МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение
высшего профессионального образования
«Оренбургский государственный университет»

А. И. СЕРДЮК, Р. Р. РАХМАТУЛЛИН,
А. И. СЕРГЕЕВ, А. С. РУСЯЕВ

ОСНОВЫ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Рекомендовано Ученым советом государственного образовательного учреждения высшего профессионального образования «Оренбургский государственный университет» в качестве учебного пособия для студентов, обучающихся по программам высшего профессионального образования по специальности 230104 – Системы автоматизированного проектирования

Оренбург 2009

ББК 32.965-5-05я7
УДК 65.011.56(075.8)
С 38

Рецензенты
доктор технических наук, старший научный сотрудник Т. З. Аралбаев, заведующий кафедрой вычислительной техники ГОУ ОГУ,
кандидат технических наук, доцент А. М. Черноусова, заместитель директора АКИ ГОУ ОГУ

С 38 **Основы защиты компьютерной информации: учебное пособие / А. И. Сердюк, А. И. Сергеев, Р. Р. Рахматуллин, А. С. Русяев. – Оренбург: ГОУ ОГУ, 2009. - 200 с.**
ISBN

Пособие предназначено для практического изучения и систематизации начальных знаний студентов по методам защиты компьютерной информации. Рассматриваются средства для проведения атаки на компьютеры пользователей и для их защиты.

Представлен практический материал к циклу из 9 тем, включая способы защиты и восстановления операционных систем, работу с системным реестром, противодействие компьютерным вирусам и сетевым атакам.

За основу для разработки пособия взята книга под редакцией С. В. Глушакова «Секреты хакера. Защита и атака», адаптированная под использование в учебном процессе.

Пособие рассчитано на студентов, обучающихся по техническим специальностям высшего профессионального образования, связанным с разработкой и использованием компьютерных средств автоматизации производства.

Пособие может быть полезно инженерно-техническим работникам, связанным с сопровождением компьютерных приложений для автоматизации решения производственных задач.

Для самоконтроля теоретических знаний и практических навыков представлено около 250 контрольных вопросов и заданий.

С $\frac{0605010201}{6Л9\text{-}08}$ ББК 32.965-5-05я7

ISBN

Содержание

Введение

Первые электронные вычислительные машины возникли в 40-х годах прошлого века. Это были электрические схемы, занимающие огромные помещения и используемые для решения ограниченного круга задач, главным образом математических вычислений. За прошедшее время, ситуация коренным образом изменилась. Компьютер стал общедоступен, вошел в жизнь людей дома и на работе, стал задействован практически во всех областях производства и научной деятельности. А, следовательно, возникла необходимость в умении грамотного обращения с ним и полного использования его возможностей. К сожалению, иногда глобальное внедрение компьютеров приводит к возникновению новых видов преступлений связанных с использованием людьми своих знаний и умений работы на компьютере в противозаконных целях. А подчас незнание пользователями элементарных правил безопасности и способов настройки операционной системы ведет к упрощению задачи злоумышленника.

В данном пособии раскрываются основные способы тонкой настройки ОС семейства Windows и восстановления её после сбоев. Рассматриваются прикладные программы повышения безопасности компьютера и защиты данных. Проводится классификация видов вирусов, их поведения в системе, а так же рекомендуются способы борьбы с ними. Дается представление о модели передачи данных и сетевых технологиях. Описываются простейшие способы "обхода" защиты программ, что позволяет, при написании своих программ, повысить их защищенность от нелицензионного использования.

1 Блокировка доступа к локальному компьютеру

1.1 Экранная заставка Windows

Итак, основной функцией программы-заставки является так называемое «запирание» монитора, т.е. блокировка доступа к компьютеру.

В операционной системе (ОС) **Linux** опция «запирания» экрана предусмотрена по умолчанию. То есть перед тем как пользователь отойдет от компьютера, он может активировать заставку, предполагающую отображение диалогового окна с просьбой ввести пароль пользователя для продолжения работы (если посторонний попытается убрать заставку движением мыши или нажатием любой клавиши).

В **Windows** эта функция активируется установкой определенной опции. Для активизации заставки с паролем необходимо открыть «Панель управления» (с помощью команды «Пуск \ Настройка \ Панель управления»), в которой двойным щелчком выбрать пункт «Экран». В результате отобразится диалоговое окно свойств экрана (рисунок 1.1).

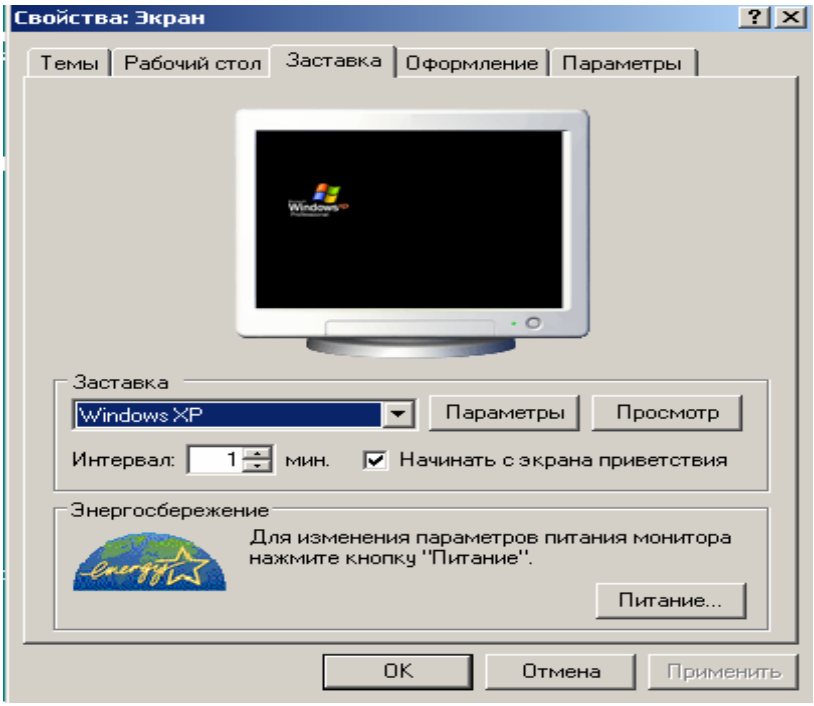


Рисунок 1.1 - Диалоговое окно свойств экрана

Другой способ активизации этого окна - щелчком правой кнопки мыши

по свободной поверхности «Рабочего стола» вызвать контекстное меню и выбрать пункт «Свойства».

На закладке «Заставка» следует (для **Windows XP**):

1) выбрать желаемую заставку;

2) установить интервал простоя компьютера, по истечении которого запускается заставка;

3) установить флажок «Начинать с экрана приветствия».

В системах **Windows NT/2000/XP** вместе с программой-заставкой следует использовать входной пароль, который запрашивается при входе в систему.

Защита с помощью программы-заставки имеет недостатки.

Программа запускается только через определенный интервал времени, когда с компьютером не совершают никаких действий. Этого интервала вполне может хватить взломщику, чтобы получить доступ к компьютеру, пока заставка не сработала.

Решается эта проблема достаточно просто. В уже знакомой закладке «Заставка» нажимаем кнопку «Просмотр», после чего заставка функционирует в нормальном режиме.

Программа-заставка не отключает функцию «Автозапуск». То есть недоброжелатель может вставить в **CD-ROM** диск с вредоносной программой, которая запустится посредством функции «Автозапуск».

Для решения данной проблемы необходимо отключить функцию «Автозапуск» (рисунок 1.2).

1.2 Программы для блокировки доступа к компьютеру

Существуют специально разрабатываемые программы, позволяющие блокировать доступ к компьютеру в отсутствие пользователя. Две из таких программ рассмотрим в данном разделе.

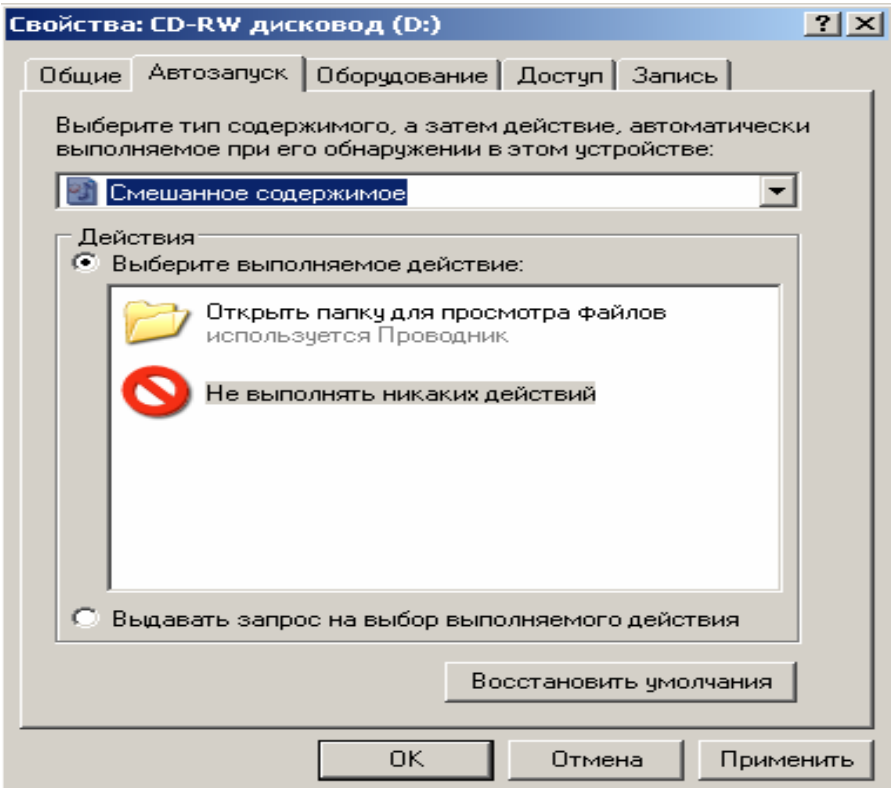


Рисунок 1.2 – Диалоговое окно отключения режима автозапуска **CD-ROM**

1.2.1 ScreenLock Pro

Хорошо зарекомендовала себя программа от компании **iJEN Software ScreenLock Pro**. Загрузить семидневную испытательную версию программы можно по адресу: **http://www.screenlock.com**. Программа поддерживает возможность запирания экрана при кратковременном отсутствии пользователя, а также может выступать в качестве «входного контроля» в ОС. При установке **ScreenLock Pro** требует, чтобы пользователь ввел вопрос, который будет задаваться при попытке входа в систему, и пароль для снятия защиты. После установки программа записывает себя в раздел реестра «Автозапуск», вследствие чего для мгновенного запирания экрана достаточно дважды щелкнуть левой кнопкой мыши по ярлыку программы, расположенному на «Рабочем столе» (или один щелчок по значку программы в системном лотке). При этом как вопрос, так и ответ (т.е. пароль) можно менять в любой момент - нужно активизировать программу, затем раскрыть подменю **Setting/Primary Account**. Здесь для изменения вопроса следует выбрать пункт **Change the PRIMARY**

account's Question, а для изменения ответа - пункт **Change PRIMARY account's Answer**. После разблокирования, если была неудачная попытка ввести пароль, программа выдает соответствующее сообщение, указывая, в котором часу это произошло, а также отображая пароль, введенный злоумышленником (рисунок 1.3).

Рисунок 1.3 - Сообщение о попытках входа в систему

Также программа представляет возможность организовать «входной контроль», т.е. запрашивает пароль при попытке войти в **Windows**. Бесспорно, она эффективнее, чем ее аналог в **Windows 95/98**. Для того чтобы программа проводила входную регистрацию, необходимо раскрыть подменю **Setting/Preferencer/ Windows Startup Protection** и выбрать пункт **YES: Use ScreenLock Protection on Computer Startup**.

1.2.2 Black Magic

Отличительной особенностью этой программы является то, что ее нельзя назвать программой-заставкой в чистом виде, так как во время блокировки экрана заставку она не использует.

Остановимся на способах задания пароля. В **Black Magic** значительно проще варьировать пароль. Программа требует ввести пароль и подтвердить его в соответствующих полях. Можно при каждом включении вводить новый пароль или же, активировав соответствующую опцию, запомнить его. Для того чтобы запомнить пароль, необходимо нажатием кнопки **Options** вызвать диалоговое окно свойств программы и установить флажок **Remember Password**. Программа поддерживает возможность блокировки доступа при загрузке **Windows**. Для этого в диалоговом окне **Black Magic Options** нужно установить флажок **Auto Lock on Startup**.

Недостаток тот же, что и у предыдущей программы - она не блокирует функцию «Автозапуск» со всеми вытекающими последствиями.

Общим недостатком обеих программ-заставок также является то, что их пароли шифруются не лучшим образом. Существует множество программ, позволяющих использовать эту уязвимость.

Следует отметить, что **LOG-файл** (т.е. файл, куда записывается вся информация о работе программы) представляет собой не что иное, как обычный текстовый файл (рисунок 1.4). Это дает возможность злоумышленнику уничтожить следы своего пребывания. Ведь если нажать **Delete Log** в окне **Black Magic Options**, то удаление всей информации сразу бросится в глаза; из **LOG-файла** же возможно удаление отдельных строк. У программы **ScreenLock Pro** такой недостаток отсутствует. Наверное, единственным преимуществом программы **Black Magic** по сравнению со **ScreenLock Pro** является ее бесплатное распространение. Из всего вышесказанного следует, что подобные программы способны обеспечивать безопасность только при кратковременном отсутствии пользователя, и возлагать на них большие надежды все же не стоит.

1.3 Пароль BIOS

Если защита с помощью программы-заставки кажется малоэффективной ввиду условий, в которых приходится работать, имеет смысл использовать более серьезные средства безопасности. Рассмотрим защиту компьютера с помощью **BIOS** и методы физической блокировки доступа.

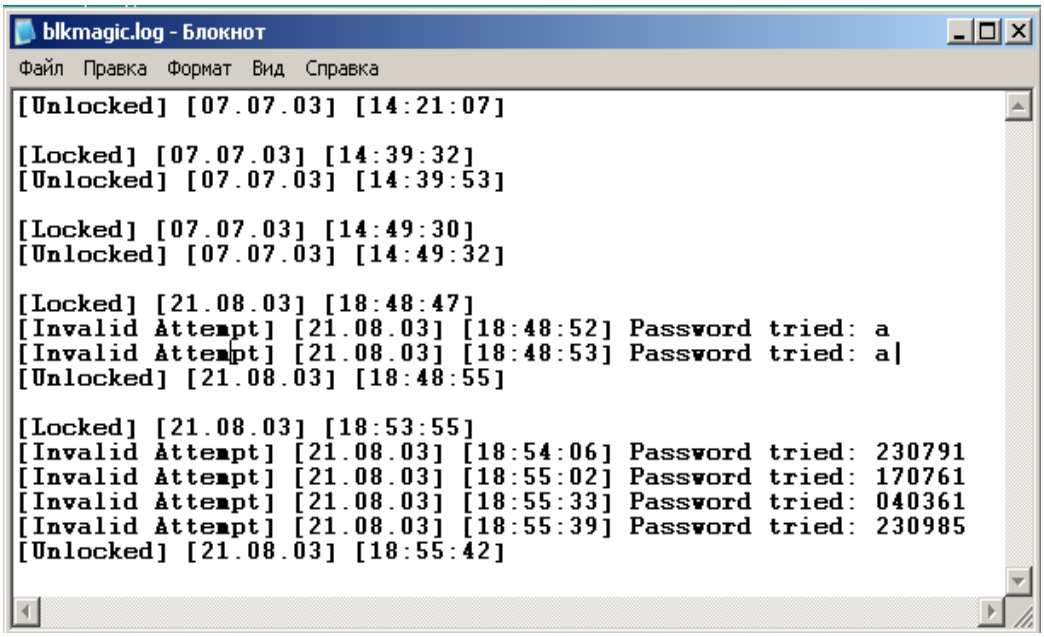


Рисунок 1.4 – **Log-файл** программы **Black Magic**

1.3.1 Защита с помощью BIOS

На каждом персональном компьютере (ПК) имеется встроенная в него система **BIOS** (**Basic Input Output System** - базовая система ввода-вывода), представляющая собой несколько низкоуровневых процедур, тестирующих компьютер после включения его питания и запускающих операционную систему. Большинство **BIOS** поддерживают возможность задания так называемого пароля включения. Если пароль задан, то компьютер выполнит любую операцию только после правильного указания пароля.

Для того чтобы задать пароль **BIOS**, необходимо при загрузке компьютера, когда в правом нижнем углу появится надпись **Press DEL to enter Setup**, нажать клавишу **Delete** (или другую указанную), после чего следовать подсказкам, появляющимся при выделении какого-либо пункта меню. Здесь не будут даваться рекомендации по настройкам **BIOS**, т.к. их выпуском занимаются много производителей: **IBM, AWARD, AMI** и т.д.

Рассмотрим механизм задания пароля **BIOS** для **AWARD BIOS** и **AMI BIOS**. При этом необходимо иметь в виду, что при работе с **BIOS** необходимо соблюдать предельную осторожность, так как неправильная настройка может негативно сказаться на функционировании компьютера или даже привести к

выходу из строя некоторых его узлов.

Существует два типа паролей, которые можно задавать в **BIOS**:

- пароль на загрузку компьютера;

- на загрузку меню **Setup BIOS**.

1.3.2 Задание пароля AWARD BIOS

Для начала рассмотрим, как задается пароль в **BIOS** производства **Award**. При загрузке компьютера необходимо нажать клавишу **Delete**, после чего можно выбрать один из двух вариантов задания пароля:

– **Set User Password** (Установить пароль пользователя) – он может задаваться либо на вход в меню **Setup BIOS**, либо на вход в **Setup** и загрузку компьютера, для того чтобы выбрать любой из вышеперечисленных методов блокировки, необходимо в меню **Advanced BIOS Features** выбрать строку **Password Check,** затем, после нажатия клавиши **Enter** в появившемся окне следует выделить либо **Setup** (пароль только на **Setup BIOS**), либо **System** (пароль на загрузку системы и **Setup BIOS**);

– **Set Supervisor Password** (Установить пароль супервизора) – имеет приоритет перед паролем пользователя, все остальные функции и настройки такие же, как у **User Password**.

1.3.3 Задание пароля AMI BIOS

Вызов окна настроек **AMI BIOS** осуществляется нажатием клавиши <**F2**> в процессе тестирования оборудования после включения компьютера. Здесь для задания пароля необходимо выбрать вкладку **Security**, в которой доступны **Set Supervisor Password** и **Set User Password**. Характерной особенностью **AMI BIOS** является то, что пользователь, знающий **Supervisor Password**, может ограничивать возможности пользователя, знающего только **User Password**. Для того чтобы задать пароль, необходимо подсветить желаемый тип пароля. После нажатия клавиши **Enter** отобразится окно с двумя полями: в первом поле необходимо ввести пароль, а во втором - продублировать его.

1.3.4 Способы обхода пароля BIOS

Невзирая на то, что **BIOS** является мощным средством защиты, существуют различные способы обхода установленного пароля.

Пользователь может попасть в весьма затруднительную ситуацию, если забудет установленный пароль на загрузку системы. Это может принести к необходимости покупки новой системной платы.

В подобных случаях можно воспользоваться «черным ходом» **BIOS**, который также применяется хакерами. Принцип его действия построен на следующем. Установленный пароль хранится в памяти **CMOS** (**Complimentary Metal-Oxide-Semiconductor** - комплиментарный металло-оксидный полупроводник), которая, в свою очередь, должна постоянно поддерживаться батарейкой, установленной на материнской плате. Место расположения батарейки на различных системных платах отмечено стрелками на рисунке 1.5.

Отсюда следует, что если батарейку извлечь на некоторое время, можно добиться очистки **BIOS**, т.е. потери установленных параметров и паролей.

Но дело в том, что извлечь батарейку не всегда возможно без использования вспомогательного инструмента, поэтому имеет смысл прибегнуть к способу, описанному в некоторых инструкциях к системной плате.

На большинстве системных плат установлены выводы для очистки памяти **CMOS**. Как правило, эти выводы находятся рядом с батарейкой. Если пользователь в силу различных причин не может их найти, следует обратиться к инструкции на системную плату, которая должна входить в комплект документов, получаемых пользователем при покупке компьютера. Инструкцию к материнской плате также можно скачать из **Internet**, с сайта фирмы-производителя.

Перед началом манипуляций по очистке памяти CMOS следует отключить питание компьютера, т.е. все действия при очистке памяти CMOS нужно производить, только когда компьютер выключен! В противном случае это повлечет выход системной платы из строя.

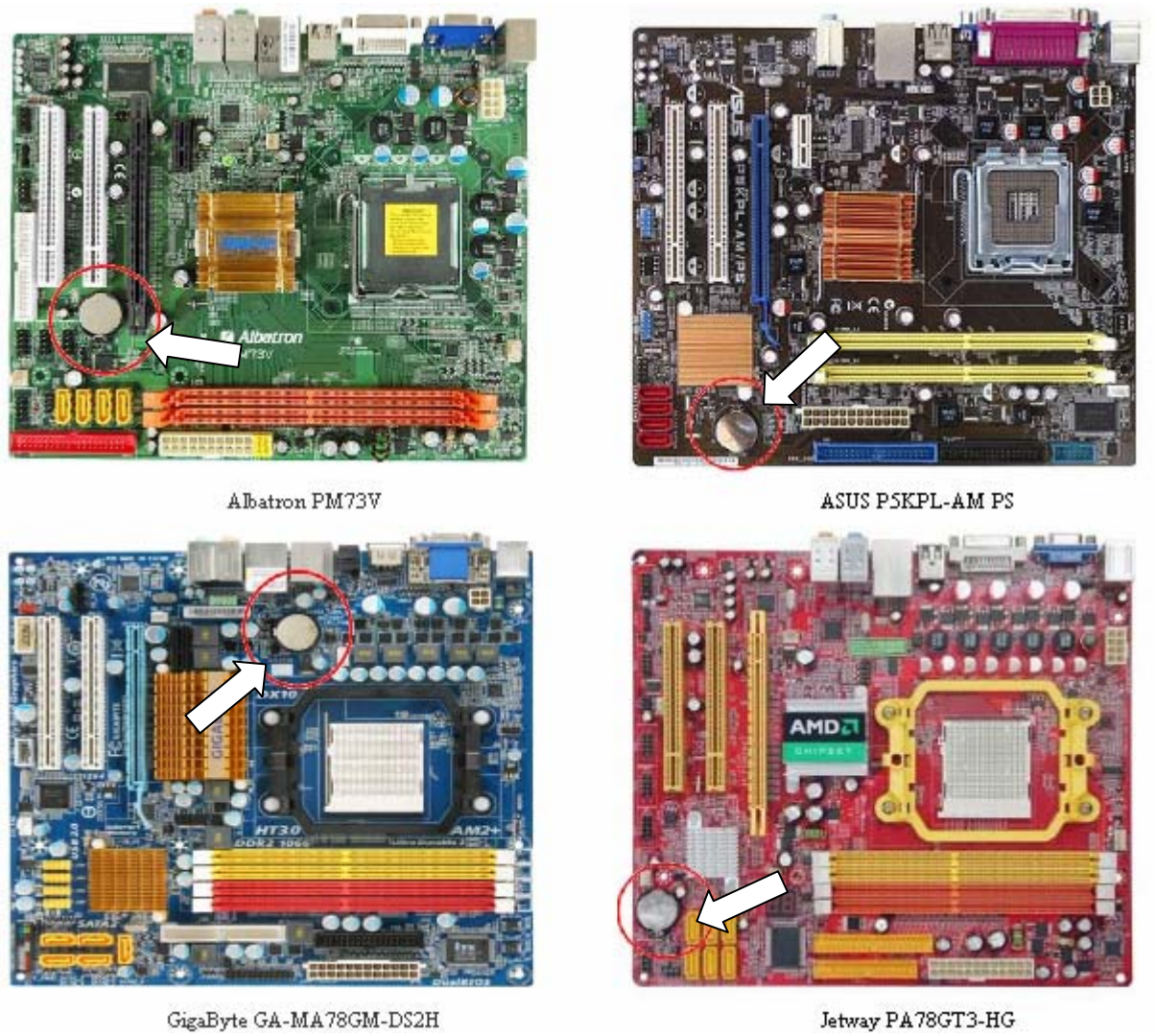


Рисунок 1.5 - Расположение батарейки на различных системных платах

После того как питание отключено, с помощью документации на системную плату нужно найти выводы для очистки памяти **CMOS** и замкнуть их. Далее включить компьютер, заново выставить настройки **BIOS**, запоминить их и осуществить перезагрузку.

В случае, когда документация отсутствует, на выключенном компьютере следует попробовать поочередно замкнуть все выводы на плате, проверив затем, был ли снят пароль.

Если все вышеперечисленные манипуляции не привели к нужному результату, следует попытаться применить так называемый инженерный пароль. Но при этом необходимо помнить о том, что он работает только на достаточно старых версиях **BIOS**, а также о том, что он может варьироваться от версии к версии. В таблице 1.1 приведены пароли для **BIOS** производства фирм

AWARD и **AMI**.

Таблиц 1.1 – Инженерные пароли для **BIOS** фирм **AWARD** и **AMI**

Производитель	Возможные пароли	
AWARD	award	Condo
	01322222	d8on
	589589	HLT
	589721	J262
	595595	J332
	ALPAROMB	J64
	Ally	Lkwpeter
	ALLY	LKWPETER
	aLLy	Pint
	aPAf	PINT
	AWARD PW	SER
	AWARD SW	SKY_FOX
	AWARD SW	SYXZ
	Awkward BIOSTAR	TTPTHA
	CONCAT	ZJAAADC
AMI	A.M.I.	CONDO
	AAAMMMIII	HEWITT RAND
	AMI	LKWPETER
	AMI7SW	PASSWORD
	AMI SW	SER
	BIOS	

1.3.5 Утилита debug

На практике часто бывает, что пользователь, устанавливая пароль на **BIOS**, делает его слишком сложным и впоследствии забывает. При этом вытащить батарейку он по какой-то причине не может, например, ввиду высокой вероятности повредить гарантийные пломбы. В этом случае можно воспользоваться стандартной утилитой **Windows debug.exe**, которую необходимо запускать из консольного режима.

Для запуска программы **debug.exe** необходимо в меню «Пуск» выбрать пункт «Выполнить», после чего в появившемся окне ввести имя программы **debug.exe** (рисунок 1.6).

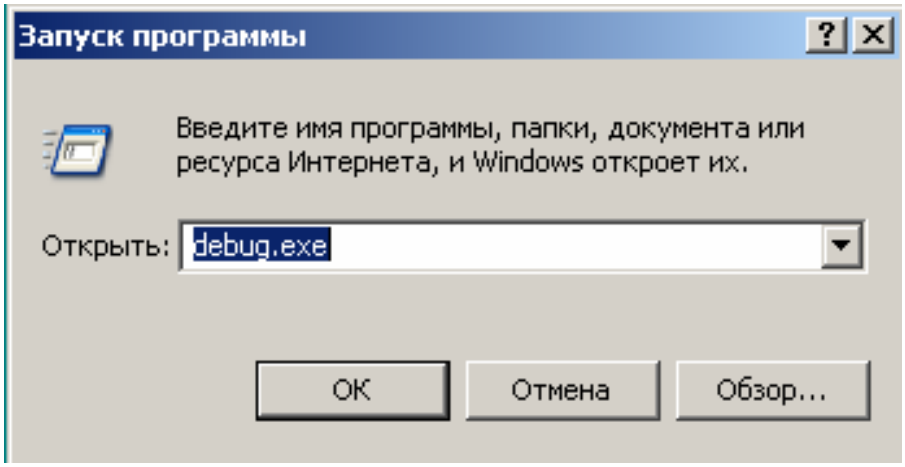


Рисунок 1.6 - Запуск программы **debug.exe**

Затем в появившемся консольном окне необходимо ввести следующую последовательность команд, выполняя перевод строки клавишей **Enter**:

-o 70 33

-o 71 33

-q.

В результате пароль на **BIOS** будет снят. Необходимо отметить, что с выполнением этой команды снимаются некоторые настройки **Windows**, поэтому после перезагрузки для дальнейшей корректной работы системы может потребоваться инсталляционный диск **Windows**.

1.4 Контрольные вопросы

1.4.1 Какие способы блокировки доступа к локальному компьютеру Вы знаете?

1.4.2 Для чего служит входной пароль в **Windows**?

1.4.3 В чем отличие использования входного пароля и экранной заставки **Windows**?

1.4.4 Как разблокировать компьютер, защищенный экранной заставкой и входным паролем: а) в **Windows 95/98**; б) в **Windows NT/2000/XP**?

1.4.5 Чему равен минимальный период включения заставки в **Windows,** как уменьшить этот период?

1.4.6 Как можно использовать **CD-ROM** для обхода заставки с паролем?

Как устранить этот недостаток?

1.4.7 Какие программы для блокировки доступа к ПК Вы знаете?

1.4.8 Укажите фирму - разработчик программы **ScreenLock Pro**?

1.4.9 В чем общие недостатки программ **ScreenLock Pro** и **Black Magic**?

1.4.10 Что Вы можете сказать о **Log-файле** программы **Black Magic**?

1.4.11 Для каких операционных систем целесообразно применять **ScreenLock Pro и Black Magic**, почему?

1.4.12 Что такое **BIOS**?

1.4.13 В чем особенности защиты с помощью пароля **BIOS**?

1.4.14 Какие типы паролей можно задавать в **BIOS**?

1.4.15 Какие способы обхода паролей **BIOS** Вы знаете?

1.4.16 Где хранится пароль **BIOS**?

1.4.17 Каково обязательное требование при манипуляциях по очистке памяти **CMOS**?

1.4.18 Что такое инженерный пароль и в чем недостатки его использования?

1.4.19 В каких случаях рекомендуется использование утилиты **debug.exe**?

2 «Взлом» архивов и программ

2.1 Архивация данных и «взлом» архивов

При эксплуатации компьютера по самым разным причинам возможны порча или потеря информации на магнитных дисках. Для того чтобы уменьшить потери, следует иметь архивные копии используемых файлов и систематически обновлять копии изменяемых файлов.

Различными разработчиками были созданы специальные программы для упаковки файлов. Как правило, эти программы позволяют помещать копии файлов на диске в сжатом виде в архивный файл, извлекать файлы из архива, просматривать оглавление архива и т.д.

Архивный файл представляет собой набор из одного или нескольких файлов, помещенных в сжатом виде в единый файл, из которого их можно при необходимости извлечь в первоначальном виде. Архивный файл содержит оглавление, позволяющее узнать, какие файлы содержатся в архиве. В оглавлении архива для каждого содержащегося в нем файла хранится следующая информация:

– имя файла;

– сведения о каталоге, в котором содержится файл;

– дата и время последней модификации файла;

– размер файла на диске и в архиве;

– код циклического контроля для каждого файла, используемый для проверки целостности архива.

Наиболее популярные архиваторы - **WinZip** и **WinRAR** - позволяют задавать пароль на открытие архива. Однако существуют программы, с помощью которых можно «взламывать» архивные файлы.

Программы для «взлома» архива можно условно разбить на две группы:

– специализированные - программы, которые «взламывают» пароли только одного архиватора (например, **Azpr**, специализирующаяся на взломе паролей **WinZip**);

– универсальные - программы, которые могут работать с двумя и более видами архиваторов (например, **Archpr**, работающая со всеми известными ви-

дами архивов под **Windows**).

Очевидно, что универсальные «взломщики» архивов предпочтительнее специализированных, ведь намного проще иметь одну программу для всех видов архивов вместо множества программ, количество которых равно числу архиваторов. Единственным (несущественным) недостатком универсальных «взломщиков» является их несколько больший объем (1 Мб **Archpr** против 991 Кб **Azpr**). Рассмотрим **Archpr** подробнее.

2.1.1 «Взломщик» архивов Archpr

Программа **Archpr** (**Advanced Archive Password Recovery**) относится к группе универсальных «взломщиков» паролей. Приятный интерфейс, интуитивно понятное меню со всплывающими подсказками (рисунок 2.1), простота в использовании делают **Archpr** одной из лучших программ в своем классе.

Рисунок 2.1 - Окно **Archpr**

Рассмотрим пример использования этой программы. Допустим, что не-

обходимо «взломать» некий архивный файл **test**, причем не имеет значения, каким архиватором пользовались для создания файла - механизм действия во всех случаях один и тот же. Вначале необходимо нажать кнопку **«Load file into the project»** и выбрать «взламываемый» файл **test** (рисунок 2.1). После этого на закладке **«Length»** можно выбрать предполагаемую длину пароля (от 1 до **S** символов), на закладке **«Range»** - символы, которые будут использоваться при проверке пароля; на этой же закладке в полях **«Start from** и **End at»** задаются символы, с которых будет начинаться или, соответственно, которыми будет заканчиваться перебор.

Для того чтобы облегчить задачу, предположим, что пароль состоит только из цифр - опция **«All digits»**, и нажмем кнопку **«Start!».** При этом начнется процесс подбора паролей, по окончании которого появится окно с отчетом (не показано).

Здесь в поле **«Total passwords»** отображается число перебранных вариантов, в поле **«Total time»** - затраченное время на подбор, в поле **«Average speed»** - средняя скорость подбора (в паролях за секунду), и наконец в поле **«Password for this file»** - пароль к файлу. Можно сохранить полученный результат, нажав кнопку **«Save»**.

Теперь остановимся на том, как можно предотвратить «взлом» архива.

2.1.2 Защита от «взлома» архива

Защититься от «взлома» архива, также как и компьютера полностью невозможно. Но существуют приемы, которые способны затруднить «взлом». Прежде всего отметим, что бесплатные версии «взломщиков» паролей (и **Archpr** в том числе) способны подбирать пароль, состоящий не более чем из пяти символов. То есть если пароль будет состоять хотя бы из шести символов, бесплатный «взломщик» с ним не справится.Существуют и платные версии «взломщиков», которые способны работать практически с любым количеством символов в пароле. В таких случаях остается лишь максимально усложнить ему работу. Для этого следует использовать как можно больше символов, а пароль должен выглядеть приблизительно так:

Ф!G@v&*%235+4456?dfgG!.

Конечно, чем сложнее пароль, тем труднее его «взламывать». Однако подобный пароль с трудом поддается запоминанию, что вызывает дополнительные трудности.

2.2 Методы «взлома» программ

Достаточно часто пользователь сталкивается с тем, что утилиты, входящие в стандартный пакет **Windows**, не удовлетворяют его запросам, а бесплатные программы не всегда оказываются способны справиться с поставленной задачей. В таких случаях пользователь обычно начинает поиск так называемых **share-программ**, для использования которых необходимо перечислить некую сумму разработчикам.

Такие программы имеют определенный срок действия, который ограничивается, как правило, либо количеством запусков, либо количеством дней, по истечении которых программа перестает работать вплоть до ввода регистрационных данных. Обычно небольшие компании или отдельно взятые разработчики не используют каких-либо мощных средств защиты собственных программ по целому ряду причин.

Во-первых, разработка хорошей защиты требует немало времени, потеря которого может привести к тому, что свободную нишу на рынке программного обеспечения займет какой-то другой разработчик со своим продуктом.

Во-вторых, какой бы мощной ни была защита, все равно «взломщики» программного обеспечения найдут способ ее обойти. Поэтому в большинстве случаев защита может остановить только неопытных пользователей.

Ниже приведено описание различных способов обхода защиты программ: поиск «крека» (**crack**), изменение системной даты и редактирование реестра.

2.2.1 Поиск «крека»

Самый простой способ поискать так называемый «крек» (т.е. программу для обхода защиты) в сети **Internet**. Существует множество различных сайтов, посвященных этой тематике. Но, к сожалению, не всегда удается найти тот или

иной «крек» ввиду большого количества программ. Поэтому пользователю необходимо владеть элементарными навыками продления срока службы программы, приведенными ниже.

2.2.2 Изменение системной даты

Один из способов ограничения срока службы программы - это установка разработчиком количества дней, на протяжении которых будет работать программа.

В большинстве случаев перед установкой достаточно перевести системную дату вперед, например на пять лет (с 2007 на 2012). Затем после установки вернуть ее в исходное значение, после чего программа будет работать пять лет и определенное количество дней.

Для изменения системной даты необходимо дважды щелкнуть левой кнопкой мыши на индикаторе времени в системном лотке, в результате чего появится диалоговое окно свойств даты и времени. Все, что требуется, - это изменить счетчик лет в сторону увеличения (рисунок 2.2).

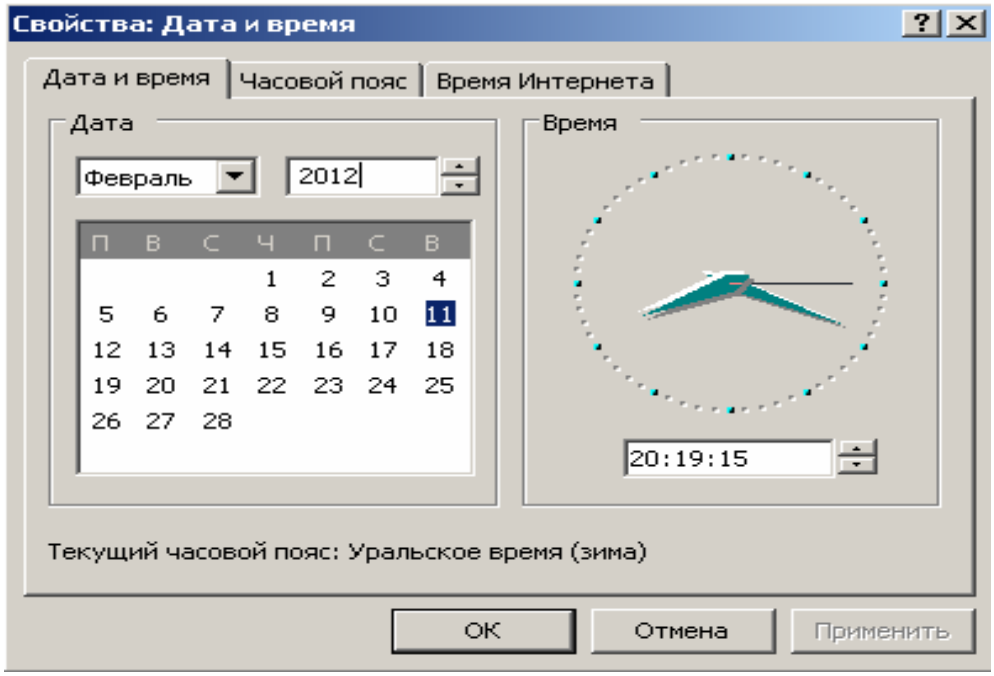


Рисунок 2.2 – Окно изменения системной даты

2.2.3 Изменение параметров реестра в программе Regedit

Ситуация несколько осложняется в том случае, если использование программы ограничивается количеством запусков. В этом случае для того, чтобы продлить срок службы программы, придется провести несколько несложных действий в реестре.

Для начала следует попробовать следующий способ. Вначале необходимо запустить «Редактор реестра» (можно через раздел «Пуск \ Выполнить \ Regedit»). Внешний вид появившегося окна показан на рисунке 2.3.

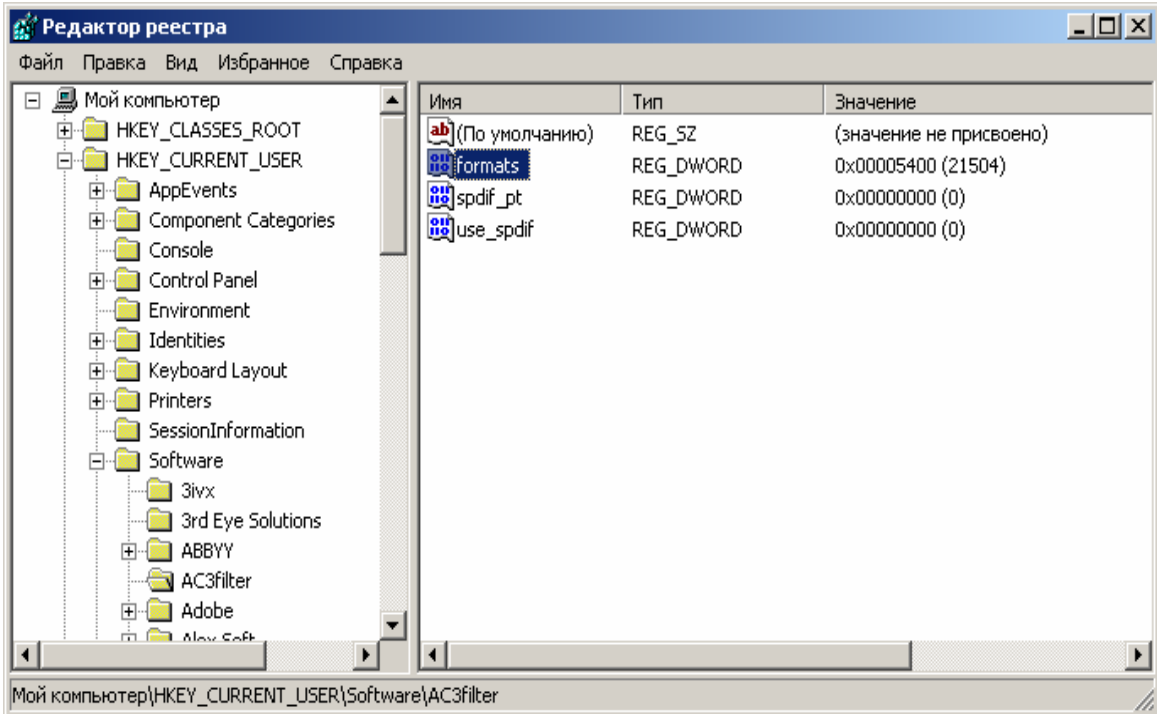


Рисунок 2.3 – Внешний вид окна «Редактора реестра»

Затем в окне «Редактора реестра» выделить щелчком мыши раздел **HKEY_CURRENT_USER/Software/имя_программы** и выполнить команду **File/Export**. Далее в появившемся окне необходимо указать имя **REG-файла**, который будет создан.

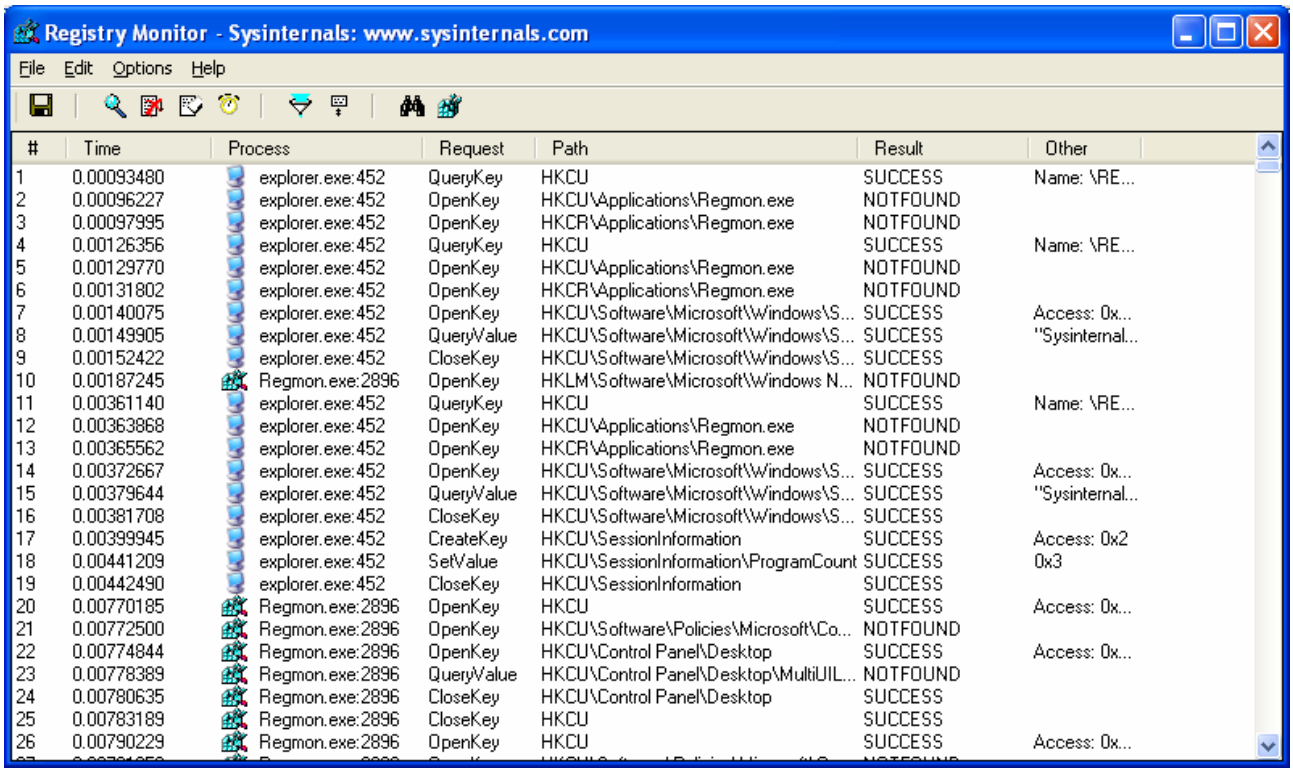
В результате на диск будут скопированы данные о программе, которые записываются в реестр в процессе ее инсталляции. Впоследствии, когда лимит запусков программы будет исчерпан, следует перезаписать сохраненные данные из файла в указанный выше раздел реестра, воспользовавшись командой

File/Import.

Однако описанный способ может по каким-либо причинам не принести к нужному результату. В этом случае следует воспользоваться одной из специальных программ редактирования системного реестра **Windows**. Примерами таких программ могут служить **Regmon** или **Registry Trash Keys Finder (RTKF)**.

2.2.4 Использование программы Regmon

Основное окно приложения **Regmon** приведено на рисунке 2.4. В данном случае отображаются процессы, связанные с обращением к реестру программы электронной почты **OutLock Express**.



#	Time	Process	Request	Path	Result	Other
1	0.00093480	explorer.exe:452	QueryKey	HKCU	SUCCESS	Name: \RE...
2	0.00096227	explorer.exe:452	OpenKey	HKCU\Applications\Regmon.exe	NOTFOUND	
3	0.00097995	explorer.exe:452	OpenKey	HKCR\Applications\Regmon.exe	NOTFOUND	
4	0.00126356	explorer.exe:452	QueryKey	HKCU	SUCCESS	Name: \RE...
5	0.00129770	explorer.exe:452	OpenKey	HKCU\Applications\Regmon.exe	NOTFOUND	
6	0.00131802	explorer.exe:452	OpenKey	HKCR\Applications\Regmon.exe	NOTFOUND	
7	0.00140075	explorer.exe:452	OpenKey	HKCU\Software\Microsoft\Windows\S...	SUCCESS	Access: 0x...
8	0.00149905	explorer.exe:452	QueryValue	HKCU\Software\Microsoft\Windows\S...	SUCCESS	"Sysinternal...
9	0.00152422	explorer.exe:452	CloseKey	HKCU\Software\Microsoft\Windows\S...	SUCCESS	
10	0.00187245	Regmon.exe:2896	OpenKey	HKLM\Software\Microsoft\Windows N...	NOTFOUND	
11	0.00361140	explorer.exe:452	QueryKey	HKCU	SUCCESS	Name: \RE...
12	0.00363868	explorer.exe:452	OpenKey	HKCU\Applications\Regmon.exe	NOTFOUND	
13	0.00365562	explorer.exe:452	OpenKey	HKCR\Applications\Regmon.exe	NOTFOUND	
14	0.00372667	explorer.exe:452	OpenKey	HKCU\Software\Microsoft\Windows\S...	SUCCESS	Access: 0x...
15	0.00379644	explorer.exe:452	QueryValue	HKCU\Software\Microsoft\Windows\S...	SUCCESS	"Sysinternal...
16	0.00381708	explorer.exe:452	CloseKey	HKCU\Software\Microsoft\Windows\S...	SUCCESS	
17	0.00399945	explorer.exe:452	CreateKey	HKCU\SessionInformation	SUCCESS	Access: 0x2
18	0.00441209	explorer.exe:452	SetValue	HKCU\SessionInformation\ProgramCount	SUCCESS	0x3
19	0.00442490	explorer.exe:452	CloseKey	HKCU\SessionInformation	SUCCESS	
20	0.00770185	Regmon.exe:2896	OpenKey	HKCU	SUCCESS	Access: 0x...
21	0.00772500	Regmon.exe:2896	OpenKey	HKCU\Software\Policies\Microsoft\Co...	NOTFOUND	
22	0.00774844	Regmon.exe:2896	OpenKey	HKCU\Control Panel\Desktop	SUCCESS	Access: 0x...
23	0.00778389	Regmon.exe:2896	QueryValue	HKCU\Control Panel\Desktop\MultiUIL...	NOTFOUND	
24	0.00780635	Regmon.exe:2896	CloseKey	HKCU\Control Panel\Desktop	SUCCESS	
25	0.00783189	Regmon.exe:2896	CloseKey	HKCU	SUCCESS	
26	0.00790229	Regmon.exe:2896	OpenKey	HKCU	SUCCESS	Access: 0x...

Рисунок 2.4 - Основное окно программы **Regmon**

Каждое обращение имеет несколько характеристик, описание которых приведено ниже:

– # - порядковый номер обращения;

– **Time** - время обращения;

– **Process** - процесс, обратившийся к реестру;

– **Request** - тип запроса;

– **Path** - путь к программе, обратившейся к реестру;

– **Result** - результат запроса;

– **Other** - другие параметры процесса.

Рассмотрим работу **Regmon** на примере программы **Myro**. Пользователь должен действовать следующим образом. Вначале необходимо найти строку со следующими параметрами:

– **Process** равен **Myrodeskt;**

– **Request** равен **QueryValueEx.**

Дело в том, что **QueryValueEx** отвечает за извлечение текущего значения; где-то рядом с этой строкой должна находиться строка с параметрами:

– **Process** равен **Myrodeskt;**

– **Request** равен **SetValueEx**.

Параметр **SetValueEx** отвечает за присвоение нового значения параметру реестра. Также в обоих случаях необходимо обратить внимание на столбец **Other**, в котором отображается текущее значение процесса. В данном случае для первой строки этот параметр равен 20, а для второй – 19 (рисунок 2.5).

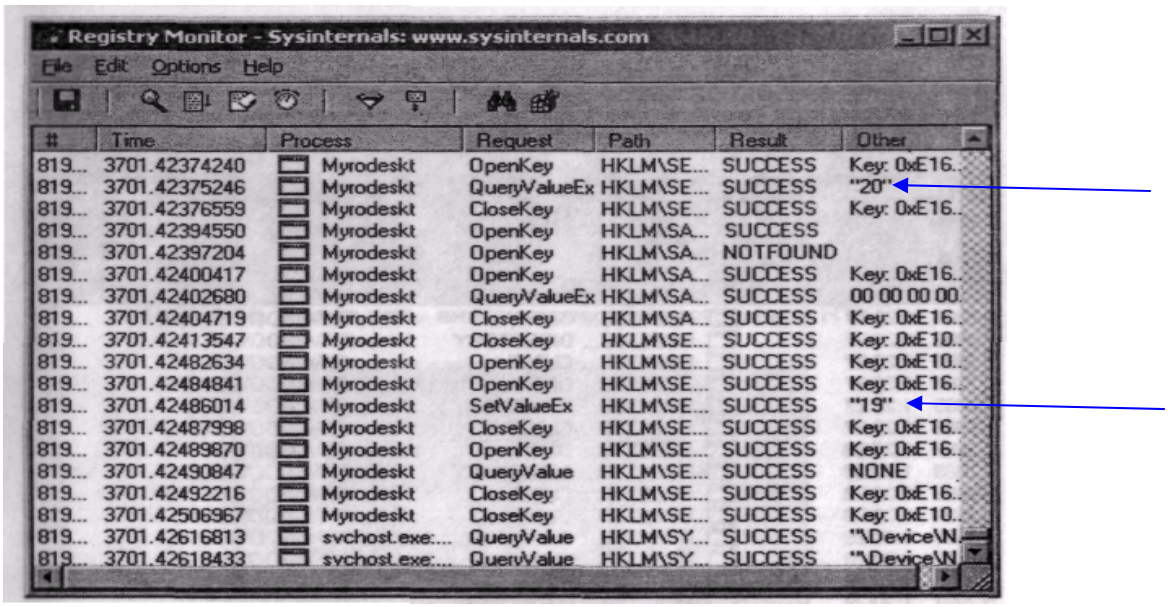


Рисунок 2.5 - Место расположения счетчика запусков программы

Несложно догадаться, что это и есть счетчик, работающий на уменьше-

ние. Причем когда значение параметра достигнет 0, программа перестанет запускаться. Чтобы продлить срок службы, необходимо увеличить для параметра **SetValueEx** значение **Other**, например, до 2000.

Программа **Regmon** не позволяет непосредственно редактировать значения ключей реестра, однако можно активизировать программу **Regedit**, предварительно выбрав ключ, значение которого требуется изменить. Вызов **Regedit** осуществляется в окне **Regmon** двойным щелчком на строке ключа либо (после выбора строки ключа) командой **Edit/Regedit/Jump**. В результате выводится окно программы **Regedit** и автоматически раскрывается ветвь реестра для выбранного ключа. Теперь щелчок правой кнопкой мыши на строке ключа вызывает контекстное меню, в котором имеется пункт «Изменить».

2.2.5 Использование программы Filemon

Хранение данных в реестре является очень удобным, но не единственным способом хранения информации. Также программа может хранить данные в отдельном файле, который она создает после установки. Последнее время этот способ встречается крайне редко, но все же не стоит забывать о нем. Способ обхода подобной защиты отличается от вышеописанного только программой, которую следует использовать. В данном случае это **Filemon** (рисунок 2.6).

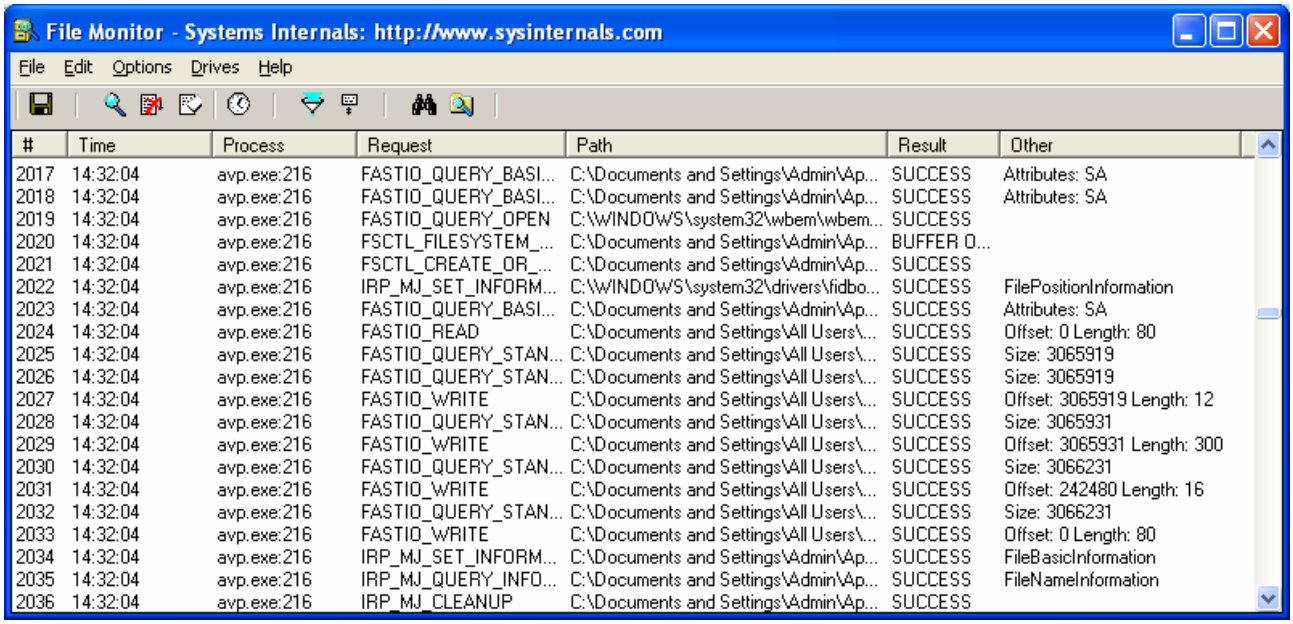


Рисунок 2.6 - Окно программы **Filemon**

2.2.6 Изменение параметров реестра в программе RTKF

Данная программа предназначена для поиска и удаления ключей, которые остаются в реестре после деинсталляции некоторых программ. Например, в случае использования пробных версий программных продуктов в реестре создаются ключи, которые «считают» количество запусков программы или хранят дату инсталляции программы. Если удалить эти ключи, то можно восстановить работоспособность пробных версий программы.

RTKF свободно распространяется через Internet, бесплатна и не требует инсталляции. Для использования программы необходимо загрузить и распаковать файл **trashreg.zip**, в котором находится программа (файл **TrashReg.exe**).

После запуска программа сканирует реестр и отображает все ключи, которые являются ошибочными (рисунок 2.7).

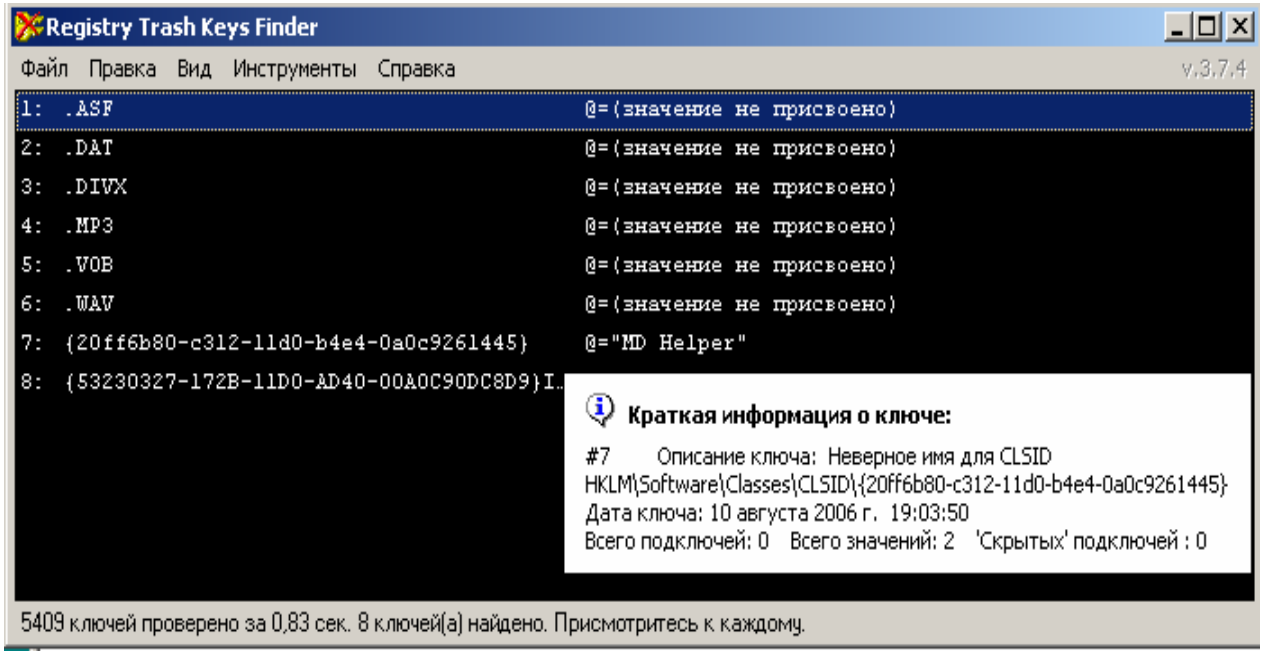


Рисунок 2.7 – Результаты анализа реестра программой **RTKF**

Далее следует выделить ключ и, используя контекстное меню (рисунок 2.8), выполнить одну из ниже перечисленных команд.

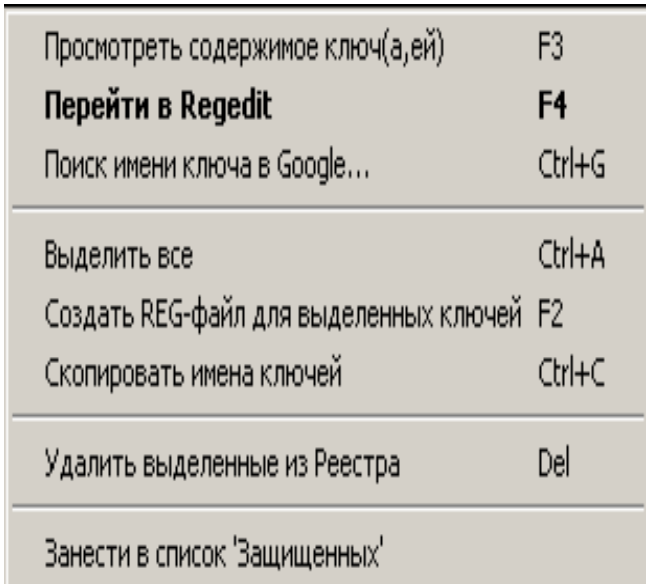


Рисунок 2.8 - Контекстное меню программы **RTKF**

Программой **RTKF** в реестре обнаруживаются ключи, оставленные **trial**-версиями программ. Если такие ключи были найдены, их следует удалить.

Теперь, когда **trial-программа** будет запущена, то она не обнаружит своих записей в реестре. Для нее это будет означать, что на данном компьютере эта программа была запущена первый раз, и в результате пользователь получит возможность работать с данной программой еще несколько дней/месяцев (или несколько запусков).

Хотя программа имеет довольно узкую направленность, она является одной из лучших в своем роде.

2.3 Создание виртуальных дисков

Еще одним способом своеобразного «взлома» программ является создание виртуальных **CD**, которые могут использоваться в том случае, если какая-либо программа не запускается без компакт-диска, а компакт-диск был взят на время.

В этом случае могут помочь специализированные программы для создания виртуальных дисков.

2.3.1 Общие сведения о виртуальных дисках

Достаточно быстрый рост емкости жестких дисков существенно отразился на типах информации, которая хранится и используется пользователями. Огромные архивы музыкальных композиций, десятки видеофильмов и файлы-образы наиболее важных данных и программ заняли почетное место на жестких дисках современных персональных компьютеров.

Понятия виртуального **CD-диска** и виртуального **CD/DVD-привода** часто встречаются в обиходе пользователей ПК, поэтому остановимся на них подробнее и попытаемся дать определение каждому из терминов.

Виртуальный CD/DVD-привод – устройство, созданное программой эмуляции **CD/DVD-приводов** и опознаваемое операционной системой как аппаратное устройство. Отличие от обычного **CD-ROM** заключается в том, что реального **CD/DVD-привода** может и не быть, а его присутствие в системе эмулируется программно (создается «виртуальный» **CD/DVD-привод**). Работа с таким приводом ничем не отличается от работы с реальным **CD/DVD-приводом**, а программу, создающую виртуальный привод, обычно называют **эмулятором CD/DVD-привода**.

Виртуальный CD/DVD-диск – файл-образ, хранящийся на жестком диске пользователя и являющийся точной копией оригинального **CD/DVD-диска**. Обычно создается программой эмуляции **CD/ DVD-привода** и может состоять как из одного, так и из нескольких файлов.

Обычно виртуальный **CD** занимает столько же места, сколько и исходный компакт-диск, однако многие программы предоставляют дополнительные возможности в процессе создания файла-образа: чтение информации из субканала компакт-диска увеличит размер, а использование компрессии данных уменьшит размер созданного файла-образа. Некоторые программы-эмуляторы **CD/DVD-**приводов имеют встроенные редакторы образов. Например, воспользовавшись таким редактором, пользователь сможет самостоятельно добавлять либо удалять информацию, содержащуюся в файле-образе.

Использование сжатия в процессе создания файла-образа может значительно уменьшить размер образа, но потребует больше ресурсов процессора, как и любая процедура архивации/разархивации. Во время использования сжатых файлов-образов нужная информация распаковывается «на лету», а степень

компрессии зависит от типа информации, содержащейся на оригинальном носителе, и алгоритма сжатия, использовавшегося при создании файла-образа.

Существует около десятка наиболее популярных программ эмуляции **CD/DVD**-приводов, каждая из которых обладает своими собственными достоинствами и недостатками, поэтому при выборе пользователь должен руководствоваться следующими критериями:

- функциональность;
- легкость в работе;
- поддержка различных типов файлов-образов.

Как ни странно, но наиболее «узким местом» программ-эмуляторов **CD/DVD-приводов** является именно поддержка различных типов файлов-образов. Большинство программ создают собственные файлы-образы и не предполагают использования внешних. В настоящее время не существует единого стандарта файлов-образов, но в качестве основных можно условно принять типы файлов-образов, созданных программами записи **CD/DVD-дисков**:

- **CloneCD Image file** (CCD);
- **CDRWIN Image file** (CUE+, BIN);
- **DiscJuggler Image file** (CDI);
- **Media Descriptor Image file** (MDS);
- **Nero-Burning Rom Image file** (NRG);
- **Standart Image file** (ISO).

Пишущие **CD/DVD-приводы** стали неотъемлемой частью современного ПК, поэтому работа программы эмуляции привода и программы записи информации на носители данных с единым типом файлов-образов открывают перед пользователями дополнительные возможности работы с информацией. Например, создав файл-образ программой **Alcohol 120 %,** можно поместить его в виртуальный привод и работать с ним как с оригинальным диском. Кроме того, пользователь получает возможность в дальнейшем записать копию оригинального **CD-диска**. В результате такой интеграции файлы-образы будут использоваться не только в качестве виртуальных дисков программами эмуляции, но и как точные копии оригинальных дисков, что позволит в любой момент воссоздать оригинал в программе записи компакт-дисков.

Еще одним важным критерием является возможность эмуляции програм-

мами различных защит от копирования компакт-дисков, так как большинство виртуальных дисков создается с целью резервного копирования данных. Например, приобретя компакт-диск и создав его виртуальный аналог, пользователь сможет работать с виртуальным образом, чем существенно снизит вероятность повреждения оригинального компакт-диска, уменьшит износ привода чтения/записи компакт-дисков и получит существенный прирост скорости при обращении к виртуальному приводу (большинство программ эмуляции виртуальных дисков считывают данные со скоростью 75-300 Mb/s).

Многие известные фирмы-производители программного обеспечения выпускают коммерческие программы эмуляции **CD/DVD-приводов**. В данном разделе будут изучены особенности работы с популярной программой эмуляции **Alcohol 120 %.**

2.3.2 Программа Alcohol 120 %

Программа **Alcohol 120 %** появилась на рынке программного обеспечения достаточно недавно, но за период менее полугода приобрела огромную популярность среди пользователей благодаря высокой функциональности, интуитивно понятному интерфейсу и возможности работы с основными типами файлов-образов внешних программ записи информации.

Основным отличием от аналогичных пакетов является то, что программа сама является и программой эмуляции виртуальных **CD/DVD-приводов**, и программой записи файлов-образов.

Например, с ее помощью можно создать точную копию защищенного компакт-диска; программа также понимает и способна эмулировать большинство систем защиты информации от копирования.

Скачать последнюю версию программы можно с сайта компании **Alcohol Soft Co. Ltd** или с сайта **www.soft-e.net**. Пользователю предоставляется возможность в течение 30 дней бесплатно работать с полной версией программы. По истечении этого срока можно воспользоваться одним из описанных выше способов по взлому подобных программ (например изменить системную дату на более раннюю, чтобы программа считала, что положенный месяц еще не прошел).

Интерфейс программы достаточно функционален: в левой части отобра-

жается три панели (**Main, Options, Help**), содержащие наиболее используемые кнопки; в основном окне расположен список файлов-образов; в нижней части приведен перечень **CD/DVD-приводов** - как аппаратных, так и виртуальных (рисунок 2.9).

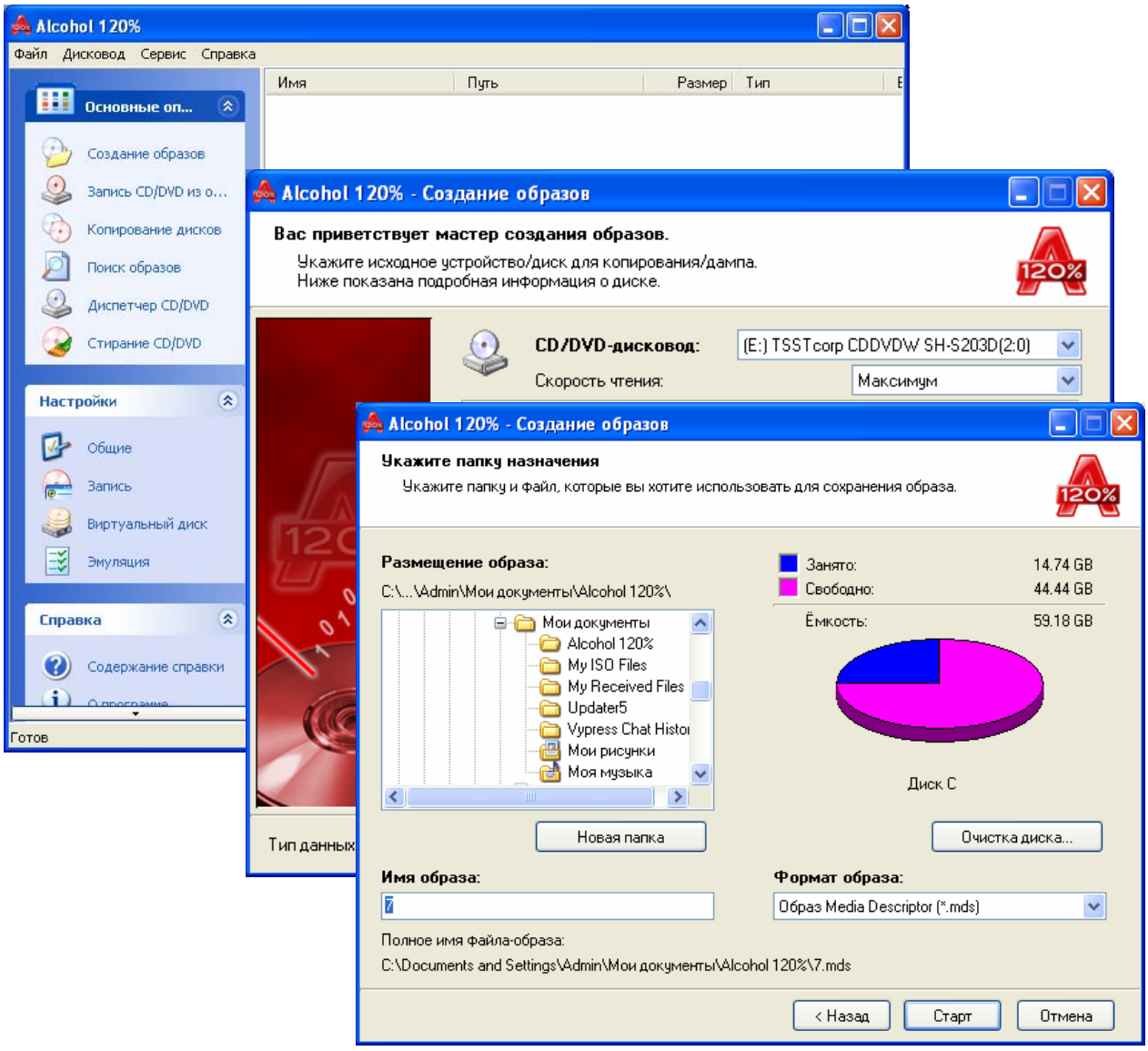


Рисунок 2.9 - Диалоговые окна программы **Alcohol 120 %**

Вызвав «Мастер» создания файла-образа, пользователь увидит основное диалоговое окно указания параметров будущего виртуального диска. Как и в большинстве аналогичных программ, требуется указать, в каком из приводов располагается оригинальный компакт-диск, файл-образ которого и требуется создать. Особое внимание следует обратить на три дополнительных параметра:

– **Skip reading errors** - пропускать ошибки чтения;

– **Fast skip error blocks** - пропускать нечитаемые сектора в ускоренном режиме (поддерживается не всеми **CD/DVD-приводами**);

– **Read Sub-Channel Data from current disc** - читать данные из субканала оригинального компакт-диска.

В левом нижнем углу «Мастера» создания виртуальных дисков располагается список **Datatype**, содержащий шаблоны настроек для различных типов компакт-дисков. Программа **Alcohol 120%** позволяет создавать образы защищенных от копирования компакт-дисков и поддерживает более 10 наиболее распространенных систем защиты от копирования: **Audio+; General Protected CD; Karaoke CD+G; Laserlock; Play Station, SufeDixc; Safe Disk 2; Securom; Securom *New; VOB ProtectCD**.

Определив тип защиты от копирования, необходимо выбрать ее в списке **«Datatype»**, после чего программа сможет корректно считать информацию с оригинального компакт-диска и выставить параметры эмуляции созданного файла образа. Затем нужно нажать кнопку **«Next»**.

В следующем диалоговом окис «Мастера» создания файлов-образов пользователю необходимо выбрать размещение на жестком диске и тип будущего файла образа. Программа способна создавать файлы-образы четырех основных типов:

– **MDS (Media Descriptor Image);**
– **CCD (CloneCD Image);**
– **CUE (CDRWIN Image);**
– **ISO (Standard ISO Image).**

Процесс создания файла-образа начинается после нажатия кнопки **«Start»**, а по окончании созданный файл-образ автоматически помещается в перечень виртуальных дисков основного окна программы.

Одной из наиболее удобных функций программы **Alcohol 120 %** можно считать возможность присвоить каждому файлу-образу собственную комбинацию клавиш, при нажатии которой образ будет автоматически помещаться в виртуальный привод.

2.4 Контрольные вопросы

2.4.1 Для чего используются архивные файлы?

2.4.2 Из чего может состоять архивный файл?

2.4.3 Что представляет собой оглавление архивного файла?

2.4.4 Как получают архивные файлы?

2.4.5 Какие программы-архиваторы Вы знаете?

2.4.6 С какой целью задается пароль архивного файла?

2.4.7 Какие программы «взлома» архивных файлов Вы знаете?

2.4.8 Какие известны способы защиты от «взлома» паролей архивных файлов?

2.4.9 Что понимается под **share-программами** и **trial-программами**?

2.4.10 Назовите способы сокращения срока использования указанных программ.

2.4.11 Перечислите известные Вам методы «взлома» программ.

2.4.12 В чем смысл способа изменения системной даты и в каких случаях он используется?

2.4.13 В чем смысл способа изменения параметров реестра и для чего он используется?

2.4.14 Назовите программу для редактирования реестра **Windows.**

2.4.15 Назовите известные Вам специальные программы редактирования системного реестра **Windows.**

2.4.16 В чем отличие в использовании программ **Regmon** и **Filemon**?

2.4.17 Назначение программы **RTKF**?

2.4.18 Что такое ключи **trial-версий** программ?

2.4.19 В чем смысл создания виртуальных **CD**?

2.4.20 Что называется виртуальным **CD/DVD-приводом**?

2.4.21 Что называется виртуальным **CD/DVD-диском**?

2.4.22 Объясните термины «эмуляция», «программа-эмулятор»

2.4.23 Назовите преимущества виртуальных **CD.**

2.4.24 Какие программы для создания виртуальных **CD** Вы знаете?

2.4.25 Как можно продлить срок использования программы **Alcohol 120 %**?

3 Компьютерные вирусы и механизмы борьбы с ними

3.1 Общие сведения о вирусах

Появление новых вирусов регулярно становится событием транснационального масштаба.

Они могут приводить к замедлению работы на отдельных участках сети **Internet**, выводить из строя почтовые **Web-серверы** и в конечном итоге причинить достаточно ущерба, который может обойтись мировой общественности в миллионы (если не миллиарды) долларов.

Компьютерные вирусы - это настоящая проблема, причем решать ее придется довольно длительное время. В этом легко убедиться после беглого взгляда на сайт, посвященный антивирусному программному обеспечению (рисунок 3.1).

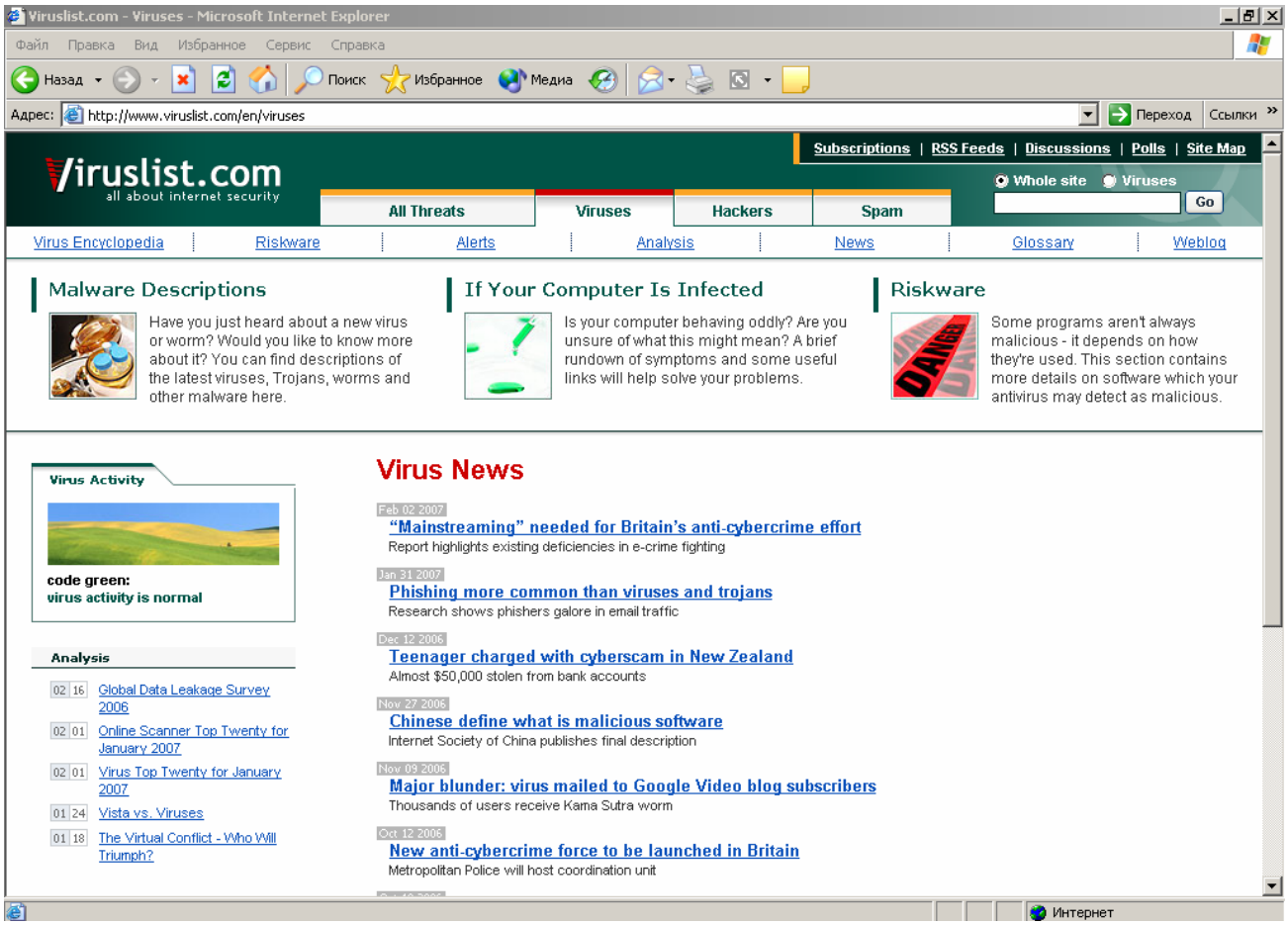


Рисунок 3.1 - Сайт антивирусного программного обеспечения

Вредительские программы и, прежде всего, вирусы представляют очень серьезную опасность для информации в компьютерной системе (КС). Недооценка этой опасности может иметь серьезные последствия для информации пользователей. Вредит использованию всех возможностей КС и чрезмерное преувеличение опасности вирусов.

Знание механизмов действия вирусов, методов и средств борьбы с ними позволяет эффективно организовать противодействие вирусам, свести к минимуму вероятность заражения и потерь от их воздействия.

3.1.1 Что понимается под компьютерным вирусом

Термин «компьютерный вирус» был введен - в середине 80-х годов. Малые размеры, способность быстро распространяться, размножаясь и внедряясь в объекты (заражая их), негативное воздействие на систему - все эти признаки биологических вирусов присущи и вредительским программам, получившим по этой причине название «компьютерные вирусы».

Вместе с термином «вирус» при работе с компьютерными вирусами используются и другие медицинские термины: «заражение», «среда обитания», «профилактика» и др.

«Компьютерные вирусы» - это небольшие исполняемые или интерпретируемые программы, обладающие свойством распространения и самовоспроизведения (репликации) в КС.

Вирусы могут выполнять изменение или уничтожение программного обеспечения или данных, хранящихся в КС. В процессе распространения вирусы могут себя модифицировать.

Вирус представляет собой злонамеренную компьютерную программу, способную после входа в компьютерную систему скрываться, а также исполнять часть своего кода во вред пользователю и дуплицировать себя через линии связи или при помощи инфицированных дисков, заражая другие программы и файлы данных.

3.1.2 Структура вируса

В самом распространенном случае компьютерный вирус состоит из двух частей – «головы», первой получающей управление, и «хвоста», расположенного отдельно от «головы».

В свою очередь, «хвост» вируса может состоять из нескольких частей или вовсе отсутствовать (например, некоторые файловые вирусы).

Для получения управления вирус записывает свою «голову» в одно из перечисленных мест:

– загрузочные модули (**COM-, EXE-файлы**);

– **MBR** (**Master Boot Record** - главная загрузочная запись) дискеты или винчестера;

– драйвер;

– объектный модуль;

– **BAT-файл**;

– исходный текст программы на алгоритмическом языке (в расчете на его компиляцию);

– файлы-документы, созданные приложениями обработки данных, которые поддерживают работу на макроязыках и т.д.

Любой вирус, независимо от принадлежности к определенным классам, должен иметь три функциональных блока:

– блок заражения (распространения);

– блок маскирования;

– блок выполнения деструктивных действий.

Разделение на функциональные блоки означает, что к определенному блоку относятся команды программы вируса, выполняющие одну из трех функций, независимо от места нахождения команд в теле вируса.

После передачи управления вирусу, как правило, выполняются определенные функции блока маскировки. Например, осуществляется расшифрование тела вируса, затем вирус осуществляет функцию внедрения в незараженную среду обитания. Если вирусом должны выполняться деструктивные воздейст-

вия, то они выполняются либо безусловно, либо при выполнении определенных условий.

Завершает работу вируса всегда блок маскирования. При этом выполняются, например, следующие действия: шифрование вируса (если функция шифрования реализована), восстановление старой даты изменения файла, восстановление атрибутов файла, корректировка таблиц ОС и др.

Последней командой вируса выполняется команда перехода на выполнение зараженных файлов или на выполнение программ ОС.

3.1.3 Размножение и проявление вируса

Следует различать два основных действия (фазы), выполняемые компьютерным вирусом: размножение и проявление.

Размножение обычно является первым и обязательным действием вируса при получении им управления.

Фаза проявления, на которой выполняются несанкционированные действия, может чередоваться с размножением, начинаться через определенный (инкубационный) период или при сочетании некоторых условий. Она может заключаться в изощренных визуальных или звуковых эффектах, включать нанесение повреждений файловой системе и т.п.

Повреждения могут быть массированными, например, когда стирается файловая таблица и другие системные блоки, или, наоборот, распределенными, когда довольно часто выполняются небольшие, трудно обнаруживаемые повреждения.

У ряда вирусов фаза проявления отсутствует, т.е. помимо размножения они никаких несанкционированных действий не выполняют.

В то же время любой вирус обладает рядом побочных эффектов, которые не были предусмотрены при создании вируса, но которые фактически относятся к его проявлениям.

Наиболее частым побочным эффектом является зависание операционной системы или потеря работоспособности некоторых (чаще всего резидентных) программ.

Другим важным побочным эффектом является появление некоторых необъяснимых сообщений операционной системы.

3.1.4 Симптомы заражения

Помимо очевидных симптомов заражения, отмеченных выше, существуют также определенные признаки, указывающие на поражение компьютера вирусами. К таким симптомам можно отнести следующие проявления:

– изменение длины командного процессора **command.com**;

– выдача сообщений об ошибке при чтении информации;

– изменение длины и (или) даты создания программы;

– замедление выполнения программы;

– возрастание времени загрузки операционной системы;

– зацикливание при загрузке;

– потеря работоспособности некоторых резидентных программ или драйверов;

– аварийное завершение ранее нормально функционировавших программ;

– необъяснимые зависания или перезагрузки системы;

– уменьшение объема системной памяти или свободной памяти после загрузки;

– резкое уменьшение доступной дисковой памяти, хотя файлы не добавлялись и не удалялись;

– появление новых сбойных кластеров, дополнительных скрытых файлов или других изменений файловой системы.

Приведенные признаки могут наблюдаться даже на здоровых компьютерах по абсолютно не связанным с вирусами причинам. Тем не менее, появление каких-то аномалий должно сразу насторожить пользователя.

Если после перезагрузки с защищенной дискеты некоторые из этих признаков исчезают, то есть смысл провести более или менее полное тестирование с помощью антивирусных программ, а также сравнить содержимое **boot-сектора** и таблицы разделов с их оригиналами.

3.1.5 Проникновение вирусов в компьютер

Причина заражения вирусами компьютера непосредственно связана с неосторожным переносом на него инфицированных программ и различных документов из **Internet**, с другого инфицированного компьютера, зараженного компакт-диска, дискеты или другого носителя информации.

Без сомнения, на первом месте в отмеченном выше ряду стоит **Internet**. При этом наибольшее число заражений приходится на макровирусы, которые проникают преимущественно при обмене письмами с вложенными документами **Word**.

В большинстве случаев пользователь зараженного редактора рассылает зараженные письма адресатам, сам при этом не подозревая, что стал звеном процесса вирусного заражения (пользователи, получившие такие письма, в свою очередь, заражают другие компьютеры и т.д.).

Для уменьшения вероятности заражения через вложенные документы достаточно потратить всего лишь несколько секунд, сохранив документ на диске, а затем проверив его антивирусной программой. Только в том случае, если вирусов в файле не обнаружено, его можно открывать.

Есть и другой, еще более простой путь - использовать антивирусную программу, осуществляющую автоматическую проверку приходящей электронной почты.

3.2 Классификация компьютерных вирусов

В настоящее время в мире насчитывается более миллиона только зарегистрированных компьютерных вирусов. Так как подавляющее большинство современных вредительских программ обладают способностью к саморазмножению, то часто их относят к компьютерным вирусам.

Все компьютерные вирусы могут быть классифицированы по следующим признакам (рисунок 3.2):

- по среде обитания;
- по способу заражения;

– по степени опасности деструктивных (вредительских) воздействий;

– по алгоритму функционирования.

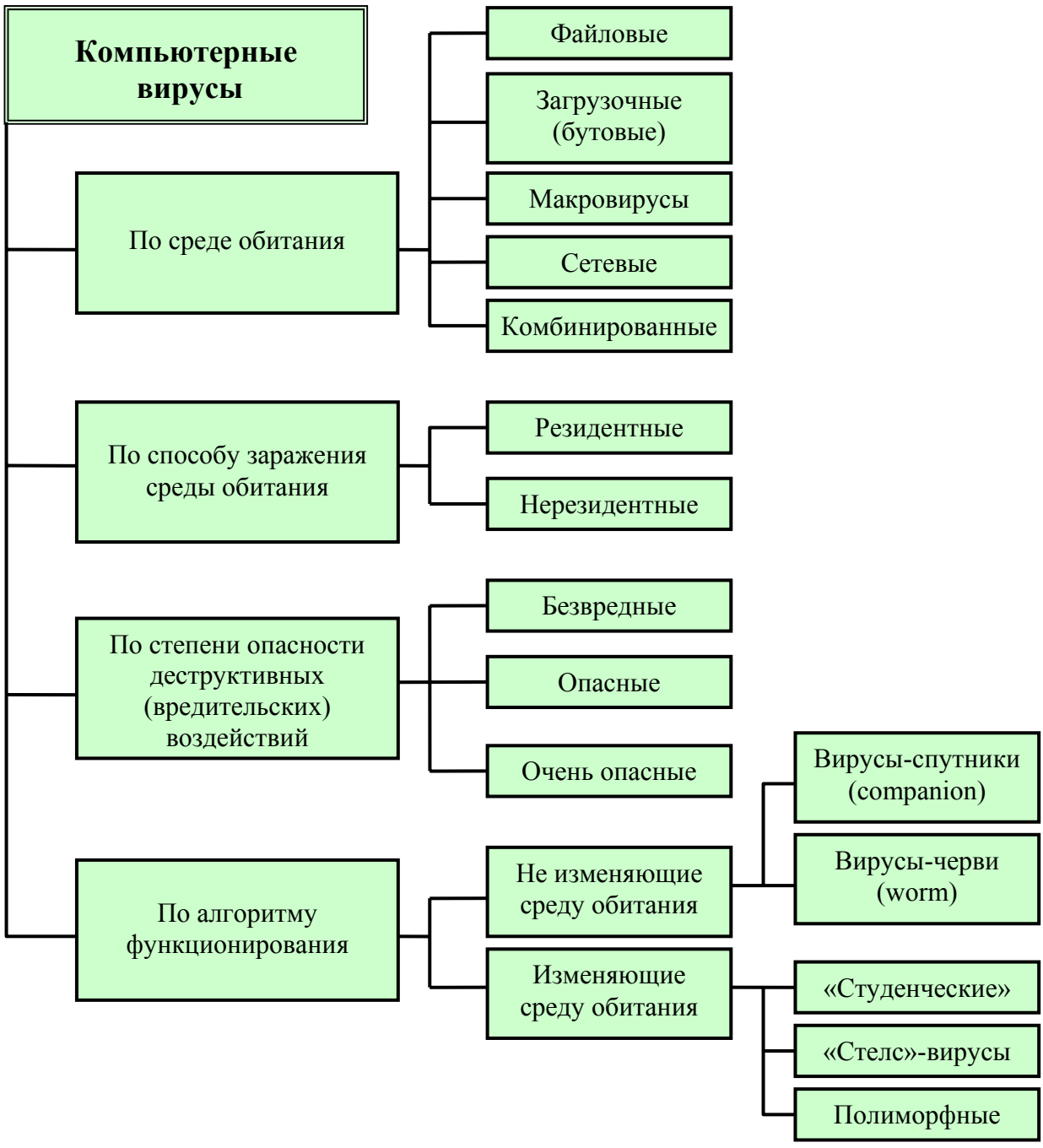


Рисунок 3.2 - Классификация компьютерных вирусов

По среде обитания компьютерные вирусы делятся на:

– файловые;

– загрузочные;

– макровирусы;

– сетевые;

– комбинированные.

Файловые вирусы - вирусы, непосредственно внедряющиеся в выполняемый файл (наиболее распространенный тип вирусов), создающие файлы-двойники либо использующие особенности организации файловой системы;

Загрузочные вирусы находятся в загрузочных секторах (областях) внешних запоминающих устройств (**boot-секторах**). Иногда загрузочные вирусы называют «бутовыми».

Макровирусы - это программы, написанные на встроенных в некоторые приложения обработки данных (**Word, Excel, Access, Ami Pro**) макроязыках, которые средствами этих приложений переносят себя из одного зараженного файла-документа в другие. Таким образом, средой обитания макровирусов может быть только соответствующее приложение, в котором вирусы получают управление при открытии или закрытии зараженного файла. Однако существуют также вирусы, использующие интеграцию некоторых программ, благодаря чему они способны заражать документы сразу нескольких приложений.

Средой обитания **сетевых вирусов** являются элементы компьютерных сетей.

Комбинированные вирусы размещаются в нескольких средах обитания. Примером таких вирусов служат загрузочно-файловые вирусы. Эти вирусы могут размещаться как в загрузочных секторах накопителей на магнитных дисках, так и в теле загрузочных файлов.

По **способу заражения среды обитания** компьютерные вирусы бывают:

– резидентные;

– нерезидентные.

Резидентные вирусы после их активизации полностью или частично перемещаются из среды обитания (сеть, загрузочный сектор, файл) в оперативную память ЭВМ.

Эти вирусы, используя, как правило, привилегированные режимы работы, разрешенные только операционной системе, заражают среду обитания и при выполнении определенных условий реализуют деструктивную функцию.

В отличие от резидентных **нерезидентные** вирусы попадают в оперативную память ЭВМ только на время их активности, в течение которого выполняют деструктивную функцию и функцию заражения. Затем вирусы полностью покидают оперативную память, оставаясь в среде обитания.

Если вирус помещает в оперативную память программу, которая не заражает среду обитания, то такой вирус считается нерезидентным.

По **степени опасности для информационных ресурсов** пользователя компьютерные вирусы можно разделить на:

– безвредные вирусы;

– опасные вирусы;

– очень опасные вирусы.

Безвредные компьютерные вирусы создаются авторами, которые не ставят себе цели нанести какой-либо ущерб ресурсам КС. Ими, как правило, движет желание показать свои возможности программиста.

К **опасным** относятся вирусы, которые вызывают существенное снижение эффективности КС, но не приводящие к нарушению целостности и конфиденциальности информации, хранящейся в запоминающих устройствах.

Последствия таких вирусов могут быть ликвидированы без особых затрат материальных и временных ресурсов. Примерами таких вирусов являются вирусы, занимающие память ЭВМ и каналы связи, но не блокирующие работу сети; вирусы, вызывающие необходимость повторного выполнения программ, перезагрузки операционной системы или повторной передачи данных по каналам связи и т. п.

Очень опасными следует считать следующие вирусы:

– вызывающие нарушение конфиденциальности, уничтожение, необратимую модификацию (в том числе и шифрование) информации;

– блокирующие доступ к информации, приводящие к отказу аппаратных средств и наносящие ущерб здоровью пользователям.

Такие вирусы стирают отдельные файлы, системные области памяти, форматируют диски, получают несанкционированный доступ к информации, шифруют данные и т. п.

Известны публикации, в которых упоминаются вирусы, вызывающие неисправности аппаратных средств. Предполагается, что на резонансной частоте движущиеся части электромеханических устройств, например, в системе позиционирования накопителя на магнитных дисках, могут быть разрушены. Именно такой режим и может быть создан с помощью программы-вируса.

Другие авторы утверждают, что возможно задание режимов интенсивного использования отдельных электронных схем (например, больших интегральных схем), при которых наступает их перегрев и выход из строя.

Использование в современных ПЭВМ постоянной памяти с возможностью перезаписи привело к появлению вирусов, изменяющих программы **BIOS**, что приводит к необходимости замены постоянных запоминающих устройств.

Возможны также воздействия на психику человека - оператора ЭВМ с помощью подбора видеоизображения, выдаваемого на экран монитора с определенной частотой (каждый двадцать пятый кадр).

Встроенные кадры этой видеоинформации воспринимаются человеком на подсознательном уровне. В результате такого воздействия возможно нанесение серьезного ущерба психике человека.

В 1997 году 700 японцев попали в больницу с признаками эпилепсии после просмотра компьютерного мультфильма по телевидению. Предполагают, что именно таким образом была опробована возможность воздействия на человека с помощью встраивания 25-го кадра.

В соответствии с **особенностями алгоритма функционирования** вирусы можно разделить на два класса:

– вирусы, не изменяющие среду обитания (файлы и секторы) при распространении;

– вирусы, изменяющие среду обитания при распространении.

В свою очередь, вирусы, **не изменяющие среду обитания,** могут быть разделены на две группы:

– вирусы-«спутники» (**companion**);

– вирусы-«черви» (**worm**).

Вирусы-«спутники» не изменяют файлы. Механизм их действия состоит

в создании копий исполняемых файлов.

Например, в **MS DOS** такие вирусы создают копии для файлов, имеющих расширение **.EXE**. Копии присваивается то же имя, что и исполняемому файлу, но расширение изменяется на **.COM**. При запуске файла с общим именем операционная система первым загружает на выполнение файл с расширением **.COM**, который является программой-вирусом. Файл-вирус запускает затем и файл с расширением **.EXE**.

Вирусы-«черви» попадают в рабочую станцию из сети, вычисляют адреса рассылки вируса по другим абонентам сети и осуществляют передачу вируса. Вирус не изменяет файлов и не записывается в загрузочные секторы дисков. Некоторые вирусы - «черви» создают рабочие копии вируса на диске, другие - размещаются только в оперативной памяти ЭВМ.

По сложности, степени совершенства и особенностям маскировки алгоритмов **вирусы, изменяющие среду обитания,** делятся на:

– студенческие;

– «стелс» - вирусы (вирусы-невидимки);

– полиморфные.

К **студенческим** относят вирусы, создатели которых имеют низкую квалификацию. Такие вирусы, как правило, являются нерезидентными, часто содержат ошибки, довольно просто обнаруживаются и удаляются.

«Стелс»-вирусы и полиморфные вирусы создаются квалифицированными специалистами, хорошо знающими принцип работы аппаратных средств и операционной системы, а также владеющими навыками работы с машиноориентированными системами программирования.

«Стелс»-вирусы маскируют свое присутствие в среде обитания путем перехвата обращений операционной системы к пораженным файлам, секторам и переадресуют ОС к незараженным участкам информации.

Вирус является резидентным, маскируется под программы ОС, может перемещаться в памяти. Такие вирусы активизируются при возникновении прерываний, выполняют определенные действия, в том числе и по маскировке, и только затем управление передается на программы ОС, обрабатывающие эти

прерывания.

«Стелс»-вирусы обладают способностью противодействовать резидентным антивирусным средствам.

Полиморфные вирусы не имеют постоянных опознавательных групп - сигнатур.

Обычные вирусы для распознавания факта заражения среды обитания размещают в зараженном объекте специальную опознавательную двоичную последовательность или последовательность символов (сигнатуру), которая однозначно идентифицирует зараженность файла или сектора. Сигнатуры используются на этапе распространения вирусов для того, чтобы избежать многократного заражения одних и тех же объектов, так как при многократном заражении объекта значительно возрастает вероятность обнаружения вируса.

Для устранения демаскирующих признаков полиморфные вирусы используют шифрование тела вируса и модификацию программы шифрования. За счет такого преобразования полиморфные вирусы не имеют совпадений кодов.

3.3 «Троянские» программы

К «троянским» программам («троянским коням») относятся программы, в зависимости от каких-либо условий (наступление определенного времени, выполнение какого-либо условия и т.п.) наносящие разрушительные действия (уничтожают информацию на дисках, парализуют операционную систему и др.).

По сравнению с вирусами «троянские» программы не получают широкого распространения по достаточно простым причинам - они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем.

«Троянские» программы можно классифицировать по нескольким категориям (рисунок 3.3): «программы-вандалы», «логические бомбы», «программы-люки», программы угадывания паролей, «дропперы» вирусов и программы скрытого администрирования.

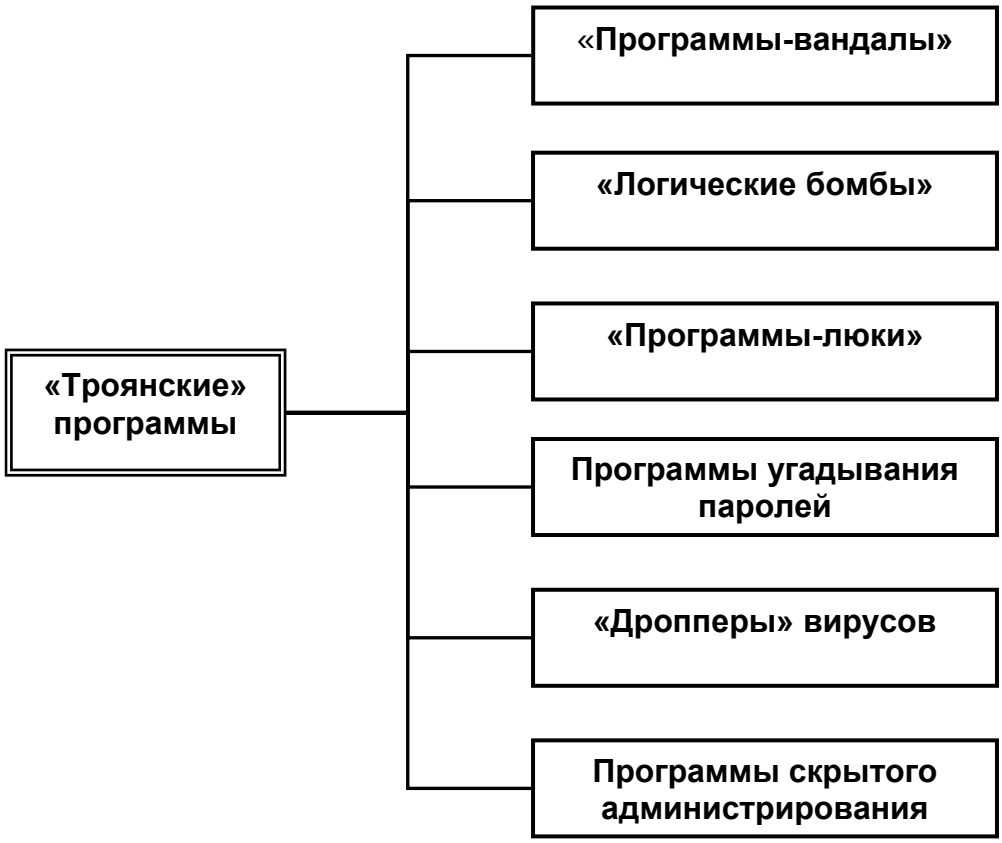


Рисунок 3.3 - Классификация «троянских» программ

«**Программы-вандалы»** обычно выполняют или имитируют выполнение какой-нибудь полезной функции или маскируются под новую версию известного программного продукта. При этом в качестве побочного эффекта они стирают файлы, разрушают каталоги, форматируют диск и выполняют другие деструктивные функции.

«Логические бомбы» считаются разновидностью «троянских программ-вандалов» и представляют собой скрытые модули, встроенные в ранее разработанную и широко используемую программу. Такой модуль является безвредным до определенного события, при наступлении которого он включается. Такого рода программы иногда используются уволенными или обиженными сотрудниками как форма мести по отношению к нанимателю.

«Программы-люки» обеспечивают вход в систему или получение привилегированной функции (режима работы) в обход существующей системы полномочий.

«Люки» часто оставляются разработчиками соответствующих компонен-

тов операционной системы для того, чтобы завершить тестирование или исправить какую-то ошибку, но нередко продолжают существовать и после того, как действие, для которого они планировались, было завершено или необходимость в нем отпала.

«Троянские» программы могут использоваться в целях разведки. К распространенным программам такого рода относятся **программы угадывания паролей**. Имеется значительное количество «троянских» программ, которые воруют пароли пользователей и прочую системную информацию и пересылают их злоумышленникам.

К «троянским» программам также можно отнести **«дропперы» вирусов** - зараженные файлы, код которых подправлен таким образом, что известные версии антивирусов не определяют вируса в файле. Например, файл шифруется каким-либо специальным образом или упаковывается редко используемым архиватором, что не позволяет антивирусу «увидеть» заражение.

«Троянские» программы этой категории **скрытого администрирования** представляют собой мощные утилиты удаленною администрирования компьютеров в сети.

По своим функциональным возможностям эти программы схожи с различными системами администрирования, разрабатываемыми и распространяемыми различными фирмами-производителями программных продуктов.

Особенность этих программ заключается в отсутствии предупреждения об инсталляции и запуске. Дело в том, что при запуске такая программа отслеживает поведение системы и при этом пользователю не выдается никаких сообщений о ее действиях. Более того, при этом в списке активных приложений может вообще отсутствовать ссылка на эту утилиту. В результате пользователь этой «троянской» программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Утилиты скрытого администрирования, установленные на компьютере, позволяют принимать/отсылать, запускать и уничтожать файлы; выводить сообщения; стирать информацию; перезагружать компьютер и т.д. В конце концов, эти программы могут быть использованы для обнаружения и передачи

конфиденциальной информации, запуска вирусов, уничтожения данных.

3.4 Особенности сетевых вирусов

Сетевыми называются вирусы, использующие для своего распространения возможности локальных и глобальных сетей. Большинство сетевых вирусов (другое название – сетевые черви) обладают способностями:

– копировать свой код на удаленный сервер или рабочую станцию;

– запускать или провоцировать пользователя на исполнение своего кода на удаленном компьютере.

Заразив компьютер, вирусы этой группы в большинстве случаев не изменяют файлы или секторы на дисках. Они проникают в память компьютеров и рассылают по этим адресам свои копии. Кроме того, такие вирусы иногда создают рабочие файлы на дисках системы, хотя могут и вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

3.5 Защита от вирусов

Между антивирусными компаниями существует постоянная конкуренция: кто первый обнаружит, назовет и опишет новые вирусы. Вначале это может вызывать некоторый беспорядок, особенно если вирус обнаружен одновременно разными компаниями. Тем не менее существуют определенные правила.

Например, если вирус называется **W32/Bagle.n@MM**, то:

– **W32** означает, что это вирус, который воздействует на 32-разрядные операционные системы класса **Windows** (например, **Windows XP**);

– **Bagle** - «имя» вируса;

– **.n** обозначает определенную версию **Bagle**;

– **MM** означает, что это массовый вирус, который старается сам себя разослать как можно большему числу пользователей.

Для удобства работы с известными вирусами используются каталоги вирусов. В каталог помещаются следующие сведения о стандартных свойствах вируса: имя, длина, заражаемые файлы, место внедрения в файл, метод зараже-

ния, способ внедрения в ОП для резидентных вирусов, вызываемые эффекты, наличие (отсутствие) деструктивной функции и ошибки. Наличие каталогов позволяет при описании вирусов указывать только особые свойства, опуская стандартные свойства и действия.

3.5.1 Правила защиты от вирусов

Прежде всего, необходимо отметить, что защитить компьютер от вирусов может только сам пользователь. Только систематическое архивирование информации, ограничение ненадежных контактов и своевременное применение антивирусных средств может защитить компьютер от заражения или обеспечить минимальный ущерб, если заражение все-таки произошло. Рассмотрим правила защиты от вирусов.

3.5.1.1 Систематическое архивирование важной информации

Единственным стопроцентным по надежности методом защиты от потери важной информации является ее резервное копирование на защищенные от записи устройства хранения данных. Более того, архивированием также нельзя пренебрегать по причине возможности потерять информацию не только из-за вирусов, но и из-за скачков напряжения в сети, поломок оборудования и т.д.

Ни одна антивирусная программа не сравнится по надежности с архивированием информации. Дело в том, что на любой алгоритм антивируса всегда найдется алгоритм вируса, невидимого для этого антивируса.

3.5.1.2 Ограничение ненадежных контактов

Второе правило, частично гарантирующее сохранность информации, - это ограничение копирования данных из ненадежных источников. Как бы вы ни старались, обмен информацией с другими пользователями и работа в локальных или глобальных сетях неизбежны. Однако кое-какие правила у себя все-таки выработать можно.

Во-первых, необходимо стараться **не запускать непроверенные файлы**, в том числе полученные по компьютерной сети. Желательно использовать только программы, полученные из надежных источников. Перед запуском новых программ обязательно следует проверить их одним или несколькими анти-

вирусами.

Во-вторых, следует обязательно **пользоваться только хорошо зарекомендовавшими себя источниками программ** и прочих файлов, хотя это не всегда спасает (например, на **WWW-сервере Microsoft** довольно долгое время находился документ, зараженный макровирусом **Wazzu**).

В-третьих, необходимо **ограничить круг людей, допущенных к работе на конкретном компьютере**. Практика показывает, что наиболее уязвимые компьютеры - многопользовательские.

И наконец, следует **стремиться к приобретению только дистрибутивного программного обеспечения у официальных продавцов**. Неоплатные, условно бесплатные или пиратские копии могут привести к заражению.

3.5.1.3 Использование антивирусных программ

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры, мониторы и ревизоры. Применяются также различного рода блокировщики и иммунизаторы (рисунок 3.4).

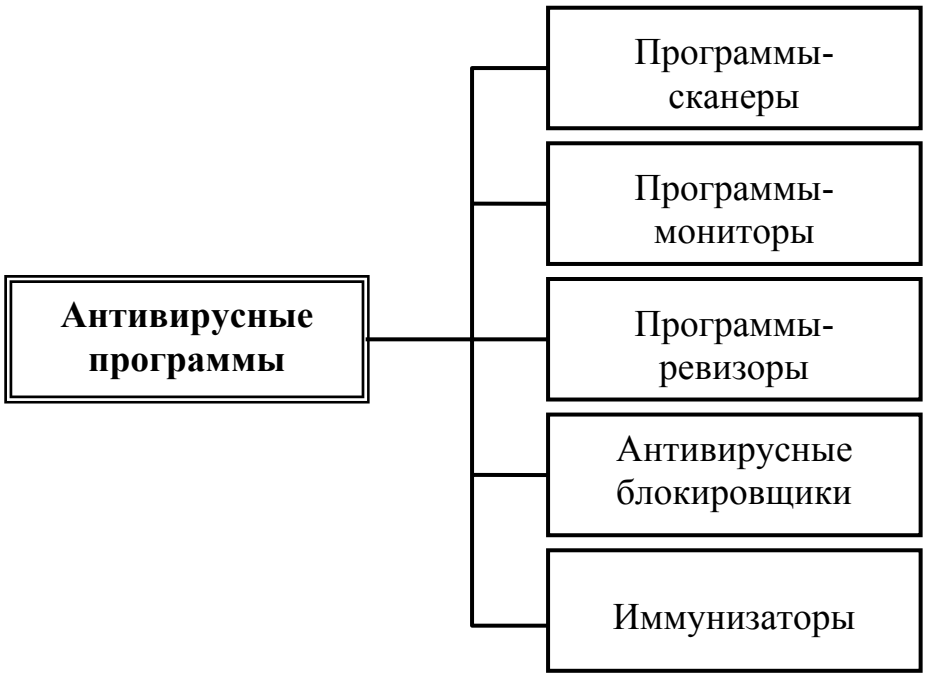


Рисунок 3.4 - Классификация антивирусных программ

3.5.2 Антивирусные программы

3.5.2.1 Программы-сканеры

Сканеры способны обнаружить фиксированный набор известных вирусов в файловой системе, секторах и системной памяти, а затем - немедленно удалить большинство из них.

Для поиска вирусов сканеры используют так называемые «маски» - некоторую постоянную последовательность кода, специфичную для этого конкретного вируса.

В случае если вирус не содержит постоянной маски (полиморфные-вирусы), используются другие методы, основанные на описании всех возможных вариантов кода на алгоритмическом языке.

Во многих популярных сканерах (например **Антивирус Касперского, Doctor Web, Norton Antivirus, McAfee, Panda Antivirus, AntiVir Personal Edition, NOD32** и др.) применяется режим эвристического сканирования, который заключается в том, что программа не просто ищет вирусы, а проводит анализ последовательности команд в каждом проверяемом объекте, осуществляет набор некоторой статистики и впоследствии принимает вероятное решение: «возможно, заражен» или «не заражен».

Эвристическое сканирование представляет собой вероятностный метод поиска вирусов, что, н конечном счете, обеспечивает возможность определения неизвестных программе вирусов, но вместе с этим увеличивает количество ложных срабатываний (сообщений о найденных вирусах н файлах, где ни самом деле их нет).

Разновидностью сканеров являются так называемые «таблетки» - специализированные программы, ориентированные на поиск определенного типа или семейства вирусов, например «троянов», макровирусов и др. (например **Anti-Trojan**, **Trojan Remover**).

Следует отметить, что использование специализированных сканеров, рассчитанных только на макровирусы, иногда бывает более удобным и надежным решением для защиты документов **MS Word** и **MS Excel**.

К недостаткам сканеров следует отнести только то, что они охватывают далеко не все известные вирусы и требуют постоянного обновления антивирусных баз.

Учитывая частоту появления новых вирусов и их короткий жизненный цикл, для использования сканеров необходимо наладить получение свежих версий не реже одного-двух раз в месяц. В противном случае их эффективность существенно снижается.

3.5.2.2 Программы-мониторы

Мониторы - это разновидность сканеров, которые, постоянно находясь в памяти, отслеживают вирусоподобные ситуации, производимые с диском и памятью (т.е. выполняют непрерывный мониторинг).

Примером таких антивирусов может быть программа **Kaspersky Anti-Virus** или **SpIDer Guard**.

К недостаткам этих программ можно отнести, например, вероятность возникновения конфликтов с другим программным обеспечением, как и для сканеров - зависимость от новых версий вирусных баз, а также способность их обхода некоторыми вирусами.

3.5.2.3 Программы-ревизоры

Ревизоры - это программы, принцип работы которых основан на подсчете контрольных сумм (**CRC-сумм**) для присутствующих на диске файлов и системных сектором. Примером такого антивируса может быть программа **ADinf32**.

Эти контрольные суммы затем сохраняются в базе данных антивируса (таблицах) вместе с сопутствующей информацией: длинами файлов, датами их последней модификации и т.д. При последующем запуске ревизоры сверяют сведения, содержащиеся в базе данных, с реально подсчитанными значениями.

Если информация о. файле, записанная в базе данных, не совпадает с реальными значениями, то ревизор предупреждает о том, что файл, возможно, был изменен или заражен вирусом.

Ревизоры умеют своевременно обнаруживать заражение компьютера практически любым из существующих сейчас вирусов, не допуская развития

эпидемии, а современные версии ревизора умеют немедленно удалять большинство даже ранее незнакомых им вирусов.

К недостаткам ревизоров можно отнести то, что для обеспечения безопасности они должны использоваться регулярно. Но несомненными их преимуществами являются высокая скорость проверок и то, что они не требуют частого обновления версий.

3.5.2.4 Антивирусные блокировщики

Это резидентные программы, перехватывающие опасные ситуации и сообщающие об этом пользователю (например, **AVP Office Guard**).

К отслеживаемым ситуациям относятся, например, открытие выполняемых файлов для записи, запись в **boot-сектора** дисков или **MBR** винчестера, попытки программ остаться резидентно и т.д. Кстати, отмеченные события характерны для вирусов в моменты их размножения.

К достоинствам блокировщиков можно отнести умение обнаруживать вирус на самой ранней стадии его размножения, а к недостаткам - способность некоторых вирусов обходить блокировщики, а также наличие ложных срабатываний.

3.5.2.5 Иммунизаторы

Это небольшие программы, которые изменяют файлы или проникают в них. В первом случае вирус будет принимать файлы как зараженные, а во втором - антивирус будет каждый раз проверять файл на изменение.

Следует отметить, что в настоящее время этот тип антивирусов не имеет большого распространения среди пользователей.

3.5.3 Технологии функционирования антивирусных программ

Антивирусные программы развивались параллельно с эволюцией вирусов. По мере того как появлялись новые технологии создания вирусов, усложнялся и математический аппарат, который использовался в разработке антивирусов.

3.5.3.1. Первые антивирусные алгоритмы

Первые антивирусные алгоритмы строились на основе сравнения с этало-

ном. Речь идет о программах, в которых вирус определяется классическим ядром по некоторой маске. Смысл алгоритма заключается в использовании статистических методов. Маска должна быть, с одной стороны, маленькой, чтобы объем файла был приемлемых размеров, а с другой – достаточно большой, чтобы избежать ложных срабатываний.

Первые антивирусные программы, построенные по этому принципу (так называемые сканеры-полифаги), знали некоторое количество вирусов и умели их лечить.

Создавались эти программы следующим образом: разработчик, получив код вируса (код вируса поначалу был статичен), составлял по этому коду уникальную маску (последовательность 10-15 байт) и вносил ее в базу данных антивирусной программы.

Антивирусная программа сканировала файлы и, если находила данную последовательность байтов, делала заключение о том, что файл инфицирован. Данная последовательность (сигнатура) выбиралась таким образом, чтобы она была уникальной и не встречалась в обычном наборе данных. Описанные подходы использовались большинством антивирусных программ вплоть до середины 90-х годов, когда появились первые полиморфные вирусы, которые изменяли свое тело по непредсказуемым заранее алгоритмам.

Тогда сигнатурный метод был дополнен так называемым эмулятором процессора, позволяющим находить шифрующиеся и полиморфные вирусы, не имеющие в явном виде постоянной сигнатуры. Принцип эмуляции процессора демонстрируется на рисунке 3.5.

Если обычно условная цепочка состоит из трех основных элементов: ЦПУ→ОС→Программа, то при эмуляции процессора в такую цепочку добавляется эмулятор. Эмулятор как бы воспроизводит работу программы в некотором виртуальном пространстве и реконструирует ее оригинальное содержимое. Эмулятор всегда способен прервать выполнение программы, контролирует ее действия, не давая ничего испортить, и вызывает антивирусное сканирующее ядро.

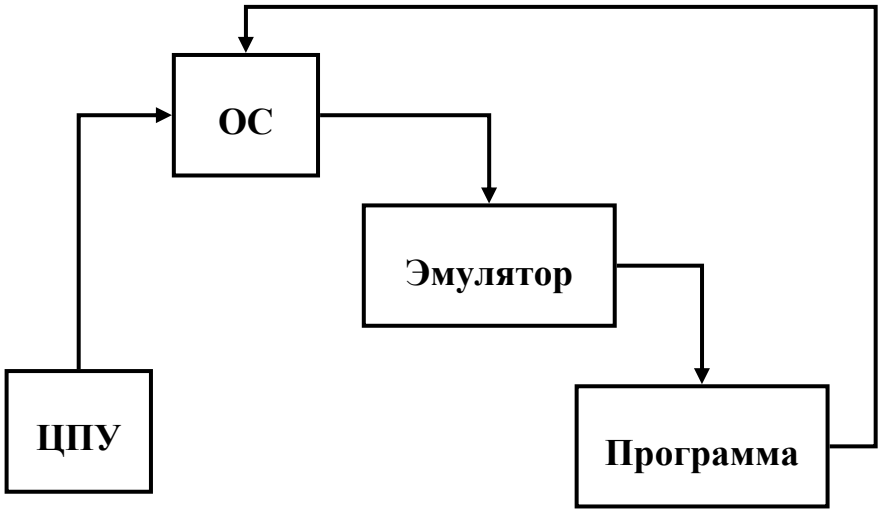


Рисунок 3.5 - Схема работы эмулятора процессора

3.5.3.2 Эвристический анализ

Механизм, появившийся в середине 90-х годов и использующийся всеми антивирусами. Дело в том, что аппарат эмуляции процессора, который позволяет получить выжимку действий, совершаемых анализируемой программой, не всегда дает возможность осуществлять поиск по этим действиям, но позволяет произвести некоторый анализ и выдвинуть гипотезу типа «вирус или не вирус?».

В данном случае принятие решения основывается на статистических подходах. А соответствующая программа называется эвристическим анализатором.

Для того чтобы размножаться, вирус должен совершать какие-либо конкретные действия: копирование в память, запись в сектора и т.д. Эвристический анализатор (он является частью антивирусного ядра) содержит список таких действий, просматривает выполняемый код программы, определяет, что она делает, и на основе этого принимает решение, является данная программа вирусом или нет.

При этом процент пропуска вируса, даже неизвестного антивирусной программе, очень мал. Данная технология сейчас широко используется во всех антивирусных программах.

3.4.4 Еще одна классификация антивирусных программ

Классифицируются антивирусные программы на чистые антивирусы и антивирусы двойного назначения (рисунок 3.6).

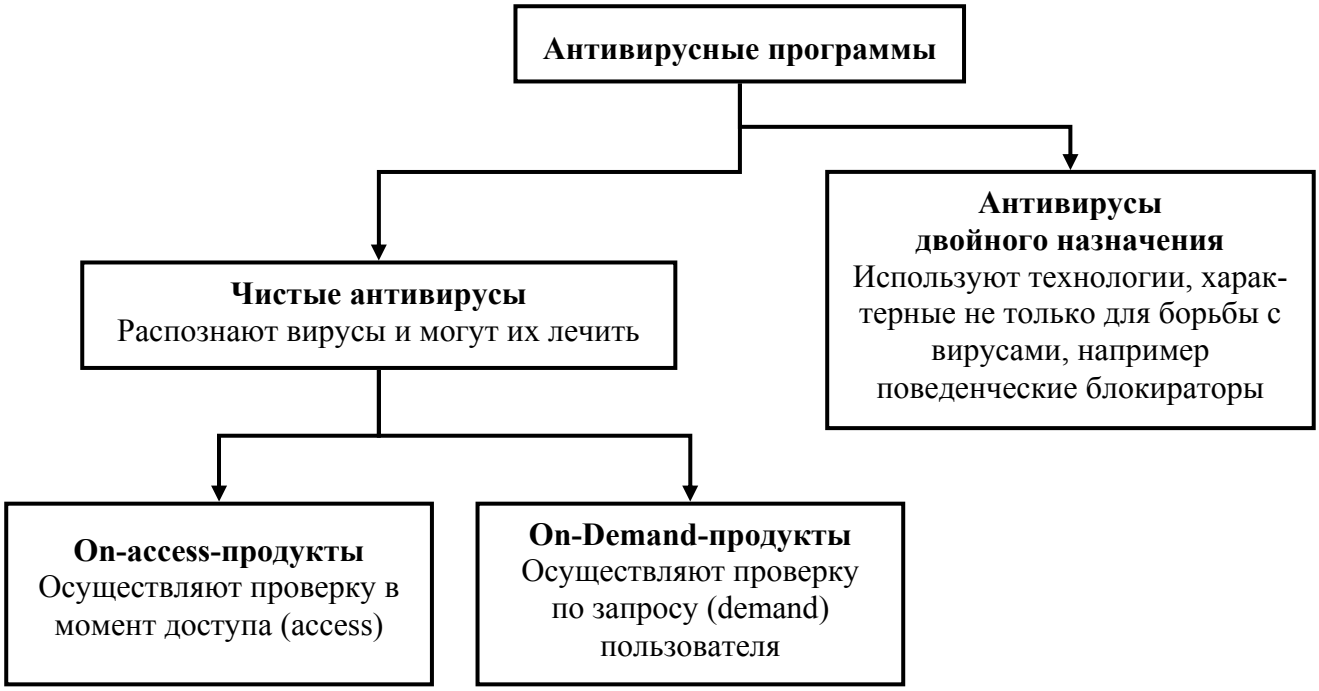


Рисунок 3.6 - Классификация антивирусных программ

Чистые антивирусы отличаются наличием антивирусного ядра, которое выполняет функцию сканирования по образцам. Принципиальным в этом случае является то, что возможно лечение, если известен вирус.

Чистые антивирусы, в свою очередь, по типу доступа к файлам подразделяются на две категории: осуществляющие контроль по доступу (**on access**) или по требованию пользователя (**on demand**).

Обычно **on access**-продукты называют мониторами, а **on demand**-продукты – сканерами.

On demand-продукт работает по следующей схеме: пользователь хочет что-либо проверить и выдает запрос (**demand**), после чего осуществляется проверка. **On access**-продукт – это резидентная программа, которая отслеживает доступ и в момент доступа осуществляет проверку.

Кроме того, антивирусные программы, так же как и вирусы, можно разделить в зависимости от платформы, внутри которой данный антивирус работает. В этом смысле наряду с **Windows** или **Linux** к платформам могут быть отнесены **Microsoft Exchange Server, Microsoft Office, Lotus Notes**.

Программы двойного назначения – это программы, используемые как в антивирусах, так и в ПО, которое антивирусом не является. Например, **CRC-checker** – ревизор изменений на основе контрольных сумм – может использоваться не только для ловли вирусов. Разновидностью программ двойного назначения являются поведенческие блокираторы, которые анализируют поведение других программ и при обнаружении подозрительных действий блокируют их. От классического антивируса с антивирусным ядром, распознающего и лечащего от вирусов, которые анализировались в лаборатории и которым был прописан алгоритм лечения, поведенческие блокираторы отличаются тем, что лечить от вирусов они не умеют, поскольку ничего о них не знают. Данное свойство блокираторов позволяет им работать с любыми вирусами, в том числе и с неизвестными. Это сегодня приобретает особую актуальность, поскольку распространители вирусов и антивирусов используют одни и те же каналы передачи данных, то есть Интернет. При этом антивирусной компании всегда нужно время на то, чтобы получить сам вирус, проанализировать его и написать соответствующие лечебные модули. Программы из группы двойного назначения как раз и позволяют блокировать распространение вируса до того момента, пока компания не напишет лечебный модуль.

3.5 Контрольные вопросы

3.5.1 Что понимается под компьютерным вирусом?

3.5.2 Из чего состоит компьютерный вирус?

3.5.3 Что поражает компьютерный вирус?

3.5.4 Каковы способы проникновения компьютерного вируса в компьютер?

3.5.5 Каковы основные признаки заражения компьютерным вирусом?

3.5.6 Назовите основные признаки классификации компьютерных виру-

сов.

3.5.7 Как подразделяются вирусы по среде обитания?

3.5.8 Какой ущерб могут принести очень опасные вирусы?

3.5.9 Что понимается под макровирусами?

3.5.10 Что представляют собой «стелс» - вирусы?

3.5.11 Что понимается под «троянскими» программами?

3.5.12 Перечислите разновидности «троянских» программ

3.5.13 В чем отличие «программ-вандалов», «логических бомб», «программ-люков», программ угадывания паролей, «дропперов» вирусов и программ скрытого администрирования?

3.5.14 В чем особенности сетевых вирусов?

3.5.15 Перечислите правила защиты от вирусов.

3.5.16 Перечислите разновидности антивирусных программ.

3.5.17 В чем особенности программ-сканеров, мониторов, ревизоров, блокировщиков, иммунизаторов?

3.5.18 Укажите недостатки программ-сканеров, мониторов, ревизоров, блокировщиков, иммунизаторов.

3.5.19 Опишите алгоритмы функционирования антивирусных программ.

3.5.20 В чем отличие режимов функционирования антивирусных программ **on access** и **on demand**?

4 Восстановление Windows после сбоя

4.1 Точки восстановления

4.1.1 Общие сведения

Возможность создания контрольных точек восстановления системы (**System Restore**) стала доступна только после появления **Windows XP**. Теперь в случае возникновения неполадок при помощи специальной утилиты можно восстановить сохраненное ранее состояние компьютера без потери личных данных.

Работает этот механизм следующим образом. Каждый раз при запуске **Windows** в оперативную память загружается служба **System Restore**, которая периодически создает «снимки» всех важных системных файлов (таких как данные реестра, загрузочные и защищенные файлы, данные о настройках и др.) и сохраняет их в качестве точек восстановления.

Создание точек восстановления осуществляется автоматически всякий раз, когда в системе происходят события, способные негативно влиять на работу операционной системы (установка нового программного обеспечения или драйверов, выполнение процедуры обновления **Windows** и т.д.). При этом у пользователя сохраняется возможность вручную создать точку восстановления, когда он почувствует в этом необходимость, экспериментируя с компьютером.

Сохраненный в результате этой операции образ компьютера представляет собой некий «слепок» данных системного реестра и других необходимых для нормального функционирования операционной системы файлов.

Таким образом, если при последующих загрузках компьютера система (либо какое-то приложение) работает нестабильно, с помощью созданных архивных данных можно воссоздать одно из предыдущих, работоспособных, состояний.

Если же система вообще не запускается, можно попытаться выполнить те же действия, предварительно загрузившись при помощи последней удачной конфигурации системы, безопасного режима либо консоли восстановления.

Следует иметь в виду, что если выбранная точка восстановления была создана до установки какой-либо программы, то все ссылки на эту программу будут потеряны, а файлы самой программы удалены не будут.

Если программа после восстановления системы не будет работать или же будет, но неправильно, то ее нужно переустановить заново, удалив предварительно ее старые файлы. Также программа восстановления системы не отслеживает и не восстанавливает перенаправленные или удаленные папки и любые настройки, связанные с перемещаемыми профилями пользователей.

Однако в некоторых случаях при восстановлении системы восстанавливаются папки, имена которых совпадают с именами существующих папок. Чтобы не переписывать существующие файлы, после восстановления системы такие папки переименовываются (к имени будет добавлен числовой суффикс).

Что касается личных документов (папка «Мои документы») или других данных (например, паролей), то после восстановления системы они удалены не будут. Последнее справедливо в том случае, когда расширение файла-документа известно программе восстановления, которая идентифицирует этот файл как документ и не удаляет его (восстанавливает позднее состояние).

Это правило распространяется на всю файловую систему за исключением папки «Мои документы» (файлы, находящиеся в ней, не подвергаются никаким изменениям). Поэтому, если пользователь не уверен, что расширение его файла-документа известно программе восстановления, рекомендуется поместить его в папку «Мои документы». К расширениям, известным программе восстановления, относятся, например, **DOC**, **XLS** и т.д.

4.1.2 Параметры системы восстановления

Параметры системы восстановления задаются на закладке «Восстановление системы» апплета «Свойства системы» (рисунок 4.1), а также в реестре. Окно «Восстановление системы» можно активизировать с использованием следующей команды: «Пуск \ Панель управления \ Система».

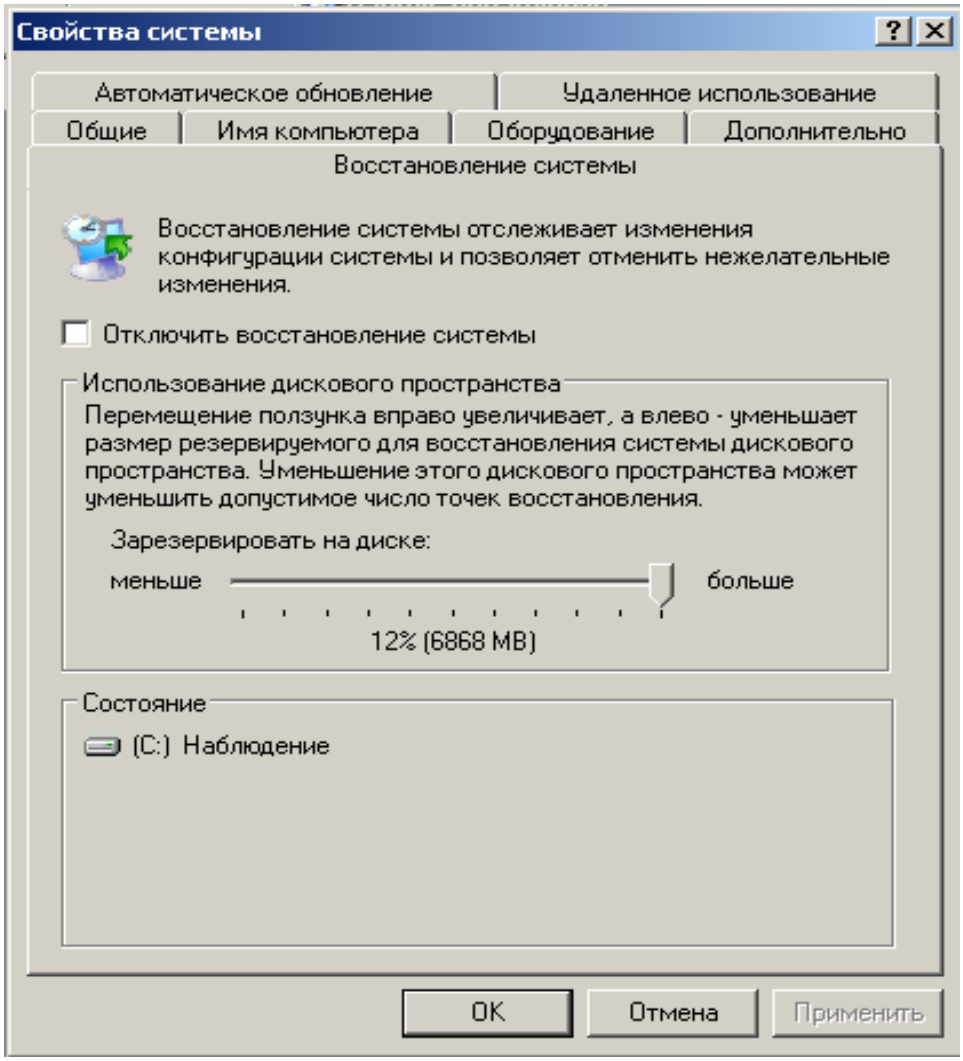


Рисунок 4.1 – Окно «Свойства системы»

В поле «Доступные диски» можно просмотреть все логические диски компьютера, для которых возможно использование функции восстановления. По умолчанию эта функция включена как для загрузочного, так и для всех остальных дисков. Отключить наблюдение штатными средствами **Windows** можно, однако только для не загрузочного диска.

Объем информации восстановления может быть разным и регулируется пользователем в окне «Параметры диска X», где **X** - это логическая буква того диска, за которым осуществляется наблюдение. Для вызова этого окна достаточно выделить один из дисков и щелкнуть по кнопке «Параметры». Регулировка объема данных восстановления может быть полезной, когда служба **System Restore** ощутимо влияет на производительность системы, а сохраненная информация о точках восстановления занимает много места на жестком диске.

При этом следует учитывать, что задание минимального размера сведет к минимуму количество создаваемых точек восстановления. Максимальный размер резервируемою пространства составляет 12 % от дискового пространства.

В реестре регулируемые параметры **System Restore** хранятся в разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows.NT\ CurrentVersion\SystemRestore**.

К параметрам, которые возможно использовать в настройке, следует отнести **DiskPercent**, **RPGIobalInterval** и **RPLifelnterval**.

С помощью первого параметра можно увеличить размер отводимого места на диске для хранения точек восстановления (по умолчанию выделяется 12% дискового пространства).

Второй параметр используется для выбора временного интервала между моментами создания точек восстановления.

По умолчанию контрольные точки создаются один раз в сутки, что соответствует 86400 секундам. Если, например, достаточно создавать контрольную точку один раз в неделю, необходимо поменять это значение на 604800.

Параметр **RPGIobalInterval** предназначен для установки времени жизни точки восстановления (по умолчанию через 90 дней контрольная точка удаляется). Если, например, задать значение 1 209 600, то время жизни каждой точки сократится до двух недель.

4.1.3 Создание точки восстановления

Как уже отмечалось выше, точки восстановления создаются автоматически при появлении каких-либо важных системных событий. Для их создания вручную предназначен «Мастер Восстановление системы», найти который можно по следующему пути «Пуск \ Стандартные \ Служебные \ Восстановление системы».

«Мастер» вызывает два диалоговых окна. В первом окне достаточно установить флажок «Создать точку восстановления», а во втором - ввести ее описание. В качестве описания может выступать, например, причина, по которой «Мастер» был запущен.

4.1.4 Восстановление системы при нестабильности ее работы

В первую очередь следует подчеркнуть, что пользоваться системой восстановления нужно только в тех случаях, когда нет другого способа возобновить работоспособность системы.

Так, например, если после установки нового или обновления старого драйвера какого-либо устройства система стала работать нестабильно, достаточно просто удалить драйвер или вернуться к его предыдущей версии. Для этого следует вызвать апплет «Диспетчер устройств», щелкнуть правой кнопкой мыши на названии устройства, для которого требуется удалить драйвер (или установить его предыдущую версию), и выбрать команду «Свойства». Затем на закладке «Драйверы» окна «Свойства» выбрать одну из команд «Обновить», «Откатить» либо «Удалить» (рисунок 4.2).

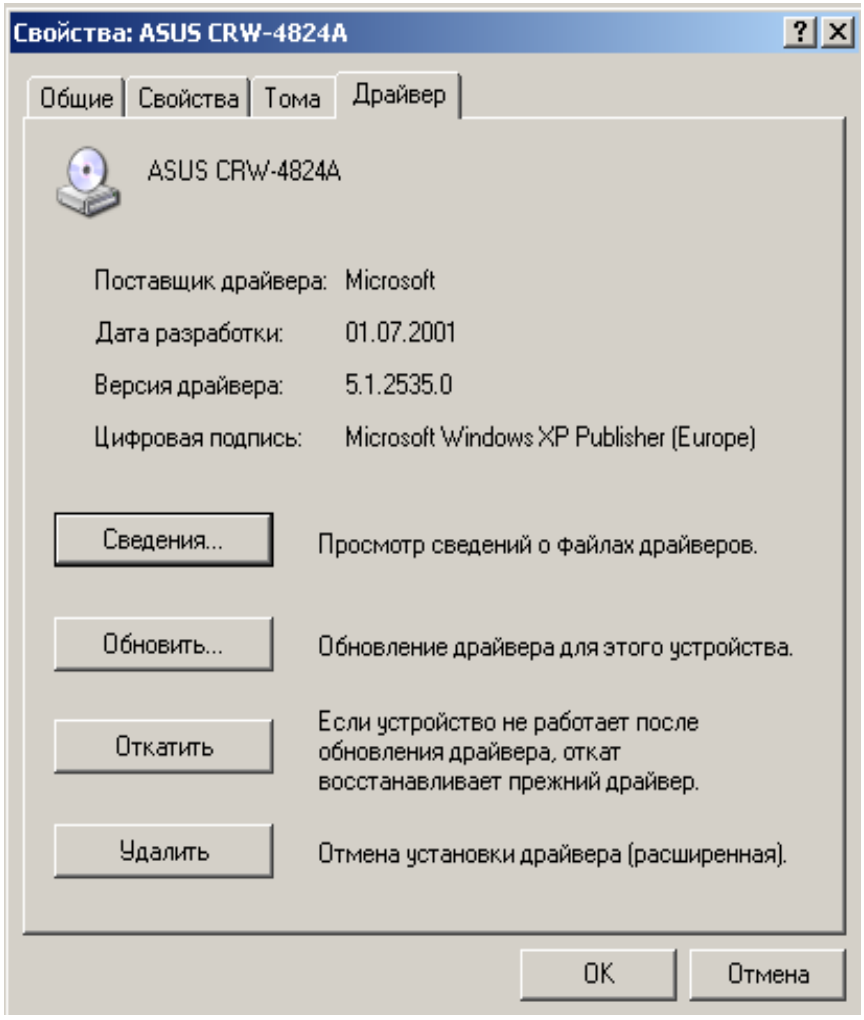


Рисунок 4.2 – Окно «Диспетчер устройств»

После выполнения отмеченных действий в большинстве случаев ошибка должна быть нейтрализована.

Если же причиной сбоев является какая-либо программа, то ее нужно удалить или переустановить. Только тогда, когда идентифицировать причину неполадок не удалось, остается воспользоваться программой восстановления системы. Для запуска программы восстановления используется тот же «Мастер», что и при создании контрольных точек.

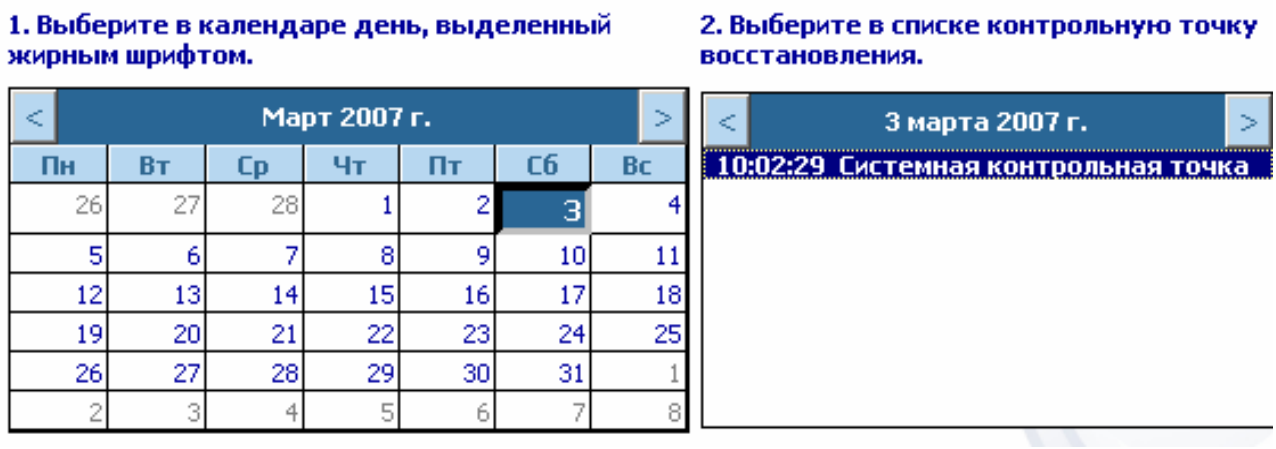


Рисунок 4.3 - Выбор точки восстановления

В первом окне «Мастера» нужно поставить флажок «Восстановление раннего состояния компьютера», а во втором - выбрать точку восстановления. Для этого нужно в календаре (рисунок 4.3) выбрать день (дни, которые содержат точки восстановления, выделены жирным шрифтом), а списке справа - подходящую контрольную точку. После этого достаточно щелкнуть по кнопке «Далее» - программа восстановления начнет выполняться. После перезагрузки компьютера работа системы должна быть стабильна. Теперь осталось только навести порядок в файловой системе, проверить работоспособность программ, устройств и стараться больше не выполнять с системой никаких манипуляций, способных вывести ее из строя.

4.2 Резервное архивирование данных

4.2.1 Архивация данных

Восстановить работоспособность системы **Windows 2000**, **XP Professional** можно также при помощи архивной копии основных системных файлов либо копии данных целого жесткого диска. Для формирования таких архивов в **Windows** имеется специальная программа сохранения данных о состоянии системы или создания «снимка» состояния тома, представляющего собой, в конечном счете, точную копию содержимого жесткого диска на определенный момент времени.

Восстановление из архива может быть осуществлено как в текущем сеансе работы системы, так и до запуска (при ее аварийном отказе). В последнем случае в дополнение к архиву должна быть создана дискета аварийного восстановления системы **ASR (Automated System Recovery**), на которую записываются данные, необходимые для восстановления.

Для создания архива системных файлов необходимо осуществить следующие действия:

а) выполнить команду «Свойства» для конкретного жесткого диска, после чего на вкладке «Сервис» нажать кнопку «Выполнить архивацию»;

б) в открывшемся диалоговом окне «Программа архивации» (рисунок 4.4) выбрать закладку «Архивация», установить в левой панели флажок **System State** и в поле «Носитель архива или имя файла» с помощью кнопки «Обзор» выбрать путь и имя файла будущего архива, обычно данные восстановления помещаются на компакт-диски или ленточные накопители (стримеры);

в) далее, в параметрах программы восстановления нужно просмотреть (и в случае необходимости - изменить) набор файлов-исключений, т.е. файлов, не попадающих в архив;

г) затем достаточно нажать кнопку «Архивировать», при необходимости назначить дополнительные параметры архивации и подождать несколько минут, наблюдая за процессом в окне «Ход архивации» (рисунок 4.5).

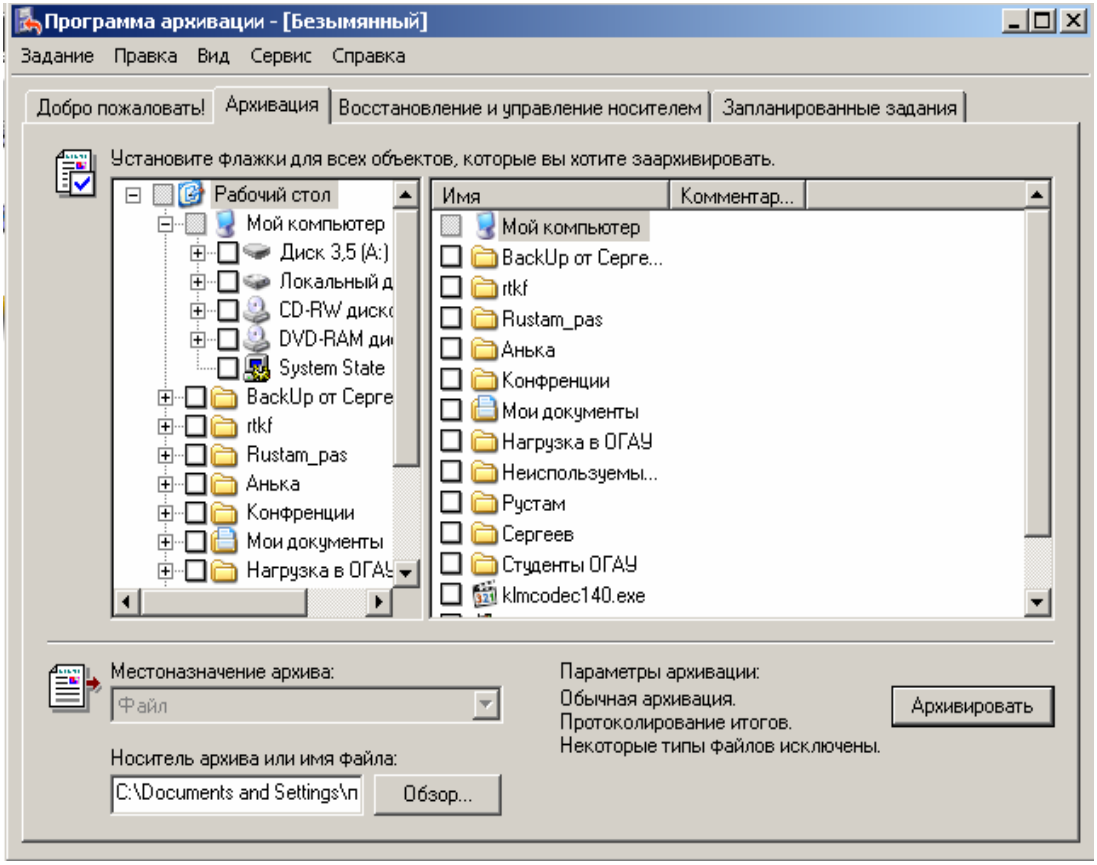


Рисунок 4.4 – Главное окно программы архивации данных

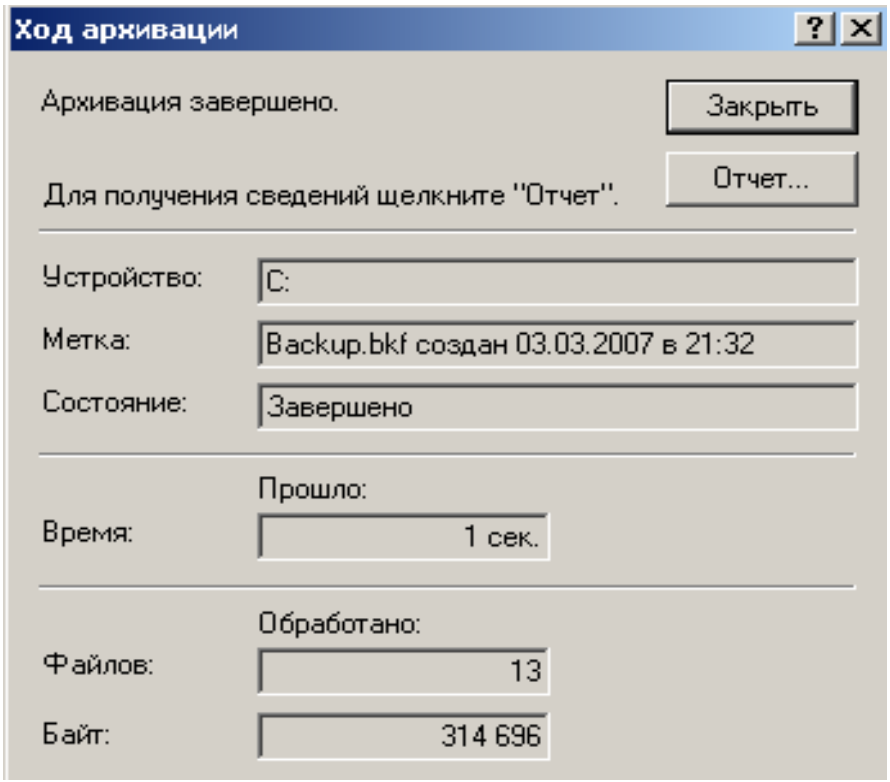


Рисунок 4.5 - Окно наблюдения за ходом архивации

Результатом отмеченной последовательности действий будет файл с рас-

ширением **BKF**, включающий в себя:

– данные реестра;

– базу данных регистрации классов **COM+**;

– базу данных службы каталогов **Active Directory**;

– базу данных служб сертификации;

– системные данные (в том числе – защищенные) и загрузочные файлы.

Для уменьшения объема этого файла до 10-30 Мб можно ограничиться только данными реестра, для чего следует при выборе объектов архивации (рисунок 4.4) отметить только содержимое папки **\WINDOWS\System32\Config**.

Чтобы создать копию данных жесткого диска на определенный момент времени, достаточно на втором этапе отметить флажком нужный диск. При этом следует обращать внимание на размер создаваемого архива (его объем должен соответствовать объему используемого накопителя). В случае создания очень большого архива (более 700 Мб) его рекомендуется разбивать и, соответственно, создавать поэтапно.

Чтобы вместе с архивированием данных создавалась дискета аварийного восстановления системы, необходимо:

а) выполнить команду «Свойства» для конкретного жесткого диска, после чего на вкладке «Сервис» нажать кнопку «Выполнить архивацию»;

б) далее, при необходимости, в параметрах программы восстановления изменить набор файлов-исключений;

в) на вкладке «Добро пожаловать»выбрать «Мастер аварийного восстановления системы»;

г) затем следует указать путь для создаваемого архива;

д) после сбора информации программа начнет процесс архивирования файлов;

е) по окончании архивирования «Мастер» предложит вставить в дисковод гибкий диск для записи на него параметров восстановления.

4.2.2 Параметры архивации

Настройки программы архивации можно задать в диалоговом окне «Параметры» (рисунок 4.6), вызываемом из меню «Сервис» главного окна программы.

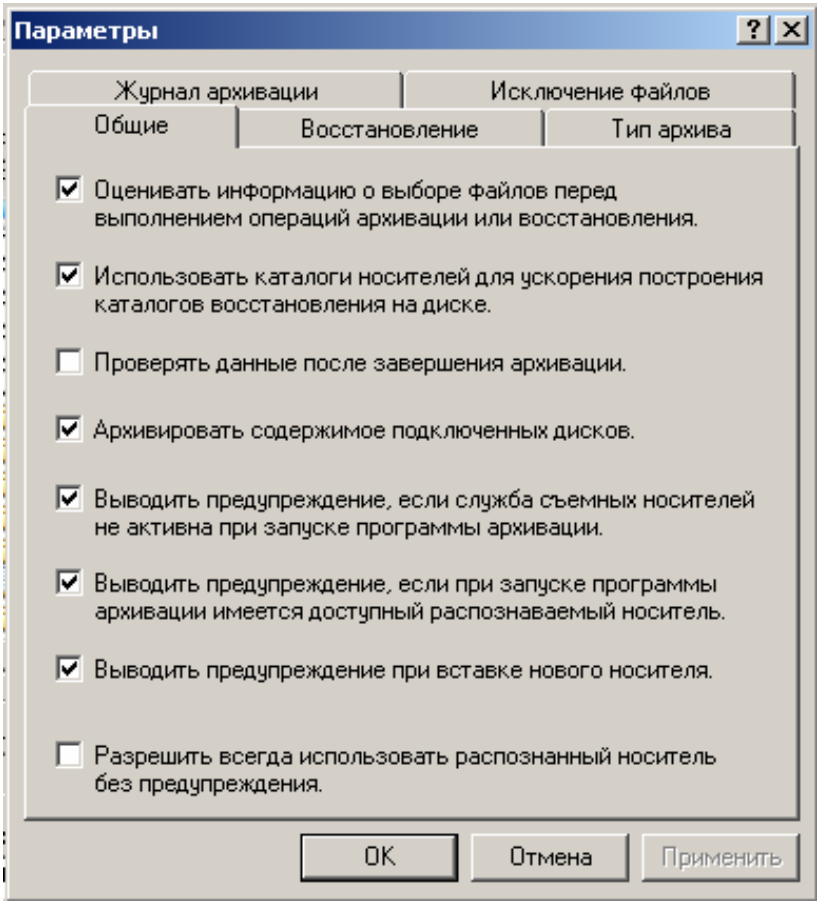


Рисунок 4.6 - Общие параметры архивации

На закладке «Общие» задаются следующие основные параметры:

– «Оценивать информацию о выборе файлов перед выполнением операций архивации или восстановления» – перед началом процесса архивации или восстановления будет подсчитано общее количества архивируемых либо восстанавливаемых файлов и байтов;

– «Использовать каталоги носителей для ускорения построения каталогов восстановления на диске» – опция, обеспечивающая наиболее быстрый способ процесса архивирования/восстановления;

– «Проверять данные после завершения архивации» – во время архива-

ции параллельно будет осуществляться проверка правильности архивации данных (данные из архива будут сравниваться с исходными данными на жестком диске);

– «Архивировать содержимое подключенных дисков» – архивации также будут подвергаться данные, хранящиеся на присоединенном диске (диск, заданный как папка **NTFS**, не имеет логической буквы);

– «Выводить предупреждение, если служба съемных носителей не активна при запуске программы архивации» – в случае, если служба «Съемные ЗУ» не работает, пользователь будет уведомлен об этом предупреждающим сообщением, после чего указанная служба запустится автоматически;

– «Выводить предупреждение, если при запуске программы архивации имеется доступный распознаваемый носитель» - в случае, если в пуле (логическое объединение съемных носителей, подчиняющееся одной политике управления) доступен новый носитель, выводит предупреждающее сообщение;

– «Выводить предупреждение при вставке нового носителя» - при обнаружении нового носителя пользователю будет выведено предупреждение;

– «Разрешить всегда использовать распознанный носитель без предупреждения» - новый импортированный носитель будет автоматически добавлен в пулы носителей архивации.

На вкладке «Тип архива» (рисунок 4.7) можно выбрать способ формирования архива.

Существует пять типов архивов:

– «Обычный» - выполняется архивирование всех выбранных файлов со снятием атрибута «архивный»;

– «Копирующий» - архивация распространяется на все заданные типы файлов без снятия атрибута «архивный» (используется кик промежуточный тип архивирования между обычными и добавочными архивами);

– «Разностный» - архивируются только те файлы, которые были изменены, либо вновь созданные файлы с момента последнего обычного или добавочного архивирования (атрибут «архивный» не снимается);

– «Добавочный» – архивируются только измененные либо вновь создан-

ные файлы с момента последнего обычного или добавочного архивирования (атрибут «архивный» снимается);

– «Ежедневный» – архивация распространяется на файлы, измененные в течение суток до архивирования.

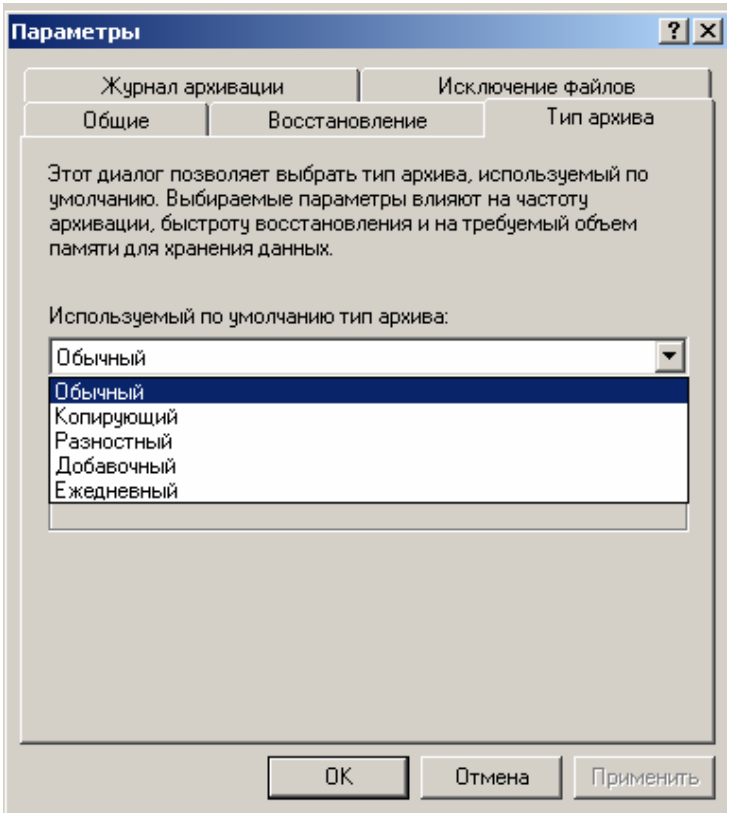


Рисунок 4.7 - Выбор типа создаваемого архива

Выбор типов файлов для исключения из архивации осуществляется на вкладке «Исключение файлов». В списке этого окна можно просмотреть типы файлов, уже исключенные из архивирования. По умолчанию в этот набор входят:

– файл подкачки (**pagefile.sys**);

– файл, создаваемый при использовании спящего режима (**hiberfil.sys**);

– контрольные точки восстановления;

– временные файлы;

– файлы некоторых журналов.

Следует отметить, что в зависимости от установленного на компьютере программного обеспечения этот список может автоматически корректироваться. Так, например, если ранее был установлен **Norton Antivirus**, то в список

исключений добавляется его база обновлений. Таким образом, после восстановления системы необходимость повторного обновления антивирусной базы этого пакета отпадет.

Чтобы добавить в этот список другие виды файлов, достаточно нажать кнопку «Добавить» и в диалоговом окне «Добавление исключаемых файлов» указать исключаемые файлы. Если нужно исключить один из типов файлов, распознаваемых установленными на компьютере приложениями, достаточно выбрать его в списке «Зарегистрированный тип файла».

Если нужно указать одно из незарегистрированных расширений файлов, нужно ввести его в поле «Особая маска файла» (например **.jkl**).

И, наконец, если эти исключения должны распространяться на какую-либо отдельную папку, нужно указать путь к ней в поле «Применяется к пути».

4.2.3 Дополнительные параметры архивирования

Дополнительные параметры создания архивов можно увидеть, если перед самым запуском процесса архивирования в окне «Сведения о задании архивации» (рисунок 4.8) нажать кнопку «Дополнительно».

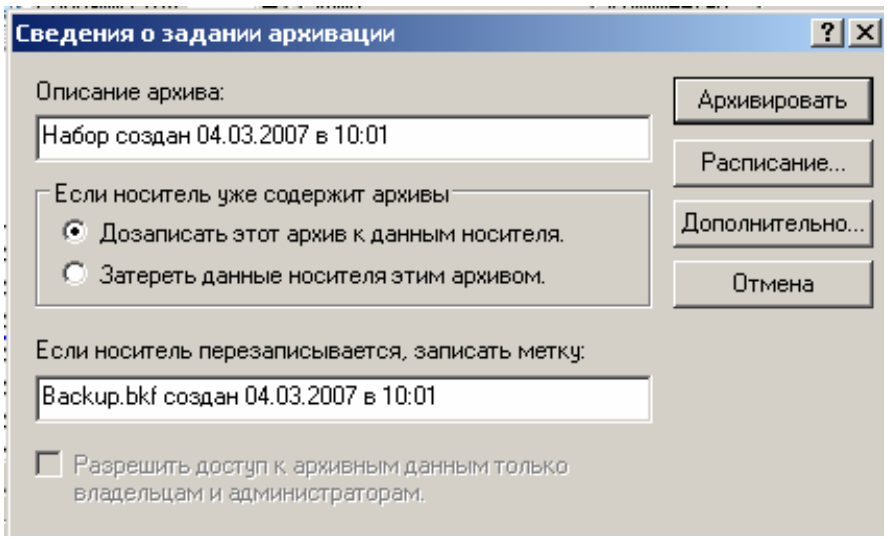


Рисунок 4.8 - Сведения о задании архивации

После этого открывается окно «Дополнительные параметры архивации», в котором выбирается одна из следующих опций:

– «Архивация данных из внешних хранилищ» - выполняется архивация

данных, предназначенных для внешнего хранилища (службы, переносящей редко используемые файлы с локального хранилища на внешнее; восстановление данных из внешнего хранилища возможно только на том NTFS);

– «Проверка данных после архивации» - после архивации будет выполнено сравнение данных из архива и исходных данных (значительно увеличивает время выполнения архивации);

– «Если возможно, сжимать архивируемые данные» – данные при архивации будут помещаться на используемый накопитель в сжатом виде (уменьшает размер архива);

– «Автоматически архивировать защищенные системные файлы вместе с состоянием системы» – в архив будут добавлены файлы, используемые для загрузки, настройки и работы системы (значительно увеличивает размер архива);

– «Отключить теневое копирование состояния тома» – будет создаваться стандартный снимок состояния системы на момент выполнения архивации времени (этот флажок не рекомендуется снимать).

4.3. Восстановление файлов при нестабильности работы системы

Для восстановления данных (системных файлов, личных файлов или папок) из архива необходимо выполнить следующие действия.

Шаг 1. Выполнить команду «Свойства» для конкретного жесткого диска, после чего на закладке «Сервис» нажать кнопку «Выполнить архивацию».

Шаг 2. В открывшемся диалоговом окне «Программа архивации» выбрать закладку «Восстановление и управление носителем» (рисунок 4.9), отметить флажком восстанавливаемый объект.

Шаг 3. В раскрывающемся списке «Восстановить файлы в:» выбрать место, куда будут скопированы файлы архива:

– «Исходное размещение» - файлы архива будут восстановлены, т.е. все текущие данные системы будут удалены, а на их место скопированы данные из архива;

– «Альтернативное размещение» - файлы архива будут скопированы в папку, указанную в поле «Альтернативное размещение» (поле появляется при

выборе соответствующего режима).

Шаг 4. Затем достаточно нажать кнопку «Восстановить», при необходимости назначить дополнительные параметры архивации и подождать несколько минут, наблюдая за процессом в окне «Ход восстановления».

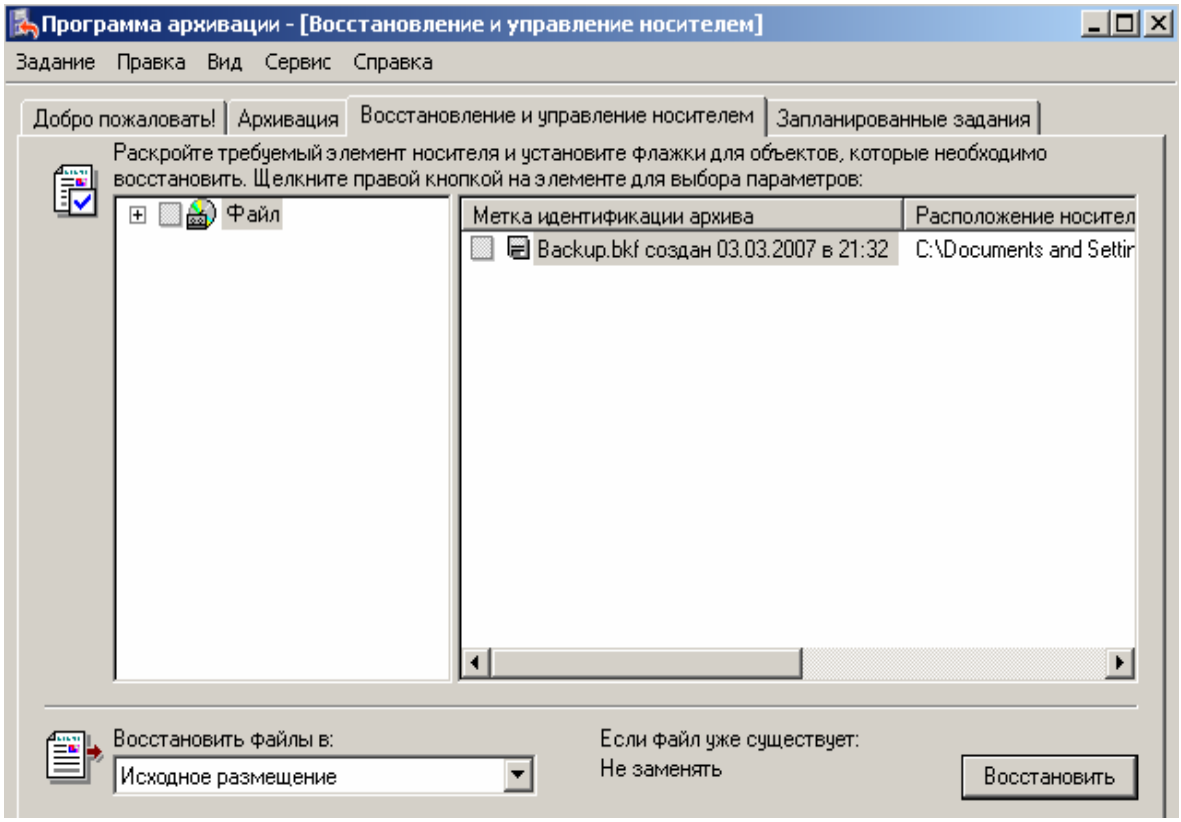


Рисунок 4.9 - Главное окно программы восстановления данных

4.3.1 Параметры восстановления

Опции восстановления можно задать в диалоговом окне «Параметры», вызываемом из меню «Сервис» главного окна программы. На закладке «Восстановление» (рисунок 4.10) задаются следующие основные параметры:

– «Не заменять файл на компьютере (рекомендуется)» – при восстановлении файлы, которые уже содержатся на жестком диске, не будут заменяться новыми;

– «Заменять файл на компьютере, только если он старее» – если файлы на жестком диске имеют более позднюю дату создания, чем такие же файлы в архиве, то в ходе восстановления они будут заменяться;

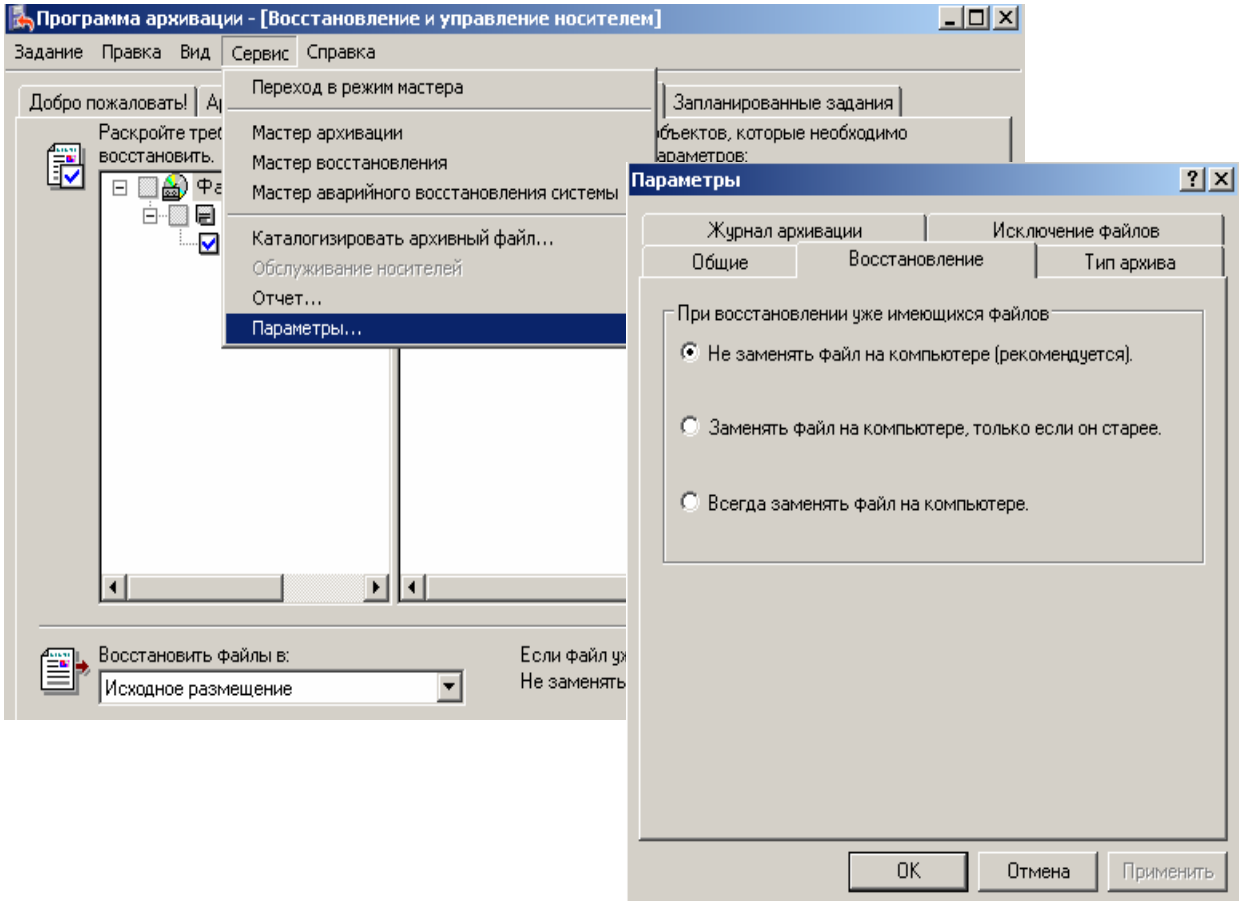


Рисунок 4.10 - Основные параметры восстановления

– «Всегда заменять файл на компьютере» – файлы на жестком диске будут восстанавливаться независимо от того, какая дата у файлов в архиве.

4.3.2 Дополнительные параметры восстановления

Дополнительные параметры восстановления при помощи архивов можно увидеть, если перед самим запуском процесса восстановления в окне «Подтверждение восстановления» (рисунок 4.11) нажать кнопу «Дополнительно».

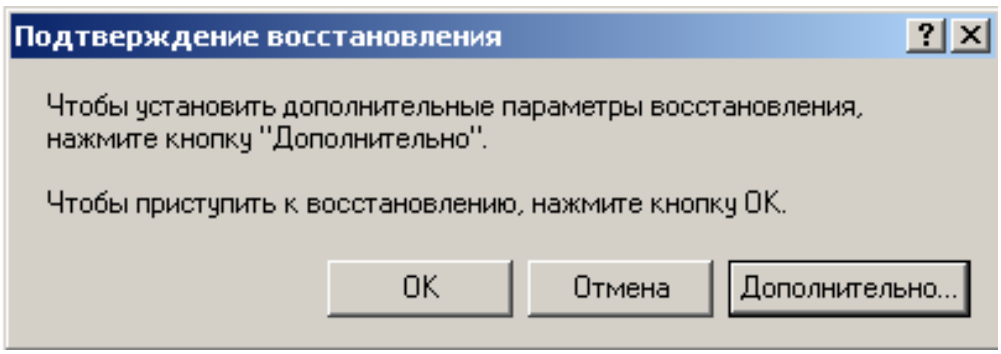


Рисунок 4.11 - Запрос на подтверждение восстановления

После этого открывается окно «Дополнительные параметры восстановления» (рисунок 4.12), в котором могут быть выбраны следующие опции:

– «Восстановление безопасности» - при восстановлении файлов и папок также обновляются параметры безопасности (параметры доступа, элементы журнала безопасности, ин формация о владельце);

– «Восстановление точек соединения, а также ссылок для файлов и папок ниже соединения на исходное размещение» – при восстановлении будут созданы потерянные точки соединения (указатели на данные, размещенные в другом месте диска, другом устройстве или присоединенном диске);

– «При восстановлении реплицируемых наборов данных помечать восстановленные данные как основные для всех реплик» – устанавливается при восстановлении данных службы репликации файлов (**FRS**) на серверы;

– «Восстанавливать реестр кластера на кворумном диске и других узлах» - устанавливается при восстановлении базы данных кворума кластера на все узлы в кластере серверов;

– «Сохранить существующие точки подключения томов» - при восстановлении не выполняется обновление точек подключения томов (опция выбирается для восстановления данных на целом диске или разделе).

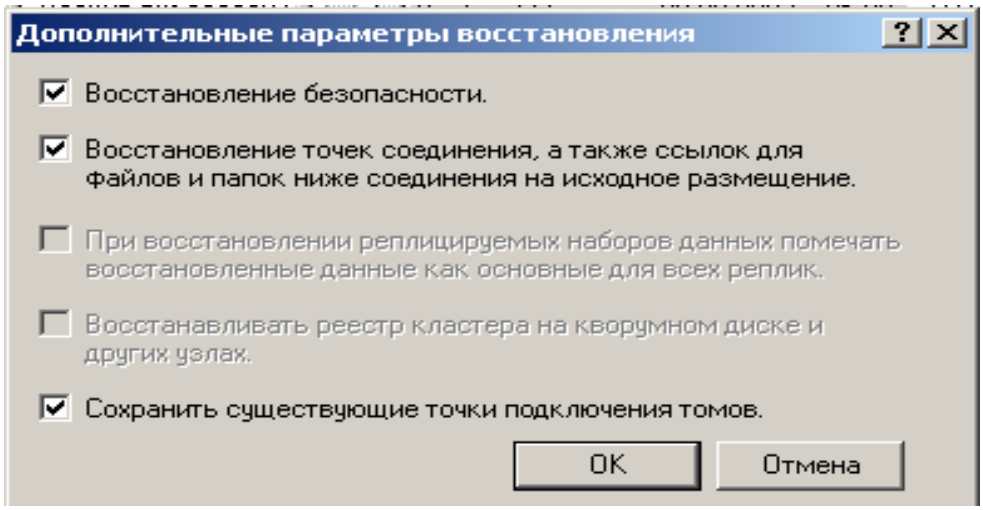


Рисунок 4.12 - Дополнительные параметры восстановления

4.4 Восстановление системы в случае ее отказа

В случае, когда систему не удается загрузить в обычном режиме, предва-

рительно следует попытаться загрузиться при помощи:

– последней удачной конфигурации системы (доступно только для **Windows 2000, XP**);

– безопасного режима.

Если это сделать удалось – осуществить восстановление с использованием контрольных точек (**Windows XP**) или архивов (**Windows 2000, XP Professional**).

И только если отмеченные рекомендации оказались неосуществимыми, остается воспользоваться архивами **ASR** или консолью восстановления (**Windows 2000, XP**).

4.4.1 Последняя удачная конфигурация

Для восстановления последней удачной конфигурации необходимо перед загрузкой операционной системы нажать клавишу **<F8>** и при помощи стрелок выбрать в меню пункт «Загрузка последней удачной конфигурации». В случае если на компьютере установлено несколько операционных систем, отмеченную клавишу следует нажать на вопрос выбора одной из них для загрузки.

Выбор этой команды позволяет восстановить только данные в разделе реестра **HKLM\System\CurrentControlSet** (любые изменения в других разделах реестра сохраняются).

Данный вариант загрузки не устраняет неполадки, вызванные повреждением или отсутствием драйверов или файлов, однако в некоторых случаях может восстановить работоспособность системы.

4.4.2 Безопасный режим

Для использования безопасного режима необходимо перед загрузкой операционной системы нажать клавишу <**F8>** и выбрать в меню «Безопасный режим» (**Safe Mode)**, после чего нажать <**Enter>**.

Выбор этой команды позволяет исключить сетевые подключения и загрузить только основные файлы и драйверы (драйверы мыши, монитора, клавиатуры, дисков, базового видеоадаптера; стандартные системные службы). Если

был выбран безопасный режим с загрузкой сетевых драйверов, то загружаться будут все вышеперечисленные драйверы и вместе с ними - основные сетевые службы и драйверы.

При загрузке в безопасном режиме с поддержкой командной строки вместо графического интерфейса пользователя запускается командная строка.

Следует отметить, что безопасный режим предназначен для выявления причин неполадок. Если в нем система работает стабильно, достаточно удалить настройки по умолчанию, а также оставить минимальный набор драйверов устройств, так как именно они могут быть причиной возникновения сбоев.

Если причиной сбоев является какое-либо устройство или драйвер, безопасный режим можно использовать для удаления этого устройства или драйвера.

4.4.3 Восстановление системы при помощи архивов ASR

Для воссоздания системы с использованием подготовленного ранее диска потребуется непосредственно сам архив, **ASR-дискета**, а также загрузочный диск **Windows XP**.

При наличии отмеченного комплекта для автоматического восстановления файлов необходимо выполнить следующие действия:

- загрузиться с помощью загрузочного диска и выбрать задачу установки **Windows XP**;
- далее, после появления в строке состояния приглашения, достаточно нажать <**F2>**;
- на требование «Вставьте диск» под названием «Диск автоматического восстановления системы **Windows**» в дисковод для гибких дисков следовать инструкции;
- затем программа восстановления выполнит чтение необходимых для восстановления данных с дискеты и после загрузки основных драйверов осуществит форматирование системного раздела винчестера;
- после этого автоматически будет выполнена начальная установка **Windows XP**;

 далее автоматически будет запущен мастер аварийного восстановления системы для копирования файлов из архива в систему.

4.4.4 Консоль восстановления

Как последняя удачная конфигурация, так и безопасный режим не всегда позволяют загрузить систему. Также возможна ситуация, когда пользователь не создавал или потерял **ASR-пакет**. При сочетании всех отмеченных ситуаций остается только одна надежда - «Консоль восстановления».

Запустить консоль восстановления можно, загрузившись с установочного компакт-диска и выбрав соответствующий пункт меню. Для того чтобы консоль восстановления запускалась с локального компьютера как один из вариантов загрузки, необходимо во время одного из предыдущих сеансов работы **Windows** вставить в дисковод для компакт-дисков установочный компакт-диск и в командной строке ввести:

X:\i386\winnt32.exe /cmdcons

где **X** - это логическая буква дисковода компакт-дисков.

Для восстановления системы с использованием консоли чаще всего копируют сохраненные ранее (например на компакт-диске) системные папки (**\Windows\System, System32**) на жесткий диск. Последнее достигается использованием команды **Copy** со следующим синтаксисом:

Copy [исходный файл] [конечный файл],

где **исходный файл** - имя копируемого файла с указанием пути к нему (данный атрибут может представлять собой имя диска (например **C:**), имя папки или имя файла);

конечный файл - имя файла и путь, который нужно восстановить (данный атрибут может состоять из имени диска, папки или файла).

Кроме того, в режиме консоли восстановления имеется ряд команд, с помощью которых можно выполнять как простые операции (смена текущей папки, просмотр содержимого папок), так и сложные (восстановление загрузочного сектора, форматирование дисков, запуск и остановка системных служб), а также выполнять операции чтения-записи на диски и другие операции.

Чтобы получить информацию об именах и назначениях команд консоли восстановления, достаточно во время сеанса ее работы ввести **help** для получения списка команд, либо **help [имя команды**] - для вывода информации о назначении конкретной команды.

Среди наиболее полезных команд консоли восстановления следует отметить следующие: **listsvc**, **disable** и **enable**, **fixboot** и **fixmbr**.

Первая из них отображает на экране список системных служб и драйверов с информацией о способе их загрузки.

Вторая команда осуществляет блокировку той службы (или драйвера устройства), которая, по мнению пользователя, является причиной отказа системы.

Команда имеет следующий синтаксис:

disable [имя службы] [имя драйвера],

где **имя службы** - имя отключаемой системной службы;

имя драйвера - имя отключаемого драйвера устройства.

Так, например, если необходимо отключить службу **Messenger**, необходимо в командной строке консоли ввести:

disable Messenger.

Команда **enable**, наоборот, включает отмеченные службы и драйверы. Команда имеет следующий синтаксис:

enable [имя службы] [имя драйвера] [тип запуска]

где **имя службы** - имя включаемой системной службы;

имя драйвера - имя включаемого драйвера устройства;

тип запуска - способ запуска включаемой службы.

Отметим, что включить службу или драйвер можно со следующими типами запуска:

- **Service_boot_start** - при включении компьютера;
- **Service_system_start** - при запуске системы;
- **Service_auto_start** - автоматически;
- **Service_demand_start** - вручную.

Например, для того чтобы служба **Messenger** запускалась одновременно с запуском системы, достаточно в командной строке консоли ввести:

enable messenger service_system_start.

И, наконец, команды **fixboot** и **fixmbr** позволяют восстановить, соответственно, загрузочные файлы и **MBR (Master Boot Record**).

Например, для записи на диск D: загрузочного сектора необходимо ввести:

fixboot d:

Для записи основной загрузочной записи жесткого диска:

fixmbr \Device\HardDisk0

В последнем случае, перед тем как вводить команду, следует проверить наименование устройства в формате **Advanced RISC Computing (ARC),** а для этого достаточно предварительно ввести команду:

map arc

После этого будет выведен список дисков с указанием логических букв для текущих сопоставлений физическому устройству в формате **ARC**. Например:

D: NTFS 10001 MB multi(0)disk(0)rdisk(0)partition(2)

4.5 Переустановка Windows

4.5.1 Стандартная переустановка Windows

Как показывает практика, нередко при работе может возникнуть ситуация, когда система **Windows** в результате неполадок перестает запускаться, и единственным выходом остается полная переустановка системы.

В этом случае пользователь обычно выполняет стандартные действия, приведенные ниже.

Шаг 1. Перенос всех данных пользователя с логического диска **C:** на другой логический диск (если таковой имеется) или на иной носитель информации (**CD, flash-drive** и пр.).

В частности, для **Windows XP** необходимо целиком скопировать папку C:\Documents and Settings\Имя_пользователя, в которой хранятся:

 документы (папка \Мои документы);

 шаблоны (папка \Application Data\Microsoft\Шаблоны);

 избранные ссылки **Internet** (папка \Избранное);

 адресная книга **Outlook Express** (папка \AppIicationData\Microsoft\Address Book);

 база сообщений **Outlook Express** (папка C:\Documents and Settings\Admin\Local Settings\Application Data\Identities\{093E029D-CE58-4383-8397-F2C8B07484DB}\Microsoft\).

Аналогичные файлы для **Windows 98**, в свою очередь, хранятся и следующих папках:

 документы (папка C:\Мои документы);

 шаблоны (папка C:\Windows\Application Data\Microsoft\Шаблоны);

 избранные ссылки **Internet** (папка C:\Windows\Избранное)

 адресная книга **Outlook Express** (папка C:\Windows\Application Data\Microsoft\Address Book);

 база сообщений **Outlook Express** (папка C:\Windows\Local Settings\AppIication Data\Windows98\{набор_символов}\Microsoft\Outlook Express).

Шаг 2. Далее необходимо проверить, не списывались ли в другие каталоги диска **C:** какие-либо полезные файлы (драйверы, инсталляционные файлы различных программ, документы и пр.). Если таковые имеются, также сохранить их на другом диске.

Шаг 3. После этого необходимо убедиться в наличии инсталляционного диска с регистрационным кодом для требуемой версии **Windows**. Желательно, чтобы этот диск был загрузочным.

Шаг 4. Затем нужно отформатировать диск C:. Для этого следует перезагрузить компьютер с использованием загрузочной дискеты (способ загрузки системы - с дискеты, с **CD-ROM**, с винчестера - задается в **BIOS**) и указать в командной строке следующую команду:

format c:

Шаг 5. Следующий шаг - задать в **BIOS** способ загрузки системы с **CD-ROM**, после чего вставить инсталляционный **CD** и перезагрузить систему.

Шаг 6. После этого нужно следовать всем указаниям программы инстал-

ляции **Windows**. По завершении установки следует перезаписать скопированные ранее каталоги с личными файлами на их прежнее место.

4.5.2 Переустановка Windows без драйверов

Описанная выше процедура переустановки будет успешной только в том случае, если на все имеющиеся устройства (системная плата, видеокарта, звуковая карта, модем, принтер) имеются диски с драйверами этих устройств.

Очевидно, при потере одного из этих дисков может возникнуть проблема в процессе инсталляции, если программа установки **Windows** не сможет подобрать по своей базе устройств драйвер, например, на видеокарту.

Выход из этой ситуации нельзя назвать очень простым. Вероятно, в этом случае следует обойтись без форматирования диска **C:.**

Алгоритм действий пользователя для данной ситуации приведен ниже.

Шаг 1. Прежде всего, необходимо скопировать на диск C: для удобства дальнейшей работы файловый менеджер, например **Norton Commander (NC)**. Его файлы будут находиться в папке C:\NC, выполняемый файл - C:\NC\nc.exe.

Шаг 2. Следующий шаг - перезагрузка системы в режиме командной строки. Для этого в процессе перезагрузки нужно нажать <**F8>** и выбрать вариант **Command prompt only** (Только командная строка). После этого, когда появится приглашение командной строки, нужно указать команду вызова **NC**:

C:\NC\nc.exe

Шаг 3. Далее необходимо переименовать папку C:\Windows, например, на C:\Windows.OLD (переименование в **NC** – клавиша <**F6>**). Кроме того, нужно удалить системную папку C:\Program Files (удаление в **NC** - клавиша <**F8>**).

Шаг 4. Теперь, когда системы **Windows** на компьютере нет, необходимо вставить инсталляционный компакт-диск и перезагрузиться.

В процессе инсталляции, когда установочная программа будет спрашивать, где находятся драйверы того или иного устройства, нужно указывать системную папку C:\Windows.OLD\System, либо (в случае неудачи) C:\Windows.OLD\System32. Именно в этих каталогах хранятся файлы с расширением **DRV**, т.е. драйверы установленных в **Windows** устройств.

4.6 Контрольные вопросы

4.6.1 Что понимается под точками восстановления системы в **Windows XP**?

4.6.2 Как называется служба, отвечающая за создание точек восстановления?

4.6.3 Что происходит с документами в папке «Мои документы» при восстановлении системы по контрольной точке?

4.6.4 В каком разделе меню осуществляется настройка параметров **System Restore**?

4.6.5 Как часто по умолчанию создаются контрольные точки?

4.6.6 Каково по умолчанию время жизни контрольной точки восстановления системы?

4.6.7 Как можно вручную создать точку восстановления? В каких случаях рационально использование данного режима?

4.6.8 Что нужно попытаться сделать перед восстановлением системы при нестабильности ее работы?

4.6.9 Назовите порядок работы с программой восстановления системы.

4.6.10 В чем преимущества и недостатки использования архивации данных для восстановления системы?

4.6.11 Назовите последовательность создания архива системных файлов.

4.6.12 Что представляет собой дискета **ASR**? В каких случаях она используется?

4.6.13 Какое расширение имеет файл архива системных данных?

4.6.14 Как можно свести к минимуму объем архивного файла?

4.6.15 Что такое «пул»?

4.6.16 Сколько существует типов архивов и в чем их особенности?

4.6.17 Назовите последовательность восстановления данных из архива при нестабильной работе системы?

4.6.18 Перечислите основные параметры восстановления системы из архива?

4.6.19 Приведите пример одного из дополнительных параметров восстановления?

4.6.20 Перечислите последовательность восстановления системы в случае ее отказа?

4.6.21 В чем особенности режима восстановления «Загрузка последней удачной конфигурации»?

4.6.22 В чем особенности режима восстановления **Safe Mode**?

4.6.23 Назовите последовательность восстановления с помощью архива **ASR**?

4.6.24 В каких случаях используется восстановление системы с помощью «Консоли восстановления»?

4.6.25 С помощью какой команды можно получить список команд консоли восстановления?

4.6.26 Перечислите последовательность стандартной переустановки **Windows XP**?

4.6.27 Какую папку необходимо скопировать при стандартной переустановке **Windows XP**, почему?

4.6.28 Как сохранить необходимые данные при переустановке **Windows XP**, если на компьютере только один логический диск?

4.6.29 В каких случаях рекомендуется переустановка **Windows** без драйверов?

4.6.30 Укажите последовательность переустановки **Windows** без драйверов.

5 Оптимизация Windows

5.1 Оптимизация дисков

Информация на логических дисках становится фрагментированной при создании и удалении файлов и папок, установки новых программ или загрузке файлов из **Internet**. Файлы и папки не обязательно хранятся операционной системой целиком в одном месте: они сохраняются в первом доступном месте диска. После того, как большая часть логического диска была использована для хранения файлов и папок, большинство файлов сохраняется в виде фрагментов, находящихся в разных частях диска. Оставшееся после удаления файлов и папок свободное место заполняется в произвольном порядке при сохранении новых файлов и папок.

Если диск содержит много фрагментированных файлов и папок, системе требуется большее время для обращения к ним, поскольку приходится выполнять дополнительные операции чтения с диска их отдельных частей. На создание файлов и папок также уходит больше времени, поскольку свободное пространство на диске состоит из разрозненных фрагментов. Системе приходится сохранять новые файлы и папки в разных местах тома.

Дефрагментацией называется процесс поиска и объединения фрагментированных файлов и папок.

Программа «Дефрагментация диска» перемещает разрозненные части каждого файла или папки в одно место тома, после чего файлы и папки занимают на диске единое последовательное пространство. В результате доступ к файлам и папкам выполняется эффективнее.

Объединяя отдельные части файлов и папок, программа дефрагментации также объединяет в единое целое свободное место на диске, что делает менее вероятной фрагментацию новых файлов.

В **Windows 98** выполнять дефрагментацию может любой пользователь. Однако в **Windows XP** осуществлять дефрагментацию могут только лица, обладающие правами администратора, поэтому, если пользователь работает под другой учетной записью или не является членом группы «Администраторы»,

ему необходимо предварительно загрузить систему под учетной записью «Администратор».

Для запуска программы дефрагментации следует нажать кнопку «Пуск», выбрать меню «Программы \ Стандартные \ Служебные», а затем команду «Дефрагментация диска».

Окно программы дефрагментации диска (рисунок 5.1) разделено на две основные области. В верхней части перечислены тома (логические диски) данного локального компьютера.

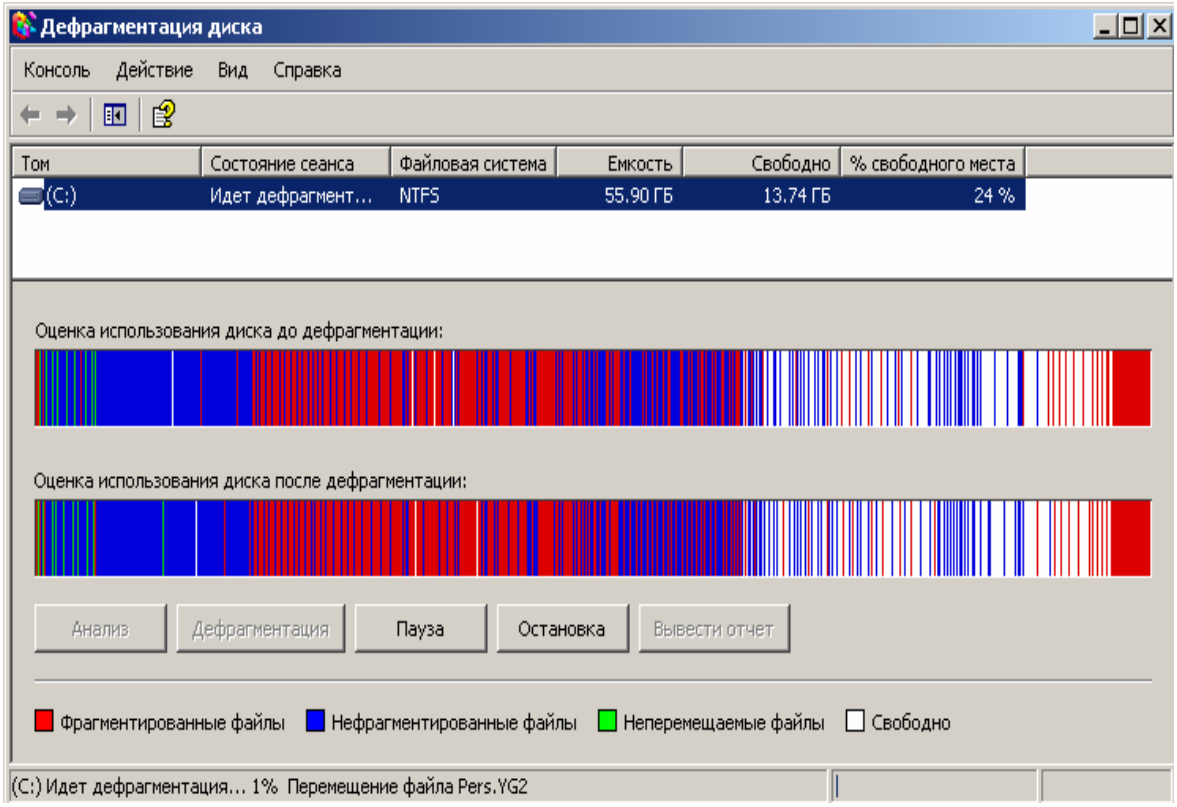


Рисунок 5.1 - Основное окно программы дефрагментации диска

В нижней части отображается графическое представление того, насколько фрагментирован диск. Цветами показываются состояния тома:

- красным отображаются фрагментированные файлы;
- синим в программе выводятся непрерывные (нефрагментированные) файлы;
- белым отображается свободное пространство тома;
- зеленым отмечаются системные файлы, которые не могут быть переме-

щены программой дефрагментации диска: эти системные файлы не являются частью операционной системы **Windows**, а принадлежат файловой системе.

Перед выполнением дефрагментации можно найти все фрагментированные файлы и папки, нажав кнопку «Анализ» и проанализировав выбранный логический диск. После проведения анализа отображается диалоговое окно с рекомендацией к действию. Анализ следует проводить регулярно, а дефрагментацию - только после соответствующей рекомендации программы дефрагментации диска. Полученные сведения позволят узнать, как много фрагментированных файлов и папок содержит том, и решить, следует ли выполнять дефрагментацию.

Для запуска процесса дефрагментации достаточно нажать на кнопку «Дефрагментация» в основном окне программы или в окне «Анализ завершен».

Время, необходимое для дефрагментации диска, зависит от нескольких факторов, в том числе от размера жесткого диска, числа файлов на диске, процента его фрагментации и доступных ресурсов системы.

Особое внимание следует обратить на то, что допускается дефрагментация логических дисков только локальной файловой системы и выполнение только одной процедуры дефрагментации диска одновременно.

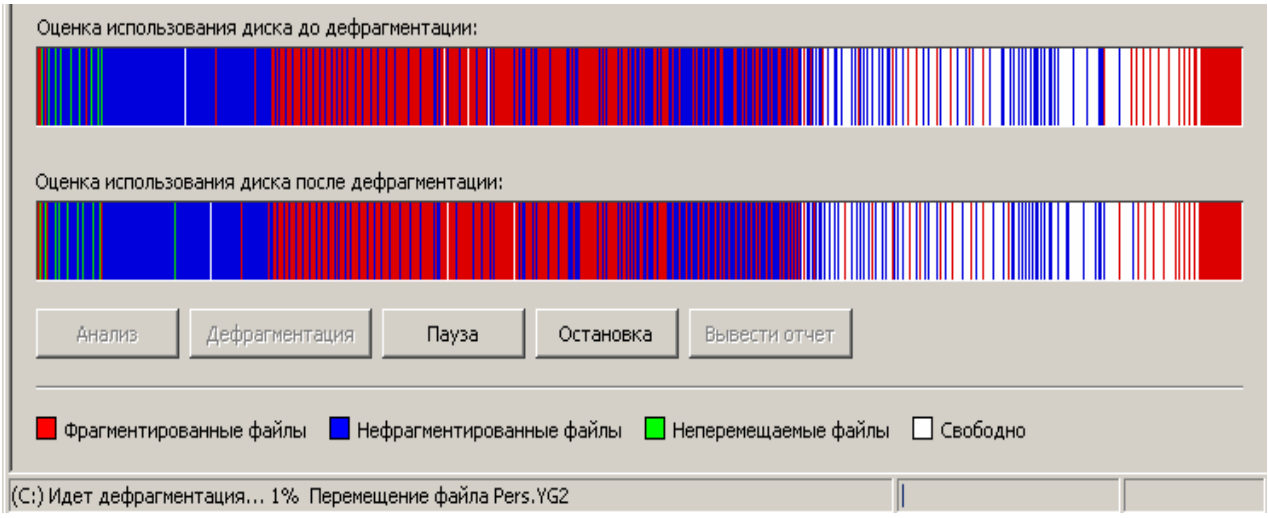


Рисунок 5.2 - Наглядное отображение работы программы дефрагментации дисков (до и после дефрагментации)

В областях «Результаты анализа» и «Результаты дефрагментации» (рису-

нок 5.2) можно увидеть степень улучшения в структуре тома после дефрагментации. Более подробную информацию о проанализированных файлах и папках можно получить, нажав кнопку «Вывести отчет» основного окна дефрагментации.

5.2 Советы по оптимизации Windows

5.2.1 Очистка диска

Одной из причин медленной работы системы может быть недостаточное количество свободного места на диске. При этом даже опытные пользователи иногда забывают вовремя очищать «Корзину», что может привести к «замусориванию» диска, если его объем сравнительно небольшой (до 10 Гб).

Другим, не менее «популярным» источником большого количества ненужных файлов являются папки для хранения временных файлов при работе в **Internet**. В **Windows 98** временные файлы **Internet** хранятся в каталоге C:\Windows\Temporary Internet Files, а в **Windows XP** - в каталоге C:\Documents and Settings\Имя_пользователя\Local Settings\Temporary Internet Files. При этом в случае достаточно интенсивной работы в **Internet** через пару месяцев объем этих папок будет составлять сотни мегабайт. Поэтому следует регулярно очищать указанные папки.

В **Windows** для очистки диска от этих и других ненужных файлов имеется стандартное средство, которое вызывается командой «Пуск \ Программы \ Стандартные \ Служебные \ Очистка диска».

При этом, при наличии на компьютере нескольких логических дисков, вначале появляется окно «Выбор диска», в котором выбирается подлежащий очистке диск.

Затем программой очистки автоматически производится анализ объема дискового пространства, которое может быть освобождено (рисунок 5.3).

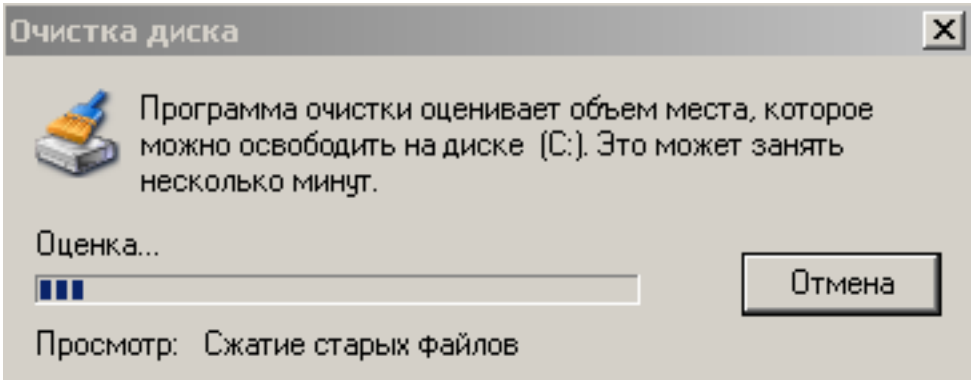


Рисунок 5.3 - Анализ объема дискового пространства, которое можно освободить

Результаты проведенного анализа отображаются в отдельном окне (рисунок 5.4), в котором показан список категорий удаляемых файлов.

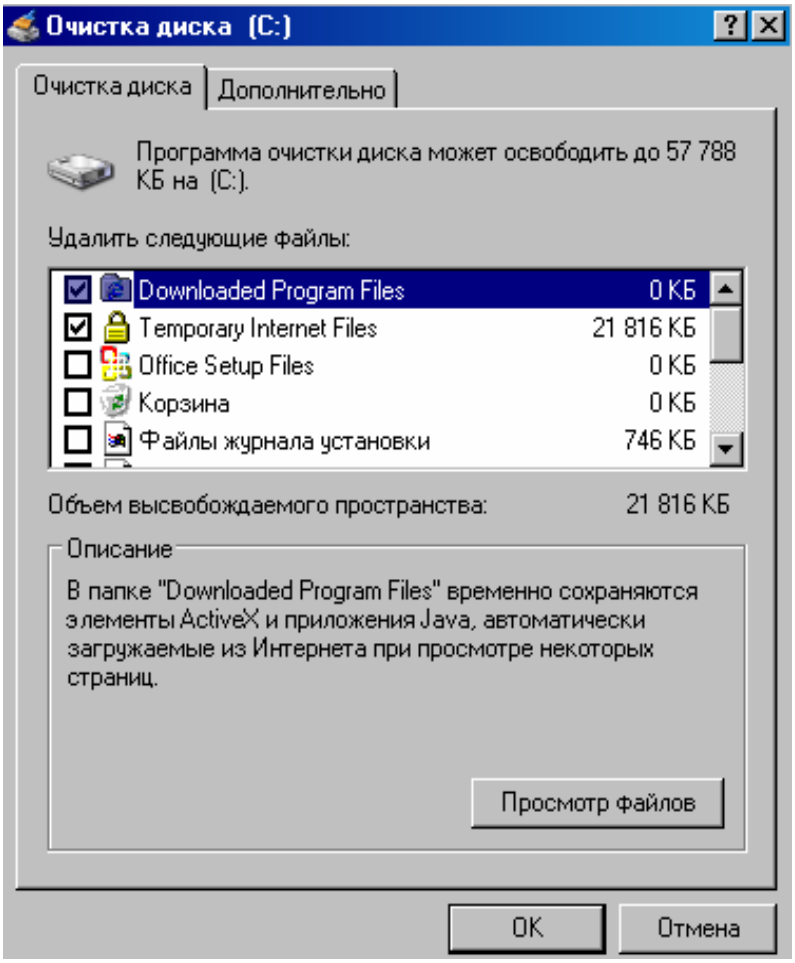


Рисунок 5.4 - Выбор категорий файлов, подлежащих удалению

Ниже приведено описание наиболее важных категорий:

- «Temporary Internet Files» - хранит файлы посещенных Web-страниц

(прежде всего рисунки) для быстрого просмотра;

- «Корзина» - содержит файлы, удаленные в «Корзину»;
- «Восстановление системы» - позволяет удалить старые контрольные точки восстановления системы;
- «Временные файлы» – позволяет удалить ненужные временные файлы. В **Windows** имеется специальная папка **Temp**, где различные программы хранят временную информацию, которая обычно автоматически удаляется при их закрытии. Если какие-то временные файлы содержатся в папке **Temp** больше недели, их можно удалить.

Пользователь может выбрать те категории файлов, которые действительно необходимо удалить, установив рядом с ними флажки. Процедура удаления ненужных файлов запускается нажатием кнопки «**ОК**». При этом будет выведено окно, иллюстрирующее процесс удаления файлов на выбранном диске.

«Точки восстановления системы» - это очень полезное средство **Windows XP**, однако каждая из них занимает на диске значительное место (несколько десятков или даже одну-две сотни мегабайт).

В том случае, если пользователь хочет удалить все точки восстановления, оставив лишь одну (последнюю), следует раскрыть закладку «Дополнительно» в окне «Очистка диска» и в разделе «Восстановление системы» нажать кнопку «Очистить» (рисунок 5.5).

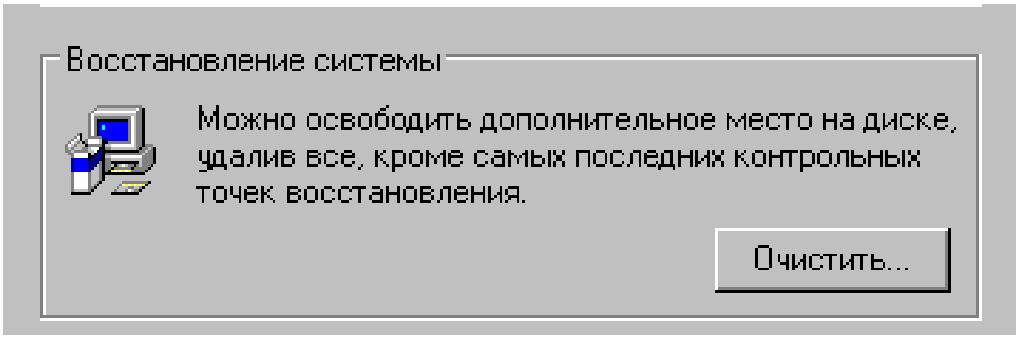


Рисунок 5.5 - Удаление всех точек восстановления, кроме последней

5.2.2 Параметры виртуальной памяти

Windows позволяет задавать объем виртуальной памяти (так называемый «файл подкачки», или **swap-файл**), которая используется процессором в качестве временного хранилища для выполнения программ, превышающих размер доступной оперативной памяти. То есть если для данных какой-либо программы отсутствует свободное место в оперативной памяти, они сохраняются в «файлах подкачки».

Чтобы установить параметры виртуальной памяти, вначале следует вызвать диалоговое окно «Свойства системы» - проще всего одним из указанных ниже способов:

- щелчком правой кнопкой мыши на ярлыке «Мой компьютер» и выбором команды «Свойства»;
- сочетанием клавиш **Win+Pause**.

Далее нужно раскрыть закладку «Дополнительно», где в разделе «Быстродействие» нажать кнопку «Параметры» (рисунок 5.6).

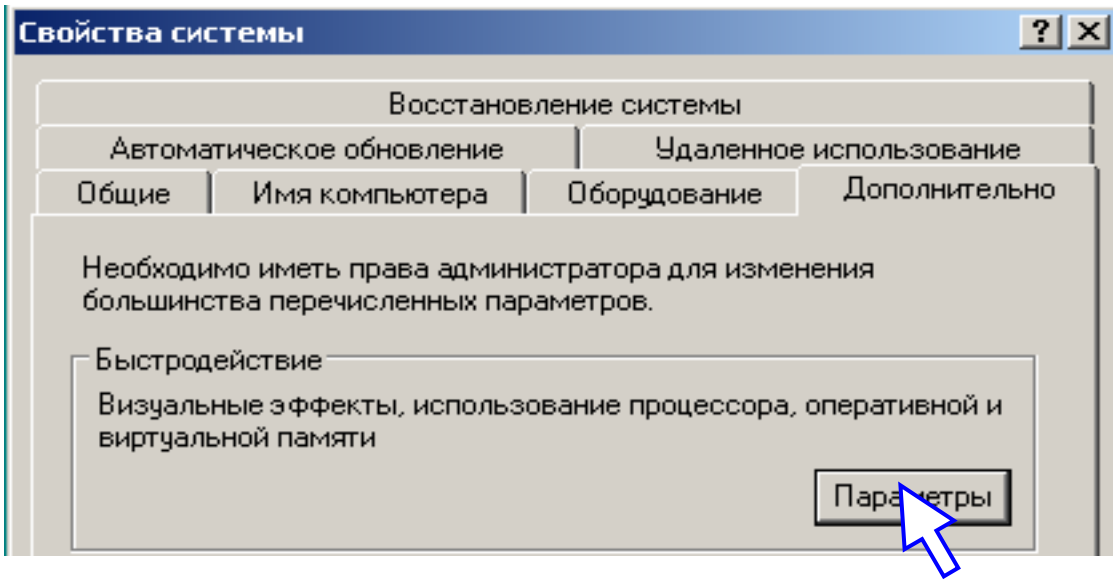


Рисунок 5.6 - Установка параметров быстродействия системы

После этого раскроется окно «Параметры быстродействия», в котором также следует выбрать закладку «Дополнительно». Здесь имеется раздел «Виртуальная память», в котором нужно нажать кнопку «Изменить» (рисунок 5.7).

В результате откроется окно «Виртуальная память» (рисунок 5.8). В нем необходимо выделить название того логического диска, на котором будет изменяться «файл подкачки» (в данном случае – диск **C:**). При этом во всех полях отобразятся соответствующие параметры «файла подкачки» именно для этого диска.

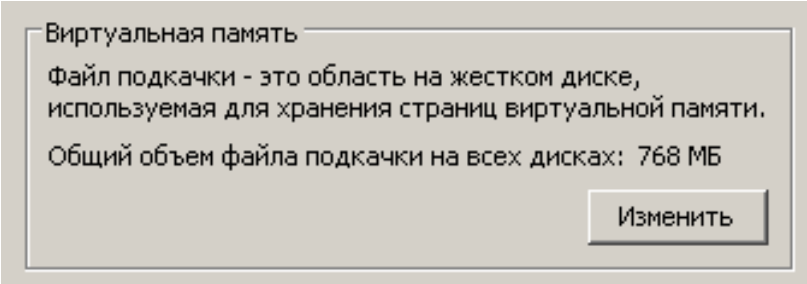


Рисунок 5.7 - Изменение параметров виртуальной памяти

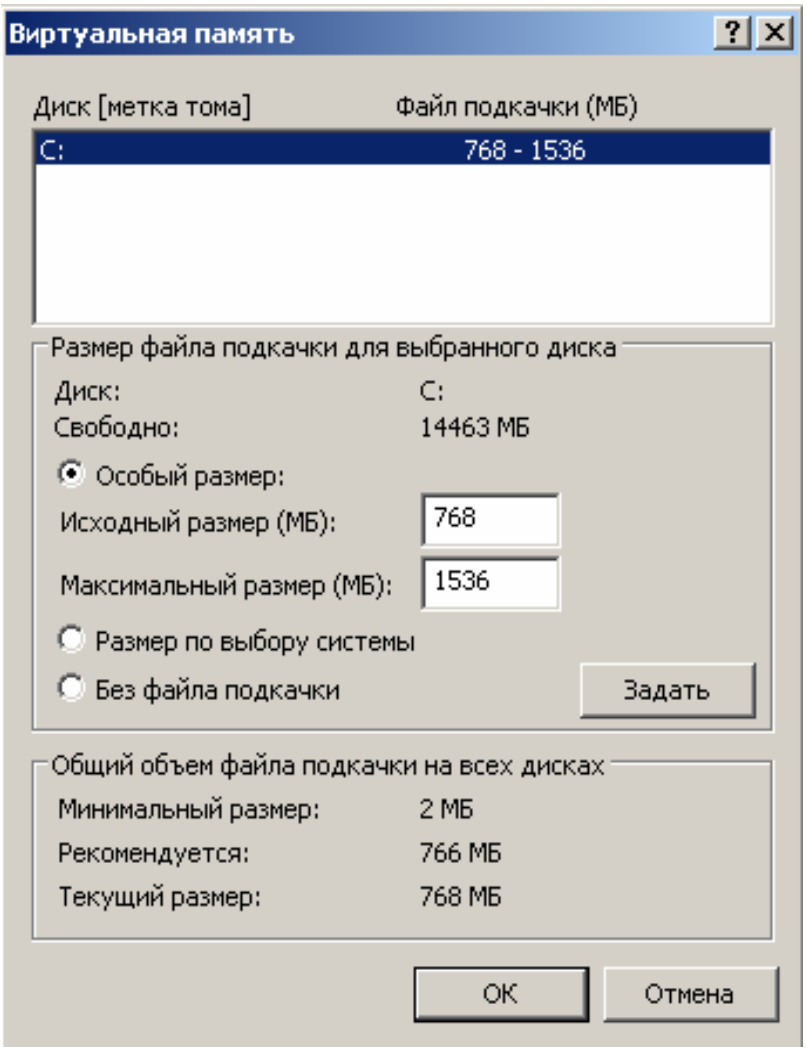


Рисунок 5.8 - Установка размеров и расположения «файла подкачки»

Чтобы установить другой размер «файла подкачки», нужно выбрать переключатель «Особый размер» и задать значения в полях «Исходный размер» (Мб) и «Максимальный размер» (Мб).

Рекомендуется задавать эти значения одинаковыми и равными 512 Мб. Если же указать границы, в которых размер «файла подкачки» сможет изменяться, то очень скоро возникнет эффект фрагментации, что существенно замедлит процедуру обращения системы к «файлу подкачки» и снизит общую производительность.

Если будет выбран переключатель «Размер по выбору системы», то автоматически будет предложен размер «файла подкачки», в 1,5 раза превышающий объем оперативной памяти (ОЗУ – оперативного запоминающего устройства).

Наконец, выбор варианта «Без «файла подкачки» позволяет убрать «файл подкачки» для данного логического диска. Это вариант следует использовать, если «файл подкачки» будет располагаться на другом диске.

Полностью же убирать «файл подкачки» со всех дисков можно только в том случае, когда на компьютере установлено, по крайней мере, 512 Мб ОЗУ (а лучше - 1024 Мб). Тогда можно с определенной долей уверенности предполагать, что система справится с обработкой всех данных, обходясь только оперативной памятью, без подключения виртуальной.

Фиксация установленных значений осуществляется кнопкой «Задать», после чего можно перейти к выбору параметров «файла подкачки» для другого диска.

Существуют различные рекомендации по поводу размера и расположения «файла подкачки». Например, разработчики **Microsoft** рекомендуют задавать его объемом в 1,5 раза больше, чем объем оперативной памяти, и располагать не на том логическом диске, на котором находятся системные файлы. Однако и первое, и второе утверждение верно далеко не всегда.

Что касается размера «файла подкачки», то он зависит от объема установленной на компьютере оперативной памяти. При этом следует «отталкиваться» от объема памяти в 512 Мб, что является на данный момент своеобразным оп-

тимумом для домашнего ПК.

Итак, если на компьютере установлено 512 Мб ОЗУ, то «файлу подкачки» также можно задать размер 512 Мб. Если же объем ОЗУ составляет всего 256 Мб, то в этой ситуации целесообразно установить «файлу подкачки» в 2 раза больший объем, т.е. 512 Мб.

Вообще говоря, задание слишком большого объема «файла подкачки» может так же негативно сказаться на быстродействии системы, как и установка малого объема. Дело в том, что **Windows** постоянно выполняет оптимизацию «файла подкачки» - аналог дефрагментации диска, поэтому дефрагментация большего объема памяти, очевидно, будет забирать больше системных ресурсов.

Исходя из всего вышесказанного, можно порекомендовать в любом случае подбор размера «файла подкачки» начинать с 512 Мб, а затем экспериментировать с его увеличением или уменьшением, контролируя быстродействие системы с помощью специальных тестов (например, **3DMark**).

Что касается расположения «файла подкачки», его следует размещать на том логическом диске, который менее подвержен изменениям. При этом **ни в коем случае не следует располагать файлы подкачки на разных логических дисках** (например, 256 + 256), т.к. это существенно снизит быстродействие системы.

В качестве примера рассмотрим стандартную конфигурацию: на диске **C:** размещается система и все прикладные программы, а на диске **D:** располагаются данные, устанавливаются игры, содержатся файлы с фильмами и музыкой.

Может показаться, что диск **C:** изменяется наиболее интенсивно. Однако если все основные программные средства (офисные программы, графические пакеты, переводчики и пр.) уже проинсталлированы, то целесообразно разместить «файл подкачки» именно на диске **C**:, после чего выполнить дефрагментацию (см. выше) этого диска. В этом случае расположение «файла подкачки» будет наиболее оптимальным.

5.2.3 Настройка Рабочего стола

На компьютерах с небольшим объемом ОЗУ (не выше 64 Мб) и с малопроизводительным процессором (не выше **Pentium II**) одним из элементов, существенно «отнимающих» память, является картинка на **Рабочем столе** (занимает примерно 2 Мб ОЗУ).

Фон «Рабочего стола» задается в свойствах экрана («Панель управления \ Экран») на вкладке «Рабочий стол» для **Windows XP** (рисунок 5.9) или на вкладке «Фон» (для **Windows 98**).

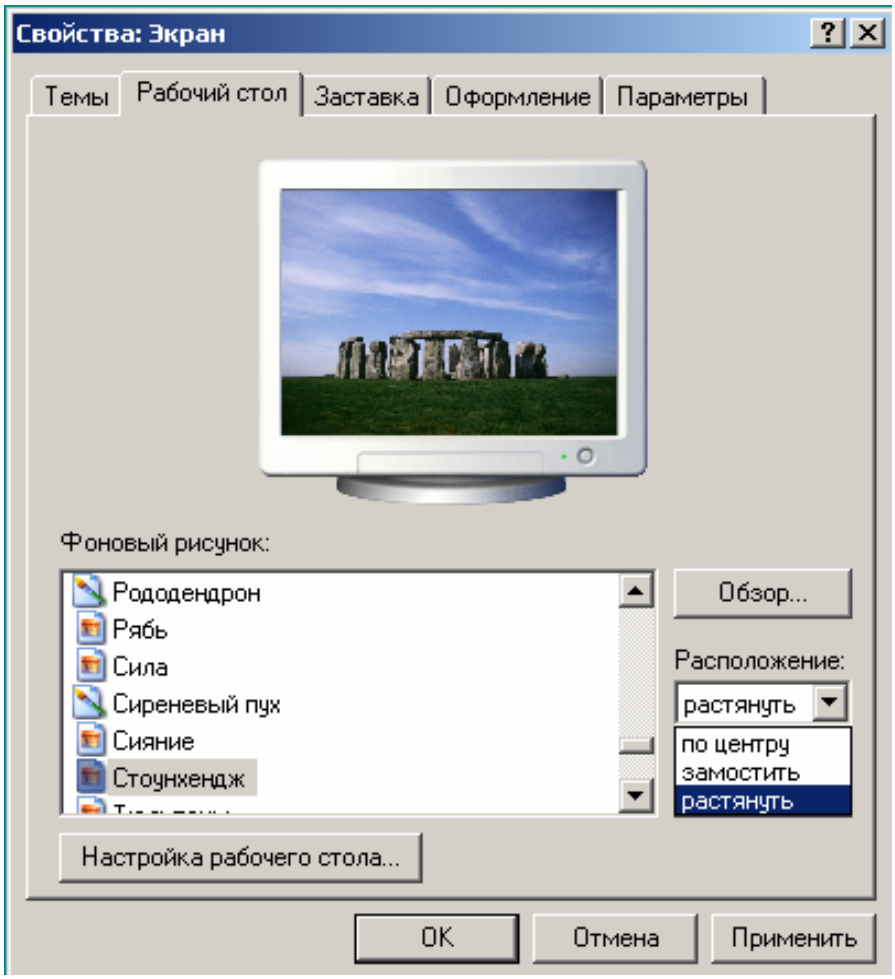


Рисунок 5.9 - Установка фонового рисунка для «Рабочего стола»

При этом самым худшим (в смысле быстродействия) является настройка расположения «растянуть», задавать которую крайне нежелательно. Таким образом, **если объем ОЗУ составляет более 128 Мб (для Windows 98) либо 256 Мб (для Windows XP), то можно украсить свой «Рабочий стол» фоновым**

рисунком. В противном же случае лучше воздержаться от этого, выбрав из списка «Фоновый рисунок» вариант «(Нет)».

Еще одной причиной, по которой производительность системы значительно снижается, является **чрезмерное количество ярлыков** на «Рабочем столе». Здесь необходимо руководствоваться тем соображением, что чем меньше элементов на «Рабочем столе», тем лучше.

5.2.4 Визуальные эффекты

Внешне **Windows XP** выглядит намного красивее любой из своих предшественниц. Здесь реализовано анимированное раскрытие меню, отображение тени для указателя мыши и диалоговых окон, возможность сглаживания шрифтов. Однако указанные эффекты значительно снижают быстродействие системы.

Выбор тех или иных эффектов задается в окне свойств экрана («Панель управления \ Экран»), в котором на вкладке «Оформление» имеется кнопка «Эффекты», нажатие на которой приводит к отображению одноименного диалогового окна (рисунок 5.10).

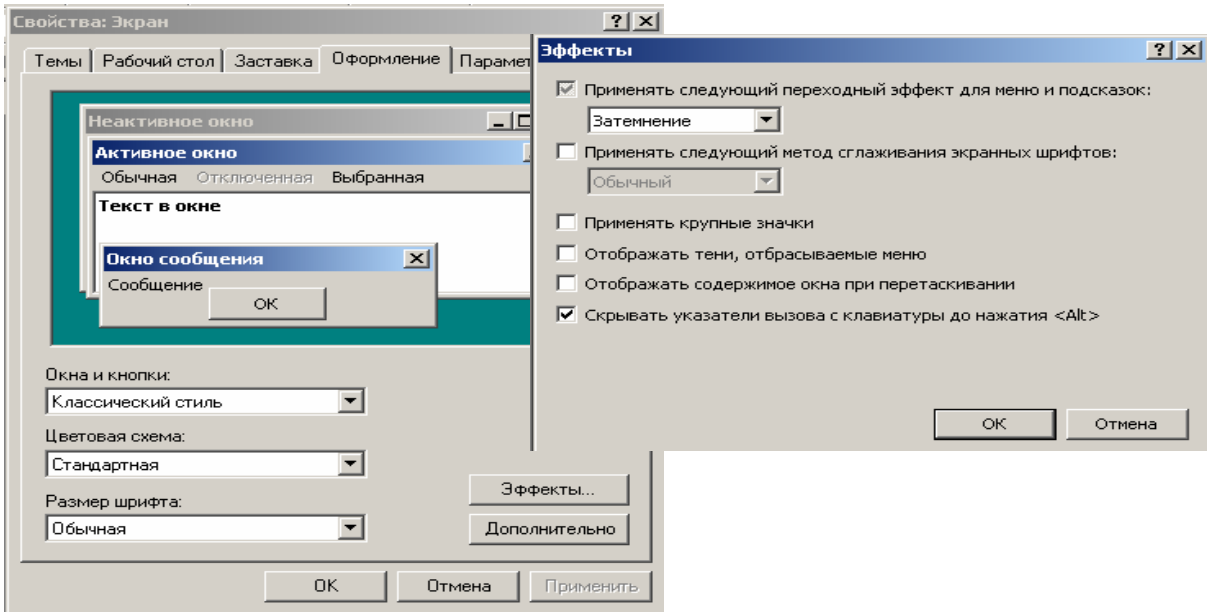


Рисунок 5.10 - Установка графических эффектов

Для повышения быстродействия целесообразно убрать все предлагаемые

эффекты:

 переходный эффект для меню и всплывающих подсказок («Затемнение» или «Развертывание»);

 применение метода сглаживания экранных шрифтов («Обычный» – для настольных мониторов; **«ClearType»** – для портативных компьютеров и других мониторов с плоским экраном);

 применение крупных значков для отображения файлов, папок и ярлыков на «Рабочем столе»;

 отображение теней, отбрасываемых раскрытыми меню;

 отображение содержимого окна при его перетаскивании по экрану;

 скрытие указателей вызова с клавиатуры до нажатия клавиши <**Alt>**.

Продолжить настройку графического интерфейса **Windows** можно с помощью диалогового окна «Свойства системы», которое проще всего вызвать сочетанием клавиш <**Win+Pause>** (подраздел «Параметры виртуальной памяти»). Далее на закладке «Дополнительно» нужно в разделе «Быстродействие» нажать кнопку «Параметры».

Появится окно «Параметры быстродействия», где необходимо активизировать закладку «Визуальные эффекты» (рисунок 5.11).

Здесь имеется целый ряд визуальных эффектов (анимация икон, отображение теней для меню, указателя мыши и значков на «Рабочем столе»; сглаживание экранных шрифтов и т.д.); некоторые из них повторяют рассмотренные выше, в окне «Эффекты».

Для того чтобы система работала максимально быстро, следует отключить все визуальные эффекты. Проще всего это сделать, выбрав переключатель «Обеспечить наилучшее быстродействие».

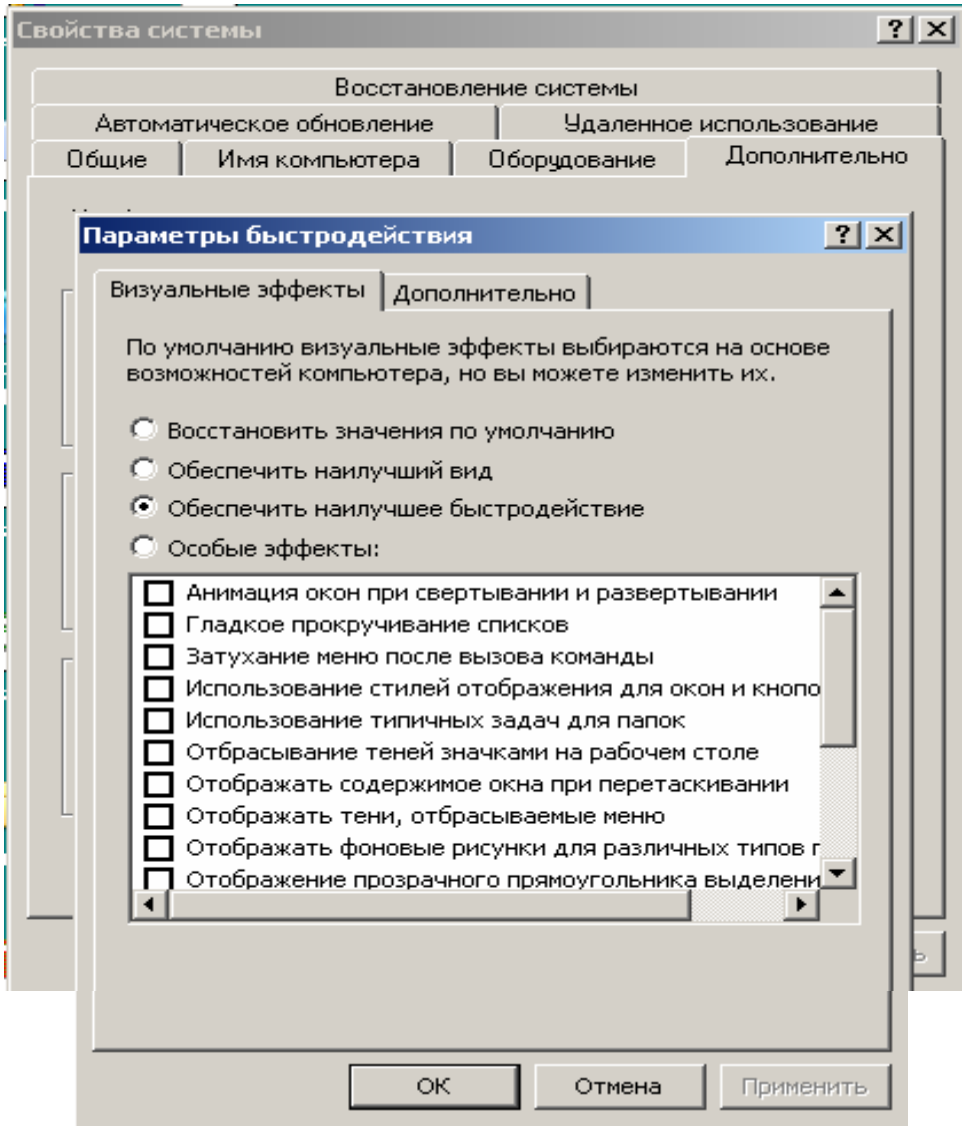


Рисунок 5.11 - Отмена визуальных эффектов для повышения быстродействия

5.2.5 Отключение всех звуков Windows

Но умолчанию **Windows** сопровождает различные события (вход и выход из **Windows**, открытие и закрытие программ, завершение работы **Windows**, сообщение об ошибке и др.) соответствующими звуками.

Поскольку в настоящее время у многих пользователей во время работы на компьютере постоянно работает какой-либо музыкальный проигрыватель (как правило, это **Winamp**), слышать параллельное озвучивание системных событий мало кому покажется привлекательным. Поэтому системные звуки **Windows** лучше отключить.

Для выбора соответствующей звуковой схемы используется окно звуков и аудиоустройств («Панель управления \ Звуки и аудиоустройства»), в котором на закладке «Звуки» имеется раскрывающийся список «Звуковая схема». Здесь следует выбрать вариант «Нет звуков», как показано на рисунке 5.12.

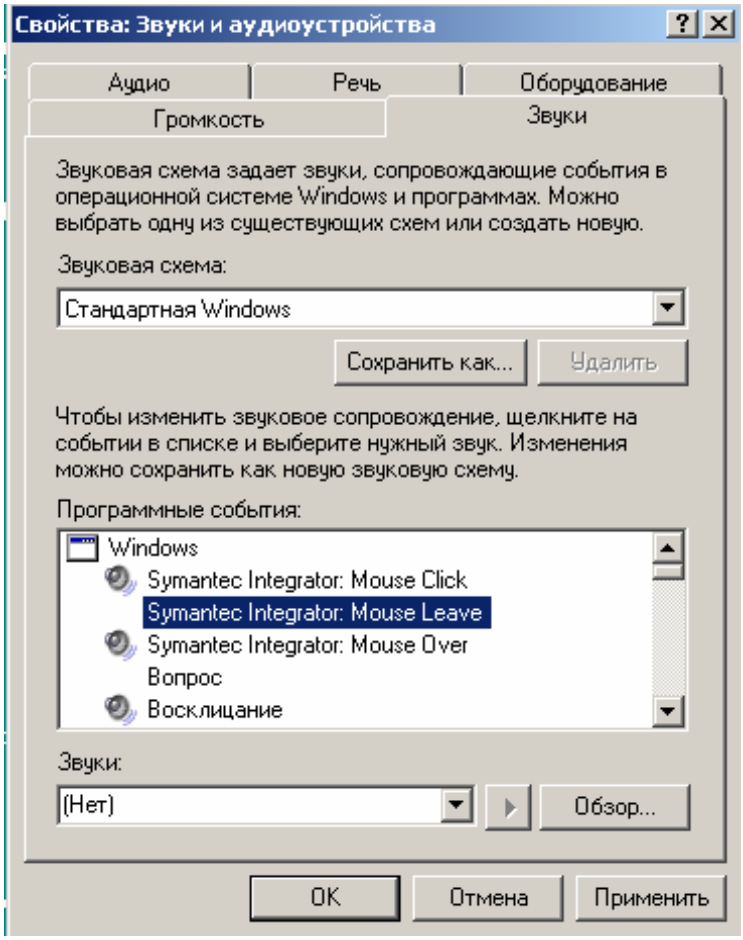


Рисунок 5.12 - Отмена звукового сопровождения системных событий

5.2.6 Удаление лишних шрифтов

Если в системе установлено много шрифтов (порядка сотни), это негативно скажется на быстродействии системы, т.к. **Windows** загружает их все в оперативную память.

Конечно, есть шрифты, которые устанавливаются автоматически при инсталляции тех или иных прикладных программ. Однако многие пользователи дополнительно устанавливают понравившиеся шрифты из коллекций на компакт-дисках. Если таких шрифтов несколько, то работа системы существенно не замедлится. Но если, например, установить из коллекции все шрифты (как

бы «на всякий случай»), а их там может быть несколько сотен, то очень скоро станет заметно замедление работы **Windows**.

Установка и удаление шрифтов производится в разделе «Шрифты» «Панели управления».

5.3 Редактирование списка автозагрузки

Во всех версиях **Windows**, начиная с **Windows 98**, имеется утилита «Настройка системы» (**msconfig.exe**), которую проще всего запустить командой «Пуск \ Выполнить», указав в поле «Открыть» строку «**msconfig**» (рисунок 5.13).

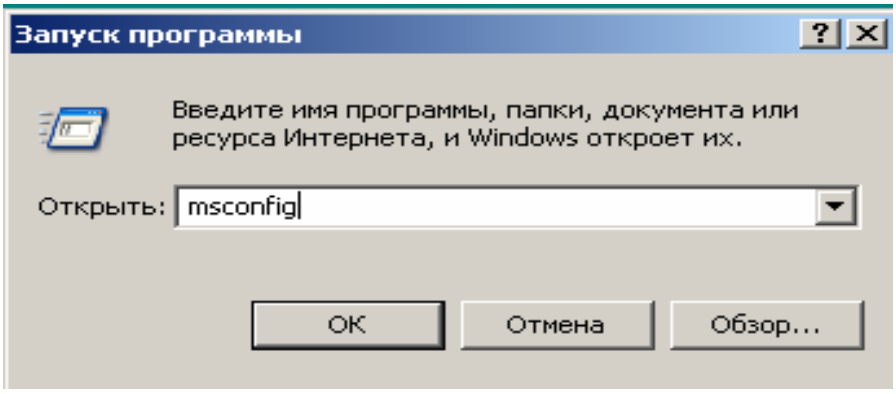


Рисунок 5.13 - Запуск программы **msconfig.exe**

Окно «Настройка системы» содержит такие закладки (рассмотрим версию **Windows XP**):

– «Общие» - выбор варианта запуска **Windows** (обычный, диагностический или выборочный);

– «SYSTEM.INI» - содержимое файла **system.ini**, в **Windows XP** добавлено для совместимости с предыдущими версиями;

– «WIN.INI» - содержимое файла **win.ini**, в **Windows XP** добавлено для совместимости с предыдущими версиями;

– «Службы» - список служб **Windows XP**, позволяет включать и отключать загружаемые службы;

– «Автозагрузка» - список программ, автоматически загружаемых при запуске **Windows**.

Закладка «Автозагрузка» (рисунок 5.14) является наиболее полезной и позволяет убрать из списка автозагрузки ненужные программы (например, **Windows Messenger** - элемент **msmsgs**).

При этом никаких глобальных изменений в системе не происходит и выбранная программа не удаляется, но после перезагрузки системы эта программа уже не будет автоматически загружаться и занимать память. С другой стороны, если пользователь по ошибке уберет из списка автозагрузки какую-то системную программу, то он всегда может исправить положение, снова отметив ее в окне «Настройка системы».

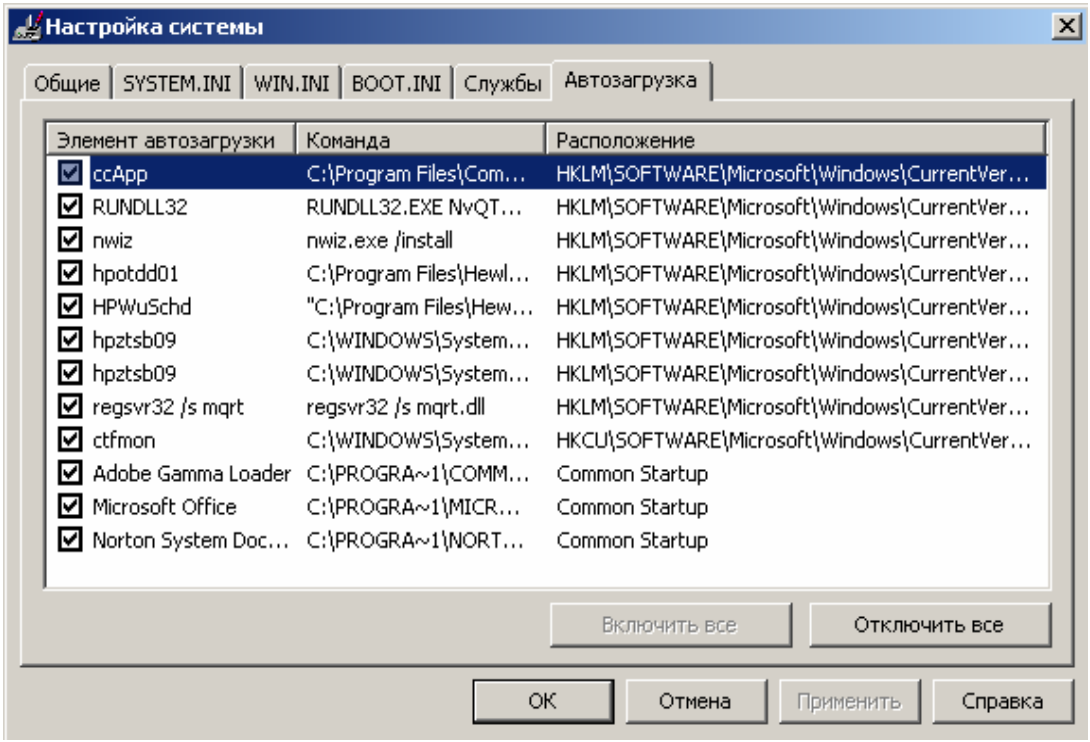


Рисунок 5.14 - Список автозагрузки **Windows XP** в окне утилиты **msconfig.exe**

5.4 Удаление скрытых компонентов Windows

При инсталляции **Windows** устанавливает некоторые компоненты (такие как **Windows Messenger**) по умолчанию, и их достаточно проблематично удалить. Дело в том, что эти компоненты не отображаются в списке установленных программ («Панель управления \ Установка и удаление программ»). Можно с уверенностью сказать, что многие пользователи были бы рады не только убрать **Windows Messenger** из списка автозагрузки, но и вообще удалить его из

системы.

Для того чтобы **Windows Messenger** и другие аналогичные скрытые программы отобразились в окне «Установка и удаление программ», необходимо определенным образом отредактировать файл **sysoc.inf**, находящийся в каталоге C:\Windows\Inf.

Итак, открываем файл **sysoc.inf** двойным щелчком (рисунок 5.15) и ищем заголовок **Components**, после которого следует ряд параметров различных приложений.

Для некоторых из этих параметров указывается ключевое слово **hide** (от англ. **hide** - скрыть). Теперь необходимо найти параметры требуемых приложений и убрать слово **hide**.

Например, строка параметров для **Windows Messenger** выглядит следующим образом:

msmsgs=msgrocm.dll,OcEntry,msmsgs.inf,hide,7

Эта же строка, но без ключевого слова **«hide»**, будет иметь следующий вид:

msmsgs=msgrocm.dll,OcEntry,msmsgs.inf,,7

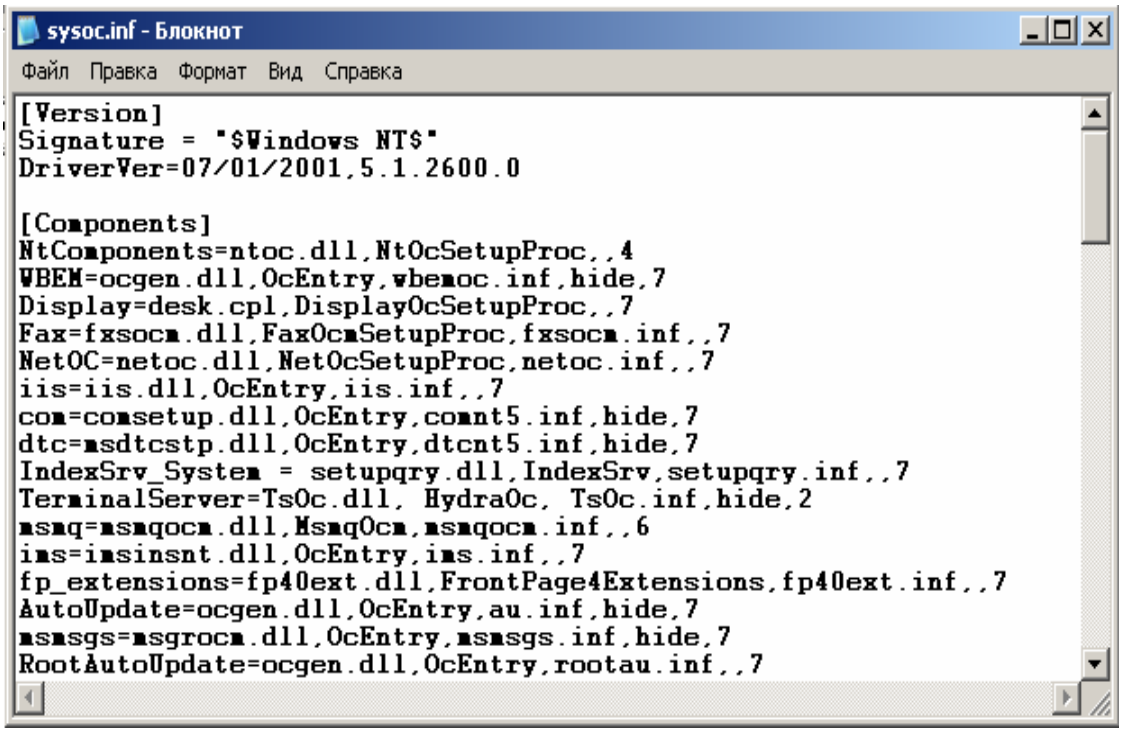


Рисунок 5.15 - Фрагмент файла **sysoc.inf**

После того как изменения в файле **sysoc.inf** будут сохранены, следует открыть окно «Установка и удаление программ» и нажать в нем кнопку «Установка компонентов Windows». В результате отобразится список установленных компонентов **Windows XP**, среди которых будет и **Windows Messenger** (рисунок 5.16).

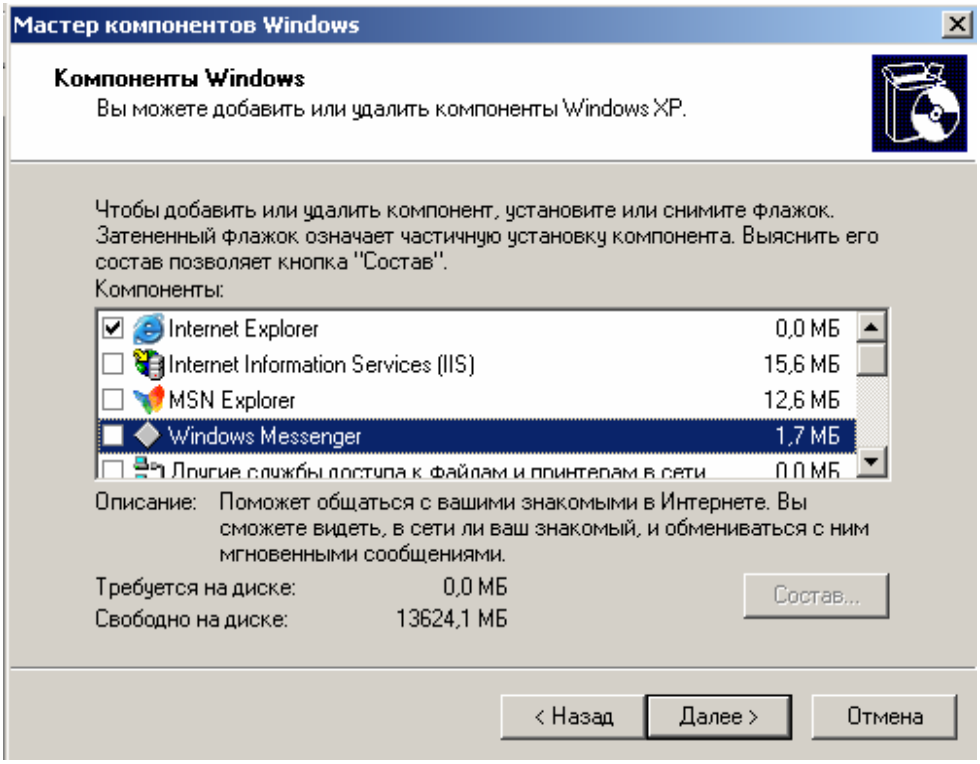


Рисунок 5.16 - Удаление скрытого компонента **Windows Messenger**

Для удаления этого компонента достаточно снять рядом с ним флажок и нажать «Далее». Аналогичным образом можно отобразить (с возможностью удаления) и другие скрытые компоненты **Windows**.

5.5 Утилита для настройки Windows XP Tweaker

Одной из популярных утилит настройки компьютера является **XP Tweaker** (рисунок 5.17), которую можно бесплатно загрузить с сайта **http://www.xptweaker.narod.ru**. Эта программа очень удобна в работе и обладает красивым русскоязычным интерфейсом. Кроме этого, она изменяет конфигурацию операционной системы только путем модифицирования реестра, что

делает не обязательным ее загрузку при запуске компьютера.

Для установки **XP Tweaker** необходимо загрузить файл **xpt140b57.zip**, а затем распаковать его во временный каталог. При распаковке архива во временном каталоге будет создан файл **XPTweakerSetup.exe**, который и следует запустить для установки программы.

После запуска программы будет отображено окно, показанное на рисунке 5.17, а также окно **Registry console** (рисунок 5.18), которое предназначено для отображения изменений, вносимых программой в реестр операционной системы.

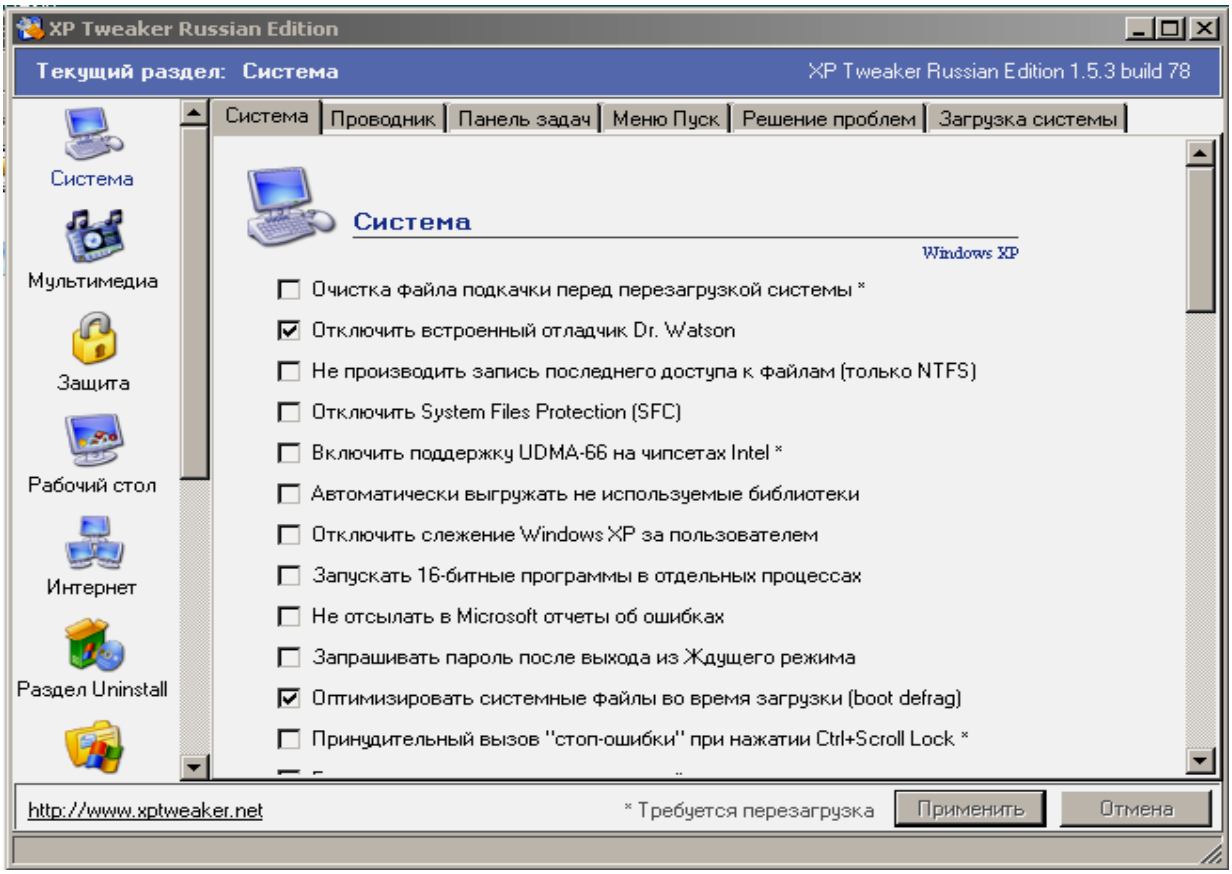


Рисунок 5.17 - Окно программы **XP Tweaker**

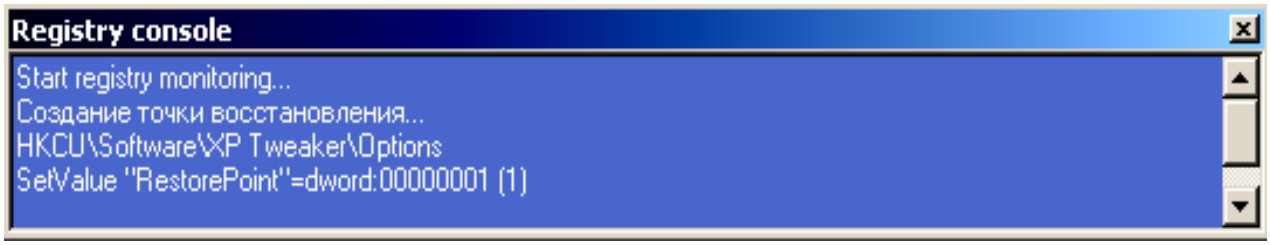


Рисунок 5.18 - Окно **Registry console**

Хотя программа предназначена для настройки всей операционной системы, в нее включены возможности по конфигурированию безопасности. Для настройки параметров безопасности необходимо перейти в раздел **Защита** и установить требуемые параметры защиты компьютера.

Следует отметить, что программа разрабатывалась специально для **Windows XP**. поэтому авторы не гарантируют ее корректную работу в других операционных системах семейства **Windows**.

Программа **XP Tweaker** разработана русским программистом, снабжена очень подробной справочной системой и, естественно, имеет русскоязычный интерфейс.

5.6 Контрольные вопросы

5.6.1 Что понимается под оптимизацией логических дисков компьютера?

5.6.2 Что понимается под дефрагментацией диска?

5.6.3 Из-за чего возникает фрагментация диска?

5.6.4 Как запустить программу дефрагментации диска в **Windows XP**?

5.6.5 Что может быть причиной медленной работы компьютера?

5.6.6 В чем состоит работа утилиты очистки диска, что соответствует термину **Temporary Internet Files**?

5.6.7 Какие категории файлов удаляются в процессе очистки диска?

5.6.8 В какой папке хранятся временные файлы?

5.6.9 Для чего используются временные файлы?

5.6.10 Как можно удалить "лишние" точки восстановления системы?

5.6.11 Что понимается под виртуальной памятью компьютера и для чего она используется?

5.6.12 Как можно изменить параметры **swap-файла**?

5.6.13 Какой размер файла подкачки устанавливается автоматически?

5.6.14 Какие существуют рекомендации по установлению размеров **swap-файла**?

5.6.15 К каким негативным последствиям может привести задание слишком большого объема «файла подкачки»?

5.6.16 Можно ли располагать «файлы подкачки» на разных логических дисках, почему?

5.6.17 Какие настройки **Windows**, влияющие на быстродействие системы, Вы знаете?

5.6.18 Как влияют на быстродействие компьютера настройки «Рабочего стола» **Windows**?

5.6.19 Как влияют на быстродействие компьютера визуальные эффекты, звуки **Windows**, лишние шрифты?

5.6.20 Как отключить визуальные эффекты, звуки **Windows**, удалить лишние шрифты?

5.6.21 Как называется утилита настройки системы в **Windows**?

5.6.22 Какие закладки содержит окно «Настройка системы» **Windows XP**?

5.6.23 Что представляет собой список «Автозагрузка» **Windows** и как его можно отредактировать?

5.6.24 Какие компоненты **Windows** называются скрытыми?

5.6.25 В каком файле хранятся параметры скрытых компонентов **Windows**?

5.6.26 Как можно удалить скрытые компоненты **Windows**?

5.6.27 Какие утилиты для настройки компьютера Вы знаете?

5.6.28 Какие особенности имеет утилита **XP Tweaker**?

5.6.29 Где можно взять и как можно установить **XP Tweaker** на домашний компьютер?

5.7 Задание для самостоятельного выполнения

Установите утилиту **XP Tweaker** на домашний компьютер и изучите её возможности.

6 Базовые сведения о реестре Windows

Большинство компьютерных вирусов, применяемых злоумышленниками для получения контроля над ПК, используют реестр операционной системы **Windows** для перехвата некоторых системных функций или для автоматической загрузки тела вируса при включении компьютера. Кроме того, злоумышленник может удалить некоторые (или все) файлы реестра, что приведет к полной неработоспособности компьютера, или скопировать их к себе на компьютер, что даст ему возможность подобрать пароли к учетным записям пользователей.

Однако умелое использование реестра позволит администратору компьютера не только защитить ПК от несанкционированных действий пользователей, но и существенно упростит и ускорит настройку рабочей станции.

Из вышесказанного следует, что изучение реестра, правильное его использование, а также тонкая настройка системы с его применением, позволят свести к минимуму вероятность «взлома» компьютера.

6.1. Назначение и структура реестра

6.1.1 Назначение реестра

Реестр операционной системы **Windows** представляет собой базу данных различных настроек и параметров ОС, а также настроек приложений, которые установлены на компьютере.

Все операционные системы и приложения обладают различными параметрами, которые используются при работе с ними. В ранних версиях операционной системы **Windows** такие настройки хранились в **INI-файлах**. Эти файлы требовались для обеспечения корректной работы операционной системы, приложений и аппаратных устройств, но управление ими было сложной и трудоемкой задачей. Кроме этого, **INI-файлы** имеют ряд существенных недостатков. В частности:

а) размер таких файлов не может быть больше 64Кб;

б) число конфигурационных файлов как самой операционной системы, так и прикладных программ на жестком диске может достигать нескольких сотен, что затрудняет управление ими;

в) **INI-файлы** могут быть отредактированы в любом текстовом редакторе.

Последнее является большим пробелом в системе безопасности, поскольку пользователь может случайно или удалить **INI-файл**, или изменить прописанные в нем параметры. В свою очередь, такие действия могут привести к краху системы.

Исходя из этого, корпорация **Microsoft** при разработке операционной системы **Windows NT 3.5** приняла решение заменить **INI-файлы** на специальную структуру, которая обеспечивала бы эффективное управление средой **Windows**.

Следует отметить, что практически все версии **Windows** (кроме **Windows 3.1**) имеют схожий реестр, однако имеется ряд существенных отличий, основным из которых является организация корневых разделов.

Windows 98 хранит реестр в двух файлах - **system.dat** и **user.dat**, находящихся в каталоге, в который была установлена операционная система.

Реестр операционных систем **Windows NT** хранится в нескольких файлах, которые находятся в каталогах

Для **Windows NT 4.0**:

– **%SystemRoot%\System32\Config**;

– **%SystemRoot%\Profiles\Username**.

Для **Windows 2000/XP**:

– **%SystemRoot%\System32\Config**;

– %**SystemDrive%\Documents and Settings\Username**.

Здесь **%SystemRoot%** представляет собой каталог, в который была установлена операционная система, а **%SystemDrive%** - системный диск.

Структура реестра является иерархической (рисунок 6.1), т.е. представляет собой некоторое дерево, которое включает пять основных ветвей.

В свою очередь, каждая ветвь содержит элементы данных, которые назы-

ваются параметрами (**value entries**), а также вложенные разделы (**subkeys**). Просмотр и редактирование реестра осуществляется программой **Regedit**, описание которой приведено ниже, в разделе «Программа **Regedit**».

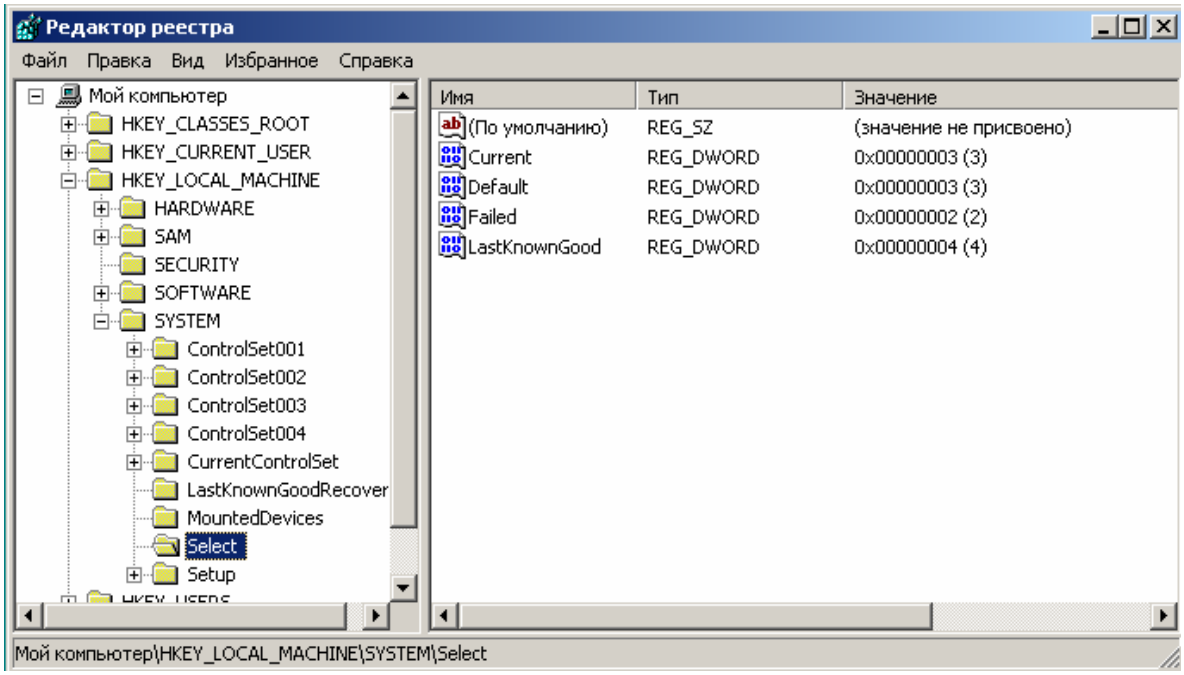


Рисунок 6.1 - Иерархическая структура реестра

6.1.2 Корневые разделы реестра

HKEY_LOCAL_MACHINE – данный раздел хранит общую информацию о компьютере и операционной системе. В разделе содержится информация о физических устройствах, установленных на компьютере, и их драйверах. Также данный раздел реестра используется операционной системой при загрузке компьютера. Информация, хранящаяся в этом разделе, оказывает влияние на все профили пользователей, существующие на компьютере.

HKEY_CLASSES_ROOT – в этом разделе заключена информация о типах файлов и ассоциациях между приложениями и типами файлов (по расширениям файла). Раздел также хранит информацию **OLE (Object Linking and Embedding**), ассоциированную с объектами **COM**, а также данные по ассоциациям файлов и классов.

HKEY_CURRENT_CONFIG – раздел содержит информацию о текущей аппаратной конфигурации компьютера. Аппаратная конфигурация объединяет

в себе набор изменений, которые были внесены в стандартную конфигурацию служб и устройств, определенную данными разделов **Software** и **System** корневого раздела **HKEY_LOCAL_MACHINE**.

HKEY_CURRENT_USER – этот раздел отвечает за хранение данных о профиле пользователя, который работает с компьютером в настоящее время. В нем хранятся данные о настройках «Рабочего стола», программ, а также периферийного оборудования, такого, как сетевые подключения и принтеры.

HKEY_USERS – в данном разделе содержатся все профили пользователей, которые созданы на компьютере. В этом же разделе находится профиль, используемый по умолчанию (**.Default**), и профиль, описываемый разделом **HKEY_CURRENT_USER**.

В каждом из этих разделов, в свою очередь, содержатся подразделы, которые и являются хранилищем различных параметров, при этом каждый параметр имеет свои атрибуты, такие, как имя, тип данных и значение переменной.

6.1.3 Типы данных, используемые в реестре

REG_DWORD – данные этого типа, в основном, используются для определения параметров драйверов устройств и сервисов. Длина значения может достигать 4 байт. Отображается в двоичном, шестнадцатеричном и десятичном форматах.

REG_BINARY – значения этого типа являются двоичными данными. Их используют большинство аппаратных компонентов. Редакторы реестра отображают эту информацию в шестнадцатеричном формате.

REG_SZ – текстовые данные. Параметры данного типа наиболее часто используются для описания каких-либо компонентов системы, поскольку они легко воспринимаются пользователем.

REG_MULTI_SZ – многострочное поле. Значения, которые фактически представляют собой списки текстовых строк в формате, удобном для восприятия человеком, обычно имеют этот тип данных. Строки разделены символом **NULL**.

REG_EXPAND_SZ – расширяемая строка данных. Может динамически

изменяться при вызове со стороны приложения.

6.1.4 «Кусты» и ветви реестра

Каждая из вышеперечисленных ветвей реестра представляет собой иерархическую структуру. Большинство ветвей получили название «куст», или «улей» (от англ. **hives**).

«Кусты» являются постоянной частью реестра, они не создаются при загрузке компьютера и не удаляются из реестра при его выключении. Существуют также ветви, которые создаются динамически при загрузке, например, раздел **HKEY_LOCAL_MACHINE\HARDWARE**, который содержит описание установленного на ПК оборудования. Такие ветви «кустами» не являются.

«Кусты» реестра хранятся на жестком диске компьютера в специальных файлах. В таблице 6.1 перечислены стандартные «кусты» реестра **Windows NT/2000** и поддерживающие их файлы.

Таблица 6.1 – Файлы, содержащие ветви реестра **Windows NT**

Ветвь реестра	Имена файлов
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL MACHINE\SECURITY	Security, Security.log, Security.sav
HKEY_LOCAL MACHINE\SOFTWARE	Software, Software.log, Software.sav
HKEY LOCAL MACHINE\SYSTEM	System, System.alt, System.log, System.sav
HKEY_CURRENT CONFIG	System, System.alt, System.log, System.sav
HKEY_USERSVDEFAULT	Default, Default.log, Default.sav
HKEY_CURRENT USER	Ntuser.dat, Ntuser.dat.log
Файлы, не ассоциированные с разделами	Userdiff, Userdiff.bg

Все вышеперечисленные файлы «кустов» реестра, за исключением **Ntuser.dat** и **Ntuser.dat.log**, хранятся в подкаталоге **%System-Root%\ System32\Config**. Файлы **Ntuser.dat** и **Ntuser.dat.log** находятся в каталогах **%SystemDrive%\ Documents and Settings\ %Username%** и хранят пользовательские профили.

6.1.5 Восстановление реестра

Реестр **Windows** является важным компонентом операционной системы, и неосторожное обращение с ним может привести к полной неработоспособности компьютера. В связи с этим рекомендуется перед модификацией реестра создать его резервную копию, а при возникновении ошибки - восстановить его.

6.1.5.1 Восстановление реестра **Windows 98**

Как было сказано выше, реестр **Windows 98** содержится в двух файлах – **system.dat** и **user.dat**, расположенных в каталоге **WINDOWS** и имеющих атрибуты **Hidden** (Скрытый) и **System** (Системный).

Прежде, чем вносить какие-либо изменения в реестр, настоятельно рекомендуется сохранить эти файлы в каком-либо каталоге или вообще на другом носителе информации. В случае повреждения реестра следует загрузить компьютер в режиме **MS-DOS** (это можно сделать с помощью загрузочного диска **Windows 98**) и заменить поврежденные файлы.

Однако в **Windows 98** существует технология защиты системного реестра от повреждений. В подкаталоге **SYSBCKUP**, находящемся в системном каталоге **WINDOWS**, хранятся архивы (файлы с расширением **CAB**, по умолчанию их пять), в которые система, после успешной загрузки компьютера, копирует весь реестр.

Эти архивы можно использовать для восстановления поврежденного реестра, для чего следует загрузить компьютер в режиме **MS-DOS** и выполнить команду:

SCANREG /RESTORE.

В результате будет отображен список доступных копий, который дает возможность выбрать необходимую копию, после чего реестр будет полностью восстановлен. В том случае, если необходимо создать копию реестра (например, после установки и настройки какого либо оборудования), можно воспользоваться командой **SCANREG /BACKUP** которая, в случае нормально прошедшей проверки, создаст резервную копию.

6.1.5.2 Восстановление реестра **Windows 2000/XP**

Восстановление реестра этих операционных системы является сложной задачей, поскольку реестр хранится в большом количестве файлов (таблица 6.1) и для их восстановления необходимо получить доступ к каталогам, в которых они находятся. Также следует иметь полный комплект файлов реестра, поскольку они все взаимосвязаны и синхронизируются в процессе работы.

В **Windows 2000/XP** предусмотрена функция загрузки компьютера с использованием последней удачной конфигурацией. Для этого следует:

– включить компьютер;

– в момент начала загрузки операционной системы нажать клавишу <**F8>**;

– в появившемся списке вариантов загрузки следует выбрать пункт «Запуск последней удачной конфигурации» и затем нажать клавишу <**Enter>**.

Следует учесть, что этот способ восстановления реестра подходит только в том случае, если на компьютер было установлено новое оборудование и оно вызывает какой-либо конфликт с имеющимися устройствами. На самом деле, восстанавливается только та информация, которая хранится в разделе **HKEY_LOCAL_MACHINE\System\CurrentControlSet**, а остальные разделы остаются нетронутыми. Данный способ не позволяет восстановить работоспособность компьютера в случае удаления драйвера устройства или его повреждения, а также при удалении файлов реестра.

Наряду с этим, существует более сложный метод восстановления реестра, который заключается в архивировании каталога **%SystemRoot%\ System32\ Config**, а также файлов **Ntuser.dat** и **Ntuser.dat.log** находящихся в каталогах **%SystemDrive%\Documents and Settings\%User name%.**

Однако простое копирование данных файлов невозможно, поскольку они постоянно используются системой и доступ пользователя к ним запрещен. Поэтому необходимо использовать специальную программу «Архивация данных», которая входит в комплект служебных утилит (рисунок 6.2). Для ее запуска необходимо выполнить команду «Пуск \ Все программы \ Стандартные \ Служебные \ Архивация данных».

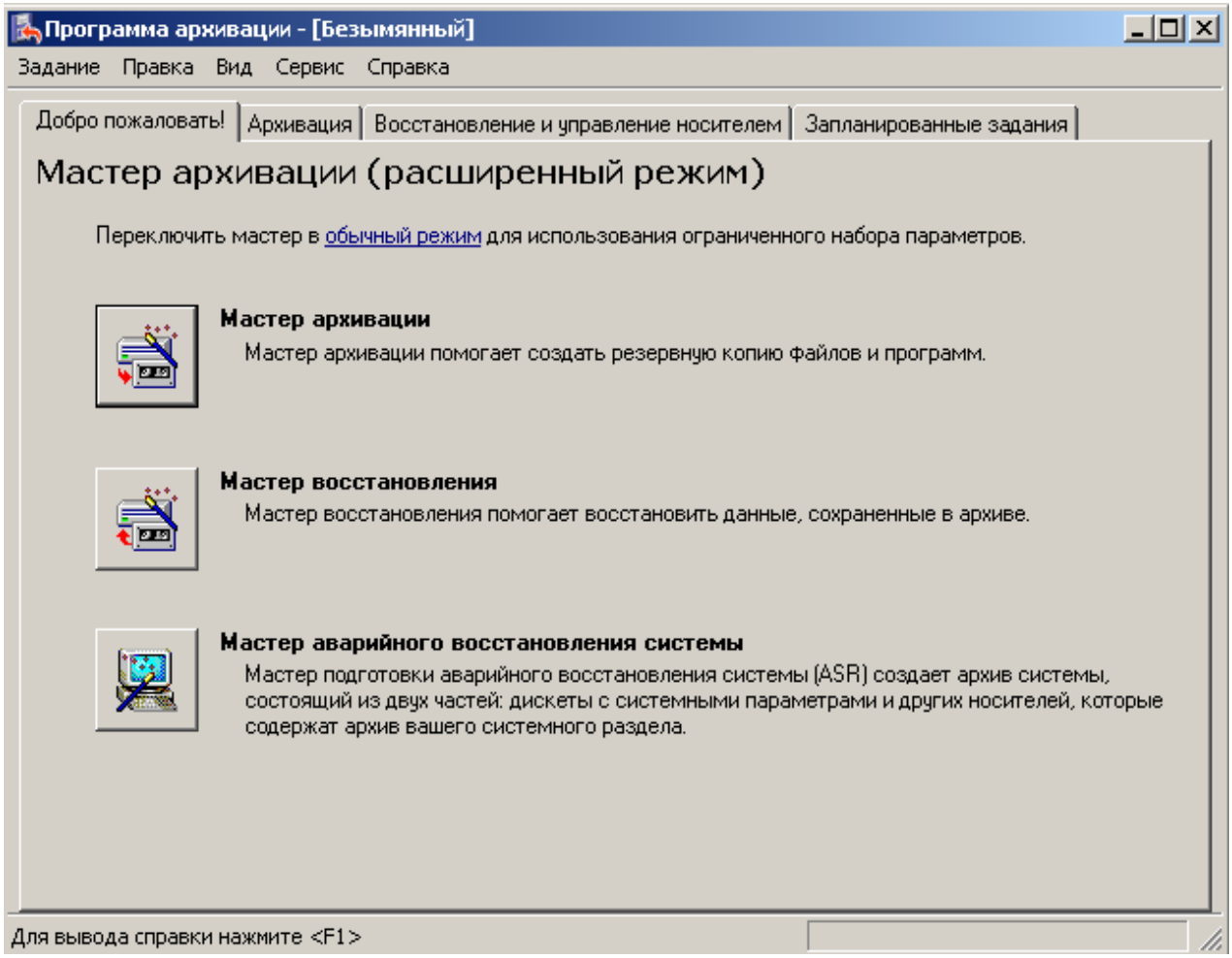


Рисунок 6.2 - Программа Архивация данных

Далее следует выбрать в меню «Сервис» команду «Создание диска аварийного восстановления» либо нажать на кнопку «Диск аварийного восстановления». В появившемся диалоговом окне следует установить флажок «Архивировать реестр в папку восстановления» и нажать кнопку **«ОК»**.

После выполнения операции архивирования в каталог **%System Root%\ Repair** будут помещены все файлы, содержащие «кусты» реестра; эти файлы будут также скопированы на дискету. Затем следует переписать указанные файлы на другой носитель информации (например на другой компьютер или на компакт-диск) и использовать их в случае повреждения реестра.

6.2 Запуск Windows в случае неполадок

В том случае, если загрузить **Windows 2000/XP** обычным способом не удается, можно использовать некоторые специальные приемы, позволяющие выйти из этого положения. К ним, в частности, относится создание специаль-

ных системных (загрузочных) дискет, а также запуск **Windows** в безопасном режиме (**Safe mode**).

6.2.1 Создание системных дискет

Системные дискеты совершенно необходимы в том случае, если операционная система вообще не загружается с жесткого диска. Такая ситуация может возникнуть, например, если некоторые системные файлы операционной системы были повреждены в результате действия вируса или «взлома» компьютера злоумышленником.

В отличие от предыдущих версий **ОС**, создание загрузочных дискет во время инсталляции **Windows XP** на жесткий диск компьютера не предусмотрено. Эту операцию можно сделать после того, как система установлена на компьютер, для чего служит специальная программа, которая входит в дистрибутив операционной системы.

Для того чтобы создать системные дискеты, нужно выполнить следующие действия:

– открыть меню «Пуск» и выбрать команду «Все Программы \ Стандартные \ Проводник»;

– вставить компакт-диск с дистрибутивом **Windows XP** в привод **CD-ROM**;

– найти с помощью «Проводника» на компакт-диске папку **Bootdisk**;

– запустить для создания комплекта аварийных дискет файл **makeboot.exe**, который находится в палке **Bootdisk** (рисунок 6.3);

– после запуска программы следует вставить первую дискету в дисковод и следовать указаниям программы.

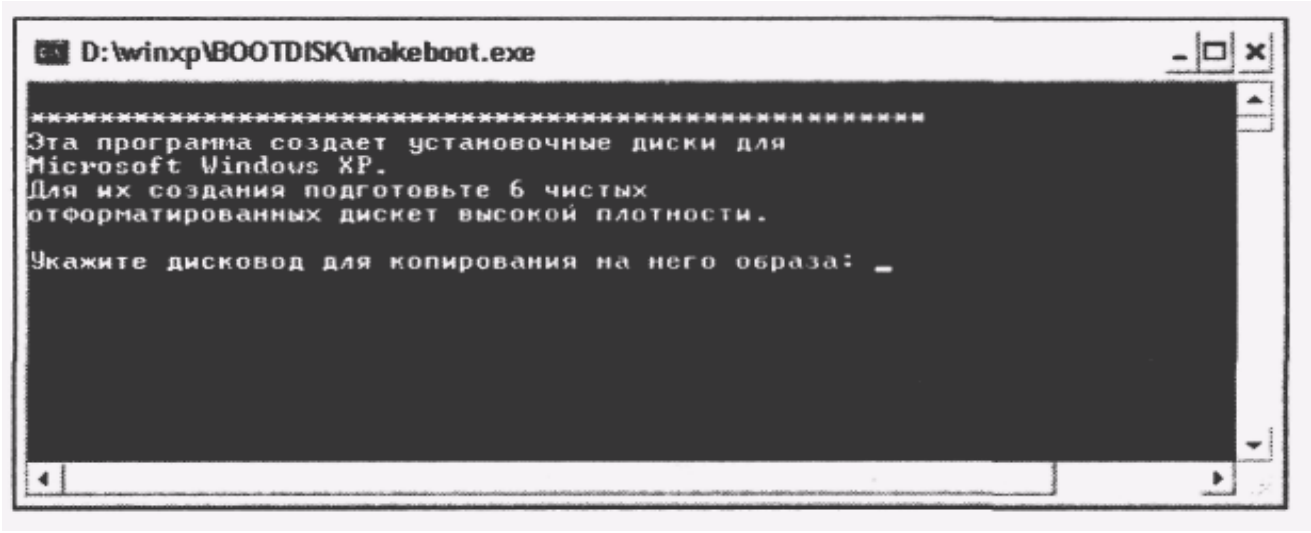


Рисунок 6.3 - Окно программы создания системных дисков

Чтобы воспользоваться системными дискетами, необходимо вставить первую из них в дисковод и перезагрузить компьютер. По завершении загрузки можно будет приступить к устранению неполадок.

6.2.2 Режим зашиты от сбоев

В некоторых случаях, когда не удается запустить **Windows** обычным образом, может помочь режим защиты от сбоев. В этом случае **Windows** использует базовые установки параметров, принимаемые по умолчанию, которые должны позволить загрузить **Windows**, после чего можно приступить к устранению ошибок.

В режиме защиты от сбоев **Windows** не выполняет загрузку драйверов и программ, которые задействованы в обычном режиме. Принимаемые по умолчанию установки параметров рассчитаны на стандартный драйвер дисплея **VGA**, отсутствие работы в сети, стандартный драйвер мыши **Microsoft** и минимальный комплект прочих драйверов, необходимых для запуска **Windows**.

Запустив **Windows** в режиме защиты от сбоев, пользователь не получит доступа к устройствам чтения лазерных дисков **CD-ROM**, принтерам и другому дополнительному оборудованию.

Существует несколько вариаций режима защиты от сбоев. Для использования одного из них необходимо выполнить следующую последовательность

действий:

– нажать кнопку «Пуск» и выбрать команду «Выключение»**,** затем в диалоговом окне «Выключить компьютер» выбрать команду «Перезагрузка»;

– подождать некоторое время до появления надписи «Выберите операционную систему для запуска»**,** при появлении этой надписи сразу же нужно нажать клавишу **<F8>**;

– на экране появится меню загрузки, в нем можно выбрать различные режимы загрузки системы, режим защиты от сбоев имеет номер 1, тот же режим с поддержкой сети (**Safe mode with Network suppor**t) – номер 2;

– ввести номер подходящего режима, рекомендуется выбрать первый или, если пользователь хочет использовать сеть, то второй.

6.2.3 Безопасный режим (Safe mode)

При загрузке в данном режиме операционная система использует только самые необходимые драйверы устройств. В безопасном режиме отсутствуют сетевые подключения, и видеосистема работает в режиме **VGA**. Также загружаются стандартные службы, которые необходимы для обнаружения причин сбоя компьютера. Безопасный режим помогает определить причину неполадок.

Если при загрузке в безопасном режиме неполадки не возникают, можно изменить настройки по умолчанию и минимальный набор драйверов устройств как возможные причины возникновения этих неполадок. Если причиной возникающих неполадок является добавление нового устройства или смена драйвера, безопасный режим можно использовать для удаления этого устройства или отмены изменений.

Также безопасный режим может помочь в том случае, когда неполадки вызывает новое программное обеспечение. При загрузке в безопасном режиме можно изменить настройки нового программного обеспечения либо удалить его с компьютера.

«Безопасный режим с загрузкой сетевых драйверов» – данный режим основан на безопасном режиме, однако дает возможность загрузить сетевые драйверы и службы, которые, в свою очередь, позволят использовать локальную

сеть.

«Безопасный режим с поддержкой командной строки» – данный режим идентичен обычному безопасному режиму, но вместо графического интерфейса пользователя запускается командная строка.

«Включить протоколирование загрузки» – данный режим позволяет найти точную причину неполадок при загрузке системы, поскольку в процессе загрузки система создает файл **ntbtlog.txt**, который хранится в каталоге **%SystemRoot%** и в который записывается перечень всех загруженных (или не загруженных) драйверов и служб.

Если же компьютер был загружен в одном из безопасных режимов, то в этот файл записывается список всех загружаемых драйверов и служб.

«Включить режим **VGA**» – данный режим позволяет устранить неполадки, вызванные в результате неправильной конфигурации видеосистемы. Очень часто причиной неправильной загрузки **Windows** является использование нового драйвера для видеоадаптера, что приводит к отсутствию изображения на мониторе. Основной драйвер видеоадаптера всегда используется при загрузке в безопасном режиме («Безопасный режим», «Безопасный режим с загрузкой сетевых драйверов» или «Безопасный режим с поддержкой командной строки»).

«Загрузка последней удачной конфигурации» – данный режим позволяет выполнить откат системы к тому моменту, когда ее работа была стабильной. Сам режим не устраняет неполадки; кроме того, все изменения, сделанные со времени последней успешной загрузки, будут утеряны.

«Восстановление службы каталогов» – этот вариант предназначен для серверных операционных систем и используется только для восстановления каталога **SYSVOL** и службы каталогов **Active Directory** на контроллере домена.

«Режим отладки» – этот вариант загрузки позволяет отправить данные об отладке на другой компьютер, используя прямое кабельное подключение.

Если для установки **Windows XP** используется или использовалась служба удаленной установки, могут быть доступны дополнительные варианты, связанные с восстановлением системы при помощи служб удаленного доступа.

6.3 Программа Regedit

Для запуска программы **Regedit**, используемой при просмотре и редактировании записей реестра, необходимо в меню «Пуск» выбрать команду «Выполнить», после чего в появившемся диалоговом окне (рисунок 6.4) указать команду **regedit**. В результате выполнения этой команды будет отображено окно, показанное на рисунке 6.1.

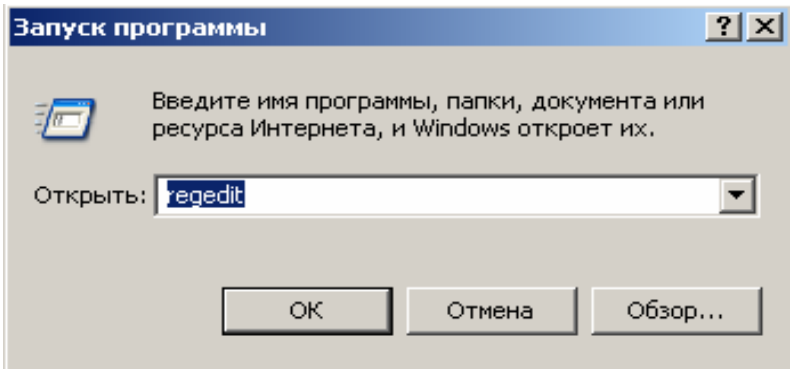


Рисунок 6.4 - Запуск программы **Regedit**

Интерфейс этой программы очень похож на интерфейс файлового менеджера «Проводник», который встроен в **Windows**. Окно программы разделено на две части. В левой отображается сама иерархическая структура реестра, а в правой – содержимое выбранного раздела.

Прежде чем приступить к работе с реестром, следует научиться выполнять элементарные действия, такие, как создание и удаление разделов и параметров и др.

6.3.1 Работа с разделами

Так же как и каталоги на жестком диске компьютера, разделы предназначены для структуризации реестра и хранения внутри себя каких-либо параметров.

Для того чтобы создать раздел, необходимо выбрать требуемую ветвь и воспользоваться командой «Создать \ Раздел» меню «Правка». При этом будет создан новый раздел, который получит название «Новый Раздел #N».

Например, для того чтобы создать раздел «Пробный» в разделе

HKEY_LOCAL_MACHINE\ SOFTWARE, следует:

– в левом окне программы **Regedit** выбрать раздел **HKEY_LOCAL_ MACHINE**, а затем - раздел **SOFTWARE**;

– выделив раздел **SOFTWARE**, выбрать в меню «Правка» группу «Создать», а в ней - команду «Раздел»**,** при этом будет создан новый раздел, который является дочерним по отношению к разделу **SOFTWARE**.

Вновь созданный раздел можно переименовать, для чего следует из контекстного меню этого раздела выбрать команду «Переименовать» (рисунок 6.5).

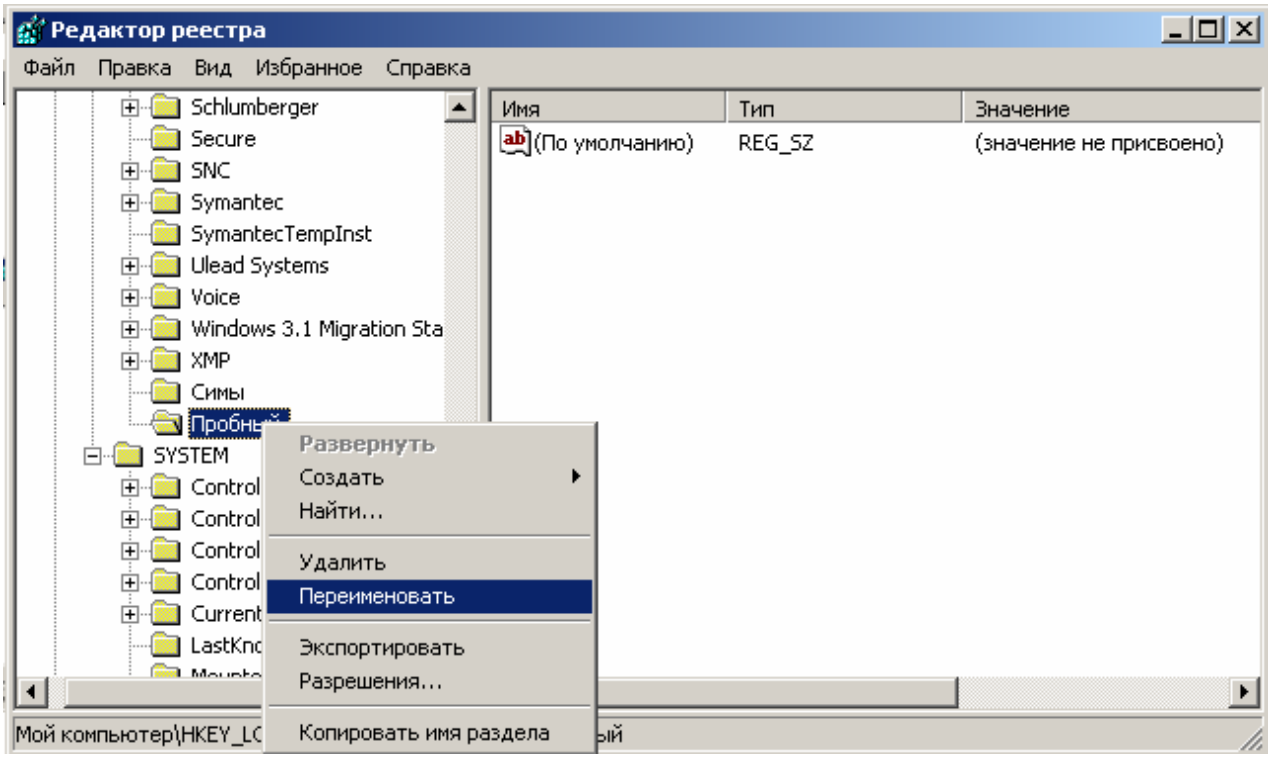


Рисунок 6.5 - Переименование раздела

Название раздела примет вид текстового поля и его можно будет изменить, например в качестве имени раздела указать **MyKey**.

Для удаления раздела необходимо выделить раздел и в меню «Правка» выбрать команду «Удалить» или просто нажать клавишу **<Delete>**.

6.3.2 Работа с параметрами

Параметры разделов в реестре предназначены для хранения каких-либо значений, которые, в свою очередь, используются операционной системой или

приложением для выполнения некоторых действий. Для добавления какого-либо параметра необходимо указать его имя, тип и значение.

Создадим в разделе «Пробный» параметр **MyValue** типа **REG_DWORD** со значением, равным 1. Для этого:

– в левом окне программы **Regedit** выбираем раздел **HKEY_LOCAL_MACHINE\SOFTWARE\Пробный**;

– выбираем в меню «Правка» группу «Создат»ь, а в ней – команду «Параметр **DWORD**». В разделе появится новый параметр, для которого следует указать название, например **MyValue**.

При работе с параметрами одним из основных действий является изменение их значения. Удобнее всего это сделать следующим образом:

– выделить параметр, значение которого необходимо изменить;

– щелкнуть на нем правой кнопкой мыши и выбрать команду «Переименовать», при этом будет открыто диалоговое окно, показанное на рисунке 6.6;

– в данном окне в поле «Значение» следует ввести требуемое значение для этого параметра и нажать кнопку «ОК».

Для удаления параметра необходимо:

– выделить параметр в правой части окна;

– в меню «Правка» выбрать команду «Удалить» или просто нажать на клавиатуре клавишу **<Delete>**.

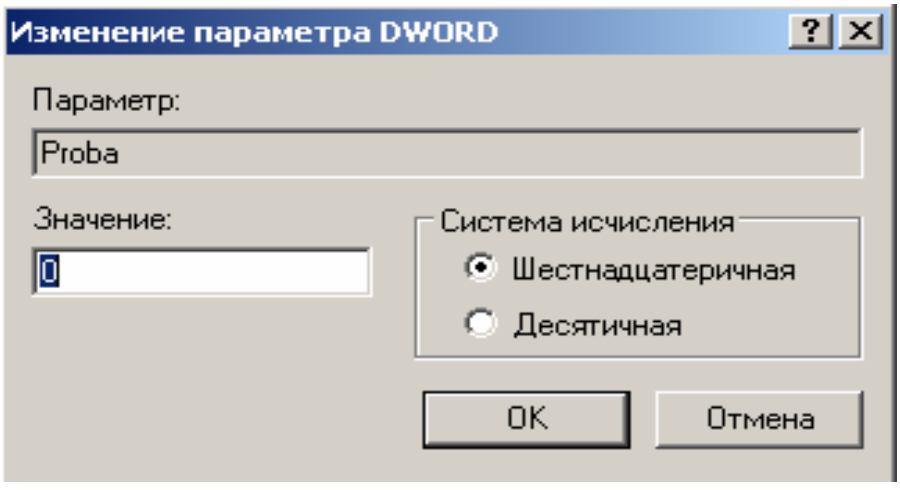


Рисунок 6.6 - Переименование параметра

6.4 Ключи реестра

6.4.1 Имя пользователя

При работе с компьютером желательно держать в тайне не только пароль доступа к нему, но и имя пользователя, поскольку это уменьшит вероятность входа злоумышленника в компьютер, ведь он не будет знать, к чему подбирать пароль.

Для того чтобы убрать из окна приветствия имя предыдущего работавшего с системой пользователя, следует, запустив редактор реестра, перейти в раздел **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\Current Version\Winlogon** и изменить значение параметра **DontDisplayLastUserName** (тип **REG_SZ**) на **1**.

6.4.2 Автозагрузка программ

Для того чтобы вирус или другая вредоносная программа смогла выполнить на компьютере пользователя какие-либо действия, она, естественно, должна быть загружена. Сделать это может или сам пользователь, например запустив на выполнение какой либо файл, или операционная система. **Windows** хранит два списка программ, которые следует запускать при загрузке системы.

Первый список представляет собой папку «Автозагрузка» главного меню, в которую пользователь может поместить ярлык программы, в результате чего она будет загружаться каждый раз при включении компьютера.

Второй список представляет собой разделы реестра, в которых находятся параметры текстового типа, а в качестве их значений хранятся пути к файлам, которые необходимо запустить.

Разделы, используемые для хранения этих параметров, называются **Run**, **RunOnce**, **RunOnceEx** и содержатся в разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion.**

Параметры могут иметь произвольные имена, но по их значениям, т.е. по именам файлов, можно выяснить, какой программе принадлежит параметр и, исходя из этого, принять решение, нужно ли оставлять программу в автоза-

грузке. Также следует обратить внимание на подраздел **Run**, расположенный в разделе **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion**.

В нем также могут находиться параметры, запускающие программы, однако все они помещаются туда пользователем, а не системой.

Следует отметить, что после установки системы все эти разделы являются пустыми, кроме **HKEY_LOCAL_MACHINE\SOFTWARE\Micosoft\Wlndows\CurrentVersion\Run**, в котором находится загрузчик **SystemTray**.

Разделы, в названии которых присутствует слово **Once**, используются для запуска программ только один раз, например при запуске программы конфигурации после установки какого-либо программного продукта. Такие ключи после своего запуска автоматически удаляются

6.4.3 Скрытые административные ресурсы

При установке операционных систем **Windows2000/XP** на компьютер, системой создаются скрытые административные ресурсы (**ADMIN$, C$, D$** и т.д.), доступные через сеть. Они предназначены для администратора компьютера и предоставляют полный доступ ко всем жестким дискам. Особенностью этих ресурсов является то, что их невозможно закрыть стандартными способами (т.е. через вкладку «Доступ» диалогового окна свойств объекта).

Если же для удаления этих ресурсов использовать раздел «Общие папки» апплета «Управление компьютером», то после перезагрузки они появятся снова.

Злоумышленник может предпринять попытку проникновения на компьютер с использованием этих ресурсов, поэтому рекомендуется их закрыть.

Сделать это можно с помощью системного реестра. Следует открыть раздел **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters** и добавить следующий параметр:

– имя - **AutoShareWks**;

– тип - **REG_DWORD**;

– значение - **0**.

В том случае, если используется серверная ОС **Windows**, имя параметра следует изменить на **AutoShareServer**. Скрытые административные ресурсы не видны в таких файловых менеджерах, как «Проводник» или **Total Commander**. Для того чтобы получить к ним доступ, можно использовать программу **FAR** и установленный подключаемый модуль **Network**. В свойствах данного модуля необходимо задать опцию «Показывать скрытые общие ресурсы».

6.4.4 Запрет на открытие доступа к ресурсам

Очень часто неопытные пользователи открывают сетевой доступ к каталогам для обмена информацией с другими пользователями, а потом забывают закрывать его. Это может привести к тому, что будет потеряна важная информация. На практике очень часто встречаются ситуации, когда в сети предприятия можно найти компьютеры, на которых полностью открыты все жесткие диски. А ведь это может быть компьютер секретаря директора, на котором хранится множество важных документов.

Для того чтобы полностью запретить пользователю открывать ресурсы, необходимо добавить параметр типа **REG_DWORD NoRleSharingControl** в раздел **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network** и изменить его значение на 1.

6.4.5 Запрет на просмотр ресурсов анонимными пользователями

Для того чтобы запретить анонимным пользователям просматривать учетные записи и открытые ресурсы, необходимо в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CumentControlSet\Control\Lsa** создать параметр **RestrictAnonymous** типа **REG_DWORD** и присвоить ему значение 1. Для отмены работы ключа необходимо изменить его значение на 0.

При установке данного параметра ни один хакер не сможет удаленно подключиться к компьютеру пользователя, не пройдя проверку. Только в том случае, если пользователь авторизуется на компьютере, к которому подклю-

чается, он сможет получить доступ к открытым ресурсам.

6.4.6 «Изменение» версии Windows

В настоящее время большое число компьютерных вирусов ориентировано на те или иные операционные системы или версии этих систем. Например, существуют вирусы, которые перед заражением компьютера проверяют версию операционной системы, и в случае, если она не совпадает с той, для которой они предназначены, не производят на компьютере различных несанкционированных действий. Этот факт можно использовать для защиты компьютера, поскольку в **Windows** имеется возможность «изменения» версии.

Для выполнения операции «изменения» версии Windows следует открыть раздел **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion** и найти в нем параметры **CurrentBuild, CurrentType, CurrentVersion** (рисунок 6.7). Можно изменить эти параметры на произвольные, обеспечив тем самым защиту от заражения некоторыми типами вирусов.

В данном разделе также можно изменить параметр **SourcePath**, который хранит путь к дистрибутиву **Windows**. Если данный параметр будет иметь ложное значение, то при установке дополнительных компонентов инсталлятор **Windows** будет запрашивать дистрибутив.

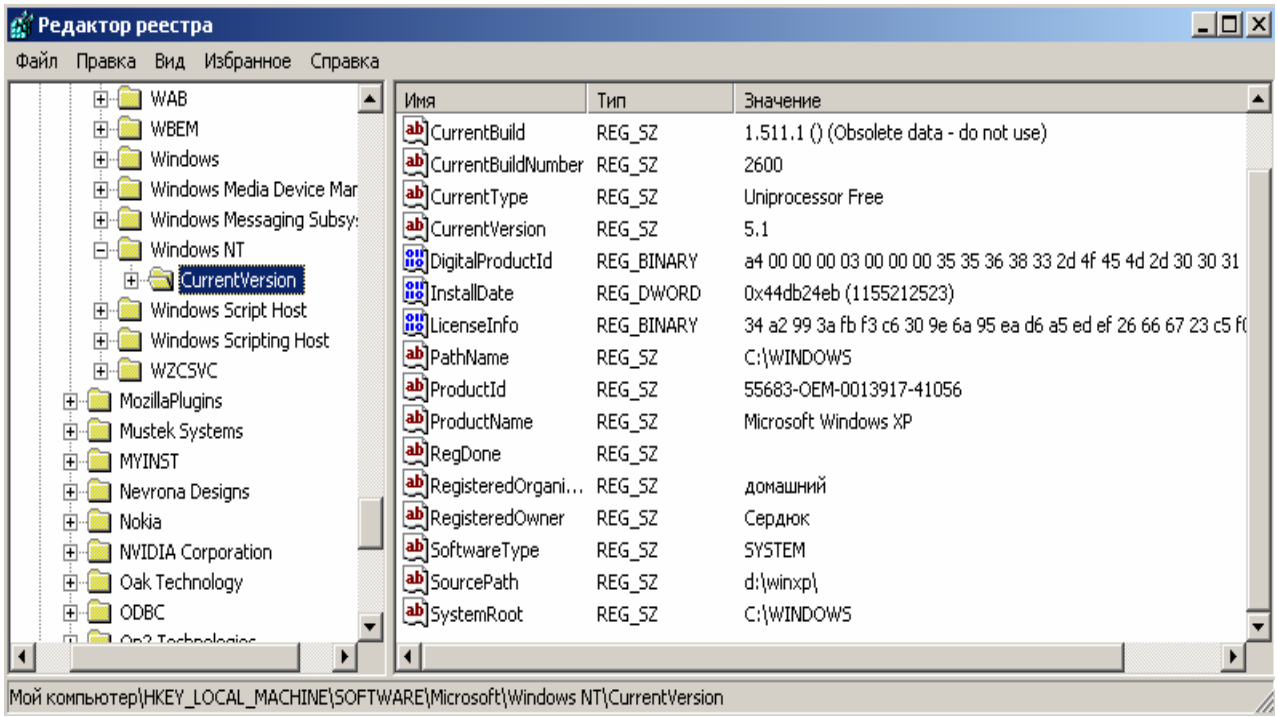


Рисунок 6.7 – Изменение» версии **Windows**

6.4.7 Заставка по умолчанию

В **Windows** существует заставка но умолчанию, которая запускается, когда компьютер включен, но вход в систему еще не выполнен. Существует возможность изменить как саму заставку, так и некоторые ее параметры, в частности время ее активирования.

Для изменения заставки необходимо поместить файл новой заставки в папку **%SystemRoot%\System32** и в разделе реестра **HKEY_USERS\ .DEFAULT\ControlPanel\Desktop** изменить строковый параметр **SCRNSAVE.EXE**, прописав в качестве его значения имя файла новой заставки. Стандартным же значением является **logon.scr** - файл экранной заставки, который находится в каталоге **%SystemRoot%\System32**.

Кроме этого параметра, можно изменять параметр **ScreenSaveTimeOut**, который отвечает за период, через который появляется заставка.

Так как файл с расширением **scr** является таким же бинарным файлом, как и другие, он может быть замещен на «вражеский», что также грозит непредвиденными последствиями.

Во избежание этого в разделе **HKEY_USERS\ .DEFAULT\ ControlPanel\ Desktop** необходимо создать (если отсутствует) или изменить параметр **ScreenSaveActive**. Для него нужно указать тип - **REG_SZ**, значение - **0**, т.е. заставка отключена (по умолчанию **ScreenSaveActive = 1**, т.е. **logon.scr** запускается автоматически через указанный в настройках экрана промежуток времени).

6.4.8 Пароль после «Ждущего режима» (Windows XP)

Можно настроить систему таким образом, чтобы при включении компьютера после «Ждущего режима» появлялось диалоговое окно с приглашением ввести пароль. Для этого в разделе **HKEY_CURRENT_USER\ Software\Policies\ Microsoft\Windows\System\Power** создаем параметр типа **REG_DWORD PromptPasswordOnResume** со значением 1.

6.4.9 Разрешение на запуск программ

В **Windows** имеется возможность разрешить запуск только определенных программ, что позволит избежать случайного запуска вируса или другой нежелательной программы. Для этого программы, разрешенные к запуску, должны быть занесены в специальный список, сформированный в реестре. Для создания списка необходимо выполнить указанную последовательность действий:

– необходимо открыть раздел **HKEY_CURRENT_USER\Software\ Microsoft\Windows\ CurrentVersion\Policies\Explorer**;

– добавить или отредактировать параметр **RestrictRun**, который имеет тип **REG_DWORD** (для включения этой функции его значение должно быть равно 1);

– в указанном выше разделе создать раздел **RestrictRun** и в нем указать имена EXE-файлов, которые могут запускать пользователи, для этого необходимо в разделе **RestrictRun** создать параметры типа **REG_SZ** и в качестве их значений указать имена исполняемых файлов программ (при этом можно указать путь к файлу);

– перезагрузить компьютер для того, чтобы изменения вступили в силу, обязательно следует внести в этот список редактор реестра (**regedit.exe**), иначе система не даст его загрузить и невозможно будет внести в него какие-либо изменения.

Следует также учесть то, что любой пользователь может переименовать любой файл в разрешенный (например **game.exe** в **regedit.exe**) и запустить любую программу.

6.4.10 Запрет на управление принтерами

Windows позволяет установить запрет на управление принтерами, а точнее на установку новых принтеров и удаление их из системы.

Для удаления из системы «Мастера установки принтеров» следует в разделе **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion**

\Policies\Explorer создать параметр **NoAddPrinter** типа **REG_DWORD** со значением, равным 1.

Если же требуется запретить пользователю удалять установленные в системе принтеры, следует в разделе **HKEY_CURRENT_USER\Software\ Microsoft\Windows\CurrentVersion\Policies\Explorer** создать параметр **NoDeletePrinter** типа **REG_DWORD** и присвоить ему значение 1.

6.4.11 Запрет завершения сеанса

Если необходимо запретить завершение сеанса, следует в разделе реестра **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer** создать параметр **NoLogOff** типа **REG_ DWORD** и присвоить ему значение 1. После перезагрузки компьютера пользователь не сможет завершить сеанс работы с помощью программных средств, т.е. не сможет воспользоваться кнопкой **Завершение сеанса** главного меню.

6.4.12 Запрет завершения работы

Установка параметра **NoClose** чипа **REG_DWORD** в разделе **HKEY_CURRENT_USER\Software\Microsoft\Wlndows\CurrentVersion\Policies\Explorer** позволяет запретить завершение пользователем работы компьютера стандартными методами. При этом кнопка «Выключить» из меню «Пуск» становится скрытой.

Следует отметить, что специальные программы (такие как планировщики, дефрагментаторы и т.д.) при этом могут завершать работу системы.

6.4.13 Запрет вызова «Диспетчера задач»

Для того чтобы лишить пользователя возможности просматривать список процессов, запущенных на компьютере, изменять их приоритет, следует использовать параметр **DisableTaskMgr** типа **REG_DWORD**, расположенный в разделе **HKEY_CURRENT_USER\Software\Microsoft\Windows\ Current Version \ Policies\System.** При установке значения этого параметра, равного 1, пользователь не сможет вызвать «Диспетчер задач». Кроме этого, он не сможет

выключить, перезагрузить или приостановить работу компьютера с помощью «Диспетчера задач»**.**

6.4.14 Запретить запуск апплетов в «Панели управления»

Если требуется лишить пользователя возможности настраивать компьютер с помощью «Панели управления», необходимо создать параметр **NoControlPanel** типа **REG_DWORD** в разделе **HKEY_CURRENT_USER\ Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**. При этом будет запрещен запуск всех апплетов в «Панели управления», а также запрещен запуск **CPL-файлов**.

6.4.15 Запрет на изменение свойств экрана

Параметр **NoDispCPL** типа **REG_DWORD** запрещает запуск апплета настройки экрана (настройки тем, фонового рисунка, разрешения экрана и др.). Он находится в разделе **HKEY_ CURRENT_USER\Software\ Microsoft\ Windows\CurrentVersion\Policies\ System.**

Также можно просто запретить изменение фона **Рабочего стола**, для чего следует создать параметр **NoChangingWallpaper** типа **REG_DWORD** в разделе **HKEY_CURRENT_USER\ Software\Microsoft\Windows\CurrentVersion\ Policies\ActiveDesktop** и установить его равным 1.

6.4.16 Сделать недоступным контекстное меню «Проводника»

Очень часто системные утилиты, которые устанавливаются на компьютере, используют контекстное меню «Проводника» для ускоренного вызова программы и обслуживания того или иного объекта. Это может послужить причиной случайного удаления или повреждения данных пользователями, не умеющими работать с такими программами. Для того чтобы при щелчке правой кнопкой мыши, а также при нажатии **<Shift+F10>** контекстное меню «Проводника» не отображалось, необходимо создать параметр **NoViewContextMenu** типа **REG_DWORD** в разделе **HKEY_CURRENT_USER\Software\Mlcrosoft\ Windows\CurrentVersion\Policies\Explorer** и присвоить ему значение 1. Чтобы

изменения вступили в силу, необходимо перезагрузить компьютер.

6.4.17 Контекстное меню папок и файлов

Если скрытие контекстного меню нежелательно, имеется возможность его редактирования. Для того, чтобы оставить в нем только те программы, которые действительно необходимы, требуется найти раздел **HKEY_CLASSES_ROOT*\shellex\ContextMenuHandlers**. Здесь в качестве подразделов выступают команды, отображаемые в контекстном меню любого файла, и для редактирования меню следует просто удалить те разделы, которые являются лишними.

6.4.18 Время жизни точек восстановления (Windows XP)

Данный параметр позволит администраторам **Windows XP** указать время жизни точек восстановления в секундах. Как известно, эти точки используются операционной системой в случае повреждения системных файлов или возникновения других внештатных ситуаций.

Параметр **RPLifeInterval** типа **REG_DWORD** позволяет выставить значения жизни точки от одного до 365 дней. Он расположен в разделе **HKEY_LOCAL_MACHINE\Software\Microsoft\ WindowsNT\CurrentVersion\ SystemRestore.**

6.4.19 Запись информации о доступе к файлу

Файловая система **NTFS** позволяет вести запись информации о последнем доступе к файлам. Эти данные могут быть полезны, если возникает подозрение, что какой-либо файл был похищен пользователем, работавшим за компьютером. Также данный параметр позволяет ускорить доступ к каталогам с большим количеством файлов. Чтобы включить опцию, необходимо в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FlleSystem** добавить параметр **NtfsDisableLastAccessUpdate** типа **REG_DWORD** и присвоить ему значение 1.

Следует отметить, что на работу файловой системы **FAT32** опция не ока-

зывает влияния.

6.4.20 Отключение слежения Windows XP за пользователем

Данный параметр позволяет пользователю операционной системы **Windows XP** отключить запись информации о таких действиях, как запуск программ, открытие документов, изменение списков часто вызываемых программ, недавно созданных документов и т.д. Параметр может использоваться в целях безопасности пользователя.

Следует отметить, что администратору компьютера настоятельно рекомендуется не отключать этот параметр, поскольку данные, записываемые операционной системой, могут помочь в нахождении злоумышленника.

Для изменения параметра необходимо найти раздел **HKEY_ CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ Policies\ Explorer** и изменить параметр **NoInstrumentation** типа **REG_DWORD** в соответствиями с требованиями (значение 1 позволяет отключить слежение, значение 0 - включить).

6.4.21 Запрос пароля после выхода из «Ждущего режима»

В целях безопасности локального компьютера можно установить опцию запроса пароля после выхода из «Ждущего режима». Это вынудит пользователя каждый раз вводить пароль при «пробуждении» компьютера. Для этого следует в разделе **HKEY_CURRENT_USER\Software\ Policies\Microsoft\Windows\ System\Power** создать параметр **PromptPasswordOnResume** типа **REG_DWORD** и присвоить ему значение 1.

6.4.22 Запись событий в системный журнал

Если возникает необходимость в определении момента, когда произошла какая-либо ошибка или компьютер был аварийно перезагружен, следует в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ CrashControl** создать параметр **LogEvent** типа **REG_DWORD** и присвоить ему значение 1. Особенно эта функция полезна на серверах, а также на рабочих

станциях при наличии нескольких пользователей на них.

6.4.23 Скрытие папок документов в программе «Мой компьютер»

Если необходимо скрыть из программы «Мой компьютер» папки документов, такие как «Мои документы», «Общие документы» и т.д.. необходимо удалить ключ: **HKEY_LOCAL_ MACHINE\SOFTWARE\Microsoft\Windows\ CurentVersion\Explorer\MyComputer\NameSpace\DelegateFolders\{59031a47-3f72-44a7-89c5-5595fe6b30ee}**.

Создание этого ключа позволяет вернуть папки на место.

6.4.24 Быстрое переключение пользователей (Windows XP)

Windows XP позволяет работать на компьютере нескольким пользователям одновременно, - для этого достаточно переключаться между ними с помощью функции «Быстрое переключение пользователей». Если опция включена, то при переключении на другого пользователя программы текущего пользователя будут продолжать работать, в противном случае программы будут автоматически выключаться, когда пользователь выходит из системы, и со следующим пользователем компьютер будет работать быстрее.

Однако эта опция может таить в себе скрытую угрозу. Примером может служить следующая ситуация: пользователь **A** запускает на компьютере программу слежения за клавиатурой, а затем не завершает сеанс, а просто отображает «Экран приветствия» с помощью нажатия комбинации клавиш **<Win+L>**. Пользователь **B** пытается загрузить свой «Рабочий стол» и, если он защищен паролем, вводит этот пароль. Данная информация будет записана программой слежения за клавиатурой, и, таким образом, пользователь **A** получит доступ к профилю пользователя **B**.

Во избежание подобной ситуации настоятельно рекомендуется отключить данную функцию. Для этого в разделе **HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ Winlogon** необходимо изменить параметр **AllowMultipleTSSessions** типа **REG_DWORD** с 1 на 0.

Также крайне желательно не использовать «Экран приветствия», который

хоть и обеспечивает наиболее быстрый и простой вход в систему, но является уязвимой функцией **Windows XP**. Если выключить эту опцию, будет использоваться классический вход в систему.

Для отключения «Экрана приветствия» необходимо в разделе **HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\Windows NT\ CurrentVersion\Winlogon** изменить параметр **LogonType** типа **REG_DWORD**. Значение 1 позволяет использовать «Экран приветствия», 0 - используется классический вход в систему.

6.4.25 Запретить доступ к дискам

Если необходимо запретить просмотр содержимого жестких дисков компьютера с помощью файлового менеджера «Проводник», необходимо использовать параметр **NoViewOnDrive** типа **REG_DWORD**, который расположен в разделе **HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Explorer**. Его значением является сумма дисков, к которым запрещается доступ. При этом каждый диск отмечается числом:

– **A:** 1 (2^0)

– **B:** 2 (2^1)

– **C:** 4 (2^2)

– **D:** 8 (2^3) ...

– **Z:** 33554432 (2^{25})

Например, чтобы запретить доступ к дискам **A:** и **C:**, необходимо задать значение параметра **NoViewOnDrive** равным 5 (что соответствует сумме 1+4=5). Значение 0 - разрешен доступ ко всем дискам; значение 67108863 (**hex:3ffffff**) - запретить доступ ко всем дискам (**A: – Z:**).

6.4.26 Имена и пароли в Internet Explorer

Функция автозаполнения имен пользователей и паролей в формах, которые располагаются на **Internet-страницах**, ускоряет работу в сети, а также не требует от пользователя запоминания той информации, которую он вводил, посещая сайт ранее. Однако если злоумышленник получит доступ к компьютеру,

на котором данная функция включена, он сможет без труда воспользоваться различными сервисами **Internet**, принадлежащими пользователю, например его электронной почтой.

Во избежание этой ситуации необходимо в разделе **HKEY_ CURRENT_USER\Software\ Microsoft\IntemetExplorer\Main** присвоить параметру **FormSuggest Passwords** (тип **STRING**) значение **no**. Значение **yes** позволяет включить автозаполнение имен пользователей и паролей в формах.

6.4.27 Swap-файл («файл подкачки»)

Для повышения безопасности следует включить опцию очистки «файла подкачки» (**swap-файл** в **Windows 9X** или **page-файл** в **Windows 20000**). Файл **pagefile.sys** находится в корневом каталоге каждого или только системного диска) после завершения работы.

Очищать этот файл необходимо, т.к. именно в нем система в процессе работы сохраняет всевозможные данные, в том числе и пароли. Стоит заметить, что при включении этой опции данные не удаляются в общем смысле этого слова. «Файл подкачки» представляет собой «страничный» файл, т.е. он разбит на страницы. При выключении питания все неактивные страницы заполняются нулями, а информация активных страниц все равно остается. Серьезными последствиями это не грозит, т.к. все данные, касающиеся безопасности, данная опция позволяет затереть.

Для того чтобы очистить **swap-файл**, нужно открыть раздел **HKEY LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\SessionManager\ MemoryManagement** и найти запись, подходящую под следующее описание (рисунок 6.8):

– параметр: **REG_DWORD;**

– имя параметра: **ClearPageFileAtShutdown;**

– значение параметра: 1 (0 - значение по умолчанию при выключенной опции).

Далее необходимо присвоить параметру значение 1, если необходимо производить очистку **swap-файла**, или 0 – в противном случае.

Следует заметить, что включение этой опции может несколько замедлить процесс выключения компьютера.

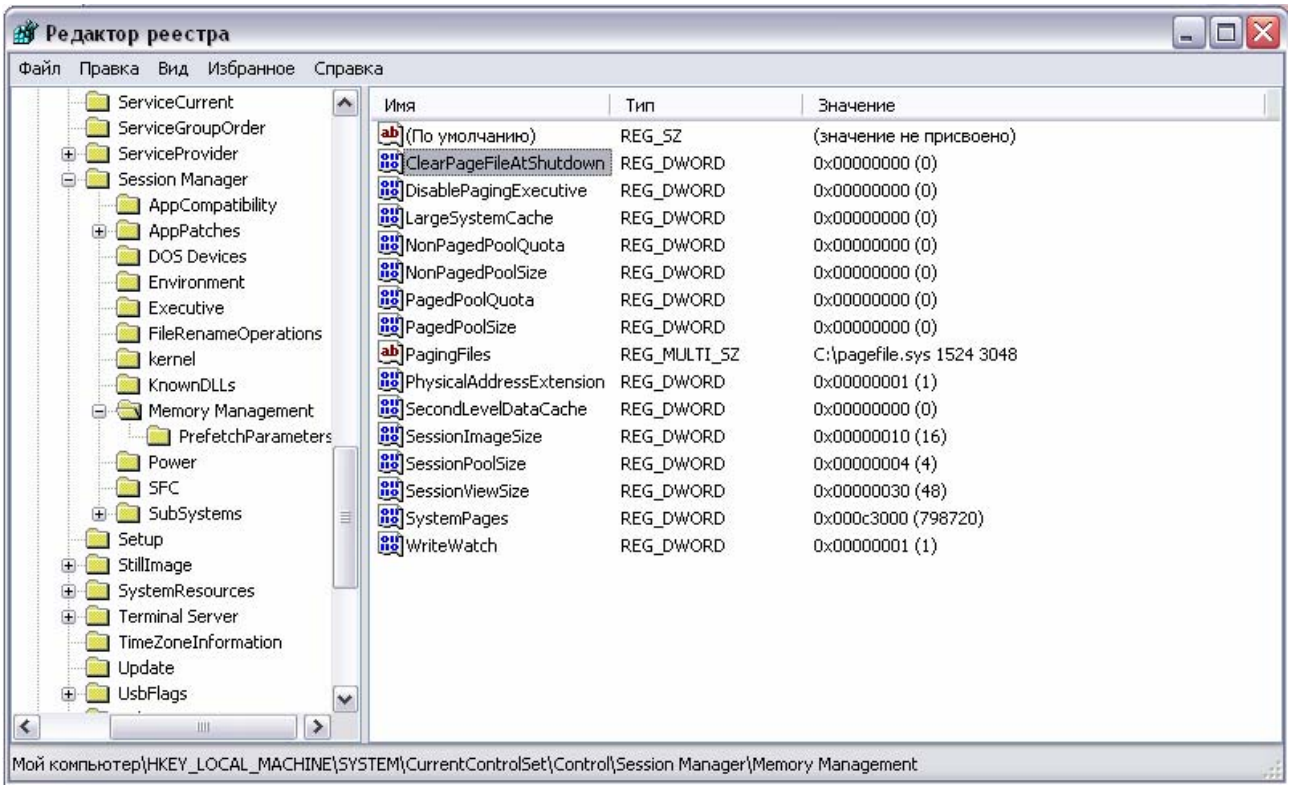


Рисунок 6.8 - Очистка файла подкачки

6.4.28 Функция «Автозапуск»

Возможность запуска «случайных» программ делает целесообразным отключение функции «Автозапуск». Решить эту проблему можно двумя способами:

– при каждом запуске **CD-ROM** нажимать и удерживать клавишу **<Shift>**;

– в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CDRom** изменить значение параметра **Autorun** (тип **REG_DWORD**) с 1 (задано по умолчанию) на 0.

6.4.29 Обеспечение сетевой безопасности

Чтобы избежать подключения к сети постороннего пользователя, желательно отключить **Network Browser**, что сделает компьютер «невидимым» из-

вне и, следовательно, исключит возможность сканирования на наличие открытых портов и прочих уязвимых мест. Следует заметить, что, зная сетевое имя компьютера, все равно можно провести сканирование, и в этом случае отключение данной опции не даст нужного результата.

Итак, в каталоге **HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\ LanManServer\Parameters** следует изменить значение параметра **Hidden** с 0 на 1. Существует возможность выполнения этой операции из командной консоли операционной системы, для чего в консоли следует ввести команду: **net config server/hidden:yes.**

Кроме того, необходимо отключить **Null-Session**, которая позволяет другому пользователю, даже не зная логинов и паролей, получить всю информацию о **share-директориях** (т.е. доступных для общего пользования), имеющихся локальных пользователях, и т.д.

Для этого в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\Lsa** необходимо создать параметр **RestrictAnonymous** типа **REG_DWORD** и присвоить ему значение 1.

Всем пользователям сети **Internet** рекомендуется вести полную запись всех событий, происходящих с модемом. Для этого в директории **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rasman\ Parameters** следует создать параметр **Logging** типа **REG_DWORD** и присвоить ему значение 1. В результате компьютер будет записывать все события и сохранять их в файле **Device.LOG**, находящемся в каталоге **%SystemRoot%\System32\RAS\.**

6.4.30 Безопасностъ ядра

Уязвимость **Windows 2000** заключается в том, что ядро этой системы можно повредить как в случае действий программы, так и вследствие неумелых действий пользователя. Но также можно и восстановить как ядро, так и просто функциональность системы. Поэтому для предупреждения возможных неполадок в работе системы, связанных с повреждением ядра, рекомендуется создавать резервную копию ядра. Для этого в каталог **%SystemRoot%\System32**

следует скопировать файлы **ntoscrnl.exe** и **hal.dll**, предварительно незначительно изменив их имя, например**, ntoscrnlalarm.exe** и **halalarm.dll.**

В случае возникновения внештатных ситуаций в файле **boot.ini** к строке загрузки системы, обычно имеющей вид **multi(0)disk(0)rdisk(0)partition(l)\Windows="Windows XP Professional" /fastdetect** добавляется (после **/fastdetect**) строка: **/kernel= ntoscrnlalarm.exe / hal=halalarm.dll,** после чего повреждение ядра не вызовет сбоя, т.к. система будет использовать созданные копии.

6.4.31 Безопасность NetBT

Если компьютер имеет постоянный **IP-адрес**, то он может быть подвержен **DoS**-атаке (**Denial of Service** - отказ в обслуживании). Причина этому – **NetBIOS**, работающий «поверх» протокола **TCP/IP** (**NetBT**).

К сожалению, реализация протокола **NetBIOS** не включает в себя проверки аутентичности. Для устранения этой ошибки нужен новый файл - **netbt.sys**, получить который можно по следующему **Web-адресу** (рисунок 6.9): http://support.microsoft.com/support/kb/articles/g269/2/39.asp:

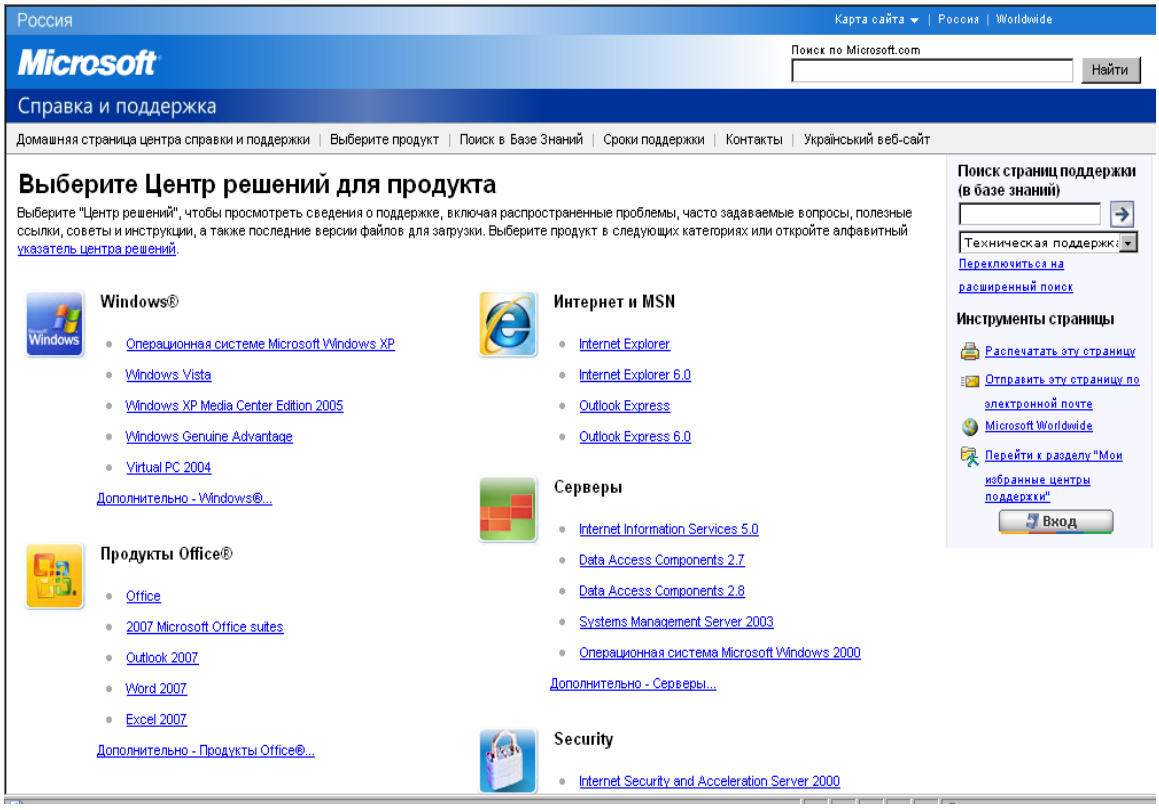


Рисунок 6.9 – Сайт поддержки операционной системы **MicroSoft**

6.5 REG-файлы

Еще одним удобным инструментом работы с реестром являются **REG-файлы**. Они представляют собой обычные текстовые файлы (созданные, например, в «Блокноте»), однако имеющие специальную структуру (рисунок 6.10).

```
Windows Registry Editor Version 5.00
 [HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Policies]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Policies\Explorer]
"NoDriveTypeAutoRun"=hex:bl,00,00,00
"NoLowDiskSpaceChecks"=dword:00000001
"RestrictRun"=dword:00000001
[HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Policies\Explorer\RestrictRun]
"l"="regedit.exe"
"2"="explorer .exe"
"3"=" winword .exe"
"4"="excel.exe"
"5"="notepad.exe"
"6"="calc.exe"
```

Рисунок 6.10 – Структура **REG-файла**

К преимуществам их использования можно отнести:

- удобную и быструю настройку большого числа компьютеров;
- простоту добавления и удаления параметров реестра;
- модифицирование реестра даже тогда, когда запрещен запуск редактора реестра.

6.5.1 Структура REG-файлов

Любой **REG-файл** начинается с указания версии реестра. Для **Windows 9x** - это **REGEDIT4** (при этом буквы должны быть прописными), а для **Windows 2000/XP - Windows Registry Editor Version 5.00**.

Следует отметить, что **Windows 2000/XP** в состоянии корректно обрабатывать файлы реестра **Windows 98**, и операция импортирования не вызовет ошибки. Если же был экспортирован файл реестра **Windows XP**, а затем перенесен в **Windows 98**, то следует изменить первую строку на **REGEDIT4**.

Далее обязательно следует пустая строка, а за ней, в квадратных скобках, указывается раздел реестра, в котором будут производиться изменения параметров. После этого, с новой строки, указывается имя параметра, его тип и значение. Следующий параметр также указывается с новой строки.

Ниже приведен пример **REG-файла**, с помощью которого можно запретить автозапуск компакт-дисков (с помощью параметра **NoDrive TypeAutoRun**), запретить проверку свободного места на жестком диске компьютера (**NoLowDiskSpaceChecks**), а также разрешить запуск только определенных программ (**RestrictRun**).

Следует учитывать, что последняя строка в **REG-файле** должна быть обязательно пустой, т.к. она указывает на его окончание.

6.5.2 Правила написания параметров

6.5.2.1 Параметры типа **REG_DWORD** можно указать следующим образом: записывается имя параметра (оно должно быть в кавычках), ставится знак «=», после него указывается тип параметра **dword** (при этом все символы должны быть строчными), а далее, после двоеточия, указывается значение параметра в шестнадцатеричном виде. Например: **«RestrictRun"=dword:00000001.**

Большинство параметров типа **dword** принимают значение либо 0, либо 1, для чего в **REG-файле** следует написать или 00000000 или 00000001 соответственно.

6.5.2.2 Строковые параметры записываются следующим образом: в ка-

вычках указывается название параметра, затем ставится знак «=», а далее, также в кавычках, - значение параметра.

Например: **«InstallVisualStyleSize»=«nORMALsIZE»**.

6.5.2.3 Для добавления двоичного параметра следует использовать следующий формат записи: **«имя параметра»=hex: значение**.

Например: **«NoDriveTypeAutoRun»=hex:bl,00,00,00.**

В каждом разделе реестра существует параметр, используемый по умолчанию, который называется (**Default**). Для изменения его значения с помощью **REG**-файла необходимо в качестве названия параметра указать символ **@**, а после знака «=» записать значение этого параметра.

Например: **@=«Windows Messenger»**.

Следует отметить, что в большинстве разделов данный параметр имеет тип **REG_SZ** и его значение не определено.

6.5.3 Удаление параметров

Для удаления параметров и разделов с помощью **REG-файлов** необходимо выполнить следующие действия.

Для удаления раздела перед его именем в квадратных скобках поставить символ «-».

Например: **[HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Policies\Explorer]**.

При этом раздел будет удален вместе со всем его содержимым;

Для удаления параметра в качестве его значения поставить знак «-». Например: **«RestrictRun»= –**.

6.6 Подключение к реестру удаленного компьютера

Программа «**Regedit**» позволяет выполнять подключение к реестру удаленного компьютера и производить над ним различные операции. Существует несколько условий, которые должны быть выполнены перед подключением:

- оба компьютера должны быть подключены к сети;
- на компьютере должно быть разрешено удаленное управление;

– на удаленном компьютере должна быть запущена служба удаленного реестра;

– пользователь должен обладать правами администратора на обоих компьютерах.

Для выполнения данной операции необходимо запустить программу **Regedit.exe**, после чего в меню «Файл» следует выбрать команду «Подключить сетевой реестр». В диалоговом окне **Подключение сетевого реестра** (рисунок 6.11) необходимо ввести **NetBIOS**-имя компьютера, реестр которого требуется подключить.

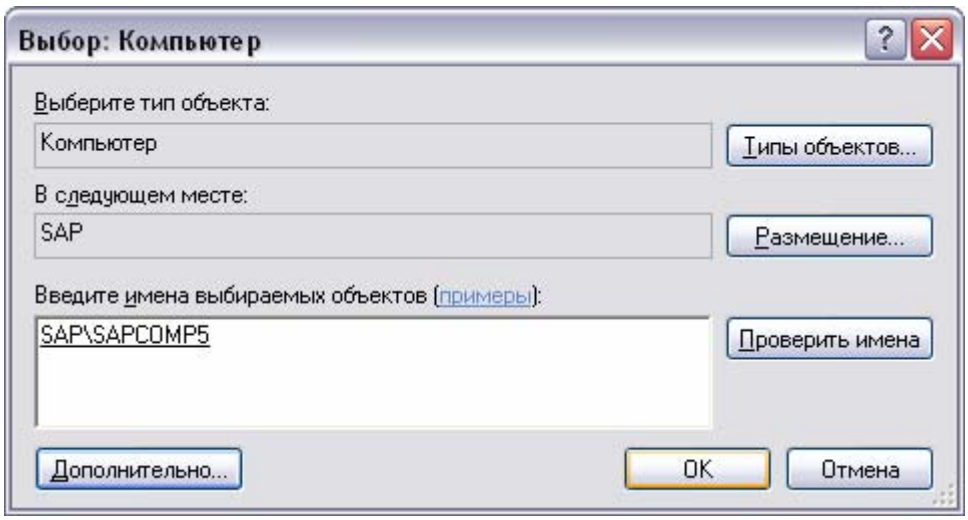


Рисунок 6.11 - Подключение к реестру удаленного компьютера

После этого пользователь имеет возможность производить различные манипуляции с реестром удаленного компьютера, может добавлять и удалять параметры и разделы, т.е. полностью управлять компьютером.

Для отключения реестра удаленного компьютера следует в меню «Файл» выбрать команду «Отключить сетевой реестр». При этом будет отображено диалоговое окно «Отключение сетевого реестра» (рисунок 6.12), где пользователю предлагается выбрать имя компьютера, реестр которого следует отключить.

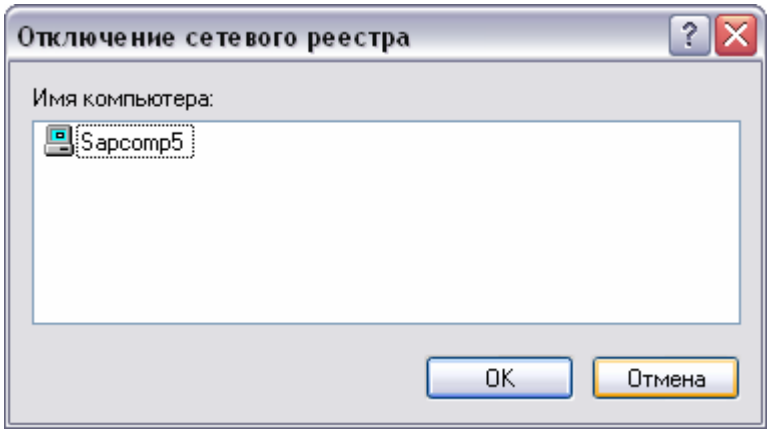


Рисунок 6.12 - Отключение реестра удаленного компьютера

6.7 Контрольные вопросы

6.7.1 Что представляет собой реестр операционной системы **Windows**?

6.7.2 Как может быть использован реестр злоумышленниками?

6.7.3 Что представлял собой реестр в ранних версиях операционной системы **Windows**?

6.7.4 В каких файлах хранится реестр операционной системы **Windows 98**?

6.7.5 В каких папках хранится реестр для **Windows NT 4.0** и для **Windows 2000/XP**?

6.7.6 Перечислите корневые разделы реестра.

6.7.7 Какая информации хранится в разделе **HKEY_LOCAL_MACHINE?**

6.7.8 Какая информации хранится в разделе **HKEY_CLASSES_ROOT?**

6.7.9 Какая информации хранится в разделе **HKEY_CURRENT_CONFIG?**

6.7.10 Какая информации хранится в разделе **HKEY_CURRENT_USER?**

6.7.11 Какая информации хранится в разделе **HKEY_USERS?**

6.7.12 Дайте характеристику типов данных, используемых в реестре?

6.7.13 Что называется «кустом» реестра?

6.7.14 В каких папках хранятся файлы «кустов» реестра?

6.7.15 Какие расширения могут иметь файлы кустов реестра?

6.7.16 Как защитить системный реестр от повреждений в **Windows 98**?

6.7.17 Опишите функцию загрузки компьютера с использованием по-

следней удачной конфигурацией в **Windows 2000/XP**. В каких случаях ее можно использовать?

6.7.18 В чем смысл создания дисков аварийного восстановления?

6.7.19 Какой каталог и какие файлы архивируются в процессе создания диска аварийного восстановления?

6.7.20 Какая папка создается при создании диска аварийного восстановления?

6.7.21 С какой целью и как создаются системные дискеты?

6.7.22 В чем смысл режима защиты от сбоев, как он загружается и в каких вариантах?

6.7.23 Какие известны варианты режима **Safe Mode** и в чем их особенности?

6.7.24 Как создать новый раздел реестра с помощью программы **RegEdit**?

6.7.25 Опишите технологию добавления нового параметра в раздел реестра с помощью программы **RegEdit**?

6.7.26 Как убрать из окна приветствия имя предыдущего работавшего с системой пользователя?

6.7.27 Охарактеризуйте два списка программ, которые следует запускать при загрузке системы?

6.7.28 В каких разделах реестра хранятся параметры второго списка автозагрузки?

6.7.29 Что понимается под скрытыми административными ресурсами компьютера?

6.7.30 Как блокировать доступ злоумышленника к скрытым административным ресурсам компьютера?

7 Утилиты работы с реестром. Защита документов и файловой системы

7.1 Утилиты для работы с реестром.

7.1.1 Общие сведения

Непосредственное редактирование реестра (с помощью программ **regedit.exe** и **regedit32.exe**) сопровождается некоторыми сложностями, поскольку пользователь должен точно знать, за что отвечает тот или иной ключ, и какие значения он может принимать. В случае установки некорректного значения ключа или его добавления/удаления может произойти сбой системы, вплоть до полной потери работоспособности.

Во избежание подобных ситуаций рекомендуется использовать специализированные утилиты, которые обладают следующими преимуществами:

– удобным графическим интерфейсом;

– функцией контроля значений, которая не позволяет установить ошибочные значения;

– функцией отката, автоматически создающей резервные копии измененной части реестра;

– модулем отслеживания изменений, который отображает все изменения, выполненные программой, и др.

Все утилиты для работы с реестром **Windows** можно разделить на следующие категории:

– редакторы;

– диагностика и лечение;

– оптимизаторы;

– мониторы;

– многофункциональные.

Необходимо отличать редакторы реестра и утилиты-оптимизаторы, которые, в конечном итоге, настраивают систему только путем модификации реестра, от утилит оптимизации работы **Windows** (например, **Customizer XP**,

PCMedik и др.), которые для выполнения своих задач должны быть постоянно загружены в оперативную память ПК и, тем самым, забирают часть ресурсов компьютера.

В следующем разделе будет приведено описание программы, использующейся для мониторинга и очистки реестра (**Reg Organizer**).

7.1.2 Утилита Reg Organizer

Reg Organizer является мощным инструментом, предназначенным для работы с реестром **Windows**. Он может применяться и как редактор реестра, и как утилита обслуживания реестра, которая в автоматическом режиме может провести очистку реестра от неиспользуемых ключей.

Данная программа была разработана Константином Поляковым и ее можно бесплатно загрузить с официального сайта www.chemtable.com. **Reg Organizer** поставляется в виде **ZIP-архива** с названием **regon.zip**, который содержит установочный исполняемый файл **setup.exe**, а также файл краткого описания программы. Для жителей бывшего СССР программа является бесплатной. Для ее регистрации необходимо загрузить с сайта разработчика русскоязычный модуль, установить его, а затем в меню «Помощь» выбрать команду «Разблокировать».

Основное окно программы **Reg Organizer** показано на рисунке 7.1.

При работе с **Reg Organizer** используется один из четырех режимов:

– «Редактирование реестра» – d данном режиме программу можно использовать как мощный редактор реестра, который обладает всеми функциями программы **Regedit**, а также позволяет клонировать ключи реестра, получать информацию о любом выбранном ключе и т.д.;

– «Чистка реестра» – данный режим используется как для ручной, так и для автоматической чистки реестра от неиспользуемых ключей;

– «Редактирование файлов» – этот режим используется для редактирования **INI-файлов**, которые, так же как и реестр, используются для хранения настроек программ;

– «Поиск и замена» – в случае необходимости поиска и/или замены тре-

буемой информации в системном реестре следует использовать инструменты этого раздела.

Для переключения между режимами можно использовать меню «Режим» или панель **Reg Organizer**, которая расположена в левой части окна.

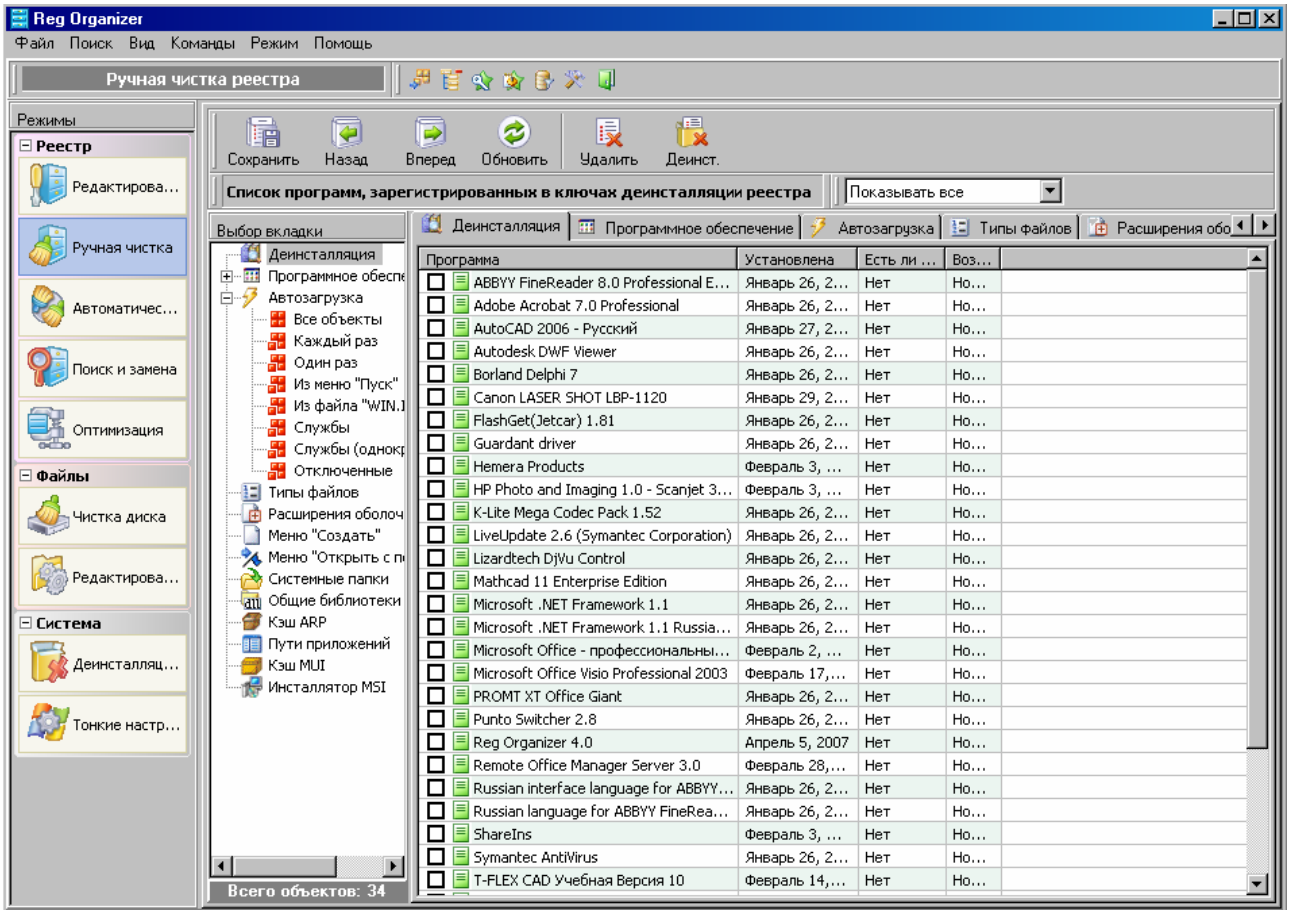


Рисунок 7.1 - Основное окно программы **Reg Organizer**

7.1.2.1 Редактирование реестра

Данный режим (рисунок 7.2) следует применять только опытным пользователям, которые желают «вручную» вносить изменения в реестр, изменять значения ключей и т.д. Помимо стандартных функций, данный режим предоставляет возможность быстрого экспорта выделенного ключа в **REG-файл** с помощью кнопки «Экспорт», а также клонирования ключа, т.е. создание точной копии.

Последнее удобно использовать при проведении различных экспериментов, поскольку, если перед внесением каких-либо изменений в раздел реестра сделать копию изменяемого ключа или всего раздела, увеличиваются шансы на

успешное восстановление работоспособности системы в случае возникновения ошибки.

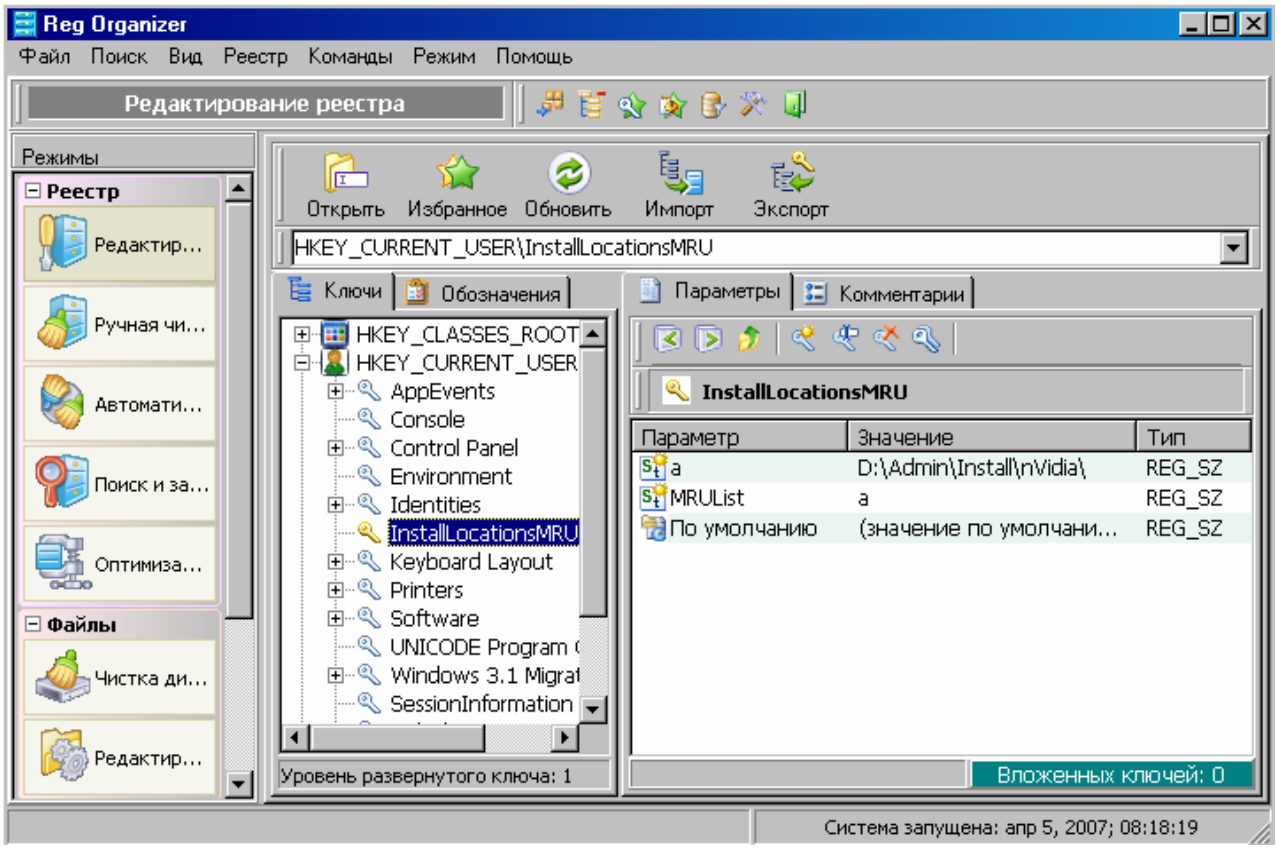


Рисунок 7.2 - Режим редактирования реестра

7.1.3 Чистка реестра

Этот режим позволяет проводить как ручную, так и автоматическую чистку реестра от неиспользуемых ключей. В данном режиме программа отображает несколько закладок, описание которых приведено ниже.

7.1.3.1 Деинсталляция

Данная закладка (рисунок 7.3) содержит список программ, которые установлены на компьютере, и позволяет либо корректно деинсталлировать программу, отметив ее и нажав на кнопку «Деинсталлировать отмеченные», либо удалить упоминание о ней из диалогового окна «Установка и удаление программ» «Панели управления» (кнопка «Удалить отмеченные»).

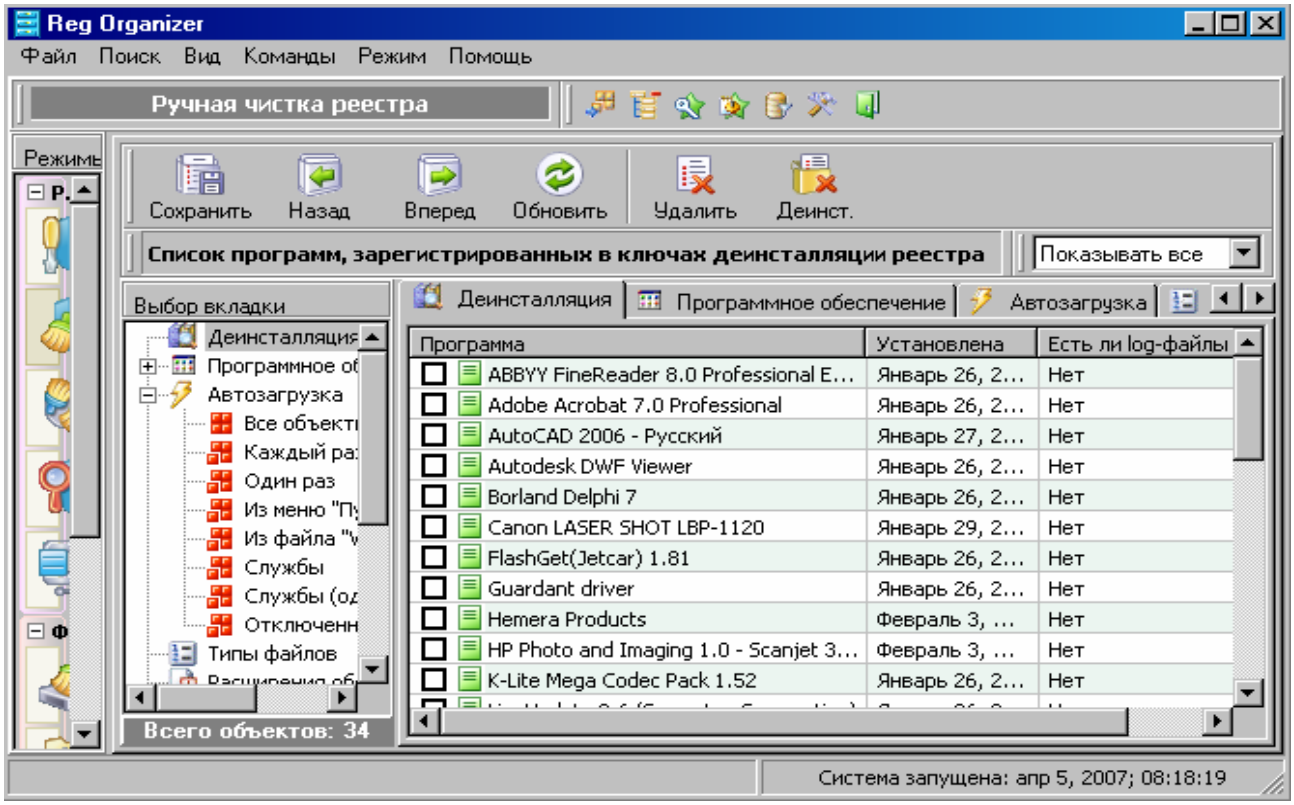


Рисунок 7.3 - Режим чистки реестра, закладка «Деинсталляция»

7.1.3.2 Программы

Закладка содержит перечень всех зарегистрированных в системе программ. В том случае, если пользователь уверен, что он удалил программу, имя которой указано в списке, следует выделить все записи, которые относятся к ней, и нажать на кнопку «Удалить отмеченные». При этом из реестра будут удалены все записи, касающиеся данной программы.

Если случайно были удалены записи о нужной программе, пользователь может столкнуться с проблемами, возникающими при запуске и в процессе работы программы. Поэтому удаление записей необходимо производить только в том случае, если пользователь твердо уверен в выполняемых действиях.

7.1.3.3 Автозагрузка

На этой закладке в виде таблицы содержится перечень всех программ, которые запускаются при старте системы. В таблице представлены следующие сведения:

– имя приложения;

– имя исполняемого файла, который используется для загрузки про-

граммы;

– ключ или ярлык, который используется для запуска программы;

– информация о «возрасте» программы (с точки зрения программы **Reg Organizer**).

Пользователь может удалить любую из ссылок, используя кнопку «Удалить отмеченные».

Полезной функцией является возможность создания нового элемента автозагрузки посредствам кнопки «Новый элемент». При создании нового элемента пользователю будет предложено указать, в какой из четырех ключей реестра, ответственных за автозагрузку (подраздел 6.4), он будет помещен.

7.1.3.4 Типы файлов

На закладке содержится информация обо всех типах файлов, которые зарегистрированы в системе, т.е. в таблице соответствия содержится расширение файла и описание типа файла. Очень часто поле «Описание типа файла» включает имя программы, которая используется для открытия файлов данного типа. Если в столбце «Описание типа файла» указано «Нет данных», то, вероятнее всего, этот тип файлов больше не нужен в системе и его можно удалить с помощью кнопки «Удалить отмеченные».

Также пользователь может получить дополнительную информацию о ключах реестра, относящихся к выбранному типу (типам) файлов, используя команду «Информация контекстного меню».

7.1.3.5 Расширения оболочки

На закладке представлен список команд, содержащихся в контекстном меню «Проводника», для каждого из типов файлов, зарегистрированных в системе.

Например, если вызвать контекстное меню **MP3-файла**, в нем будут содержатся некоторые специфические команды, такие, как **Enqueue in Winamp**, **Add to Winamp's Bookmark List** и др. Используя данную закладку, пользователь может удалить ненужные команды или добавить необходимые.

7.1.3.6 Меню «Создать»

На закладке содержится список документов (файлов), которые присутст-

вуют в группе «Создать» контекстного меню «Проводника».

Если пользователю не нужна возможность быстрого создания документа с помощью контекстного меню, он может удалить ненужные типы документов из этого меню, используя кнопку «Удалить» отмеченные на этой закладке.

Кроме перечисленных выше меню, которые используются для ручной правки реестра, в программе существует возможность автоматической чистки реестра. Для выполнения данной операции необходимо нажать на кнопку «Чистка реестра», которая находится на панели «Дополнительно», после чего будет отображено окно, показанное на рисунке 7.4. Также это окно можно вывести с помощью команды «Команды \ Чистка реестра».

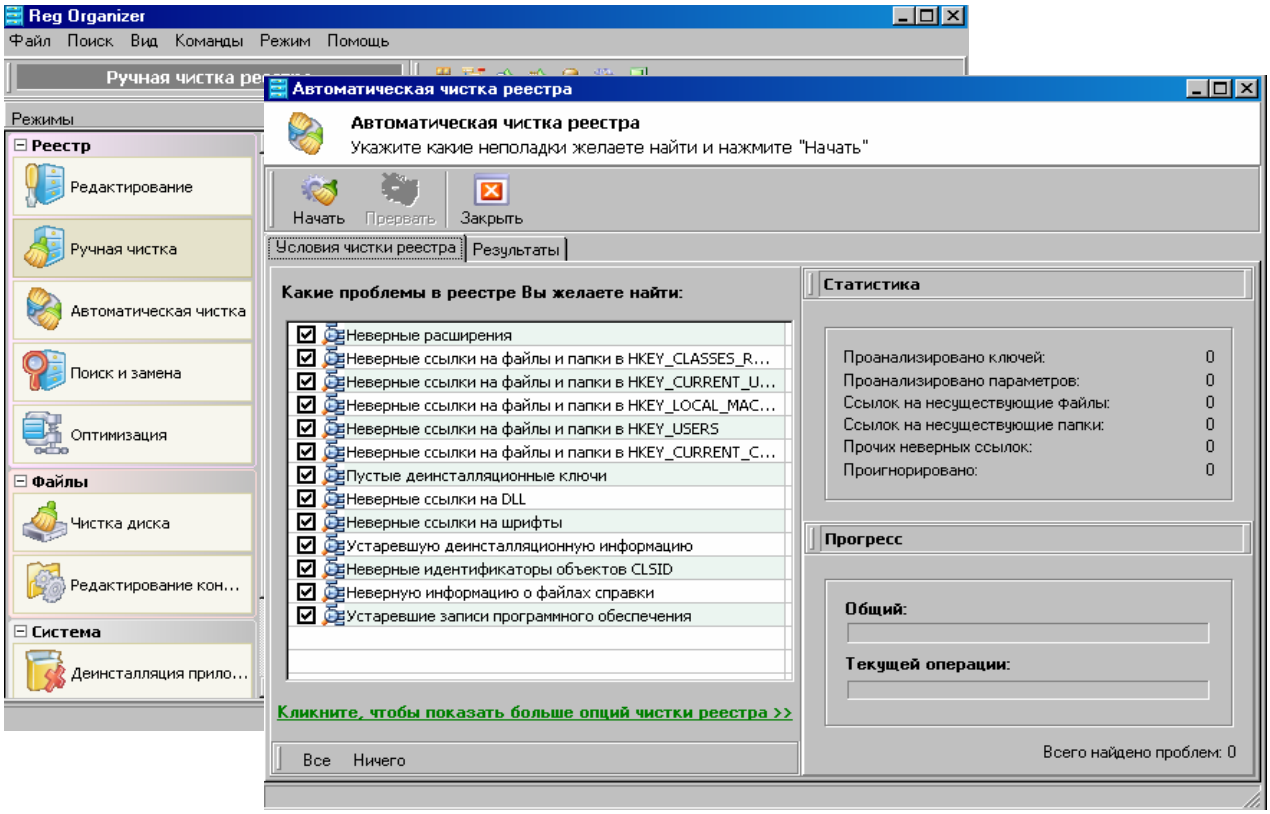


Рисунок 7.4 - Окно автоматической чистки реестра

В данном окне необходимо указать условия поиска ошибочных ключей реестра, а именно:

– «Неверные расширения» – типы файлов и классов, которые остались зарегистрированными в реестре после удаления какого-либо приложения;

– «Ссылки на несуществующие файлы» – **Reg Organizer** будет искать

ссылки на несуществующие (удаленные) файлы и папки;

– «Неверную деинсталляционную информацию» – программа выполняет проверку ключей реестра, предназначенных для хранения информации об удалении приложений;

– «Неверные ссылки на **DLL**» – производится проверка библиотек динамической компоновки (**DLL**), зарегистрированных в реестре, с помощью этого режима можно отыскать **DLL**, не используемые системой, а также ссылки на несуществующие **DLL**.

Также следует указать разделы реестра, в которых будет происходить поиск неверных ключей, и нажать кнопку «Начать».

После выполнения поиска ошибочных ключей программа отобразит окно «Результаты» (рисунок 7.5), в котором будут перечислены все ключи реестра, имеющие ошибочное значение.

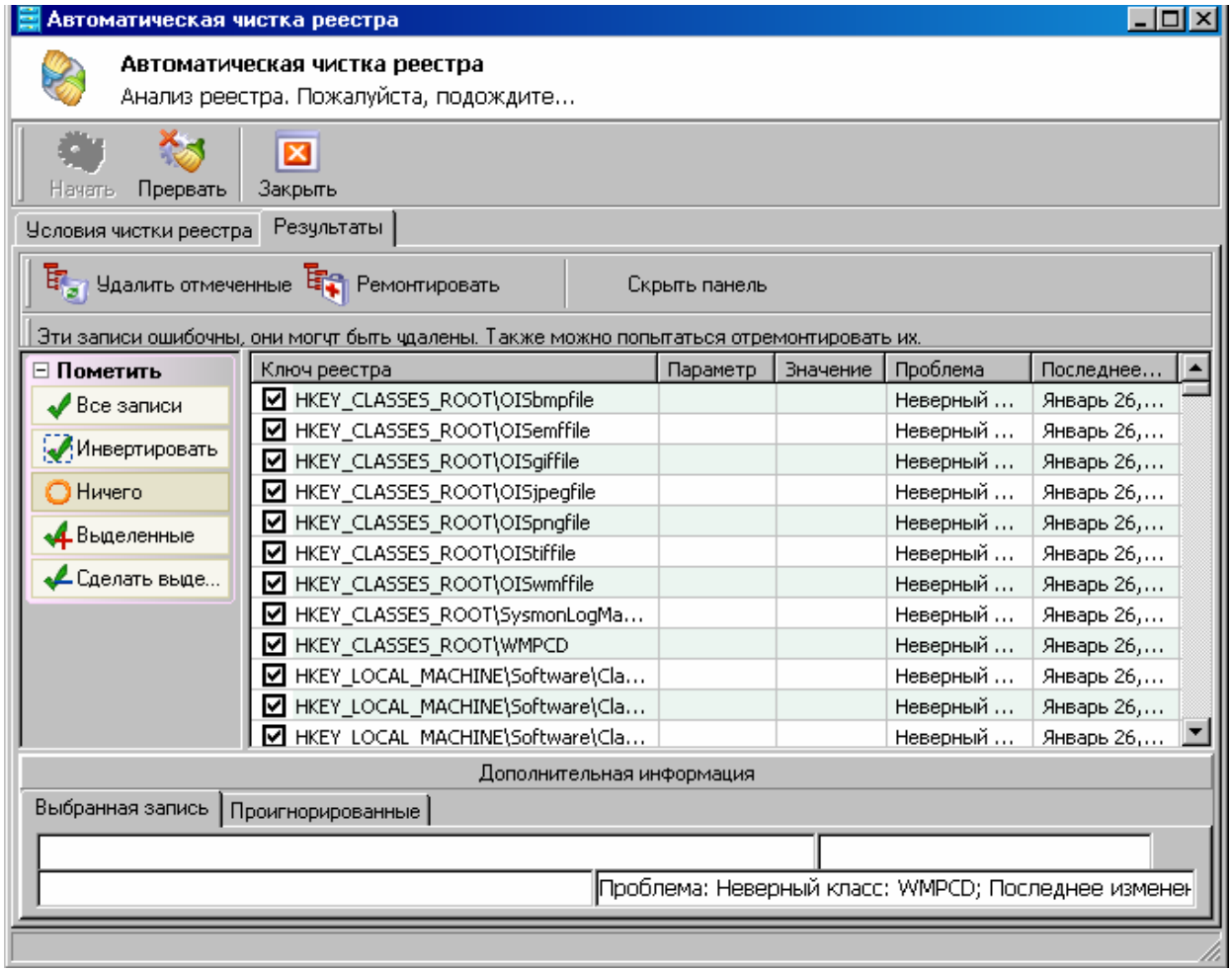


Рисунок 7.5 - Результаты автоматической чистки реестра

В большинстве случаев все найденные ссылки можно удалить, однако если необходимо исправить значение на верное, следует воспользоваться кнопкой «Ремонтировать». При этом будет открыто диалоговое окно поиска файлов и папок. Найдя требуемый файл, можно исправить значение параметра.

При удалении ключей из реестра **Reg Organizer** создает резервную копию, которая может быть использована для восстановления удаленных данных. Удаленные данные могут быть восстановлены командой «Команды \ Резервные копии».

7.1.4 Редактирование файлов

Данный режим позволяет просматривать и редактировать различные **INI-файлы**, которые используются для конфигурирования программ. Для открытия конфигурационного файла необходимо нажать кнопку «Открыть», при этом будет показано стандартное окно открытия файлов. Принцип работы с данным режимом напоминает работу с «Проводником» **Windows**, поскольку все разделы **INI-файлов** представляются в виде папок, а ключи, в свою очередь, содержатся в них.

После окончания работы с файлом его следует сохранить, для чего служит кнопка «Сохранить».

7.1.5 Поиск и замена

Этот режим используется для поиска и замены необходимых разделов и ключей. В разделе существует большое число управляющих элементов, которые позволяют максимально точно указать параметры поиска, что существенно сокращает как время поиска, так и количество параметров, удовлетворяющих указанным условиям. После задания всех требуемых параметров поиска (или замены) необходимо нажать кнопку «Искать» для начала процесса.

В том случае, если пользователем часто производится поиск с применением одних и тех же условий, рекомендуется применять «профили», т.е. наборы установок, сохраненные в файлах. Для сохранения «профиля» в файл или загрузки его из файла нужно воспользоваться закладкой «Профили».

Все результаты поиска заносятся в таблицу, присутствующую на закладке «Результаты». Пользователь может работать с найденными совпадениями (т.е. удалять или редактировать их). Для того чтобы отредактировать совпадение, необходимо выделить его и нажать кнопку «Изменить». После этого появится окно, позволяющее изменить выбранную запись (это может быть имя ключа реестра, имя параметра или значение параметра).

7.2 Защита документов Office

Как правило, пользователь работает с документами, которые не содержат никаких секретных данных, и не возникает необходимость в их защите от несанкционированного просмотра или изменения другими пользователями. Однако в некоторых случаях бывает весьма полезно установить подобную защиту, чтобы никто случайно (или намеренно) не мог менять определенный документ или даже открывать его.

В **Word** предусмотрена возможность защиты документа с помощью пароля - если пытающийся открыть документ не знает пароль, то у него ничего не получится. Однако есть и отрицательная сторона такой защиты - пользователь, установивший пароль, ни в коем случае не должен его забыть или потерять, т.к. в этом случае открыть документ будет практически невозможно, разве что прибегнуть к услугам специальных программных средств по подбору паролей.

Другая возможность защитить документ - установить пароль на его изменение. То есть любой желающий может открыть документ, однако внести в него изменения не получится, т.к. они не будут сохраняться - это так называемый режим только для чтения.

7.2.1 Защита от изменения

Итак, рассмотрим вначале более «мягкую» защиту - от изменения документа. Для этого нужно вызвать команду «Сервис \ Защитить документ», после чего отобразится диалоговое окно «Защита документа» (рисунок 7.6).

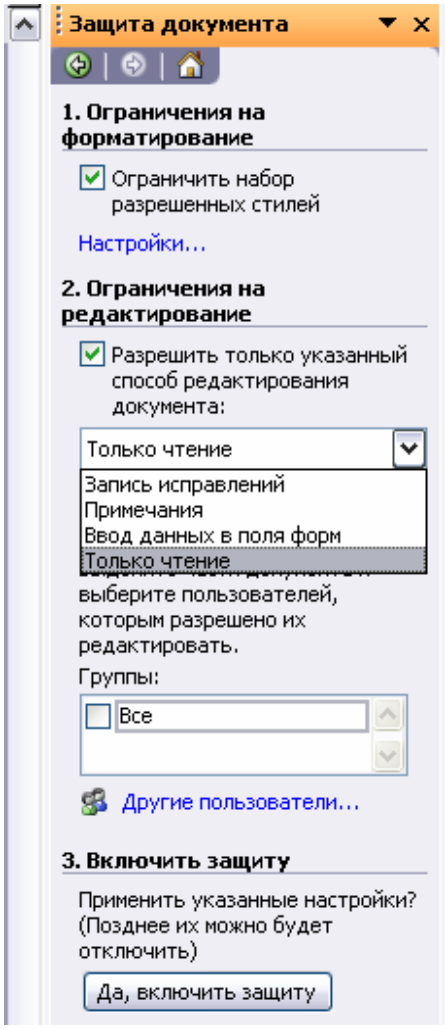


Рисунок 7.6 - Установка режима защиты документа

Здесь в верхней части имеются опции, которые позволяют запретить любые изменения, кроме:

– «Записи исправлений» - при выборе этой опции будет автоматически активизирован режим исправлений, его невозможно будет отменить (обычно это делается командой «Сервис \ Исправления»), и все изменения в документе будут отображаться в виде исправлений, внесенных рецензентами в исходный текст. Это довольно полезная опция, позволяющая установить запрет на несанкционированное внесение изменений в документ;

– «Вставки примечаний» - этот режим аналогичен предыдущему, также запрещается редактировать документ, и можно лишь вставлять примечания в то или иное место документа;

– «Ввода данных в поля форм» - эта опция может быть использована для защиты от изменения текста в том или ином разделе документа, если в доку-

менте имеется более одного раздела (т.е. вставлен хотя бы один разрыв раздела), то таким образом можно установить защиту на отдельные разделы, в то время как для всех остальных разделов изменения будут разрешены.

Вообще, снять описанную выше защиту документа достаточно просто - для этого нужно в меню «Сервис» выполнить команду «Снять защиту» (она появится вместо команды «Установить защиту» сразу после установки защищенного режима), после чего можно спокойно редактировать документ.

Соответственно, в меню «Сервис» снова появится команда «Защитить документ». Очевидно, такая защита вряд ли может претендовать на обеспечение высокого уровня безопасности документа. По этой причине в окне «Защита документа» имеется поле для ввода пароля, без которого впоследствии невозможно будет снять установленную защиту.

Для защиты документа необходимо ввести пароль в поле «Пароль» (необязателен) (рисунок 7.7). После его ввода (символы будут отображаться в виде звездочек) и нажатия кнопки необходимо еще раз ввести пароль для его подтверждения. Это делается во избежание случайного или ошибочного ввода, т.к. отменить указанный пароль после активизации защиты уже будет практически невозможно.

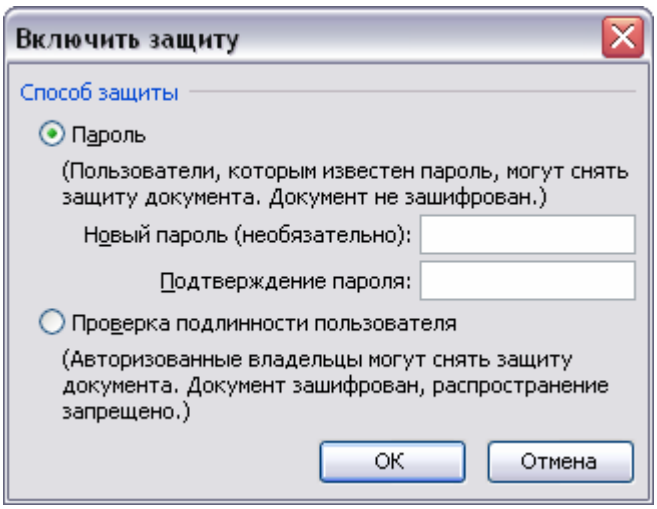


Рисунок 7.7 - Окно подтверждения пароля для защиты документа от изменений

Итак, защита от несанкционированного изменения установлена, и пароль

задан. Если через некоторое время пользователю потребуется внести некоторые изменения в документ, для этого нужно выполнить команду «Сервис/Снять защиту», после чего появится окно «Снятие защиты». Здесь нужно ввести заданный ранее пароль, и после нажатия «ОК» защита с документа будет снята.

7.2.2 Зашита от открытия

Более серьезная защита документа, которая может потребоваться для защиты конфиденциальной информации от посторонних глаз, это пароль на открытие документа. Если пароль неизвестен постороннему пользователю, то открыть документ он не сможет в принципе.

Чтобы установить защиту на открытие документа, необходимо вначале активизировать окно «Параметры» командой «Сервис \ Параметры». Затем необходимо раскрыть закладку «Безопасность» (рисунок 7.8).

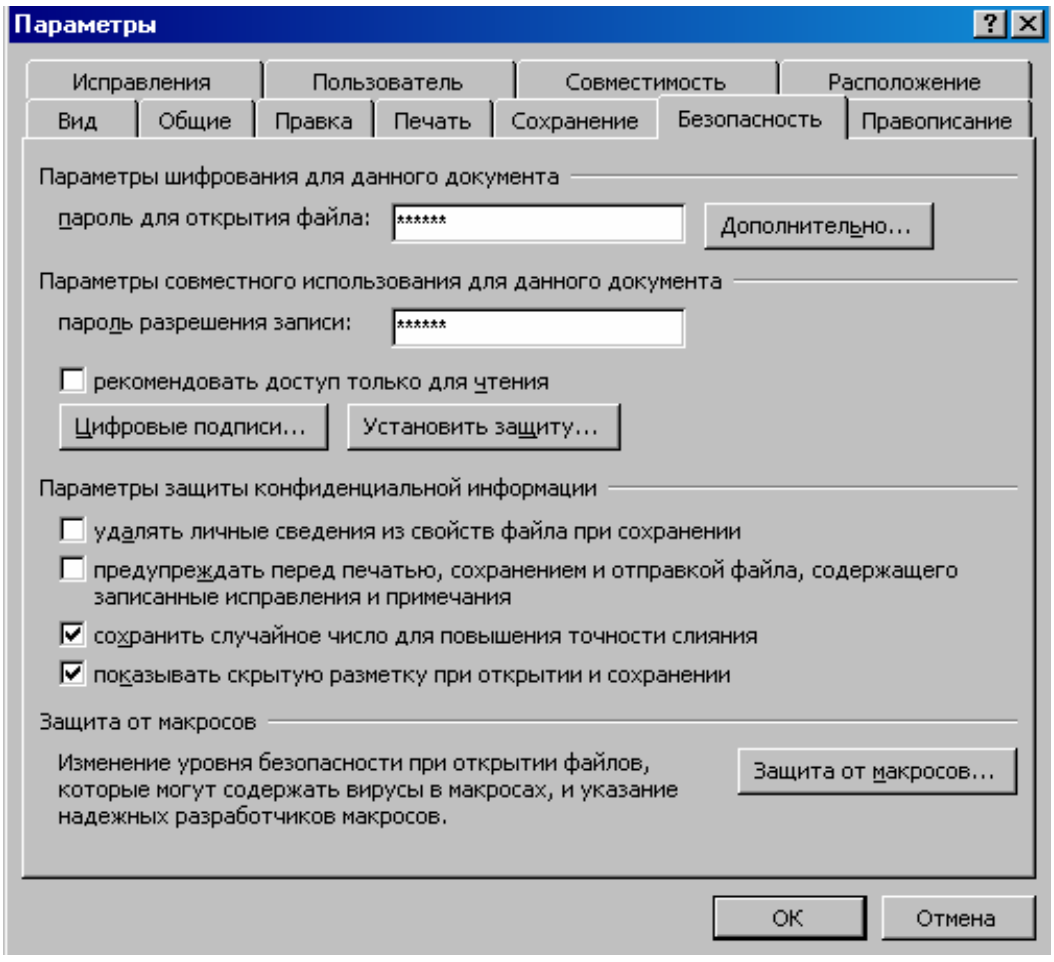


Рисунок 7.8 - Настройка параметров безопасности

Здесь имеются следующие параметры:

– «Пароль для открытия файла» позволяет установить пароль, который **Word** будет требовать при попытке открытия данного документа по умолчанию максимальная длина пароля на открытие документа составляет 15 символов. Для установки более сложного режима защиты можно воспользоваться кнопкой «Дополнительно», при нажатии которой открывается окно, где можно выбрать тип шифрования, это позволит повысить степень защиты документа и увеличить максимально допустимое количество символов в пароле (например, до 40);

– «Пароль разрешения записи» - дает возможность установить пароль, который **Word** будет требовать для изменения документа, если пользователь знает пароль на разрешение изменений, он может получить доступ к документу в режиме редактирования, если же пароль не известен, то следует воспользоваться кнопкой «Только чтение», чтобы просто ознакомиться с содержимым данного документа, наконец, если нажать здесь кнопку «Отмена», то документ не будет открыт;

– «Рекомендовать доступ только для чтения» - установка этого флажка означает, что при открытии данного файла будет предварительно отображаться окно с предложением открыть файл только для чтения, это никак не зависит от установки паролей, и может быть задано без них.

Если пользователь нажмет кнопку «Да», то документ откроется и в него можно будет вносить изменения. Однако сохранить эти изменения можно будет только в другом файле, с помощью команды «Файл \ Сохранить как». С другой стороны, если нажать «Нет», то документ откроется в обычном режиме.

Если установлен пароль разрешения записи, то выбор опции «Рекомендовать доступ только для чтения» ни к чему не приведет: будет отображаться только окно «Пароль».

Отметим, что каждый раз при задании нового пароля необходимо подтвердить выбранный пароль с целью повышения безопасности и во избежание случайного ввода.

Кнопка «Защита от макросов» окна «Параметры» позволяет установить

уровень безопасности при открытии с документов с макросами. Это очень важная настройка, т.к. в **DOC-файлах** вирусы, если таковые имеются, находятся именно в макросах.

7.2.3 Цифровая подпись

К файлу или проекту макроса также можно выполнить добавление цифровой подписи, если для этого имеется цифровой сертификат, который можно получить в коммерческом центре сертификации или у администратора внутренней безопасности.

Цифровой сертификат можно создать и самостоятельно при помощи программы **SelfCert.exe**, которая входит в поставку пакета **Microsoft Office**. Она может быть использована в распространяемых или публикуемых документах, связанных с работой организации, в окончательных и неизменных вариантах документов, предназначенных для сотрудников организации. Необходимо учитывать, что сертификаты, созданные пользователем самостоятельно, рассматриваются как неподтвержденные и при высоком или среднем уровне безопасности приводят к выводу предупреждения системы безопасности.

Приведем пример создания цифровой подписи и присоединение их к документу. Для получения цифрового сертификата необходимо в «Проводнике» **Windows** найти и активизировать файл **SelfCert.exe**. После запуска программы на выполнение на экране отобразится окно, в котором будет приглашение ввести собственную подпись, и даны некоторые рекомендации по использованию сертификата (рисунок 7.9). После ввода подписи и нажатии на кнопку «ОК» выводится окно, подтверждающее создание личного сертификата.

После активизации окна «Параметры» (команда «Сервис \ Параметры») следует раскрыть вкладку «Безопасность» и нажать кнопку «Цифровые подписи», после чего выбрать добавляемый сертификат из списка.

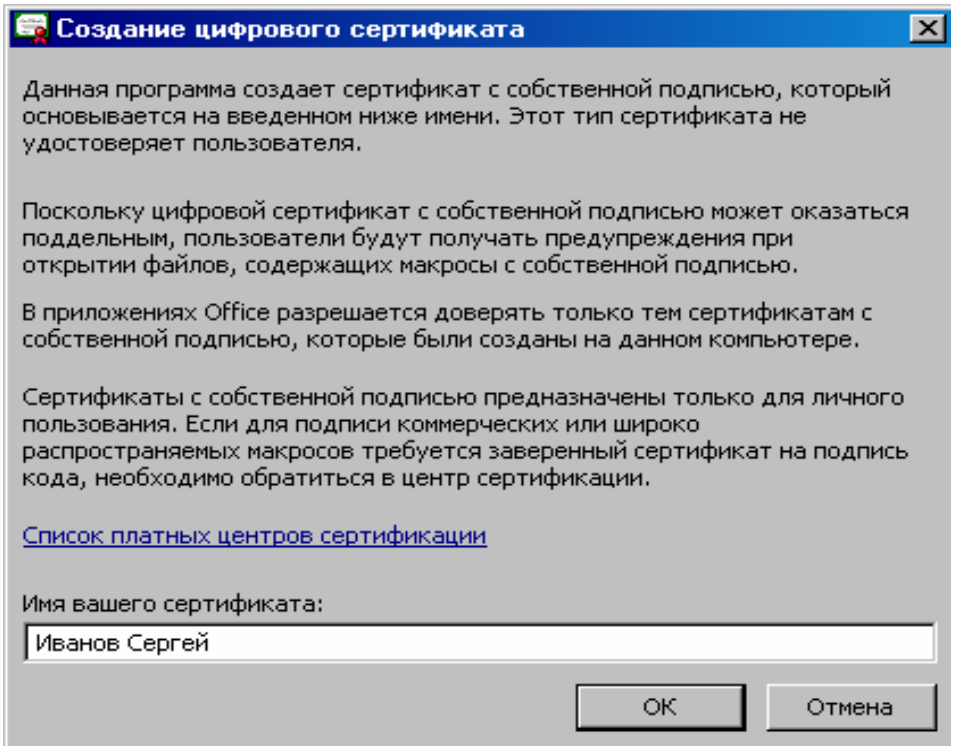


Рисунок 7.9 - Создание цифрового сертификата

7.2.4 Подбор паролей к документам Word. Advanced Office XP Password Recovery

Для взлома паролей, установленных на файл **Microsoft Word**, можно воспользоваться специально разработанными для этого программами. Необходимо отметить, что такие программы могут понадобиться не только злоумышленникам, но и пользователю, который создал и зашифровал документ, а потом в силу каких-либо обстоятельств забыл или потерял ключ, при помощи которого можно получить доступ к документу.

Примером программы взлома пароля документа **Word** служит **Advanced Office XP Password Recovery.** Данная программа была разработана специально для восстановления потерянных паролей для документов, созданных при помощи пакета **Microsoft Office 97/2000/XP**. Скачать программу можно с сайта http://www.officexppasswordrecovery.info (рисунок 7.10).

Она поддерживает следующие регистрирующие пароли:

– для **Microsoft Word** - пароль на открытие, пароль на изменение, пароль защиты документа;

– для **Microsoft Excel** - пароль на открытие, пароль на изменение, паро-

ли листа, пароль рабочей книги, общедоступный пароль рабочей книги;

– для **Microsoft Access** - пароль общего уровня.

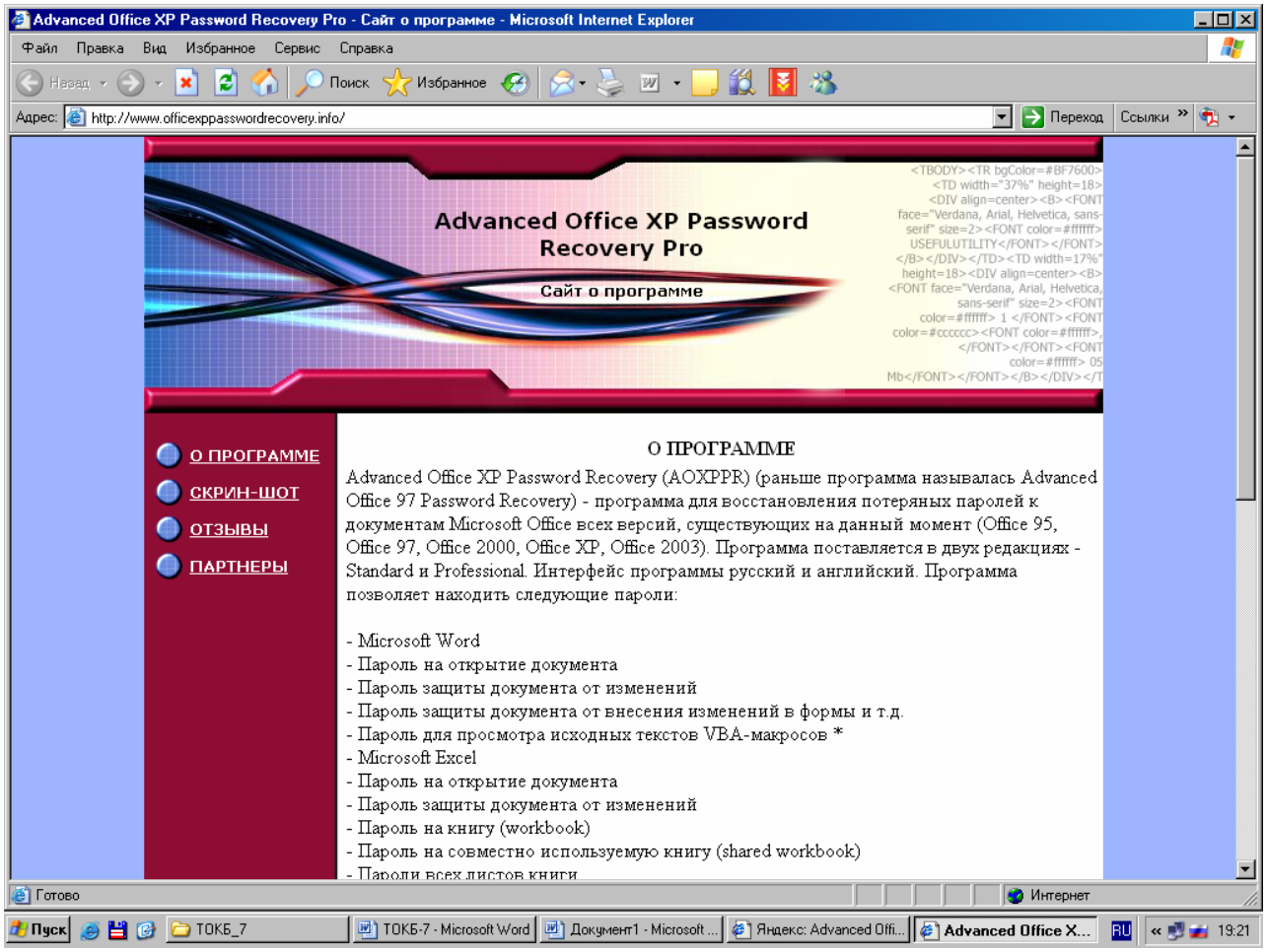


Рисунок 7.10 - Сайт программы **Advanced Office XP Password Recovery**

Приятной особенностью программы является то, что она поддерживает два языка интерфейса: английский, устанавливающийся сразу после установки программы, и русский.

Окно программы содержит несколько областей (рисунок 7.11). В верхней части размещается поле, где отображается путь к файлу, который необходимо взломать, а также переключатель выбора типа атаки. Путь к файлу можно указать, воспользовавшись кнопкой открытия файла, расположенной у левого края панели инструментов.

По центру окна располагается область настройки, в которой устанавливаются следующие параметры:

– предполагаемая длина и диапазон пароля;

– опции словаря;

– опции программы;

– тесты скорости для текущего компьютера;

– информация о текущей системе.

Ниже размещается поле сообщений, в котором отображается ход проведения дешифровки пароля.

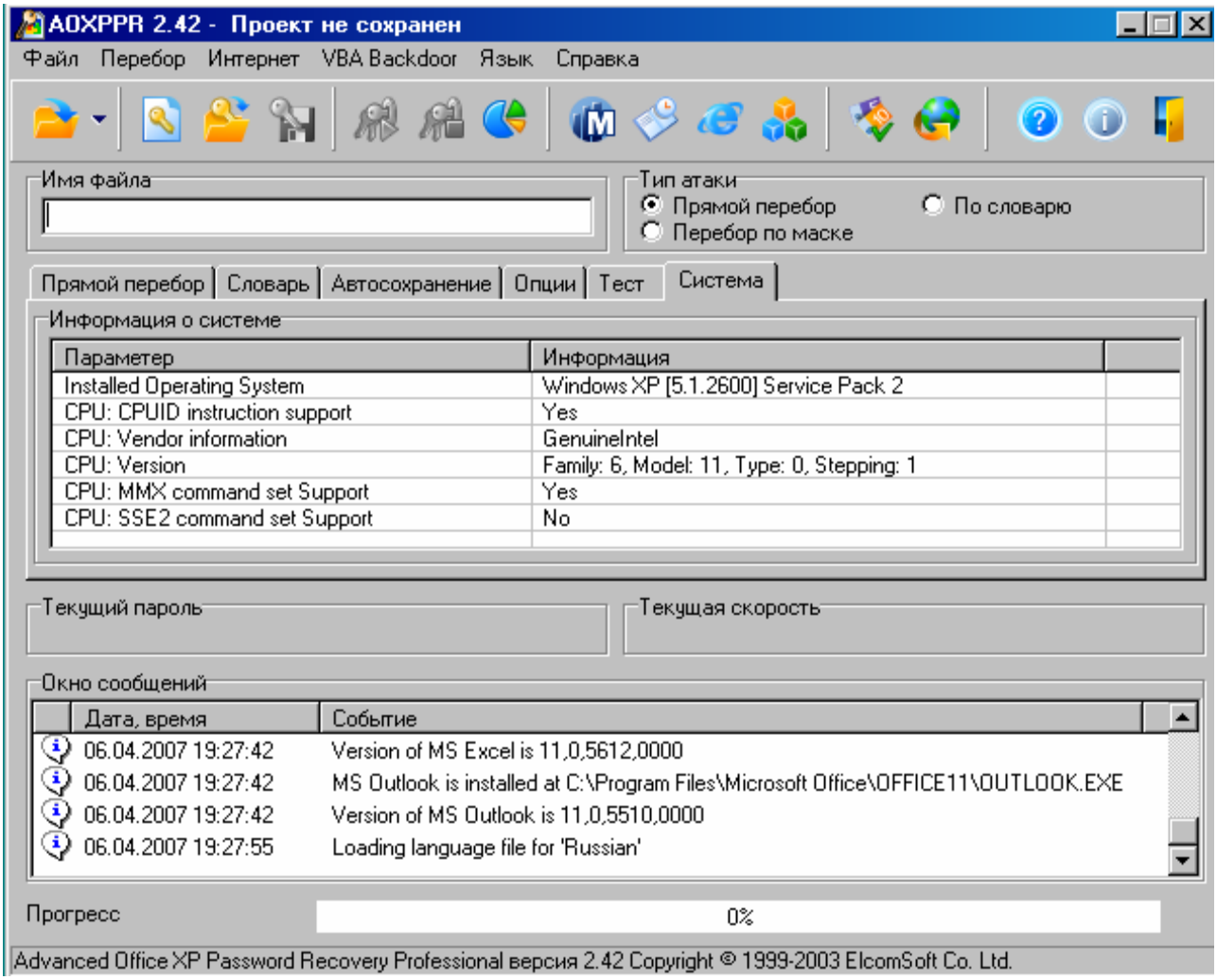


Рисунок 7.11 - Окно программы **Advanced Office XP Password Recovery**

После открытия файла для него необходимо определить настройки программы, в частности - тип атаки (прямой перебор, перебор по маске или по словарю).

«Прямой перебор» – является наиболее надежным, но довольно продолжительным способом восстановления пароля. Программа генерирует и прове-

ряет все пароли из указанного диапазона. Для этого необходимо указать диапазон используемых символов, из которых следует генерировать пароли.

«Атака по маске» – это расширенный вариант прямого перебора. Добавляется возможность задания маски для искомого пароля. При этом можно отметить неизвестные символы, и программа будет перебирать только их.

«Атака по словарю» – заключается в том, что есть словарь (текстовый файл, в котором каждая строка содержит одно слово), при помощи которого программа автоматически проверяет все слова. Такая атака удобна, если пароль является значимым словом, которое может встретиться в каком-нибудь из словарей. Словари можно составлять самому или использовать готовые. Можно рекомендовать словари, которые размещены на сайте www.outpost9.com.

Необходимо отметить, что количество значимых слов в любом языке исчисляется сотнями тысяч, которые современная техника может перебрать за считанные секунды. После определения указанных настроек выполняется нажатие на кнопку запуска перебора паролей. При этом в соответствующих полях отображается текущий проверяемый набор символов и текущая скорость перебора.

После определения пароля на экране отображается окно «Пароль успешно найден!» со статистикой.

7.3 Шифрование файловой системы

В этом разделе будут рассмотрены вопросы защиты компьютера с помощью средств криптографии, а именно: средства шифрования файлов и папок, которые предоставляет система **Windows 2000/XP.** Данные программы служат для закрытия локального доступа к файлам и папкам компьютера с использованием пароля.

7.3.1 Файловая система Windows

В систему **Windows 2000/X**P включено такое средство защиты, как шифрующая файловая система **EPS** (**Encrypted File System**). Она обеспечивает ядро технологии шифрования файлов, которое используется для хранения шифро-

ванных файлов в файловой системе **NTFS**.

Для шифрования применяется асимметричный алгоритм **DESX** с секретным 56-разрядным ключом, генерируемым для каждой папки или файла. Данный ключ шифруется открытым ключом пользователя **Windows** и присоединяется к шифруемому файлу или папке как атрибут **DDF** (**Data Decipher Field** - поле дешифрации данных), который расшифровывается закрытым ключом пользователя при открытии файла.

Шифрование является прозрачным для пользователя, зашифровавшего файл, поэтому он имеет возможность работать с этим файлом так же, как и с другими файлами или папками (без расшифровки). При работе с зашифрованными файлами и папками необходимо учитывать следующие моменты:

– шифруются только файлы и папки, находящиеся на томах **NTFS**;

– сжатые файлы и папки, а также файлы и папки, открытые для общего доступа, не могут быть зашифрованы;

– зашифрованные файлы могут стать расшифрованными, если файл копируется или перемещается на том, не являющийся томом **NTFS**;

– при перемещении незашифрованных файлов в зашифрованную папку они автоматически шифруются (обратная операция не проводится);

– не могут быть зашифрованы файлы с атрибутом **System** (Системный).

После шифрования доступ к файлу может получить либо сам пользователь, выполнивший шифрование, либо агент восстановления (пользователь, имеющий права на открытие шифрованных файлов и которому выдан сертификат открытого ключа для восстановления пользовательских данных, закодированных шифрованной файловой системой (**EFS**)).

По умолчанию таким агентом назначается локальный администратор системы, однако система **Windows 2000/XP** позволяет делегировать права агента восстановления любым пользователям, у которых имеются файлы сертификатов. Шифрование файлов и папок выполняется установкой для них свойств шифрования так же, как устанавливаются атрибуты **Read Only** (Только чтение), **Archive** (Архивный) или **Hidden** (Скрытый).

Следует отметить, что при шифровании папки пользователем все файлы и

вложенные в нее папки, созданные в ней или добавленные, также автоматически шифруются. Рекомендуется использовать шифрование на уровне папки. Для выполнения шифрования папки необходимо вызвать окно ее свойств и на вкладке «Общие» нажать кнопку «Другие», в результате чего откроется диалоговое окно «Дополнительные атрибуты». В данном окне следует установить опцию «Шифровать содержимое для защиты данных».

После подтверждения необходимости шифрования папки (нажатием на кнопку «ОК») и закрытия диалоговых окон отобразится запрос ни необходимость применения шифрования папки ко всем вложенным в нее файлам и папкам. Если подтверждение запроса получено, система шифрует все файлы и вложенные папки. Если же нет, то все файлы и вложенные папки остаются незашифрованными. Однако все добавляемые в нее при последующей работе файлы и папки будут зашифрованы.

После выбора опции шифрования и нажатия на кнопку «ОК» будет запущен процесс шифрования содержимого папки. На этом процесс шифрования папки завершается.

7.3.2 Использование команды cipher

Файлы и папки также могут быть зашифрованы или расшифрованы при помощи команды **cipher**. Чтобы получить сведения об этой команде, следует перейти в консольный режим, для чего в кнопке «Пуск \ Выполнить» ввести команду **cmd**, затем набрать команду **cipher** с ключом **/?**, в результате отобразится окно с ее описанием.

Синтаксис команды:

cipher [{/e|/d}] [/s: каталог] [/a] [/i] [/f] [/q] [/h] [/k] [/u[/n]] (путь [...]] | [/r :имя файла без расширения] | [/w:путь]

Команда имеет следующие параметры:

- **/e** шифрует указанные папки;
- **/d** - расшифровывает указанные папки;
- **/s:каталог** - указывается шифруемая папка;
- **/a** - выполняет операцию шифрования и над файлами и над каталогами;

– **/i** - продолжение выполнения указанной операции после возникновения ошибок;

– **/f** - выполнение шифрования или расшифровывания указанных объектов;

– **/q** - запись в отчет только важных сведений;

– **/h** - отображение скрытых и системных файлов;

– **/k** - создание ключа шифрования файла пользователя, при этом все остальные параметры команды не учитываются;

– **/u** - обновление ключа шифрования файла пользователя или ключа агента восстановления (применяется вместе с параметром **/n**);

– **/n** - запрет обновления ключей и поиск всех зашифрованных файлов на локальных дисках (используется только с параметром **/u**);

– **/r**:**имя_файла_без_расширения** - создание нового сертификата агента восстановления и закрытого ключа, с записью их в файлах с именем, которое указывается в параметре **имя_файла_без_расширения**;

– **/w**:**путь** - удаление данных из неиспользуемых разделов тома, параметр путь служит для указания на любой каталог нужного тома.

Команда **cipher**, заданная без параметров, отображает состояние шифрования текущей папки и всех находящихся в ней файлов. При использовании команды **cipher** имеется возможность использовать несколько имен папок и подстановочные знаки. Параметры, указываемые в ней, должны быть разделены между собой хотя бы одним пробелом. Так, чтобы зашифровать папку **Data**, расположенную в папке **Soft** на диске **D:**, необходимо выполнить следующую команду: **cipher/e D:\Soft\Data.**

Чтобы зашифровать файл **Users.doc**, находящийся в папке **Data**, необходимо ввести: **cipher/e/a D:\Soft\Data\Users.doc.**

После выполнения шифрования текстового файла пользователю выдается сообщение о том, что преобразование файла из обычного текстового формата в зашифрованный текст может оставлять фрагменты прежнего незашифрованного текста в неиспользуемом дисковом пространстве, и рекомендуется использовать команду **cipher** с ключом **/w:путь** для очистки диска после преобразова-

ния.

При попытке другого пользователя открыть зашифрованный файл или папку он получит сообщение системы о том, что данный пользователь не обладает достаточными для этого полномочиями.

7.4 Контрольные вопросы

7.4.1 В чем недостатки редактирования реестра с помощью программ **regedit.exe** и **regedit32.exe**?

7.4.2 В чем преимущества специализированных утилит редактирования реестра?

7.4.3 На какие категории делятся утилиты для работы с реестром **Windows**?

7.4.4 Чем отличаются редакторы реестра и утилиты-оптимизаторы?

7.4.5 Для чего служит утилита **Reg Organizer**?

7.4.6 Как можно установить **Reg Organizer** на домашний компьютер?

7.4.7 Перечислите режимы работы с утилитой **Reg Organizer**, в чем их особенности?

7.4.8 Какие закладки имеются в режиме «Чистка реестра» утилиты **Reg Organizer?**

7.4.9 Какие условия поиска можно задать в режиме «Автоматическая чистка реестра»?

7.4.10 Какие варианты обработки ошибочных ключей предлагает утилита **Reg Organizer**?

7.4.11 Для чего служит режим «Редактирование файлов» утилиты **Reg Organizer**?

7.4.12 Какие возможности защиты документа предусмотрены в **MS Word**?

7.4.13 Какие варианты защиты от изменений документа предусмотрены в **MS Word**?

7.4.14 В чем особенность режима записи исправлений при защите документа в **MS Word**?

7.4.15 Как установить защиту документа от открытия в **MS Word**?

7.4.16 В чем особенность дополнительной защиты документа от открытия в **MS Word**?

7.4.17 Для чего служит пароль разрешения записи в **MS Word**?

7.4.18 Для чего используется цифровая подпись документов в **MS Word**?

7.4.19 Как получить цифровой сертификат для документа **Microsoft Office**?

7.4.20 Для чего служит программа **Advanced Office XP Password Recovery**?

7.4.21 Где можно найти программу **Advanced Office XP Password Recovery**?

7.4.22 Какие режимы атаки используются в программе **Advanced Office XP Password Recovery**?

7.4.23 В чем особенности атаки по словарю в программе **Advanced Office XP Password Recovery**?

7.4.24 В чем особенности атаки прямым перебором в программе **Advanced Office XP Password Recovery**?

7.4.25 Какое средство криптографической защиты включено в систему **Windows 2000/XP**?

7.4.26 Для чего служит шифрующая файловая система **EPS** в **Windows 2000/XP**?

7.4.27 Какие особенности шифрования следует учитывать при использовании системы **Encrypted File System**?

7.4.28 Для чего служит команда **cipher?**

7.4.29 Как запустить команду **cipher?**

7.4.30 Как вывести на экран описание команды **cipher**?

8 Сетевая атака

В настоящее время, когда получение оперативной информации становится необходимостью, многие пользователи подключают свои компьютеры к сети **Internet**. Конечно, сеть имеет большое число преимуществ, таких, как мгновенное получение необходимой информации, электронная переписка с адресатами, находящимися в любых точках мира, **online-общение** и т.д. Но сеть хранит в себе и угрозу, связанную, в первую очередь, с кражей информации с компьютера пользователя. К сети может быть подключен компьютер злоумышленника, которого наверняка заинтересует информация, хранящаяся на чужом компьютере.

Хакер, используя специальные программы, может получить доступ к жесткому диску компьютера и либо скопировать с него интересующую информацию, либо оставить на компьютере пользователя какой-нибудь вирус, который будет похищать такую информацию, как пароли, личную переписку и др.

8.1 Понятие сетевой атаки

Существует несколько понятий, которые непосредственно относятся к теории компьютерной безопасности, а именно: **угрозы, уязвимости и атаки**.

Угроза безопасности компьютерной системы является, по определению, потенциально возможным событием, которое может произойти либо в результате случайных действий пользователя, либо из-за преднамеренного вмешательства в систему. Это событие может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

К уязвимостям какой-либо системы (даже не обязательно компьютерной) **относятся те ее недостатки**, некорректно установленные параметры и прочие характеристики, **которые дают возможность злоумышленнику проникнуть в нее.**

Сетевая атака - действие, производимое злоумышленником, и направленное на реализацию угрозы. Действие заключается в поиске какой-либо уязвимости компьютерной системы с применением как специализированных про-

граммных средств, так и с помощью различных психологических приемов.

В современной теории безопасности можно выделить **три основных вида угроз безопасности - это угрозы раскрытия, целостности и отказа в обслуживании**.

При угрозе раскрытия информации злоумышленник получает к ней доступ и имеет возможность ее прочитать. Фактически, происходит утечка информации из компьютерной системы или из среды передачи данных.

Угроза целостности включает в себя любое умышленное изменение (модификацию или даже удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую. Обычно считается, что угрозе раскрытия подвержены в большей степени государственные структуры, а угрозе целостности - деловые или коммерческие организации.

При угрозе отказа злоумышленник пытается выполнить такие действий, которые привели бы к блокировке доступа к некоторому ресурсу вычислительной системы. Чаще всего данная угроза возникает в том случае, когда злоумышленник не может выполнить угрозу раскрытия и угрозу целостности. Отказ компьютерной системы может быть как постоянным, так и временным, однако этого времени обычно достаточно для того, чтобы ресурс стал невостребованным.

Но возникает вопрос, что же дает нарушителю возможность проникновения в чужие системы? **К причинам, вызывающим уязвимость системы**, можно отнести:

– открытость системы, свободный доступ к информации по организации сетевого взаимодействия, протоколам и механизмам защиты;

– наличие ошибок в программном обеспечении, операционных системах и утилитах, которые открыто публикуются в сети;

– разнородность используемых версий программного обеспечения и операционных систем;

– сложность организации защиты межсетевого взаимодействия;

– ошибки конфигурирования систем и средств зашиты;

– неправильное администрирование систем;

– несвоевременное отслеживание и выполнение рекомендаций специалистов по защите и анализу случаев вторжения для ликвидации лазеек и ошибок в программном обеспечении;

– «экономия» на средствах и системах обеспечения безопасности или игнорирование этих систем;

– умолчание о случаях нарушения безопасности своего хоста или сети.

8.2 Алгоритм сетевой атаки

Любую сетевую атаку можно разбить на шесть этапов:

– выбор хоста (конечного сетевого устройства, компьютера), на который будет осуществляться атака;

– подробное изучение сетевой инфраструктуры атакуемой системы;

– перехват и анализ сетевого трафика для получения имен пользователей, паролей и другой необходимой информации;

– сканирование портов с целью определение доступных служб и сервисов;

– исполнение сетевой атаки на основании полученных данных;

– корректное завершение атаки;

Выбор жертвы зависит, естественно, от желаний злоумышленника. Подробное изучение сетевой инфраструктуры системы можно начать с посещения **Web-сервера** атакуемой фирмы, на котором можно найти сведения о ее истории, корпоративной культуре и партнерах. На этом же этапе исследуются электронные «реквизиты» партнеров, по которым часто удается обнаружить дополнительные соединения с исследуемой сетью. Обычно информационные системы удаленных офисов или мелких партнерских компаний защищены гораздо слабее основной сети.

Перед сканированием системы желательно провести «пассивное» наблюдение за ней с применением таких программ, как снифферы, если это возможно. При этом можно получить большое число полезной информации, например адреса электронной почты сотрудников фирмы, а если повезет, то логины и пароли для доступа к различным службам. Этот этап может занять до-

вольно долгое время, но поскольку само наблюдение является пассивным, его практически невозможно выявить. В том случае, если пассивное получение информации невозможно, следует переходить к сканированию портов системы с целью определение доступных служб и сервисов. Это можно осуществить с помощью различных сканеров:

– «сканеры портов» - позволяют просканировать систему и получить список портов, открытых на удаленном компьютере, а также имена служб, которые «слушают» порты (например, программа **Nmap** позволяет выполнить все вышеуказанные действия);

– «сканеры безопасности» - используются для выявления уязвимостей и системах, в отличие от сканеров портов, сканируют только те порты системы, в которых могут быть обнаружены уязвимые службы (для их определения используются данные, имеющиеся в базах уязвимостей сканера), таким образом, принцип работы сканеров безопасности аналогичен работе антивирусных программ-сканеров; для выявления новых брешей в системе необходимо постоянно обновлять базы уязвимости (для выполнения перечисленных действий следует использовать программы **Retina**, **XSpider** и др.);

– «сканеры открытых ресурсов» – применяются для автоматизации процесса поиска открытых сетевых ресурсов (например, **xSharez**).

После получения списка сервисов необходимо провести анализ и попытаться найти в них уязвимые места. Следует проверить их степени уязвимости: попытаться войти в систему с использованием стандартных логинов и паролей, нарушить работу сервисов, скопировать файлы с паролями (если имеются открытые ресурсы) и т.д. Этот этап тесно связан с первым, поскольку действия, предпринимаемые при атаке, зависят от целей. Если необходимо просто вызвать сбой в работе какой-либо службы, можно применить эксплойт (**Exploit**, **X-ploit**) - программу, использующую уязвимость в определенной службе для воздействия на нее. Естественно, какой-либо эксплойт рассчитан на применение к конкретной службе. Очень часто эксплойты поставляются разработчиками не в виде готовых программ, а в виде исходных кодов.

На следующем этапе злоумышленник должен обеспечить свою безопас-

ность, а именно - очистить файлы журнала (**LOG-файлы**), которые ведутся системой. Кроме этого, хакер может оставить «троянского коня», чтобы иметь «плацдарм» для осуществления атак на другие компьютеры сети.

8.3 Обнаружение атаки. Сканеры безопасности

Прежде чем приступить к рассмотрению способов обнаружения сетевой атаки, приведем краткие описания нескольких программ, предназначенных для проверки целостности системы. Некоторые из них осуществляют попытки поиска известных уязвимых мест системы, другие проводят сравнение системы с заранее заданным состоянием (которое, по мнению разработчиков, является наиболее безопасным и обеспечивает максимальную защиту).

Основные возможности этих программ перечислены ниже:

– выяснение восприимчивости к проникновению из незащищенных систем;

– поиск брешей в программах (**back door**) и программ типа «троянский конь»;

– определение слабых паролей;

– определение неправильных настроек **брандмауэров**, **Web**-серверов и баз данных.

Технология анализа защищенности является действенным методом реализации политики сетевой безопасности прежде, чем осуществится попытка ее нарушения снаружи или изнутри организации.

Программы, которые реализуют проверку системы на наличие уязвимых мест, называются **сканерами безопасности**. Их с успехом используют как администраторы, так и злоумышленники, поскольку цели применения в обоих случаях одинаковы - выявить незащищенные места системы.

Однако применение результатов сканирования системы выполняется поразному – администратор пытается устранить брешь в системе, а злоумышленник использует результаты для незаконного проникновения в систему.

Ниже будет приведено краткое описание программ данного типа.

8.3.1 Retina 4.9

Сканер (рисунок 8.1) разработан компанией **eEye Digital Security** (http://www.eeye.com) и обладает следующими возможностями.

– удобство в использовании, автоматизация процессов сканирования, простой интерфейс и удобное представление информации;

– слабая нагрузка на сеть, используемые технологии позволяют сканеру **Retina** вести процесс сканирования и при этом не производить больших объемов лишнего трафика, который может привести к чрезмерной нагрузке сети;

– автоматическое обновление баз безопасности – служит для загрузки с сайта производителя баз безопасности, в которых содержится описания новых уязвимых мест компьютерных систем;

– автоматическое отслеживание беспроводных подключений – предназначено для отслеживания и блокировки незаконных подключений к сети, построенной на основе беспроводных технологий.

– **Common Hacker Attack Methods (CHAM) –** технология, предназначенная для выявления атак злоумышленников, а также анализа подключений и определения их типа;

– **Auto-Fix function –** позволяет производить анализ сканируемого компьютера и в случае обнаружения уязвимостей (например ошибок в настройке реестра, в правах доступа к файлам и папкам) автоматически устранять их.

Таким образом, **Retina** обладает возможностью проверки большинства сетевых протоколов. Сканер подвергает тестированию на защищенность **SQL-серверы**, брандмауэры и прокси-серверы.

Простой и удобный интерфейс программы позволит начинающим пользователям эффективно применять программу, а встроенные подсказки помогут лучше ориентироваться во всех режимах ее работы. Возможность построения различных отчетов собирает результаты проверки в единое целое и делает их красиво оформленными.

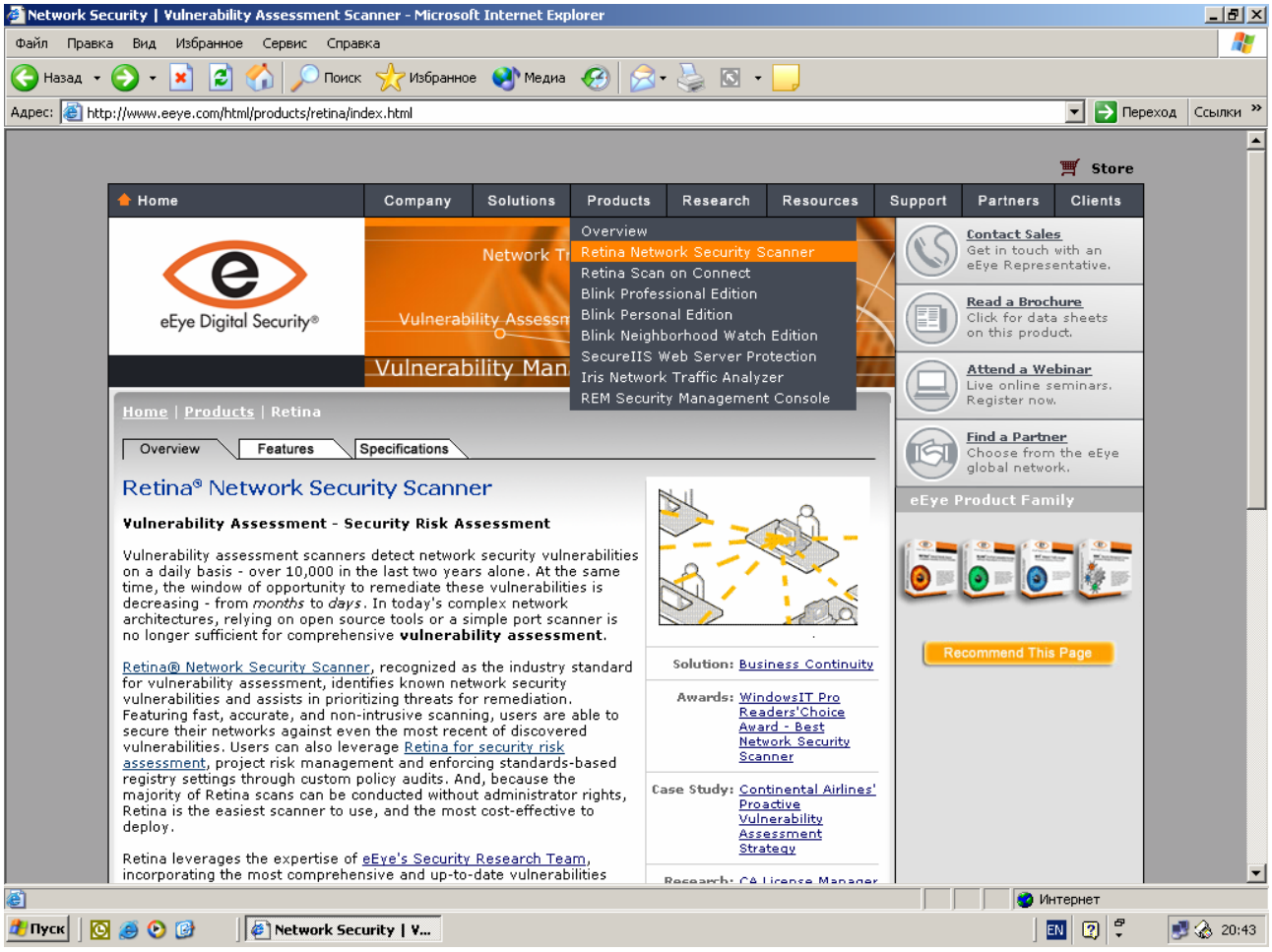


Рисунок 8.1 - Сайт компании **eEye Digital Security**

8.3.2 XSpider 7

Фирма **Positive Technologies** (http://www.ptsecuritv.ru) специализируется на разработке программ для обеспечения сетевой безопасности. Их разработка, сканер безопасности **XSpider** версии 7.5 (рисунок 8.2), обладает следующими возможностями:

– одновременное сканирование большого числа компьютеров, что позволяет упростить и ускорить процесс мониторинга сетевой безопасности в компьютерной сети любого масштаба;

– ведение подробных журналов истории проверок; создание отчетов с различными уровнями их детализации; удобный графический интерфейс;

– использование концепций «задач» и «профилей» для эффективного управления процессом мониторинга безопасности;

– гибкий планировщик заданий для автоматизации работы;

– встроенная документация, включающая контекстную справку и учеб-

ник.

Рисунок 8.2 - Сайт фирмы **Positive Technologies**

Подробнее о возможностях данного сканера можно прочесть на Web-странице http://securitylab.ru.

8.3.3 Nessus Security Scanner 2.0.7

Как и две предыдущих программы, **Nessus Security Scanner** (http://www.nessus.org) обладает большим количеством возможностей по защите персонального компьютера (рисунок 8.3). Для поиска уязвимостей используются как стандартные средства тестирования и сбора информации о конфигурации и функционировании сети, так и специальные средства, эмулирующие действия злоумышленника по проникновению в системы, подключенные к сети.

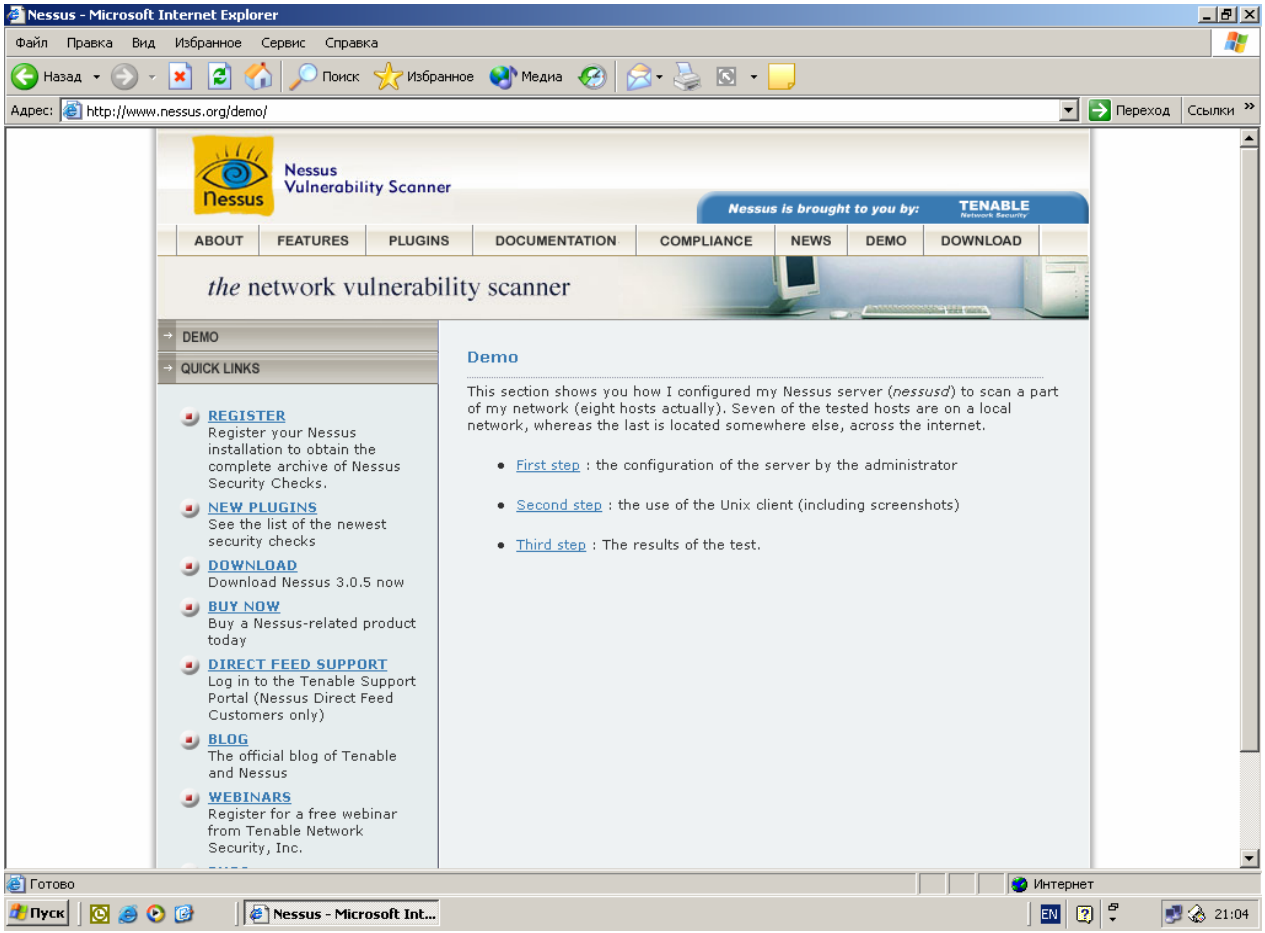


Рисунок 8.3 - Сайт сетевого сканера **Nessus**

Отличительной чертой этого сканера является наличие языка сценариев **NASL** (**Nessus Attack Scripting Language**), с помощью которого пользователь может самостоятельно создавать проверочные процедуры. К недостаткам данного сканера можно отнести невозможность прерывания сканирования, что может причинить некоторые неудобства администратору.

8.3.4 Nmap

Главным преимуществом сетевого сканера **Nmap** (http://www.insecure.org) является его свободное распространение (рисунок 8.4). Изначально разрабатываемый для **UNIX-систем**, он обладает очень большим числом возможностей, среди которых:

– сканирование сетей с любым количеством объектов;

– определение состояния объектов сканируемой сети, а также портов и соответствующих им служб.

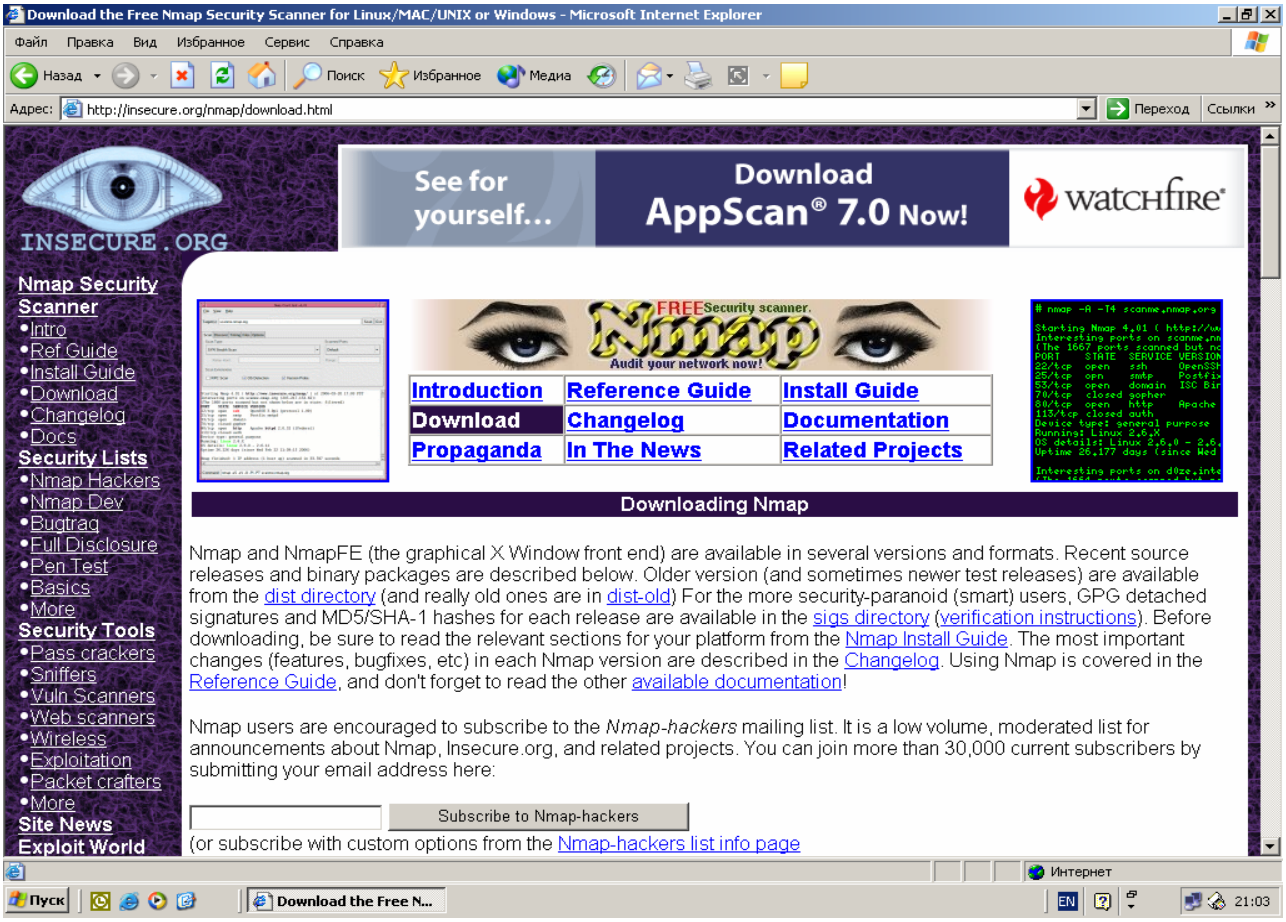


Рисунок 8.4 - Сайт сетевого сканера **Nmap**

Nmap использует различные методы сканирования. Некоторые из них:

– **UDP** – сканирование портов системы, которые для передачи данных используют протокол **UDP**;

– **TCP connect()** - сканирование с установкой **TCP**-соединения, при котором сканирующий хост пытается открыть **TCP-соединение** со сканируемым хостом;

– **TCP SYN** - сканирование с установкой так называемого «полуоткрытого» соединения, при котором сканирующий хост пытается открыть **TCP-соединение** со сканируемым хостом, однако как только сканируемый хост подтверждает установку соединения, сканирующий хост прерывает соединение, таким образом, подтверждение установки соединения со стороны сканируемого хоста говорит о том, что на нем открыт порт, который сканировали и существует возможность подключения к порту;

– **ICMP (ping)** - используется для выявления активных хостов в сети,

Nmap посылает запрос по указанному адресу, и, если хост активен, он обязательно ответит на него, что, в свою очередь, означает, что данный хост может быть просканирован;

– **FIN**, **Xmas tree**, **NULL-сканирование** – используются в случае, если на сканируемом хосте установлен брандмауэр, который блокирует **SYN-пакеты**, или установлена программа типа **Synlogger**, которая в состоянии выявить **SYN-сканирование**;

– **АСК** - дополнительный метод сканирования, используется дня определения набора правил (**ruleset**) брандмауэра, в частности, он помогает определить, защищен ли сканируемый хост брандмауэром или просто пакетным фильтром, блокирующим входящие **SYN-пакеты**.

Nmap способен также определять операционную систему удаленного компьютера, осуществлять «невидимое» и параллельное сканирование, сканирование с использованием **IP-фрагментации**, а также произвольное указание **IP-адресов** и номеров портов сканируемых сетей.

Этот сканер приобрел большую популярность у пользователей операционной системы **UNIX** и был перенесен на систему **Windows**. Однако он не имеет графического интерфейса, что делает затруднительным его использование новичками.

8.4 Признаки, свидетельствующие о взломе системы

Наиболее вероятными признаками взлома компьютера и проникновения на него злоумышленника можно считать следующие события.

Появление различного рода сообщений об ошибках. Чаще всего эти сообщения записываются в журналы событий, которые ведет операционная система. Например, сообщения могут указывать на неожиданное изменение различных системных файлов или их отсутствие. Также следует с осторожностью относиться к сообщениям о состоянии служб, которые выполняются на компьютере, а также к сообщениям самих служб.

Изменение различных системных файлов и реестра. В первую очередь, необходимо обращать внимание на наличие подозрительных процессов,

запущенных на компьютере; при этом следует использовать утилиты типа **Process Manager**, которые могут показывать все процессы, выполняющиеся в системе (в крайнем случае можно использовать «Диспетчер задач»). Также рекомендуется применять утилиты слежения за реестром, такие, как **Regmon for Windows NT/9x**, которые способны отследить малейшее изменение реестра.

Необычное поведение компьютера. Следует обращать внимание на внезапные перезагрузки системы или ее остановки, поскольку они могут быть вызваны злоумышленником для того, чтобы его изменения, произведенные на атакуемом компьютере, вступили в силу. Кроме этого, на наличие атаки указывает наличие новых сетевых соединений, информацию о которых можно получить с помощью команды **netstat**.

Состояние файловой системы. Наличие новых файлов на жестком диске, особенно в системных папках **Windows**, может говорить о том, что злоумышленник пытается установить сервер «троянского коня» или какой-либо программы удаленного администрирования компьютера.

Изменение учетных записей пользователей. Появление в системе новых пользователей или назначение пользователям прав администратора свидетельствует о попытке взлома. Также следует обращать внимание на время регистрации пользователя в системе, не свойственное ему. Несомненным признаком взлома является возможность зарегистрироваться в системе по причине неправильного пароля.

8.5 Действия пользователя при обнаружении попытки взлома

Если пользователь обнаружил попытку взлома своего компьютера, первое, что необходимо сделать, - это отключить компьютер от сети **Internet** или ЛВС. Перезагружать компьютер не рекомендуется, поскольку это может вызвать удаление информации о хакере, и также активизировать возможные программы уничтожения данных, которые были оставлены на атакуемом компьютере.

Современные компьютеры обладают достаточно емкими носителями информации, поэтому рекомендуется сохранить состояние системы для после-

дующего анализа. Наилучшим вариантом является сохранение всего образа диска, однако если это невозможно, то следует сохранить файл **pfirewall.log**, который создается брандмауэром **ICP** и ведет регистрацию всех подключений (если используется брандмауэр другого разработчика, следует сохранить его **LOG-файл**).

Также желательным является сохранение информации о запущенных процессах. В дальнейшем это поможет определить способ проникновения злоумышленника и набор действий, которые он мог выполнить.

После выполнения этих действий необходимо перезагрузить компьютер и произвести загрузку с дискет или загрузочного **CD-ROM**, а затем протестировать компьютер на наличие вирусов и других вредоносных программ. Используя сведения, полученные в результате анализа журнала безопасности и других источников, пользователь должен определить способ проникновения в систему.

Если злоумышленник успел произвести действия, которые привели к разрушению системы, следует переустановить ее, используя дистрибутивный пакет.

Выполнив все указанные действия, следует устранить причину уязвимости системы. Кроме того, можно обратиться к провайдеру **Internet** с целью определения координат злоумышленника и его наказания.

8.6 Контрольные вопросы

8.6.1 Какие понятия относятся к теории компьютерной безопасности?

8.6.2 Что понимается под угрозой безопасности компьютерной системы?

8.6.3 Какие виды угроз безопасности Вы знаете?

8.6.4 Что понимается под уязвимостью компьютерной системы?

8.6.5 Что понимается под сетевой атакой?

8.6.6 Перечислите причины, вызывающие уязвимость компьютерной системы.

8.6.7 Какие этапы обычно выделяются в сетевой атаке?

8.6.8 Что понимается под термином «хост»?

8.6.9 Какие программ осуществляют перехват и анализ сетевого трафика?

8.6.10 Что понимается под термином «сетевой трафик»?

8.6.11 С какой целью осуществляется сканирование портов системы?

8.6.12 Какие программы используются для сканирования портов?

8.6.13 Что понимается под термином «сканирование»?

8.6.14 Как в общем случае называются программы, позволяющие вызвать сбой в работе какой-либо службы компьютерной системы?

8.6.15 В чем заключается смысл корректного завершения сетевой атаки?

8.6.16 Как в общем случае называются программы для проверки системы на наличие уязвимых мест?

8.6.17 Каковы основные возможности программ проверки целостности системы?

8.6.18 Перечислите известные Вам названия сканеров безопасности?

8.6.19 Что обозначается аббревиатурой **CHAM?**

8.6.20 В чем смысл функции **Auto-Fix function** сканера **Retina**?

8.6.21 Перечислите основные возможности сканера **XSpider**?

8.6.22 В чем отличительная черта сканера **Nessus Security Scanner**?

8.6.23 Какие методы сканирования используются в сканере **Nmap**?

8.6.24 Может ли **Nmap** определить операционную систему удаленного компьютера?

8.6.25 Перечислите основные признаки, свидетельствующие о взломе системы?

8.6.26 Перечислите действия пользователя при обнаружении попытки взлома?

8.6.27 Что понимается под термином «брандмауэр» в компьютерной системе?

9 Принципы функционирования сетей

Прежде чем рассматривать работу различных программ, используемых для сетевой атаки и защиты, необходимо познакомиться с принципами построения сетей. Этот раздел посвящен разъяснению некоторых понятий и терминов, которые используются при работе с компьютерными сетями.

9.1 Основы TCP/IP

В свое время создатели ЛВС пришли к осознанию важности и возможностей межсетевых технологий для передачи данных. Результатом стали исследования и создание набора сетевых стандартов, которые детально описывают процесс взаимодействия компьютеров, а также содержат ряд соглашений при взаимодействии сетей и маршрутизации данных.

Официально названный **Transmission Control Protocol/Internet Protocol (TCP/IP)** стал промышленным стандартом протоколов, разработанных для глобальных сетей. Он может использоваться для взаимодействия компьютеров с помощью неограниченного числа сетей. Например, можно использовать **TCP/IP** для связи отдельных сетей внутри организации или предприятия, даже если связь с внешними сетями отсутствует. Технология **TCP/IP** хороша из-за своей высокой жизнеспособности, поэтому она стала базовой технологией для большого количества ЛВС.

Принципы построения сетей и тех процессов, которые в них происходят, во многом связаны со стандартами, которые называют **коммуникационными протоколами**, или **протоколами.** Протоколы реализуют способы передачи сообщений, описывают детали форматов сообщений и указывают, как обрабатывать ошибки. Однако важным является то, что они позволяют рассматривать стандарты взаимодействия вне зависимости от типа оборудования, на котором они реализованы. Другими словами, коммуникационный протокол позволяет описать или понять процесс передачи данных, не привязываясь к какому-либо конкретному оборудованию, использованному для выполнения этого процесса.

Сам протокол **TCP/IP** состоит из нескольких уровней реализации.

На нижнем уровне он поддерживает все популярные стандарты физического и канального уровней реализации: для локальных сетей это, например, **Ethernet**, **Token Ring**, **Fast Ethernet**, а для глобальных сетей это могут быть протоколы соединений **SLIP** и **PPP**.

На более высоком уровне обеспечивается межсетевое взаимодействие - здесь происходит передача пакетов данных с использованием различных транспортных технологий локальных сетей, территориальных сетей или линий специальной связи.

9.2 Протоколы TCP/IP межсетевого уровня

Internet Protocol (IP) выступает в качестве базового протокола сетевого уровня в технологии **TCP/IP**. **Internet Protocol** изначально был спроектирован как протокол передачи пакетов в составных сетях, состоящих из большого количества ЛВС, объединенных как локальными, так и глобальными связями. Именно по этой причине **IP-протокол** хорошо работает в сетях со сложной структурой, рационально используя аппаратную часть и экономно расходуя пропускную способность низкоскоростных линий связи. IP-протокол относится к такому типу протоколов, которые не гарантируют доставку пакетов до узла назначения (подтверждение в доставке может отсутствовать), но стараются это сделать.

К рассматриваемому уровню межсетевого взаимодействия относится и протокол межсетевых управляющих сообщений **ICMP** (**Internet Control Message Protocol**). Он имеет широкое распространение и предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом - источником пакета. С помощью специальных пакетов **ICMP** сообщается о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и другая служебная информация.

Например, этот протокол использует утилита **ping**, предназначенная для проверки наличия соединения между двумя узлами.

9.3 Протоколы TCP/IP транспортного уровня

Транспортный уровень **TCP/IP** является базовым и обеспечивает функционирование протокола управления передачей **TCP** (**Transmission Control Protocol**) и протокола диаграмм пользователя **UDP** (**User Datagram Protocol**).

Протокол **TCP** обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования виртуальных соединений. Протокол **UDP** обеспечивает передачу пакетов данных и выполняет функции связующего звена между сетевым протоколом и многочисленными прикладными процессами.

9.4 Протоколы TCP/IP прикладного уровня

Для обеспечения взаимодействия программ клиентов и серверов предназначен прикладной уровень **TCP/IP**. На этом уровне существует большое количество протоколов и сервисов. К ним относятся такие широко используемые протоколы, как протокол копирования файлов **FTP** (**File Transfer Protocol**); протокол эмуляции терминала **Telnet**; почтовый протокол **SMTP** (**Simple Mail Transfer Protocol**), используемый в электронной почте сети **Internet**; гипертекстовые сервисы доступа к удаленной информации, такие, как **WWW** и многие другие. Таким образом, скрытие в технологии **TCP/IP** низкоуровневых деталей взаимодействия помогает улучшить производительность. По этой причине при создании программного обеспечения не нужно знать или помнить множество деталей о конкретных параметрах оборудования.

Такие программы, разработанные с учетом самого высокого уровня **TCP/IP**, не ограничены архитектурой конкретного ПК или конкретного сетевого оборудования, их не надо изменять при замене компьютера или изменении конфигурации. Наконец, поскольку прикладные программы независимы от используемого оборудования, они могут обеспечивать прямое взаимодействие различных элементов ЛВС. Другими словами, необходимость в специальных версиях прикладных программ передачи данных для всех возможных соединений между компьютерами в сети отпадает.

9.5 Взаимодействие между разнородными сетями

При решении проблемы построения составных сетей необходимо иметь в виду, что физически две сети могут соединяться только с помощью компьютера, присоединенного к каждой из них. Однако непосредственное соединение не гарантирует, что компьютер сможет взаимодействовать с любым другим. Для обеспечения надежной связи необходимо, чтобы компьютеры умели передавать пакеты данных из одной сети в другую.

Компьютеры, соединяющие две сети и передающие пакеты из одной в другую, называются **межсетевыми шлюзами** (**gateway**) или **межсетевыми маршрутизаторами** (**router**). Практически всегда эти компьютеры выполняют роль защитного экрана (брандмауэра) между локальной сетью и внешней, которая представляет угрозу для локальной сети.

Рассмотрим функционирование шлюза на простейшем соединении двух сетей (рисунок 9.1). Компьютер, выполняющий функции шлюза, присоединен как к сети **A**, так и к сети **B**. Работа в качестве шлюза подразумевает, что он должен принимать пакеты данных из сети **A**, предназначенные компьютерам сети **B**, и передавать их адресату. Аналогично, шлюз должен принимать пакеты из сети **B**, которые предназначены компьютерам в сети **A**, и передавать их в эту сеть. Например, если пакет данных отправлен с компьютера **PC1a**, а предназначен компьютеру **PC3b**, то данные от **PC1a** передаются на шлюз, а далее шлюз адресует их на **PC3b**. Идея шлюза не является сложной, однако важна по той причине, что она обеспечивает способ взаимного соединения сетей, а не отдельных компьютеров.

Таким образом, в **Internet** все соединения между физическими сетями обеспечивают **TCP/IP**-компьютеры, называемые шлюзами. При такой архитектуре компьютеры-шлюзы являются небольшими машинами, они часто имеют небольшую дисковую и оперативную память. Причина использования маленьких межсетевых шлюзов заключена в следующем: шлюзы маршрутизируют пакеты, основываясь на сети получателя, а не на конкретном компьютере, поэтому количество информации, которую нужно хранить шлюзу, пропорцио-

нально количеству сетей, а не числу машин.

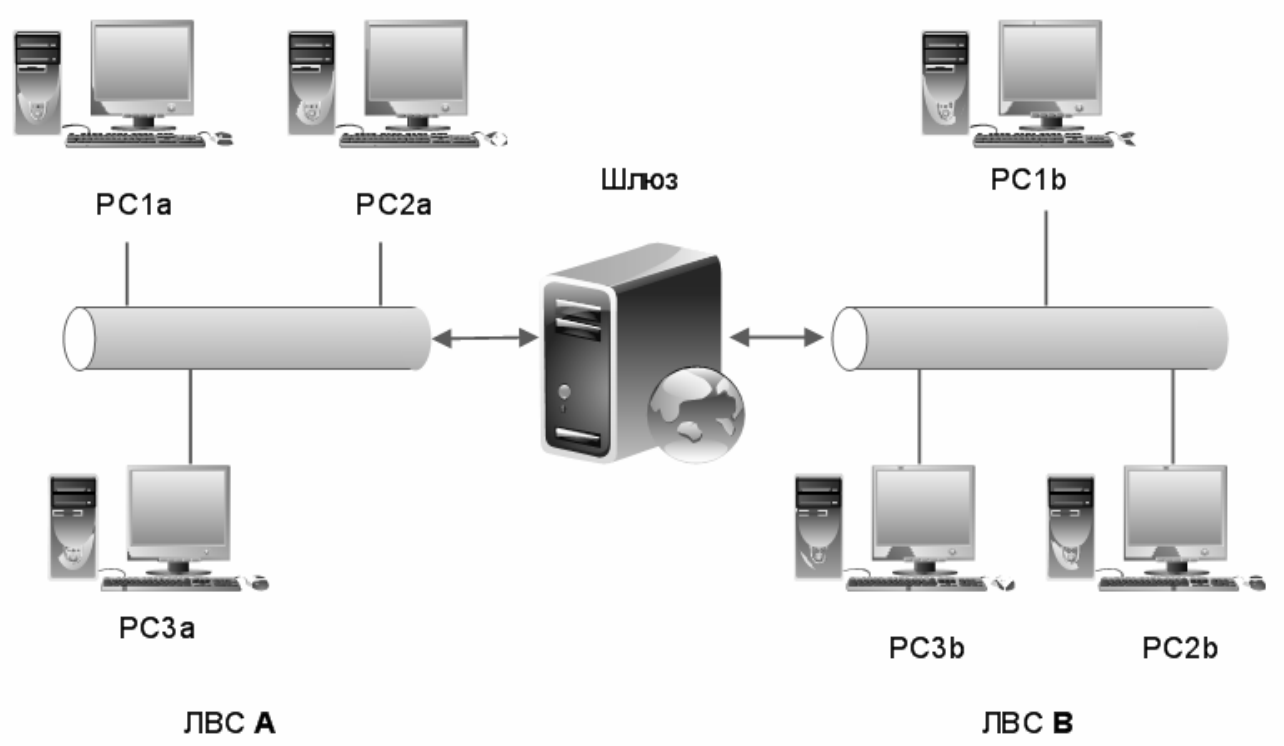


Рисунок 9.1 - Функционирование шлюза на две сети

С учетом этого существует реальная возможность иметь корректные пути для всех сетей в каждом шлюзе. Именно по этой причине прикладные программы, взаимодействующие с помощью сети, не располагают данными о деталях организации соединений, но могут запускаться в неизменном виде на любом компьютере.

Следует иметь в виду, что шлюзы не обеспечивают прямое соединение между всеми парами сетей. Поэтому передаваемым пакетам данных может понадобиться пройти через несколько промежуточных сетей.

Следовательно, каждая сеть должна обеспечивать передачу транзитных пакетов в обмен на право посылать данные через другие сети. По этой причине межсетевые **TCP/IP-протоколы** считают все сети равными, но при этом, как было замечено выше, программному обеспечению необходимо осуществлять идентификацию компьютеров.

9.6 Адресация в IP-сетях

Коммуникационная система должна обеспечивать универсальное средство взаимодействия, т.е. позволять осуществлять связь между любыми компьютерами. Чтобы сделать коммуникационную систему универсальной, нужно определить приемлемый для всех метод идентификации компьютеров, которые к ней присоединены.

Традиционно идентификаторы в сети состоят из:

– имени, указывающего на конечный объект;

– адреса, идентифицирующего то, где этот объект находится;

– маршрута, определяющего, как до него добраться.

В реальных сетях имена, адреса и маршруты определяются на разных уровнях представления **TCP/IP-идентификаторов**, причем, имена – на самом верхнем, а маршруты – на самом нижнем.

Для пользователя удобнее применять для идентификации произносимые имена, в то время как программное обеспечение лучше работает с более компактным числовым представлением идентификаторов.

В **TCP/IP-технологиях** было принято решение стандартизовать компактные, двоичные адреса, которые делают более эффективными такие вычисления, как выбор маршрута.

Для адресов разработчики **TCP/IP** выбрали схему адресации, в которой каждому компьютеру в сети назначается адрес в виде целого числа, называемый межсетевым адресом, или **IP-адресом**. При этом значения **IP-адреса** выбираются особым образом, чтобы сделать маршрутизацию эффективной.

Иначе говоря, **IP-адрес** кодирует идентификацию сети, к которой присоединен главный компьютер сети (сервер), а также идентификацию уникального компьютера в этой сети.

Поэтому каждому компьютеру в **TCP/IP** назначен уникальный 32-битовый межсетевой адрес, который используется при взаимодействии.

Для удобства пользователей в технических документах или прикладных программах **IP-адреса** пишутся как четыре десятичных числа, разделенных де-

сятичными точками, и каждое из этих чисел представляет значение групп по восемь символов двоичного IP-адреса. Поэтому 32-битовый IP-адрес

11000000 10101000 01101111 00000001

обычно записывается как

192.168.111.1.

Очевидно, что такая запись гораздо удобнее для использования, чем представление в двоичной форме. Принципиально, каждый адрес является парой «идентификатор сети - идентификатор компьютера в этой сети».

На практике каждый **IP-адрес** должен иметь одну из трех форм или классов: **A, B** или **C**, которые можно различить по первым двум битам адреса.

В таблице 9.1 приведены диапазоны номеров, соответствующие каждому классу сетей.

Таблица 9.1 – Диапазон номеров сетей разного класса

Класс	Наименьший адрес	Наибольший адрес
A	0.1.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Адреса класса **A** используются для сетей, имеющих в своем составе более чем 216 компьютеров. В этих адресах выделяется под идентификатор сети 7 бит, а под идентификатор компьютера - 24 бита.

Адреса класса **B** используются для сетей меньшего размера, включающих от 28 до 216 компьютеров. В этих адресах выделяется 14 бит под идентификатор сети и 16 бит - под идентификатор компьютера.

Сети класса **C** должны состоять менее чем из 256 компьютеров, причем в адресе выделяется 21 бит под идентификатор сети и 8 бит - под идентификатор компьютера.

Традиционно **IP-адрес** определяют таким образом, что можно быстро расширить любую из его частей. Номер узла (т.е. номер сети внутри ЛВС, ина-

че говоря - номер подсети) в протоколе **IP** назначается независимо от локального адреса узла. Деление **IP-адреса** на поле номера сети и номера узла гибкое, и граница между этими полями может устанавливаться достаточно произвольно.

Узел может входить в несколько **IP-сетей**. В этом случае узел должен иметь несколько **IP-адресов**, по числу сетевых связей. Таким образом, **IP-адрес** характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Следует иметь в виду, что адресация в **IP-сетях** основана на следующих типах адресов:

– сетевой (**IP-адрес**, рассмотренный выше);

– физический (**MAC-адрес**);

– символьный (**DNS-имя**).

Локальный адрес узла сети определяется технологией, с помощью которой построена эта сеть. Для узлов, входящих в ЛВС, это **MAC-адрес** сетевого адаптера или порта маршрутизатора (**MAC - Media Access Control**). Данные адреса назначаются производителями оборудования и являются уникальными адресами, т.к. управляются централизованно.

Для всех существующих технологий локальных сетей **MAC**-адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.

Символьный идентификатор - имя, например, xiit.kharkov.ua, которое назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес, называемый также **DNS-именем**, используется на прикладном уровне, например, в протоколах **FTP** или **Telnet**. Отображением символьных адресов и учетом соответствия **IP-адреса** его **DNS-имени** занимается служба **DNS** (**Domain Name System**).

9.7 Порты

Существуют два типа межкомпьютерного обмена данными – датаграммы и сеансы.

Датаграмма - это сообщение, которое не требует подтверждения о прие-

ме от принимающей стороны, а если такое подтверждение необходимо, то адресат должен сам послать специальное сообщение.

Для осуществления обмена данными таким способом принимающая и передающая стороны должны строго придерживаться определенного протокола во избежание потери информации.

Каждая датаграмма является самостоятельным сообщением, и при наличии нескольких датаграмм в ЛВС их доставка адресату, вообще говоря, не гарантируется. При этом датаграмма обычно является частью какого-либо сообщения, и в большинстве ЛВС скорость передачи датаграмм гораздо выше, чем сообщений в сеансах.

В сеансе предполагается создание логической связи для обмена сообщениями между компьютерами и гарантируется получение сообщений.

В то время как датаграммы могут передаваться в произвольные моменты времени, в сеансе перед передачей сообщения происходит открытие сеанса, а по окончании обмена данными сеанс должен быть закрыт.

Операционные системы большинства компьютеров поддерживают мультипрограммный режим, т.е. несколько программ выполняются одновременно (параллельно выполняется несколько процессов).

С некоторой степенью точности можно говорить о том, что процесс - это и есть окончательное место назначения для сообщения. Однако в силу того, что процессы создаются и завершаются динамически, отправитель редко имеет информацию, достаточную для идентификации процесса на другом компьютере.

Поэтому возникает необходимость в определении места назначения данных на основе выполняемых процессами функций, при отсутствии информации о тех процессах, которые реализуются этими функциями.

На практике вместо того, чтобы считать процесс конечным местом назначения, полагают, что каждый компьютер имеет набор некоторых точек назначения, называемых протокольными портами. Каждый порт идентифицируют целым положительным числом (от 0 до 65535). В этом случае операционная система обеспечивает механизм взаимодействия, используемый процессами для указания порта, на котором они работают, или порта, к которому нужен доступ.

Обычно порты являются буферизированными, и данные, приходящие в конкретный порт до того, как процесс готов их получить, не будут потеряны: они будут помещены в очередь до тех пор, пока процесс не извлечет их.

Следовательно, чтобы связаться с портом на другом компьютере, отправитель должен знать как **IP-адрес** компьютера-получателя, так и номер порта в компьютере. Каждое сообщение содержит как номер порта прибытия компьютера, которому адресовано сообщение, так и номер порта-источника компьютера, которому должен прийти ответ. Таким образом реализуется возможность ответить отправителю для каждого процесса.

Порты с номерами от 0 до 1023 являются привилегированными и используются сетевыми службами, которые, в свою очередь, запущены с привилегиями администратора (суперпользователя). Например, служба доступа к файлам и папкам **Windows** использует порт **139**, однако если она не запущена на компьютере, то при попытке обратиться к данной службе (т.е. к данному порту) будет получено сообщение об ошибке.

Порты с 1023 до 65535 являются непривилегированными и используются программами-клиентами для получения ответов от серверов. Например, **Web-браузер** пользователя, обращаясь к **Web-серверу**, использует порт 44587 своего компьютера, но обращается к 80 порту **Web-сервера**.

Получив запрос, **Web-сервер** отправляет ответ на порт 44587, который используется **Web-браузером**.

9.8 Контрольные вопросы

9.8.1 Как расшифровывается и что означает аббревиатура **TCP/IP**?

9.8.2 Что понимается под коммуникационными протоколами компьютерной системы?

9.8.3 Какие функции выполняют коммуникационные протоколы?

9.8.4 В чем особенность коммуникационных протоколов?

9.8.5 Какие уровни реализации протокола **TCP/IP** Вы знаете?

9.8.6 Что означают аббревиатуры **Ethernet**, **Token Ring**, **Fast Ethernet**?

9.8.7 Какие протоколы относятся к уровню межсетевого взаимодействия?

9.8.8 В каком типе протоколов может отсутствовать подтверждение в доставке пакетов до узла назначения?

9.8.9 Для чего используется протокол **ICMP**? Как расшифровывается аббревиатура **ICMP**?

9.8.10 Какая информация передается с помощью специальных пакетов **ICMP**?

9.8.11 Для чего используется утилита **ping**?

9.8.12 Опишите синтаксис команды **ping** консольного режима?

9.8.13 Какие протоколы транспортного уровня вы знаете?

9.8.14 Для чего используется протокол **TCP**?

9.8.15 Для чего служит протокол **UDP**? Как расшифровывается аббревиатура **UDP**?

9.8.16 Для чего используются протоколы прикладного уровня?

9.8.17 Какие протоколы прикладного уровня Вы знаете?

9.8.18 Как называется протокол копирования файлов?

9.8.19 Как называется почтовый протокол, используемый в **Internet**?

9.8.20 Как называется гипертекстовый протокол доступа к удаленной информации?

9.8.21 Что называется **межсетевым шлюзом**?

9.8.22 Что обозначают термины **gateway** и **router**?

9.8.23 Что называется брандмауэром в компьютерной системе?

9.8.24 Что понимается под коммуникационной системой в компьютерной сети?

9.8.25 Что необходимо для того, чтобы коммуникационная система была универсальной?

9.8.26 Из чего состоит **TCP/IP-идентификатор** компьютера в сети?

9.8.27 Что представляет собой **IP-адрес, к**ак **IP-адрес** пишется в технических документах?

9.8.28 Чем отличаются классы **IP-адресов A, B** и **C**?

9.8.29 К какому классу **IP-адресов** принадлежит следующий адрес: **192.168.111.1** ?

9.8.30 Какие типы адресов в **IP-сетях** Вы знаете?

9.8.31 Что понимается под **DNS-именем** компьютера? Для чего используется **DNS**-имя?

9.8.32 Какие типы межкомпьютерного обмена данными Вы знаете?

9.8.33 В чем особенности обмена данными в виде датаграмм?

9.8.34 В чем особенности обмена данными в виде сеансов?

9.8.35 Что понимается под протокольными портами? Для чего они необходимы?

9.8.36 Как идентифицируются порты?

9.8.37 Какие порты называются привилегированными?

Список использованных источников

1 **Глушаков, С. В.** Секреты хакера: защита и атака / С. В. Глушаков, Т. С. Хачиров, Р. О. Соболев. – Ростов на Дону : Феникс, Харьков: Фолио, 2005. - 416 с.

2 ScreenLock Pro : программа блокировки доступа к компьютеру [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.screenlock.com. – Проверено 17.09.2008.

3 Информационный сервер о технологиях парольной защиты [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.passwords.ru. – Проверено 17.09.2008.

4 «Хакер OnLine» [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.xakep.ru. – Проверено 17.09.2008.

5 «Территория взлома» [Электронный ресурс]. – Электрон. дан. – Режим доступа : - www.hackzone.ru. – Проверено 17.09.2008.

6 Regmon : утилита для работы с реестром [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.microsoft.com/technet/sysinternals/utilities/regmon.mspx. – Проверено 17.09.2008.

7 RTKF : программа изменения параметров реестра [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.databack4u.com/snc/rtkf_eng.html. – Проверено 17.09.2008.

8 Alcohol 120% : программа создания виртуальных CD-дисков [Электронный ресурс]. – Электрон. дан. – Режим доступа : www.alcohol-soft.com. – Проверено 17.09.2008.

9 Лаборатория Касперского дисков [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.kaspersky.ru. – Проверено 17.09.2008.

10 XP Tweaker : утилита для настройки Windows [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.xptweaker.narod.ru. – Проверено 17.09.2008.

11 Reg Organizer : утилита для работы с реестром [Электронный ресурс]. – Электрон. дан. – Режим доступа : www.chemtable.com. – Проверено 17.09.2008.

12 Advanced Office XP Password Recovery : программа взлома пароля документа Word [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.officexppasswordrecovery.info. – Проверено 17.09.2008.

13. Словари для атаки по словарю [Электронный ресурс]. – Электрон. дан. – Режим доступа : www.outpost9.com. – Проверено 17.09.2008.

14 Retina 4.9 : сканер безопасности [Электронный ресурс]. – Электрон. дан. – Режим доступа : http:// www. eeye.com. – Проверено 17.09.2008.

15 **Скляров, Д. В.** Искусство защиты и взлома информации / Д. В. Скляров. – СПб. : БХВ-Петербург, 2004. – 288 с.

16 **Фейнштайн, К.** Защита ПК от спама, вирусов, всплывающих окон и шпионских программ / Кен Фейнштайн : пер. с англ О.Б. Вереиной. – М.: НТ Пресс, 2005. – 240 с.

17 **Девянин, П. Н.** Теоретические основы компьютерной безопасности: учеб. пособие для вузов / П. Н. Девянин, [и др.]. – М.: Радио и связь, 2000. – 192 с.