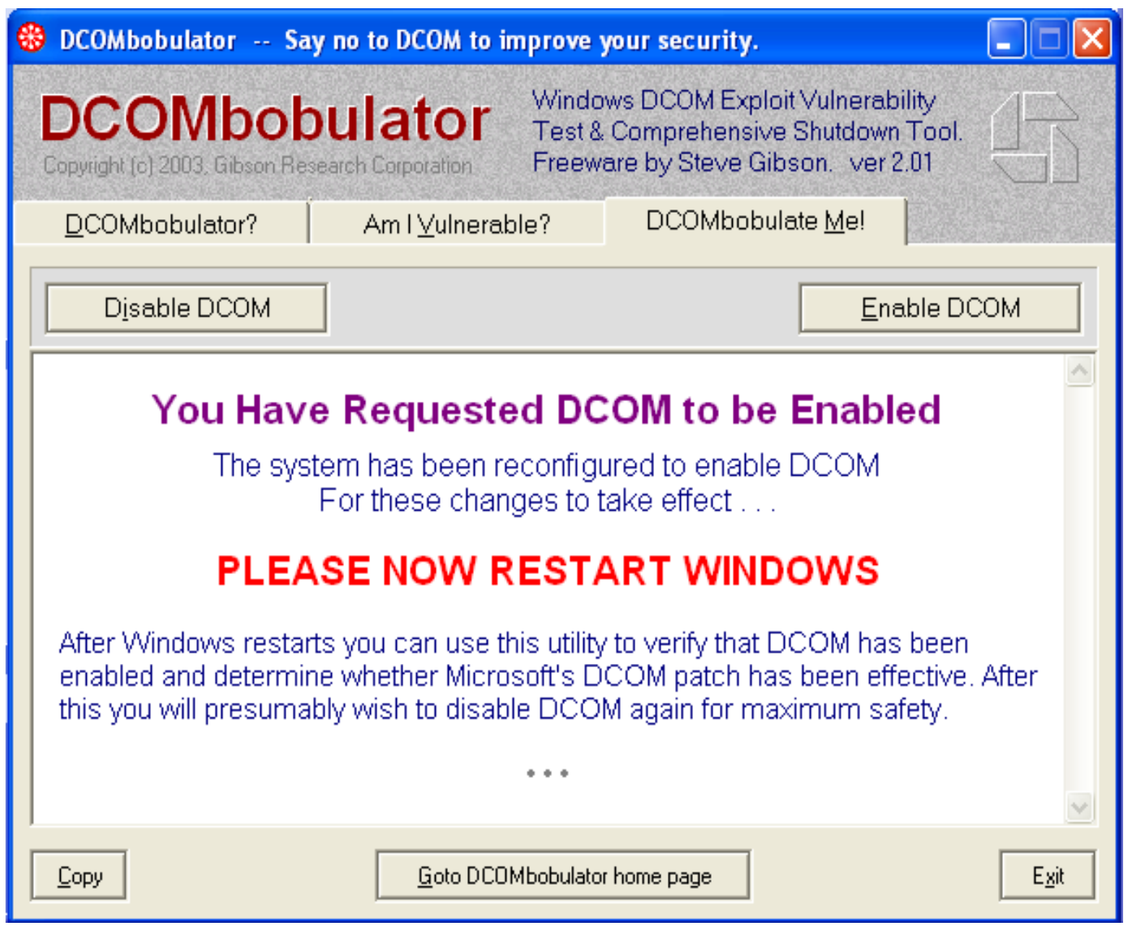

Рис. 10

Контрольные вопросы

1. Что такое брандмауэр? Для чего он используется? Что значит «односторонние» и «двусторонние» брандмауэры? Чем они отличаются?
2. Что такое DCOM?
3. Какой командой через командную строку можно вызвать «настройщик» брандмауэра Windows?
4. Чем отличается брандмауэр от антивирусной программы?
5. Если компьютер является автономным и «изолированным» от сети Интернет, нужен ли ему брандмауэр?

Содержание отчета

В отчет о выполненной работе включить следующие материалы:

1. Тему и цель работы.
2. Результаты выполнения заданий: исследуемые схемы, полученные таблицы переходов.
3. Анализ полученных результатов.
4. Ответы на контрольные вопросы.
5. Выводы по работе.