Роман Клименко

ДЛЯ ПРОФЕССИОНАЛОВ

Windows Vista

ПИТЕР®

Москва · Санкт-Петербург · Нижний Новгород · Воронеж
Новосибирск · Ростов-на-Дону · Екатеринбург · Самара
Киев · Харьков · Минск
2008

Клименко Роман Александрович

Windows Vista. Для профессионалов

Серия «Для профессионалов»

Заведующий редакцией	*Д. Гурский*
Руководитель проекта	*М. Моисеева*
Литературный редактор	*Н. Гринчик*
Художник	*Л. Адуевская*
Корректоры	*Т. Курьянович, Ю. Цеханович*
Верстка	*Г. Блинов*

ББК 32.973.2-018.2
УДК 004.451

Клименко Р. А.

К49 Windows Vista. Для профессионалов. — СПб.: Питер, 2008. — 656 с.: ил. — (Серия «Для профессионалов»).

ISBN 978-5-91180-477-0

Книга посвящена описанию новых возможностей Windows Vista, а также изменению стандартных функций данной операционной системы. Если вы являетесь опытным пользователем Windows XP и раздумываете о том, что вам даст новая система Windows Vista при переходе на нее, то эта книга для вас.

Из нее вы узнаете о тонкостях Windows Vista, об улучшениях в стандартных компонентах операционных систем семейства Windows, о новых графических приложениях и программах командной строки, входящих в состав Vista, о новых службах и параметрах реестра данной операционной системы, о стандартных и нестандартных способах оптимизации и настройки Windows Vista.

© ООО «Питер Пресс», 2008

Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.

Информация, содержащаяся в данной книге, получена из источников, рассматриваемых издательством как надежные. Тем не менее, имея в виду возможные человеческие или технические ошибки, издательство не может гарантировать абсолютную точность и полноту приводимых сведений и не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 978-5-91180-477-0

ООО «Питер Пресс», 198206, Санкт-Петербург, Петергофское шоссе, 73, лит. А29.

Налоговая льгота — общероссийский классификатор продукции ОК 005-93, том 2; 95 3005 — литература учебная.
Подписано в печать 15.08.07. Формат $70\times100^{1}/_{16}$. Усл. п. л. 52,89. Тираж 2500. Заказ 0000.

Отпечатано по технологии CtP
в ОАО «Печатный двор» им. А. М. Горького.
197110, Санкт-Петербург, Чкаловский пр., 15.

Краткое содержание

Введение 13
Главы книги на сайте издательства 14
От издательства 14
Глава 1. Нововведения Windows Vista 15
Глава 2. Установка Windows Vista 25
Глава 3. Интерфейс Windows Vista 79
Глава 4. Работа со стандартными программами Windows Vista ... 186
Глава 5. Консоль управления Microsoft 259
Глава 6. Стандартные службы Windows Vista 378
Глава 7. Администрирование Windows Vista 497

Оглавление

Введение 13
Главы книги на сайте издательства 14
От издательства 14

Глава 1. Нововведения Windows Vista 15
1.1. Новый интерфейс Windows Aero Glass 16
Боковая панель (Sidebar) 17
Windows Search Engine 17
Новый механизм передачи цвета 18
1.2. Способы защиты в новой ОС 18
Контроль учетных записей пользователей (UAC) 18
Защита доступа к сети (NAP) 19
Защитник Windows 19
1.3. Дополнительные возможности 19
Работа со звуком 19
Virtual PC Express 19
Подсистема для UNIX-приложений (SUA) 19
Шифрование диска Windows BitLocker 19
DVD-студия Windows 20
Internet Explorer 7.0 20
Почта Windows 21
Ножницы 21
Календарь Windows 22
Оценка и увеличение производительности компьютера 22
Средства распознавания речи (Speech Recognition) 22
Windows Media Center 22

Tablet PC Edition ... 22
Мобильные ПК ... 22
Новый формат образов установки WIM (Windows Imaging) ... 23
Встроенная поддержка IPv6 ... 23
Новые MSC-оснастки ... 23
Возможность самодиагностики жесткого диска и оперативной памяти ... 23
Новый набор стандартных драйверов ... 24
Новые функции WinAPI и DirectX 10 ... 24

Глава 2. Установка Windows Vista ... 25
2.1. Версии Windows Vista ... 26
Различия в редакциях операционной системы ... 26
Различия в редакциях с точки зрения реестра ... 29
2.2. Процесс установки операционной системы ... 30
Основные требования к компьютеру ... 31
Процесс установки ... 32
2.3. Дополнительные работы после установки ... 38
Настройка загрузочного меню ... 38
Перенос настроек из другой операционной системы ... 69
Активация Windows Vista ... 73
Автоматизация установки с помощью файла ответа ... 77

Глава 3. Интерфейс Windows Vista ... 79
3.1. Краткий обзор интерфейса ... 80
Окно входа в систему ... 80
Меню Пуск ... 82
Проводник ... 84
Панель управления ... 86
3.2. Настройка оболочки Windows ... 109
Настройка меню Пуск и Панели задач ... 109
Настройка Рабочего стола пользователя ... 124
Настройка Проводника ... 144

Настройка папки Панель управления 155
Вход и выход пользователя из системы 159
Настройка механизма поиска 163
Настройка оболочки 171

Глава 4. Работа со стандартными программами Windows Vista 186
4.1. Проигрыватель Windows Media 187
Проигрывание файлов 188
Копирование содержимого диска 189
Изменение битрейта при кодировании в MP3-файлы 191
Запись диска 191
Синхронизация со съемными носителями 192
Использование групповых политик 192
Настройка дополнительных параметров реестра 193
4.2. DVD-студия Windows 195
4.3. Windows Media Center 197
4.4. Internet Explorer 200
Интерфейс браузера 201
Настройка браузера 205
Команды rundll32.exe, позволяющие работать с браузером Internet Explorer 210
4.5. Почта Windows 216
Интерфейс почтового клиента 217
Работа с почтовым клиентом 220
Другие программы почтового клиента 228
4.6. Защитник Windows 229
Параметры 231
Microsoft SpyNet 231
Объекты в карантине 231
Проводник программного обеспечения 231
Разрешенные объекты 232
Веб-узел Защитника Windows 232

Настройка с помощью групповых политик 232
Параметры реестра, влияющие на работу программы Защитник Windows 233
Мастер Средство удаления вредоносных программ Microsoft Windows 234
4.7. Фотоальбом Windows 234
Интерфейс программы 235
Настройка с помощью реестра 238
4.8. Другие программы 240
Ножницы — создание снимка экрана 240
Календарь Windows — стандартный органайзер 242
Игры 243
Очистка диска от ненужных файлов 245
Записки — рисуем и записываем 247
Журнал Windows — блокнот для пера 248
Факсы и сканирование Windows — работа с факсом и сканером 249
Windows CardSpace — создание электронных пластиковых карт 250
Помощник по цифровой корзине — программа для покупки продуктов Microsoft 252
Настройка системы 253
Работа с возможностями речевого управления компьютером 254
Программа Звукозапись 256
Остальные программы 257

Глава 5. Консоль управления Microsoft 259
5.1. Работа с консолью управления Microsoft 261
5.2. Стандартные оснастки 264
Работа с файлами и файловой системой 264
Работа с сетью 269
Безопасность 278
Другие компоненты операционной системы 335

Другие оснастки ... 375

Глава 6. Стандартные службы Windows Vista ... 378
6.1. Основные сведения о службах ... 379
Параметры, описывающие службы ... 380
Настройки служб svchost ... 385
Основы работы драйверов ... 386
6.2. Работа со службами с помощью программ операционной системы ... 387
Возможности программы net.exe ... 387
Использование программы Sc.exe ... 388
6.3. Службы Windows Vista ... 392
Работа с файлами и файловой системой ... 392
Работа с оборудованием ... 403
Безопасность операционной системы ... 413
Работа в сети ... 420
Другие службы ... 481

Глава 7. Администрирование Windows Vista ... 497
7.1. Настройка разрешений и аудит доступа ... 498
Реализация защиты ... 498
Редактирование DACL объекта ... 505
Работа с SACL объекта ... 509
7.2. Архивирование и восстановление ... 514
Мастер Центр архивации и восстановления ... 515
Мастер Состояние и настройка архивации ... 518
Служба Восстановление системы ... 522
Инструмент командной строки архивации ... 525
Работа с теневыми копиями ... 526
7.3. Диагностика компонентов операционной системы ... 532
Окно Отчеты о проблемах и их решениях ... 532
Мастер Средство диагностики технической поддержки Майкрософт ... 538

Средство диагностики DirectX 539
Диагностика и восстановление томов дисков 540
7.4. Шифрование 541
Работа с системой шифрования EFS 541
Работа с механизмом BitLocker Drive Encryption 548
7.5. Работа с драйверами 557
Установка драйверов 557
Другие операции 560
7.6. Работа с файловой системой 563
Работа с разделами жесткого диска 563
Сжатие и архивация 588
Запись дисков 592
7.7. Работа с принтерами 595
Настройка работы принтера 595
Работа с принтером 602
7.8. Другие вопросы администрирования 609
Работа с цифровыми подписями файлов 609
Просмотр сведений о работе программ 610
Настройка режимов энергопотребления 613
Мастер Родительский контроль 624
Работа с автономными файлами 631
Тестирование производительности 639
Центр обеспечения безопасности 645
Механизм совместимости 651

Главы, не вошедшие в книгу

Данные главы в формате PDF можно загрузить с сайта издательства по адресу http://www.piter.com/download/.

Глава 8. Работа с сетью 657
8.1. Создание сетевого подключения 658
Использование сетевого кабеля 658
Создание беспроводного соединения 671
Создание удаленного подключения с помощью модема 674
8.2. Работа с удаленным помощником 676
Мастер Удаленный помощник Windows 676
Настройка с помощью групповых политик 679
8.3. Терминальные службы 680
Подключение к удаленному рабочему столу 681
Другие программы 686
Настройка с помощью групповых политик 688
8.4. Новые возможности программ командной строки 689
Rpcping.exe — пингование серверов удаленного доступа 689
ftp.exe — доступ к серверам FTP 691
Ipconfig.exe — отображение сведений о протоколе IP 691
Netsh.exe — настройка сетевых подключений 691
Netstat.exe — сведения о работе сетевого соединения 697
Ping.exe — пингование удаленных компьютеров 697
Route.exe — работа с функциями маршрутизации 698
Tracert.exe — отображение пути до адресата 698
Arp.exe — работа с таблицей ARP 699
8.5. Протокол iSCSI 699
Окно Свойства: Инициатор iSCSI 700

Настройка с помощью групповых политик ... 701
Использование репозитария CIM ... 701
8.6. Создание общих папок ... 722
Параметры мастера Центр управления сетями и общим доступом ... 723
Использование вкладки Доступ ... 724
Использование оснастки Общие папки ... 726
8.7. Удаленное управление операционной системой ... 727
Настройка удаленного доступа ... 727
Программа winrs.exe ... 733
8.8. Команды rundll32.exe для доступа к сетевым возможностям ... 734
Основные команды rundll32.exe ... 734
Доступ к мастерам с помощью библиотеки XWizards ... 735
8.9. Стандартные классы репозитария CIM ... 736
Win32_LogonSession ... 736
Win32_ServerSession ... 737
Win32_ServerConnection ... 737
Win32_NetworkConnection ... 738
Win32_NetworkProtocol ... 738
Win32_NetworkLoginProfile ... 739
Win32_NetworkClient ... 740
Win32_NetworkAdapter ... 740
Win32_NetworkAdapterConfiguration ... 740
Win32_IP4RouteTable ... 743
Win32_IP4PersistedRouteTable ... 743

Глава 9. Установка и удаление компонентов операционной системы ... 744
9.1. Компоненты Windows ... 745
Компоненты операционной системы ... 745
Работа с компонентами ... 766
9.2. Установка и удаление сетевых компонентов с помощью программы netcfg.exe ... 769
Работа с программой ... 769

Стандартные сетевые компоненты 770
Принцип работы программы netcfg.exe 774
9.3. Мастер Установка или удаление языков отображения 775
9.4. Установка пакетов обновлений операционной системы 775

Приложение 1. Команды rundll32 778

Приложение 2. Работа с WMI 780
Настройка WMI 780
Использование классов репозитария CIM 783
Сервер сценариев Windows 787

Приложение 3. Новые программы командной строки 792
Работа с файлами 793
Работа в сети 797
Работа со сценариями 798
Другие программы 799
wisptis.exe 802

Приложение 4. Использование ActiveX-объектов 803
Структура подразделов реестра, определяющих ActiveX-объекты 804
Добавление вкладок к окну Свойства 805
Добавление команд к контекстному меню 809
ActiveX-объекты, отображающие значки 812

Введение

В первом квартале 2007 года была официально выпущена новая операционная система от Microsoft — Windows Vista.

В самом начале ее разработки корпорация Microsoft строила огромные планы насчет этой операционной системы. Windows Vista (в начале своего создания она называлась Windows Longhorn и лишь в 2005 году была переименована в Windows Vista), по мнению разработчиков, должна была совершить революцию в мире операционных систем.

С момента начала создания новой операционной системы прошло несколько лет. За это время энтузиазм разработчиков несколько поутих. Следуя своим традициям, корпорация Microsoft уже несколько раз откладывала финальный выпуск новой ОС.

Возможно, из-за нехватки времени, возможно, из-за трудностей создания, а возможно, из-за проблем в безопасности, но на сегодняшний момент из Windows Vista было решено удалить некоторые дополнительные компоненты (например, новый язык сценариев Monad и файловую систему WinFS). В новой операционной системе вы не найдете такой стандартной программы, как Windows Messenger, с помощью которой можно было не только общаться по Интернету, но и проводить видеоконференции, передавать файлы или совместно работать с приложениями.

По сути, революцию в мире операционных систем планировали совершить именно благодаря новой файловой системе WinFS. Поэтому, как догадывались многие, кто следил за созданием новой операционной системы, революции не будет. Тем не менее не стоит пренебрежительно относиться к новой операционной системе. Да, революции не будет. Вместо этого новую ОС можно назвать продолжением линейки Windows XP и Windows 2003. Причем продолжением действительно качественным, в котором была повышена общая безопасность работы за компьютером и кардинальным образом улучшен интерфейс операционной системы.

Как утверждают разработчики Windows Vista, эта операционная система является самой безопасной из всех доступных на сегодняшний день. Этому способствует не только включенный в нее набор компонентов и методов защиты, но и модель SDL, по которой разрабатывалась Vista. Суть этой модели заключается во внимательной проверке специалистами каждого бита кода операционной системы на соответствие основным критериям сертификации. Безопасности также может способствовать то, что корпорация Microsoft наняла ряд специалистов (хакеров) для регулярной проверки и поиска новых уязвимостей в операционной системе Windows Vista.

Кроме этого, повышению безопасности операционной системы способствуют нововведения Windows Vista, среди которых можно выделить следующие.

- Теперь все службы запускаются с ограниченными привилегиями. Для этого учетные записи, используемые службами, были понижены в привилегиях. А тем службам, которым необходимы дополнительные привилегии, даются только они, а не полный административный доступ.
- Операционная система Windows Vista позволяет автоматически запрещать запуск программ для повышения прав пользователей (называемых еще руткитами), несертифицированных заплаток для операционной системы или для других программ как производства Microsoft, так и сторонних разработчиков, а также других предположительно зловредных программ.
- Возможность хранения всех данных профиля пользователя на смарт-карте с использованием шифрованной файловой системы EFS.
- Новое управление правами RMS позволит более точно настроить права доступа среди пользователей, чтобы понизить возможность кражи корпоративной информации.
- Исходящие пакеты от ядра операционной системы будут блокироваться встроенным брандмауэром Windows Vista.
- В новой операционной системе реализованы такие возможности, как Windows BitLocker Drive Encryption, User Account Protection, Network Access Protection и т. д. О них вкратце будет рассказано далее в 1-й главе.

Несмотря на отсутствие WinFS и Monad, в Windows Vista еще достаточно нововведений, чтобы удивить даже опытного пользователя. Но не только новыми функциями обзавелась операционная система Windows Vista — кардинальным образом были улучшены и ее стандартные возможности. Об этом мы тоже поговорим на страницах данной книги.

Главы книги на сайте издательства

Чтобы скачать главы 8 и 9, а также приложения 1–4, не вошедшие в издание, достаточно на сайте http://www.piter.com найти книгу «Windows Vista. Для профессионалов» и щелкнуть на ссылке Файлы к книге. После этого вы получите доступ к архиву с дополнительными главами.

От издательства

Ваши замечания, предложения и вопросы отправляйте по адресу электронной почты dgurski@minsk.piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

Главы 8 и 9, а также приложения 1–4 в формате PDF можно загрузить с сайта издательства по адресу http://www.piter.com/download/.

На сайте издательства http://www.piter.com вы найдете подробную информацию о наших книгах.

Глава 1

Нововведения Windows Vista

- **Новый интерфейс Windows Aero Glass**
- **Способы защиты в новой ОС**
- **Дополнительные возможности**

В этой главе кратко перечислены все нововведения операционной системы Windows Vista.

1.1. Новый интерфейс Windows Aero Glass

Интерфейс — это первое, что бросается в глаза человеку, впервые работающему с новой операционной системой. Новый интерфейс Aero кардинальным образом отличает Windows Vista от предыдущих версий. Теперь все окна операционной системы стали полупрозрачными (эффект матового стекла, через которое просвечиваются нижележащие элементы интерфейса Windows), что придало им больше красоты и шарма. Кроме того, в операционную систему были добавлены новые визуальные эффекты, а также некоторые новые возможности, построенные именно на интерфейсе Windows Aero. Например, к ним можно отнести окна быстрого просмотра, отображаемые при наведении указателя мыши на элемент Панели задач, технологию Flip 3D, возможность уменьшения или увеличения разрешения экрана Windows, а также более плавное перемещение окон. Уже только ради этого стоит перейти на новую операционную систему (конечно, если вы раньше работали с операционной системой Mac OS, то новый интерфейс Windows Vista не произведет на вас такого впечатления).

Отдельно стоит упомянуть еще одну особенность интерфейса Aero Glass. Теперь размер шрифта не зависит от разрешения экрана. Иными словами, при увеличении разрешения экрана вы больше не будете сталкиваться с такой проблемой, как плохо читаемый текст.

Казалось бы, интерфейс Windows Aero должен заметно тормозить систему. Именно из-за него аппаратные требования к компьютеру, на который можно установить Windows Vista, были заметно повышены по сравнению с предыдущими операционными системами. Тем не менее это практически не сказывается на общем интерфейсе Windows Vista. Да, окна Проводника открываются дольше, да и все операции стали выполняться дольше, чем в предшественнике Windows Vista. Но если отключить интерфейс Windows Aero (такая возможность существует), замечаешь, что система стала тормозить еще больше. В частности, при стандартном интерфейсе перемещение окна Проводника приводит к стопроцентной загрузке процессора компьютера, а само окно начинает двигаться рывками, тогда как при перемещении окна с использованием интерфейса Windows Aero процессор загружается меньше чем на 50 %, а окно двигается очень плавно. Что это: недоработки в коде операционной системы или так работает новый механизм повышения производительности компьютера, интегрированный в интерфейс Windows Vista (все эффекты нового интерфейса обрабатывает WCE (Windows Composition Engine), который призван повысить производительность компьютера)?

Для работы интерфейса Aero нужно, чтобы ваша видеокарта поддерживала драйвер WDDM (Windows Display Driver Model) и интерфейс DirectX 9.0, а также имела минимум 64 Мбайт оперативной памяти (рекомендуемая цифра — 128 Мбайт). Как утверждают разработчики, драйвер WDDM позволяет повысить производи-

тельность операционной системы и интерфейса Aero при работе с несколькими приложениями. Также благодаря драйверу WDDM вы теперь сможете подключать мониторы к компьютеру в горячем режиме (без отключения питания). Кроме того, драйвер WDDM больше не может напрямую обращаться к ядру операционной системы, что позволяет повысить общий уровень ее отказоустойчивости.

Следует понимать, что даже если ваша графическая плата не сможет работать с интерфейсом Aero, на работе самой операционной системы Windows Vista это не скажется. В этом случае будет использоваться стандартный интерфейс Windows.

Боковая панель (Sidebar)

Операционная система Windows Vista по умолчанию включает в свой состав новую боковую панель, на которой можно располагать специально написанные мини-приложения (еще называемые гаджетами) (по сути, боковая панель является не частью операционной системы, а отдельной программой). Они могут создаваться как программистами самой корпорации Microsoft, так и сторонними программистами и могут выполнять различные дополнительные функции. Например, в состав операционной системы входят мини-приложения, предоставляющие следующие возможности: отображение времени, отображение загруженности процессора и оперативной памяти, отображение RSS-лент и т. д.

Windows Search Engine

В состав Windows Vista также входит новый механизм поиска информации, с помощью которого вы можете найти информацию на локальном или сетевом ресурсе (автоматически ведется поиск в папках общего доступа) или в почтовых сообщениях, используя при этом не только название файла или часть того, что он содержит, но и дополнительную информацию. Например, тип и свойства файла (имя автора документа, имя владельца документа, дату создания документа, дату последнего изменения файла), метаданные, связанные с файлом (например, год издания, название альбома, имя исполнителя и название песни для музыкальных файлов).

Новый поиск контекстно-зависим, работает быстро и позволяет легко сохранить свои результаты, чтобы впоследствии вернуться к ним. Для этого достаточно нажать кнопку Сохранить условия поиска. После этого сохраненный поиск будет помещен в папку Поиски и вы всегда сможете вернуться к нему. Стоит также упомянуть, что в результаты сохраненного поиска будут автоматически добавляться новые файлы (недавно появившиеся в файловой системе), которые удовлетворяют критериям поиска.

При этом механизм поиска встроен не только в окна Проводника, но и непосредственно в меню Пуск, новый браузер Internet Explorer 7.0, почтовый клиент Почта Windows и другие стандартные программы Windows Vista. Поиск Windows Vista также использует совместный индекс с поиском из продуктов Microsoft Office (в Windows

Vista можно выполнять как полный поиск в содержимом определенной папки, так и индексный поиск). Кроме того, теперь вы сможете легко просмотреть найденные текстовые документы, даже не открывая их, — появилась возможность просмотра эскиза содержимого найденного документа.

Новый механизм передачи цвета

Операционная система Windows Vista включает в себя новый компонент работы с цветом, который был лицензирован корпорацией Microsoft у компании Canon. Благодаря этому компоненту цветовая гамма, выводимая на монитор компьютера, будет максимально приближена к той, которая будет отображаться при печати. Другими словами, в идеальном случае по умолчанию вы будете видеть на мониторе своего компьютера такие же цвета и оттенки изображения, которые будут выведены на принтер при печати данного изображения.

1.2. Способы защиты в новой ОС

Контроль учетных записей пользователей (UAC)

Механизм UAC (или UAP, что является синонимом) призван повысить общую защищенность операционной системы Windows Vista. Он позволяет запускать с пониженными правами приложения, требующие системных функций или записи в системный каталог или реестр. Для этого механизм использует виртуальное хранилище. Например, когда программа пытается записать данные в системный каталог или в реестр, она записывает их в виртуальное хранилище, не изменяя содержимое реальной файловой системы компьютера или реестра. При этом все изменения в виртуальных папках останутся после завершения работы программы (то есть они не являются временными и после повторного запуска программа будет использовать содержимое виртуальных папок, считая, что по-прежнему работает непосредственно с файловой системой компьютера), а сама файловая система компьютера окажется неизмененной.

Теперь в операционную систему добавлено несколько учетных записей, которые имеют ограниченные разрешения в системе (например, только разрешения установки программ), а некоторые стандартные учетные записи были дополнительно ограничены в разрешениях. Кроме того, теперь только пользователь Администратор может свободно чувствовать себя в системе — даже если вы имеете административные права и попытаетесь переместить какой-либо файл из одного раздела диска на другой, удалить файл, запустить какую-либо программу, требующую административных прав, или запустить оснастку консоли управления Microsoft или редактор реестра, механизм UAC обязательно спросит у вас, действительно ли вы хотите это сделать и понимаете ли вы, что это может нарушить работу операционной системы. А ряд задач можно выполнить, только войдя в операционную систему под учетной записью Администратор.

Таким образом, понижается риск случайного нанесения повреждений операционной системе.

Защита доступа к сети (NAP)

Если механизм UAP предназначен для локальной защиты операционной системы от действий различных вирусов, то механизм NAP предназначен для защиты доступа к компьютеру по сети. С его помощью вы можете более тонко настраивать списки компьютеров сети, которые могут получить доступ к вашему компьютеру. Например, вы можете указать, что к вашему компьютеру могут подключаться только те компьютеры, на которых установлены все основные заплатки и пакеты обновлений для операционной системы.

Защитник Windows

Теперь в стандартную поставку операционной системы входит программа, позволяющая защитить ваш компьютер от вредоносного программного обеспечения.

1.3. Дополнительные возможности

Работа со звуком

Если раньше операционные системы семейства Windows работали со звуком в 16-битном режиме, то Windows Vista работает в 32-битном. Это повышает качество звука, делая его более глубоким и чистым. Правда, именно из-за этого изменения больше не поддерживается аппаратное ускорение звука, поэтому скорость работы с ним уменьшится.

Раз уж мы заговорили о звуке, то стоит обратить внимание на такое нововведение Windows Vista, как отдельные регуляторы громкости для всех программ, работающих со звуком.

Virtual PC Express

С помощью нового механизма виртуализации вы можете запускать различные приложения, которые по каким-то причинам не могут работать в Windows Vista, в различных эмулируемых операционных системах, отличных от Vista.

Подсистема для UNIX-приложений (SUA)

Новая подсистема для UNIX-приложений позволит вам запускать в операционной системе Windows Vista программы, разработанные для операционных систем семейства UNIX.

Шифрование диска Windows BitLocker

Если ваш компьютер обладает новой материнской платой, содержащей микросхему TPM, то вы сможете воспользоваться такими стандартными возможностями Windows Vista, как шифрование отдельных разделов диска или всего диска на лету (также шифруются системные файлы Windows, временные файлы и файл,

создаваемый при переходе в спящий режим). При этом будет использоваться алгоритм AES 256, который, как утверждают разработчики, вызывает лишь незначительное падение производительности файловой системы.

Для реализации механизма шифрования диска Windows BitLocker вместо чипа TPM можно также использовать обычный USB-носитель.

Микросхема TPM содержит ключи, пароли и сертификаты для всех программ и компонентов операционной системы, а также для установленного на компьютере оборудования. Иными словами, пользователь, не обладающий на то соответствующими правами, не сможет не только установить нужную программу, но и изменить аппаратную конфигурацию компьютера. Это позволит полностью обезопасить компьютеры от различных троянских коней, вирусов и других вредоносных программ и драйверов, а также защитить аппаратную составляющую компьютера от несанкционированного изменения, которое может привести к взлому операционной системы, например от установки дополнительного жесткого диска со своей операционной системой для получения доступа к защищенным данным.

Работа чипа TPM основана на хэше, который вычисляется на основе хэшей всего оборудования и программного обеспечения, установленного на компьютере. При запуске компьютера чип TPM проверяет данный хэш и в случае идентичности разрешает использование любых программ. Если же оказывается, что хэши не совпадают, то будет разрешено запускать лишь обычные файлы и программы.

DVD-студия Windows

Теперь в операционную систему по умолчанию входит программа для создания DVD, содержащих видеоданные или набор слайд-шоу, которые можно будет просмотреть на большинстве проигрывателей DVD. С помощью данной программы вы можете как редактировать сами видеоданные, добавляя или удаляя свои сцены, так и создавать меню для нового диска. Другими словами, если вам для создания и записи своих видеодисков раньше приходилось пользоваться сторонними программами, например Nero, то сейчас все необходимое есть в самой операционной системе.

DVD-студия Windows поддерживает как формат PAL, так и NTSC. При этом видео можно сохранять как с соотношением сторон 4:3, так и с широкоформатным соотношением 16:9. Поскольку в программе DVD-студия Windows нет никаких средств монтажа видео, в состав операционной системы Windows Vista по-прежнему входит программа Windows Movie Maker, и вы можете импортировать свои проекты Movie Maker в программу DVD-студия Windows для записи на диск.

Internet Explorer 7.0

Новшеством операционной системы Windows Vista является браузер Internet Explorer версии 7.0. Наконец-то браузер Internet Explorer не является обязательным компонентом операционной системы и вы можете удалить его так же, как и любую другую программу. Но не стоит сразу это делать — новый браузер существенно отличается от своего предшественника. Теперь в него встроены компонен-

ты для работы с RSS-лентами, и при переходе на сайт, предоставляющий RSS-ленты, браузер сам скажет вам об этом и предложит подписаться на них. Кстати, теперь каждый сайт отображается не в виде отдельного окна Internet Explorer, а как вкладка в основном окне браузера. Теперь вы также можете легко выполнить проверку сертификата безопасности для защищенного сайта (адрес которого начинается с https://), загруженного на активной в данный момент вкладке.

В браузер Internet Explorer встроен новый механизм поиска, с помощью которого вы можете найти информацию не только с помощью поисковой системы Microsoft, но и в таких системах, как Google, Wikipedia, база знаний Microsoft или любых других, которые вы добавите. Еще одним новым механизмом Internet Explorer является механизм фильтрации сайтов (Phishing Filter), которые предположительно были разработаны людьми, создающими сайты, визуально напоминающие другие известные сайты, чтобы получить от вас конфиденциальную информацию (их еще называют фишерами). При этом механизм фильтрации пользуется данными, которые обновляются несколько раз в час.

И, конечно, не стоит забывать о таком новшестве Internet Explorer, как запуск браузера с ограниченными правами. Теперь браузер запускается от имени пользователя, который не имеет прав доступа к файловой системе компьютера или его реестру (браузер запускается в песочнице). Благодаря этому, даже если в браузере будут найдены уязвимости, хакер не сможет ими воспользоваться, так как сам браузер не будет иметь для этого достаточных прав.

В Internet Explorer реализованы такие дополнительные механизмы защиты от программ, использующих уязвимость операционной системы для выполнения действий, которые запрещены пользователю (называемых еще эксплоитами), как унифицированный разбор URL, ограничитель сценариев, запрет установки программного обеспечения в фоновом режиме, реальное отражение международных доменных имен (IDN).

Единственным недостатком нового браузера можно назвать лишь слишком большое количество ресурсов компьютера, которое он использует для своей работы.

Почта Windows

Обновился и почтовый клиент, интегрированный в операционную систему. Теперь он называется не Outlook Express, а Почта Windows и предоставляет новые антиспамовые фильтры, а также измененную систему хранения адресной книги и регистрации пользователей в почтовом клиенте.

Ножницы

Наконец-то в состав операционной системы входит приложение, с помощью которого можно создавать копии как всего экрана, так и любой отдельной его части (прямоугольной или любой другой формы). Кроме того, созданные копии вы можете сохранить в качестве рисунка, поместить в буфер обмена, создать на их основе простой HTML-документ или отправить по электронной почте.

Календарь Windows

Представляет собой простой органайзер, особенностью которого является возможность публикации своих дел для доступа другим пользователям, входящим в специальную группу.

Оценка и увеличение производительности компьютера

Еще одним нововведением Windows Vista является возможность тестирования производительности вашего компьютера. Операционная система выполняет тестирование основных компонентов компьютера (видеокарта, процессор, объем жесткого диска, оперативная память) и на полученных данных определяет его рейтинг по пятибалльной шкале.

Средства распознавания речи (Speech Recognition)

Операционная система Windows Vista содержит компоненты распознавания речи, благодаря которым вы сможете голосом отдавать команды компьютеру или диктовать ему текстовые сообщения. К сожалению, пока что вы можете диктовать только на английском языке.

Windows Media Center

Вы, наверное, знаете, что одной из версий операционной системы Windows XP была операционная система Windows XP Media Center. Она включала в себя набор программ и компонентов, с помощью которых можно было превратить ваш компьютер в настоящий домашний кинотеатр. С помощью данных программ вы могли как просматривать или записывать телевизионные передачи или фильмы на вашем компьютере, так и слушать и записывать музыку или даже подключать свою приставку Xbox.

Теперь не будет существовать отдельной редакции Windows Vista, содержащей компоненты Windows Media Center, — все эти возможности будут встроены в саму операционную систему.

Tablet PC Edition

Раньше также существовала отдельная редакция Windows XP, предназначенная специально для компьютеров Tablet PC (Windows XP Tablet PC Edition 2005). Она содержала новые компоненты, реализующие возможность доступа к интерфейсу операционной системы с помощью пера и специального чувствительного экрана, реагирующего на касания.

Теперь все компоненты Tablet PC встроены в саму операционную систему Windows Vista.

Мобильные ПК

Данный компонент операционной системы предназначен только для ноутбуков и позволяет настраивать параметры их энергопотребления.

Новый формат образов установки WIM (Windows Imaging)

В состав операционной системы входит новый формат образов установки WIM, а также программа, позволяющая создавать образы операционной системы. Особенностью данного формата является возможность хранения в одном образе нескольких операционных систем, что было достигнуто благодаря файл-ориентированности нового формата (ранее применялся сектор-ориентированный формат). При этом сам образ сжимается, а все одинаковые файлы, присутствующие в различных операционных системах, хранящихся в образе, заменяются только одним файлом (все одинаковые копии файлов удаляются, а на их место помещаются специальные ссылки на оставшийся файл). Благодаря этому размер образа существенно сокращается. Кроме того, теперь созданный образ операционной системы не будет зависеть от оборудования компьютера, на который вы устанавливаете ее, как это было ранее. Еще одним новшеством является модульность Windows Vista — теперь перед созданием образа операционной системы вы можете указать компоненты, которые будут входить в образ. Например, драйверы, обновления, поддерживаемые языки. Более того, таким образом вы легко можете редактировать содержимое уже созданного образа.

Стоит заметить, что именно с помощью образа установки WIM и будут созданы диски установки Windows Vista. И уже на примере установочного дистрибутива Windows Vista Ultimate можно заметить прелести нового образа установки: его объем равен приблизительно 3,5 Гбайт, а содержит он 7,5 Гбайт файлов операционной системы и устанавливается не намного дольше операционной системы Windows XP, имеющей намного меньший размер.

Встроенная поддержка IPv6

Теперь поддержка нового протокола IP версии 6 встроена в саму операционную систему, и большинство программ для работы в сети имеют параметры настройки данного протокола.

Новые MSC-оснастки

Кроме всего прочего, операционная система Windows Vista содержит несколько совершенно новых оснасток консоли управления Microsoft, существенно переделанные стандартные оснастки, а также новую версию самой консоли управления Microsoft (версия 3.0).

Возможность самодиагностики жесткого диска и оперативной памяти

Теперь операционная система может самостоятельно следить за состоянием жесткого диска. Если она определит, что какой-то параметр работы жесткого диска стал критически низок, то система предупредит пользователя о возможном скором выходе диска из строя. При этом она предложит выполнить архивирование содержимого диска.

Операционная система также выполняет диагностику оперативной памяти. Если она определит, что какой-то сбой в работе произошел из-за ошибок оперативной памяти, то предложит пользователю запустить процедуру диагностики памяти, в процессе которой найденные сбойные секторы ОЗУ будут помечены поврежденными и больше не станут использоваться операционной системой.

Еще одним нововведением операционной системы является инструмент исправления при запуске (Startup Repair Tool). Если в процессе запуска операционной системы произойдет какой-либо сбой, то будет автоматически запущен данный инструмент. Он выполнит проверку метаданных, хранящихся на диске, корректность системных файлов операционной системы и используемых ею драйверов, а также просмотрит все файлы журналов, создаваемые в процессе запуска компьютера, на предмет описания возникшей ошибки.

Новый набор стандартных драйверов

В состав операционной системы входят драйверы не только для стандартного оборудования, но и для более экзотических для нашей страны компонентов, например для коммуникаторов или смартфонов. Более того, теперь операционная система содержит средство для синхронизации с коммуникаторами, поэтому вам больше не придется пользоваться сторонними разработками в этой области. Данное средство называется Диспетчер синхронизации и позволяет выполнять синхронизацию компьютера не только с коммуникаторами, но и с любым другим устройством, предоставляющим такую возможность.

Новые функции WinAPI и DirectX 10

И, конечно, новая операционная система включает в себя множество новых API-функций, а также новый DirectX десятой версии. Его использование позволит повысить качество будущих видеоигр. Тем не менее пока что Windows Vista никак нельзя назвать частью игровой платформы — как показали тесты, она проигрывает своей предшественнице Windows XP в производительности в играх (до 30 %). Хочется верить, что в этом виноваты драйверы, не оптимизированные под новую операционную систему, или создатели игр, а не новая операционная система.

Глава 2

Установка Windows Vista

- **Версии Windows Vista**
- **Процесс установки операционной системы**
- **Дополнительные работы после установки**

2.1. Версии Windows Vista

Как и предыдущие операционные системы корпорации Microsoft, Windows Vista поставляется в нескольких редакциях, которые отличаются друг от друга наличием или отсутствием тех или иных компонентов, программ или возможностей операционной системы. Как вы уже знаете, больше не будет отдельных редакций операционной системы, которые содержат компоненты Windows Media Center или Tablet PC, — теперь они встроены непосредственно в операционную систему. Тем не менее, общее количество редакций операционной системы Windows Vista от этого сократилось не намного. Теперь редакции можно разделить на три группы: на предназначенные для домашних или корпоративных пользователей, а также на отдельную редакцию, содержащую все компоненты операционной системы. Все они поставляются только на DVD из-за своего большого размера (наибольшей является редакция Windows Vista Ultimate, которая занимает 3,5 Гбайт для 32-разрядных процессоров и 4,4 Гбайт для 64-разрядных).

Для домашних пользователей предназначено три версии операционной системы: Windows Vista Starter Edition, Windows Vista Home Basic Edition и Windows Vista Home Premium Edition.

Для корпоративных пользователей предназначено всего две версии Windows Vista: Windows Vista Business Edition и Windows Vista Enterprise Edition.

Особняком стоит редакция Windows Vista Ultimate Edition, включающая в себя все компоненты операционных систем Windows Vista.

Существует также две дополнительные редакции операционной системы Windows Vista, которые будут поставляться в европейские страны: Windows Vista Home N Edition и Windows Vista Business N Edition. Они отличаются от своих братьев только отсутствием программы Проигрыватель Windows Media.

Различия в редакциях операционной системы

Редакции операционных систем Windows Vista отличаются друг от друга как отсутствием отдельных программ и компонентов, так и настройками параметров реестра. При определении программ и компонентов, которые будут присутствовать в той или иной редакции операционной системы, корпорация Microsoft руководствовалась критериями пользователей, на которых эти редакции рассчитаны. При этом большинство программ, которые не будут присутствовать по умолчанию в той или иной редакции, вы сможете скачать дополнительно с сайта Microsoft.

ПРИМЕЧАНИЕ

В данной книге будет описываться редакция Windows Vista Ultimate, так как она содержит все компоненты операционной системы, которые могут быть доступны в тех или иных дополнительных редакциях Windows Vista.

Рассмотрим содержимое и назначение основных редакций операционной системы Windows Vista.

Windows Vista Starter Edition

Данная версия является усеченной редакцией Windows Vista Home Basic, имеющей в своем составе лишь минимальные функции и возможности новой операционной системы. В отличие от остальных редакций операционной системы, которые могут работать как на 32-разрядных, так и на 64-разрядных процессорах, Windows Vista Starter может работать только с 32-разрядными процессорами. Кроме того, максимальный объем оперативной памяти, который поддерживает данная операционная система, равен 256 Мбайт, а максимальное количество программ, которые возможно запускать одновременно в операционной системе, ограничено тремя. Но это еще не все ограничения. Данная операционная система также не имеет функции быстрого переключения пользователей, не позволяет устанавливать пароли на учетные записи и не поддерживает входящие сетевые подключения.

Естественно, что из-за ограниченного объема поддерживаемой оперативной памяти данная операционная система не поддерживает интерфейс Windows Aero и множество других новых возможностей операционной системы Windows Vista.

Windows Vista Home Basic Edition

В отличие от своего усеченного предшественника, данная редакция не имеет таких аппаратных ограничений, как 32-разрядность процессора, 256 Мбайт ОЗУ (тем не менее максимальный объем ОЗУ все равно ограничен — на этот раз 8 Гбайт), количество одновременно запущенных программ и т. д. Эта редакция содержит множество основных программ и компонентов, которые недоступны в операционной системе Windows Vista Starter, а максимальное количество сетевых подключений в ней равно пяти.

Тем не менее Windows Vista Home Basic имеет тот же недостаток, что и его усеченный аналог: она не поддерживает новый интерфейс Windows Aero. Кроме того, эта редакция не поддерживает возможность подключения дополнительного монитора.

При использовании лицензии Windows Anytime Upgrade данную версию операционной системы Windows Vista можно будет обновить до версии Windows Vista Home Premium Edition.

Windows Vista Home Premium Edition

Эту редакцию Windows Vista уже можно назвать полной. Она поддерживает все возможности Windows Vista Home Basic и, кроме них, интерфейс Windows Aero и такие компоненты, как Windows Media Center и Tablet PC, а также компонент Windows Media Center Extender, расширяющий мультимедийные возможности компьютера. В ней также поддерживаются следующие возможности, недоступные в предыдущих редакциях:

- EFS — шифрующая файловая система, позволяющая выполнять шифрование файлов и папок, расположенных на томах с файловой системой NTFS;
- служба Теневое копирование тома;
- возможность выполнения архивации по сети или по составленному расписанию;

- DVD-студия Windows и Windows Movie Maker;
- дополнительные игры;
- максимальное количество сетевых подключений равно десяти;
- возможность синхронизации данных между компьютерами;
- Mobility Center.

Данная редакция также имеет ограничение на максимально возможное количество оперативной памяти. На нее можно установить максимум 16 Гбайт ОЗУ. Кроме того, в этой редакции существует ограничение на количество поддерживаемых процессоров. Операционная система Windows Vista Home Premium Edition (как и Windows Vista Home Basic Edition) поддерживает не больше одного процессора.

Windows Vista Business Edition

Если предыдущие редакции предназначались для домашних пользователей и поэтому включали в себя большинство мультимедийных возможностей, эта редакция предназначена для корпоративных пользователей, и основной уклон в ней сделан на безопасность и расширенные сетевые возможности операционной системы. Поэтому Windows Vista Business Edition не содержит в своем составе компонент Windows Media Center, а также программы DVD-студия Windows и Windows Movie Maker. Вместо них она включает в себя следующие компоненты;

- удаленный Рабочий стол — позволяет выполнять удаленное управление компьютером;
- компоненты планшетных ПК — несмотря на то что компоненты Windows Media Center были удалены из данной редакции, она все еще поддерживает возможность работы с помощью пера;
- дополнительные службы для работы с Интернетом, например IIS;
- возможность полноценной работы в домене;
- дополнительные сетевые протоколы, например средства для создания одноранговых сетей;
- возможность использования автономных папок с поддержкой кэширования на стороне клиента;
- возможность поддержки двух процессоров.

Эта редакция (и следующие за ней) не требует проведения активации.

При использовании лицензии Windows Anytime Upgrade License данную версию операционной системы Windows Vista можно будет обновить до версии Windows Vista Ultimate.

Windows Vista Enterprise Edition

Как предполагается, данная редакция не будет находиться в свободной продаже — она будет распространяться как обновление для корпоративных клиентов Microsoft (будет доступна тем клиентам, которые заключили соглашение Software Assurance или Microsoft Enterprise Agreement). Windows Vista Enterprise Edition

включает в себя все компоненты редакции Windows Vista Business Edition и, кроме них, следующие компоненты:

- Virtual PC Express — позволяет запускать приложения в среде виртуального компьютера;
- MUI — многоязычный пользовательский интерфейс;
- шифрование диска Windows BitLocker — позволяет выполнять полное шифрование отдельных томов жесткого диска;
- SUA — подсистема для UNIX-приложений, позволяющая запускать их в операционной системе Windows Vista;
- механизм Secure Startup — автоматически выполняет диагностику неисправностей при неудачной попытке запуска операционной системы.

Различия в редакциях с точки зрения реестра

К сожалению, на стадии бета-версии операционной системы нет способа проверить различия в редакциях, касающиеся изменений в реестре Windows, так как доступная бета-версия содержит все возможные компоненты системы и поддерживает все ее возможные функции. Тем не менее удалось установить, что новая операционная система Windows Vista в плане разграничения редакций не отличается от своей предшественницы Windows XP. Все так же сведения о редакции операционной системы хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions`. Все так же для определения редакции используется два параметра.

- Параметр строкового типа `ProductType` определяет направленность редакции (для домашнего или корпоративного использования). Он может иметь три значения:
  - `WinNT` — система предназначена для домашнего использования;
  - `ServerNT` — система предназначена для корпоративного использования;
  - `LanmanNT` — скорее всего, больше не используется, так как применение этого значения приводит к невозможности загрузки операционной системы.
- Параметр `ProductSuite` типа `REG_MULTI_SZ` определяет конкретную редакцию операционной системы. Он может принимать следующие значения: `Embedded(Restricted)`, `Blade Personal`, `DataCenter`, `EmbeddedNT`, `Terminal Server`, `Small Business(Restricted)`, `BackOffice`, `CommunicationServer`, `Enterprise`, `Small Business`.

В указанной ветви реестра появился еще один параметр типа `REG_BINARY` — `ProductPolicy`.

По умолчанию Windows Vista Ultimate использует следующие значения параметров `ProductType` и `ProductSuite`: `WinNT` и `Terminal Server`. При этом версия операционной системы определяется как Windows Vista (TM) Build 6000 (рис. 2.1, *сверху*).

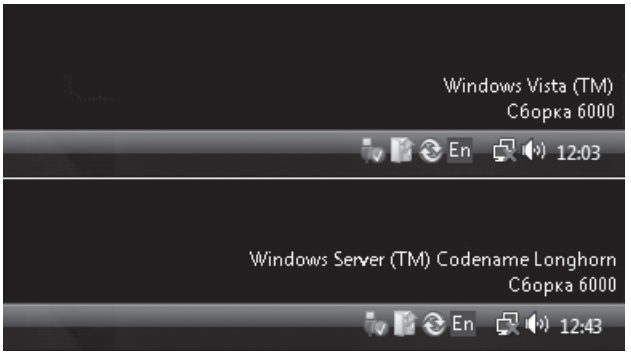


Рис. 2.1. Версии Windows Vista

Можно применять следующие сочетания значений этих параметров.

- `WinNT` и любое значение параметра `ProductSuite`, кроме `Terminal Server` и `Embedded`.
- `ServerNT` и любое значение параметра `ProductSuite`, кроме `Embedded`. Приводит к изменению версии операционной системы на Windows Server (TM) Codename Longhorn Build 6000 (рис. 2.1, *снизу*). При этом в поведении операционной системы происходят следующие изменения:
  - при входе пользователя в систему и при завершении работы отображается более полная информация о том, что именно в данный момент делает система (например, применяет групповые политики, воспроизводит мелодию запуска или завершает работу служб);
  - при завершении работы и при входе в систему отображается окно, в котором нужно указать, по какой причине необходимо завершить работу системы;
  - изменяются параметры хранения дампов памяти.
- `WinNT` и `Embedded`. Приводит к изменению версии операционной системы на Windows R Codename Longhorn Embedded Evaluation.

ПРИМЕЧАНИЕ

Поскольку не существует отдельных редакций Windows Media Center и Tablet PC, больше не поддерживается и возможность преобразования редакции операционной системы с помощью ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\WPA. Теперь данная ветвь реестра содержит только сведения о ключе активации операционной системы.

2.2. Процесс установки операционной системы

После того как мы рассмотрели краткое описание основных редакций новой операционной системы Windows Vista, остановимся детальнее на процессе ее установки.

Основные требования к компьютеру

Как правило, описание новой программы или тем более операционной системы всегда начинается с приведения минимальных и рекомендуемых требований к компьютеру, на котором будет нормально работать программное обеспечение или операционная система. Не будем отходить от правил и поговорим о рекомендуемых корпорацией Microsoft системных требованиях, которые новая операционная система предъявляет к компьютеру.

Так уж повелось, что каждая новая операционная система от Microsoft требует все больше и больше системных ресурсов. При этом каждый раз новые системные требования просто ужасали пользователей. Не стала исключением и новая операционная система Windows Vista.

Процессор: желательно иметь процессор с тактовой частотой от 3 ГГц и выше.

Материнская плата: должна поддерживать спецификацию ACPI.

Оперативная память: не менее 512 Мбайт, но рекомендуется 1 Гбайт и более.

Монитор: минимальное разрешение не ниже 800 × 600 пикселов, но желательно 1024 × 768 пикселов или выше.

Видеокарта: видеокарта должна поддерживать DirectX 9.0 или выше (то есть должна поддерживать пиксельные шейдеры[1] второй или третьей версии), должна иметь драйвер WDDM, интерфейс как минимум AGP 4x, а также не менее 64 Мбайт видеопамяти (желательно 128 Мбайт или больше, особенно если вы будете использовать высокое разрешение монитора).

Объем раздела жесткого диска: раздел жесткого диска, на который будет устанавливаться операционная система, должен иметь объем не менее 10 Гбайт (для редакции Windows Vista Ultimate). Рассчитанный объем состоит из 7,5 Гбайт файлов операционной системы, размера файла подкачки (около 1 Гбайт), размера файла, используемого при переходе в спящий режим, если вы, конечно, будете использовать этот режим (равен объему вашей оперативной памяти), а также некоторого количества свободного места для новых драйверов, шрифтов, файлов журналов и т. д. Следует обратить внимание и на то, что операционная система Windows Vista может быть установлена только на раздел, отформатированный с помощью файловой системы NTFS (она поддерживает все основные файловые системы (реализации FAT и т. д.), но устанавливаться может только на раздел с NTFS).

Следует понимать, что требования к видеокарте, оперативной памяти и процессору так высоки именно из-за нового интерфейса Windows Aero. И если ваш компьютер не соответствует указанным системным требованиям, то, скорее всего, вы все равно сможете установить на него новую операционную систему. Единственное,

---

[1] Шейдер — это программа, использующая определенные программируемые регистры видеокарты для создания графических эффектов. Существует два вида шейдеров — пиксельные и вершинные. Каждый из этих типов шейдеров обрабатывается в отдельной части графического конвейера.

чего вы лишитесь в таком случае, — возможностей нового интерфейса Windows Aero. В остальном новая операционная система будет работать нормально.

Если же вы не хотите забивать себе голову вопросом требований к аппаратной части компьютера, то можно воспользоваться специальной программой Windows Vista Upgrade Advisor, которую можно скачать с сайта Microsoft. Эта программа задаст вам несколько вопросов (для чего вы используете компьютер), после чего проверит его конфигурацию и скажет, подходит она для решения поставленных вами задач с помощью Windows Vista или придется модернизировать какой-то компонент компьютера.

Стоит упомянуть, что теперь, если ваш жесткий диск подключен с помощью RAID, вам больше не нужно копировать драйверы RAID на дискету — в Windows Vista их можно загрузить непосредственно с компакт-диска.

Процесс установки

Рассмотрим сам процесс установки новой операционной системы.

Как было сказано ранее, любая редакция Windows Vista поставляется на DVD, поэтому для ее установки вы должны иметь привод DVD. Произвести установку новой операционной системы можно как с этого диска, так и с жесткого диска, предварительно скопировав на него дистрибутив Windows Vista. Если вы будете устанавливать операционную систему с жесткого диска, то запустите файл `setup.exe` (обратите внимание, что раньше установочный файл назывался `winnt32.exe`). Теперь установочный диск не содержит папки i386. Все файлы Windows Vista находятся в папке sources, в которой хранятся файлы `boot.wim` и `install.wim` (обратите внимание на расширение этих файлов — сразу понятно, что образ операционной системы создан с помощью нового формата WIM).

ПРИМЕЧАНИЕ

Основная часть установки Windows Vista приходится на копирование ее файлов на жесткий диск. Поэтому если вы будете устанавливать операционную систему непосредственно с жесткого диска, то процесс установки займет намного меньше времени.

Начало установки

После того как файл `setup.exe` был запущен (независимо от того, был ли он запущен вами или системой в процессе загрузки), перед вами отобразится начальное окно установки (рис. 2.2). Оно содержит ссылку Установить, после нажатия которой начнется процесс установки операционной системы. Кроме того, обратите внимание на еще одну ссылку — Восстановление системы. Если в будущем установленная операционная система по каким-то причинам не будет загружаться, то с помощью этой ссылки вы можете воспользоваться одной из созданных ранее точек отката (если, конечно, вы их создавали), чтобы вернуться к конфигурации системы, определенной в этой точке отката.



Рис. 2.2. Начальная страница мастера установки Windows Vista

В данном окне также присутствует ссылка Перенос файлов и параметров настройки с другого компьютера. Если вы выполняли чистую установку (а не обновление Windows 2000 или Windows XP до Windows Vista), то с помощью данной ссылки всегда можете запустить мастер переноса всех настроек предыдущей используемой вами операционной системы в установленную Windows Vista. Обе эти ссылки более подробно мы рассмотрим далее в этой главе. А пока вернемся к установке операционной системы.

Поиск обновления установленных программ

После нажатия ссылки Установить перед вами отобразится окно, с помощью которого вы можете выполнить поиск новых драйверов и обновлений для вашей системы на сайте Microsoft (оно отображается только в том случае, если вы выполнили запуск установки Windows Vista в процессе работы в другой операционной системе) (рис. 2.3). Если ваш компьютер не подключен к Интернету или вы просто не хотите пока посещать сайт Microsoft, то выберите ссылку Не загружать последние обновления программы установки.

Начиная с этого шага, вы можете воспользоваться комбинацией клавиш Shift+F10 для вызова командной строки. После нажатия данной комбинации перед вами отобразится командная строка `cmd.exe`, загруженная от имени администратора, из которой вы сможете запустить программы, находящиеся в папке sources дистрибутива операционной системы.

В каталоге sources можно найти следующие исполняемые файлы.

- `mighost.exe` — программа миграции. Подробнее о параметрах данной программы можно узнать, введя команду `mighost.exe /?`.

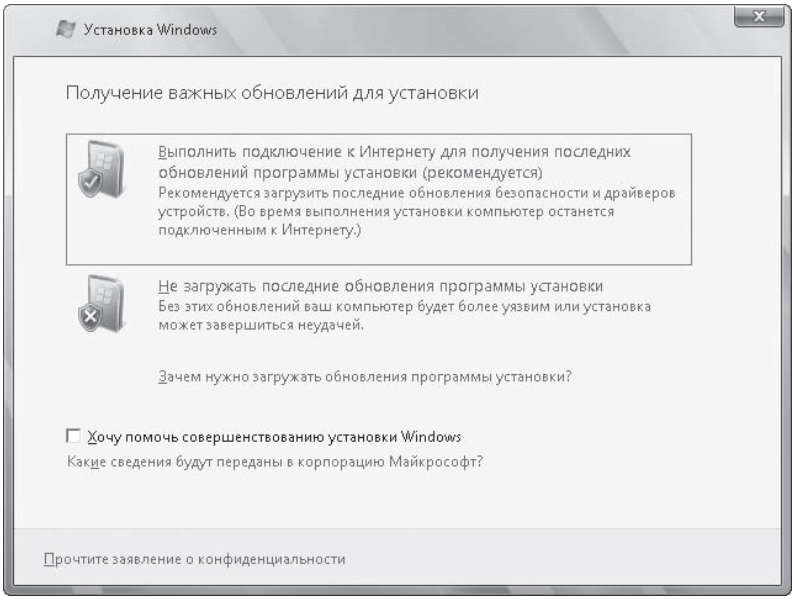


Рис. 2.3. Первый шаг установки — возможность поиска обновлений на сайте Microsoft

- `mrt.exe` — запускает программу Средство удаления вредоносных программ, которая позволяет выполнить поиск шпионских программ, установленных в операционной системе, и инфицированных файлов. Подробнее о параметрах данной программы можно узнать, введя команду `mrt.exe /?`.
- `pkgmgr.exe` — выполняет установку компонентов операционной системы. С помощью данной программы можно также изменять компоненты операционной системы, которые будут устанавливаться при инсталляции Windows Vista. Параметры этой программы будут описаны в гл. 9, посвященной установке и удалению компонентов операционной системы Windows Vista.
- `rollback.exe` — позволяет отменить установку операционной системы.
- `setuposk.exe` — запускает экранную клавиатуру, которая позволяет набирать текст с помощью мыши.
- `Adprep.exe` — эта программа находится в каталоге sources\adprep. С ее помощью можно обновить параметры работы новой операционной системы Windows Vista в домене Active Directory.

Ввод ключа продукта

Далее перед вами отобразится окно, в котором вы должны ввести код продукта вашей операционной системы (указан на коробке или в HTML-файле, если вы скачали дистрибутив из Интернета) (рис. 2.4). Обратите внимание на флажок Автоматически активировать Windows при подключении к Интернету. По умолчанию он установлен, и при вашем первом посещении Интернета система автоматически выполнит активацию вашей копии операционной системы. Конечно, вы можете выполнить ее и вручную.

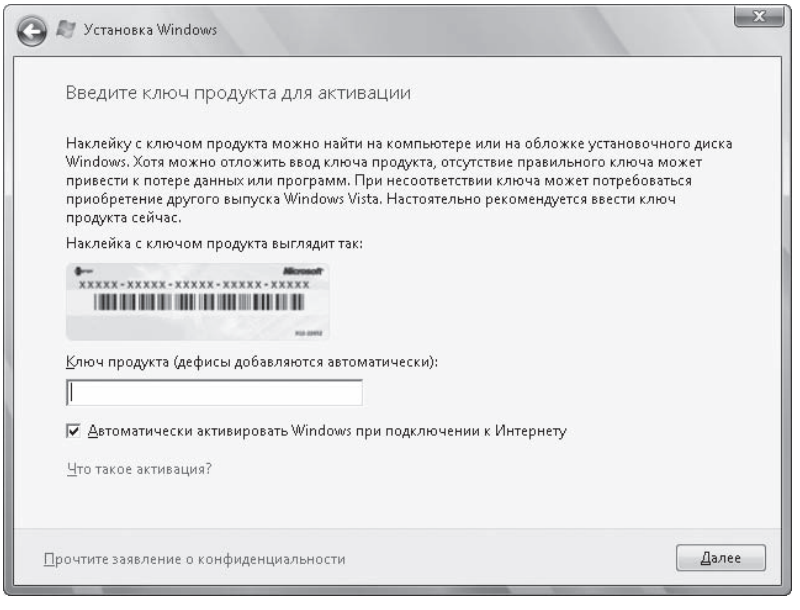


Рис. 2.4. Ввод ключа вашей операционной системы

Обратите внимание, что если вы еще не начали вводить код продукта, а кнопка Next уже активна, то установить операционную систему можно и без ввода кода продукта (однако при выполнении активации операционной системы вам все-таки придется его ввести). Для этого достаточно нажать кнопку Далее, в появившемся окне нажать кнопку Нет, а потом выбрать ваш тип операционной системы (Ultimate, Basic и т. д.), установить флажок Выбран приобретенный выпуск Windows и опять нажать кнопку Далее.

Тип установки

После того как вы введете код продукта и нажмете кнопку Далее, программа установки проверит корректность введенного кода (при этом, если выполняется установка с жесткого диска, процедура установки попросит вставить установочный диск, но после проверки корректности кода продукта установочный диск вам больше не понадобится) и отобразит новое окно (рис. 2.5). С его помощью можно выбрать, будете вы обновлять предыдущую операционную систему или выполните установку с нуля.

Выбор раздела установки

Если вы выбрали вариант чистой установки, то следующим окном, которое отобразит мастер, будет окно выбора раздела, на который будет устанавливаться операционная система (рис. 2.6). Обратите внимание, что в списке доступных разделов отображаются все разделы жестких дисков, имеющие формат файловой системы NTFS, но если вы выберете раздел, имеющий меньше места, чем нужно операционной системе (как видно на рис. 2.6, системе необходимо как минимум 6667 Мбайт свободного места), то кнопка Далее мастера будет неактивна.

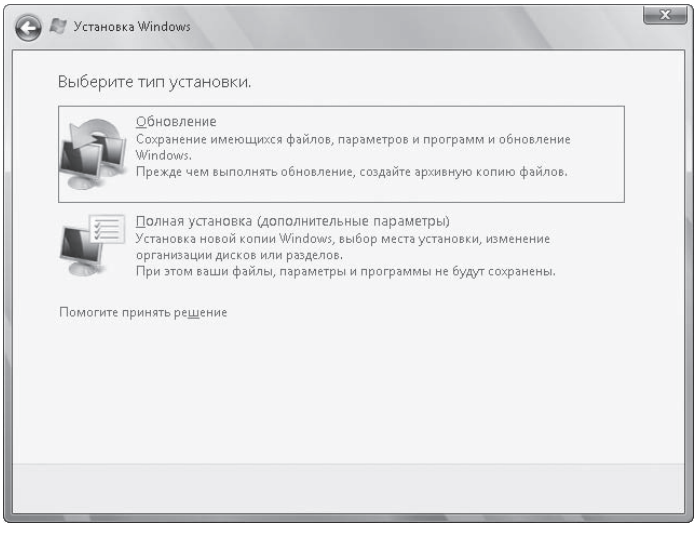


Рис. 2.5. Выбор типа установки

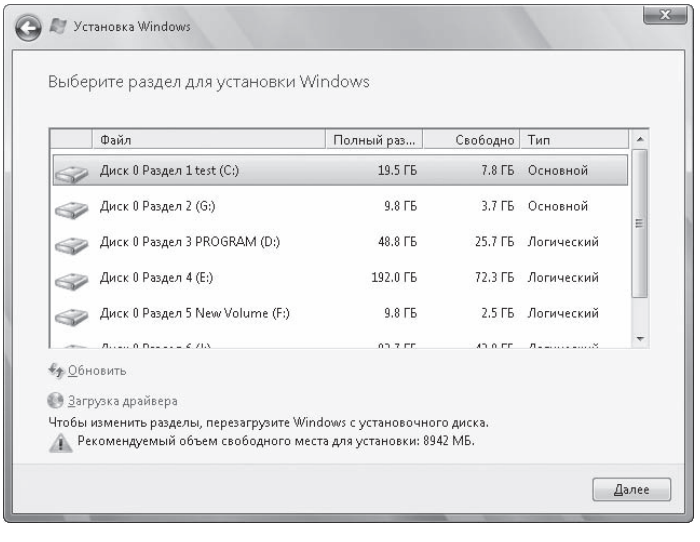


Рис. 2.6. Выбор раздела для установки операционной системы

Перед тем как выбрать раздел жесткого диска для установки операционной системы, повторим несколько известных нам сведений о процессе установки.

- Новый формат образов WIM производит неразрушающую установку. Иными словами, если вы устанавливаете новую операционную систему на раздел, содержащий другие данные, эти данные так и останутся после установки операционной системы.
- Если вы попытаетесь установить Windows Vista на раздел, содержащий другую операционную систему, то после установки Windows Vista другая система ра-

ботать не будет. Это происходит потому, что Windows Vista перемещает все найденные на установочном разделе системные файлы в специальную папку Windows.old.

- Повторим, что раздел, на который вы устанавливаете Windows Vista, должен иметь как минимум 10 Гбайт свободного места и быть отформатированным под файловую систему NTFS. Если такого раздела на вашем диске нет, но жесткий диск имеет неразмеченные области, то непосредственно в процессе установки операционной системы вы сможете создать новый раздел и отформатировать его под файловую систему NTFS.

Вы также можете обновить информацию о доступных разделах или выполнить установку драйверов RAID.

Для обновления информации достаточно щелкнуть кнопкой мыши на ссылке Обновить. Обновить информацию можно и с помощью клавиши F5.

Для установки драйвера RAID достаточно щелкнуть кнопкой мыши на ссылке Загрузка драйвера. Это же можно сделать, нажав клавишу F6. Теперь установить драйверы вы можете не только с дискеты (как в предыдущих операционных системах), но и с «флэшки» или компакт-диска (или DVD).

Первая фаза установки

Итак, раздел жесткого диска, на который будет устанавливаться операционная система, вы выбрали. После этого начнется первая фаза установки новой операционной системы — копирование файлов Windows Vista на жесткий диск компьютера (рис. 2.7). Если же вы выбрали обновление предыдущей операционной системы до Windows Vista, то первой фазой будет не копирование, а сбор сведений о программах, установленных в предыдущей версии операционной системы.

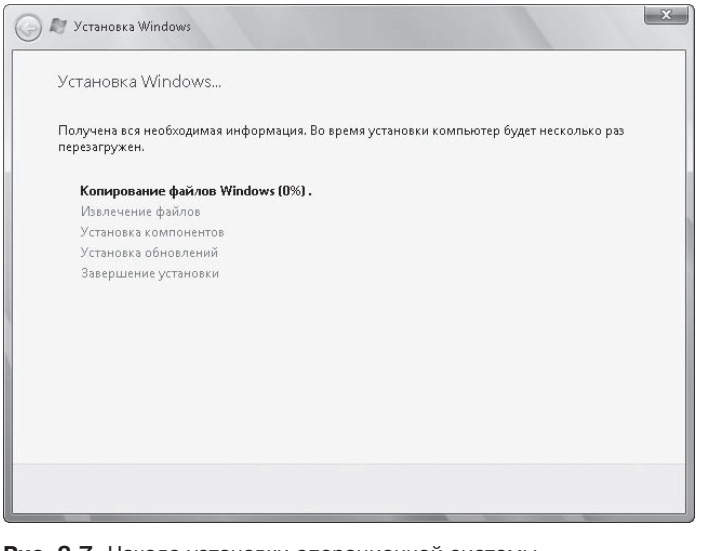


Рис. 2.7. Начало установки операционной системы

После того как этап копирования файлов на жесткий диск завершится, начнется этап извлечения данных из архивов. Если вы устанавливаете Windows Vista при загруженной другой операционной системе, то после истечения некоторого времени операционная система автоматически перезагрузит компьютер и процесс извлечения файлов продолжится.

Во время установки операционной системы на разделе диска происходит создание загрузочного сектора, содержимое которого будет участвовать в процессе загрузки операционной системы.

Продолжение установки после перезагрузки компьютера

На протяжении всего этапа установки операционной системы от вас не потребуется никаких действий, поэтому вы можете как минимум минут на 20 отойти от компьютера и заняться своими делами. Уже после того как операционная система будет полностью установлена, от вас потребуется ввести некоторые данные. Во-первых, необходимо будет указать регион, в котором вы проживаете, а также раскладку клавиатуры и страну, формат времени, денежных единиц и чисел которой будет использоваться в системе. Во-вторых, необходимо будет указать логин и пароль создаваемой учетной записи, с помощью которой вы будет входить в систему. Эта учетная запись будет иметь права администратора (по умолчанию учетная запись Администратор заблокирована). В-третьих, необходимо будет выбрать обои Рабочего стола, а также ввести имя компьютера, с помощью которого вы сможете подключиться к данному компьютеру по сети. В-четвертых, операционная система предложит вам настроить параметры безопасности компьютера и, напоследок, указать текущее время и используемый вами часовой пояс. После этого операционная система еще раз перезагрузит компьютер, и вы сможете войти в нее от имени только что созданного пользователя.

2.3. Дополнительные работы после установки

Но перед тем как начать описание интерфейса и возможностей новой операционной системы, рассмотрим несколько вопросов, которые могут быть вам интересны.

Настройка загрузочного меню

Вы, наверное, уже заметили, что операционная система Windows Vista обзавелась не только новым интерфейсом, но и новым загрузочным меню (рис. 2.8).

Если вы устанавливали Windows Vista на компьютер, уже имеющий несколько других установленных операционных систем, то не ужасайтесь — к ним по-прежнему можно будет получить доступ, если выбрать элемент Earlier version of Windows загрузочного меню. После выбора данного элемента будет выполнена обработка файла `boot.ini`, который как раз и содержал ранее загрузочное меню. Сама же операционная система Windows Vista больше не использует файл `boot.ini` и все сведения о загрузочном меню хранит в реестре. Единственным способом получения доступа к ним является программа командной строки `bcdedit.exe`. С ее помощью вы можете как редактировать текущие элементы загрузочного меню, так

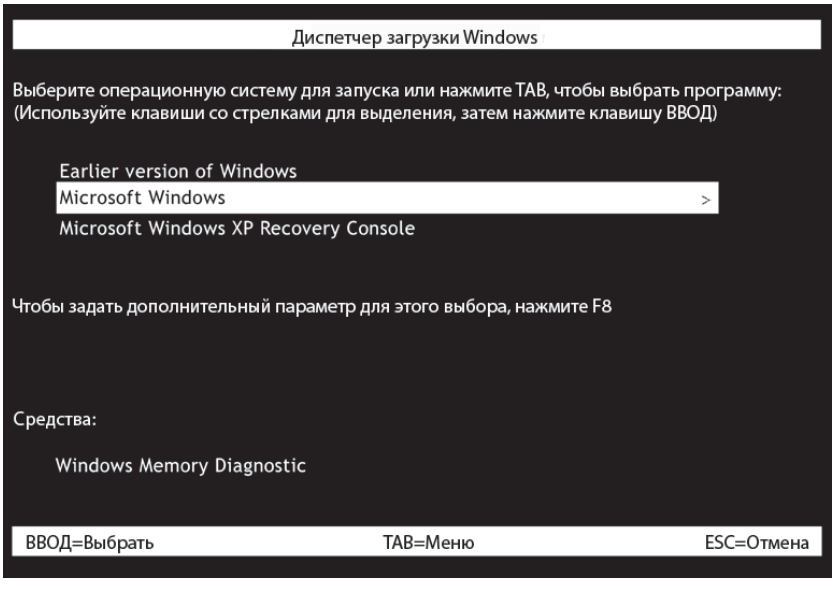


Рис. 2.8. Новое загрузочное меню Windows Vista

и создавать новые. Особенно это необходимо при установке на компьютер нескольких версий операционной системы Windows Vista — в этом случае в списке загрузочного меню все они будут иметь название Microsoft Windows, и будет довольно трудно понять, какая именно версия операционной системы скрывается за конкретным пунктом списка загрузочного меню.

Программа bcdedit.exe

В качестве примера рассмотрим некоторые команды `bcdedit.exe`, которые могут вам понадобиться. Например, если вы просто введете в командной строке `cmd.exe` строку `bcdedit`, то сможете просмотреть текущее содержимое загрузочного меню Windows (для примера выводимых данных посмотрите листинг 2.1). При этом следует заметить, что вы сможете воспользоваться программой `bcdedit`, только если зайдете в систему под учетной записью Администратор. В противном случае вы не сможете запустить программу `bcdedit`. Чтобы заново не входить в систему под учетной записью администратора, можно просто запустить командный интерпретатор `cmd.exe` от его имени. Для этого достаточно воспользоваться командой `runas /user:administrator cmd.exe`. Система попросит вас ввести пароль для учетной записи администратора, после чего отобразится окно `cmd.exe`, и вы сможете воспользоваться программой `bcdedit.exe`.

Листинг 2.1. Пример вывода содержимого загрузочного меню командой bcdedit

```
Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=D:
description             Windows Boot Manager
```

```
locale                  en-US
inherit                 {globalsettings}
default                 {default}
resumeobject            {50c73d4d-e6b3-11da-bc73-d30cdb1ce216}
displayorder            {ntldr}
                        {default}
                        {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Legacy OS Loader
------------------------
identifier              {ntldr}
device                  partition=D:
path                    \ntldr
description             Earlier version of Windows

Windows Boot Loader
-------------------
identifier              {default}
device                  partition=F:
path                    \Windows\system32\winload.exe
description             Microsoft Windows
locale                  en-US
inherit                 {bootloadersettings}
osdevice                partition=F:
systemroot              \Windows
resumeobject            {50c73d4d-e6b3-11da-bc73-d30cdb1ce216}
nx                      OptIn

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \Windows\system32\winload.exe
description             Windows (TM) Vista Ultimate (recovered)
osdevice                partition=C:
systemroot              \Windows
resumeobject            {5f951ca4-31a7-11db-8615-806e6f6e6963}
```

Как можно заметить из листинга 2.1, сначала `bcdedit` отображает сведения о настройке самого загрузочного меню (блок данных `Windows Boot Manager`), а потом сведения об элементах этого меню. Причем сведения об элементе списка, с помощью которого можно отобразить меню для выбора ранее установленных операционных систем (то есть для загрузки содержимого файла `boot.ini`), отображаются первыми (блок данных `Windows Legacy OS Loader`), а потом уже сведения об остальных элементах меню (блоки данных под заголовками `Windows Boot Loader`).

Отображаемые сведения о загрузочных разделах

Каждый из этих блоков данных может содержать следующие наиболее интересные сведения.

- `identifier` — определяет идентификатор элемента загрузочного меню и может принимать следующие значения:
  - `{current}` — говорит о том, что операционная система, определяемая этим элементом меню, загружена в данный момент;
  - `{default}` — означает, что операционная система, определяемая этим элементом меню, загружается по умолчанию;
  - `{ntldr}` — определяет элемент загрузочного меню, с помощью которого можно загрузить содержимое файла `boot.ini` (фактически определяет название файла `ntldr`, расположенного на системном диске, который раньше применялся в качестве загрузчика);
  - `{bootmgr}` — данный идентификатор говорит о том, что этот блок данных определяет параметры самого загрузочного меню (фактически определяет название файла `bootmgr`, расположенного на системном диске, который применяется в качестве загрузчика для операционной системы Windows Vista);
  - `{memdiag}` — определяет элемент загрузочного меню, с помощью которого можно выполнить диагностику состояния оперативной памяти компьютера;
  - `{CLSID-номер элемента меню}` — данный идентификатор присваивается элементу загрузочного меню, если ни один из предыдущих идентификаторов ему не подходит.

ПРИМЕЧАНИЕ

Это не полный список доступных значений поля identifier. Чтобы просмотреть полный список, воспользуйтесь командой bcdedit -? ID.

- `device` — определяет раздел диска (букву диска), который содержит загрузочные файлы операционной системы, запускаемой с помощью данного элемента меню.
- `path` — если `device` определял раздел диска, который содержит файлы операционной системы, то это поле определяет остальной путь к загрузчику операционной системы Windows Vista (в Windows Vista он называется `winload.exe`) или к старому загрузчику `ntldr`.
- `description` — определяет название элемента загрузочного меню.
- `osdevice` — определяет раздел диска (букву диска), который включает в себя системные файлы операционной системы. Как правило, в Windows Vista данное поле соответствует полю `device`.

- `systemroot` — определяет папку, содержащую системные файлы операционной системы.
- `locale` — определяет язык операционной системы.
- `displayorder` — определяет порядок расположения элементов загрузочного меню и присутствует только в блоке данных `Windows Boot Manager`. Обратите внимание, что порядок расположения определяется на основе поля `identifier`.
- `timeout` — определяет количество секунд, в течение которых система будет ждать от пользователя каких-либо действий (во время отображения загрузочного меню). После истечения данного промежутка времени будет загружена операционная система по умолчанию.
- `nx` — определяет используемый операционной системой вариант работы механизма DEP.

Основные команды программы bcdedit.exe

Теперь, когда вы научились разбираться в выводе команды `bcdedit` и определять текущие параметры загрузочного меню, рассмотрим другие ее команды.

Экспорт и импорт загрузочного меню. Самой первой командой, которой желательно воспользоваться, является команда `bcdedit /export <путь к файлу и его название без расширения>`. С ее помощью вы создаете копию загрузочного меню, которую потом сможете использовать для его восстановления, если нечаянно испортите текущее загрузочное меню. После выполнения экспортирования загрузочного меню в указанном вами каталоге будут созданы два файла — один с расширением LOG, а другой вообще без расширения. Файл без расширения как раз и хранит сведения о загрузочном меню. По сути, данный файл является просто разделом реестра и с помощью команды Файл ▸ Загрузить куст редактора реестра `regedit.exe` вы сможете загрузить его в реестр и просмотреть содержимое.

Для восстановления загрузочного меню из экспортированного файла достаточно воспользоваться командой `bcdedit /import <путь к файлу и его название без расширения>`.

Переименование элементов загрузочного меню. Итак, мы хотели переименовать какой-нибудь элемент загрузочного меню. Для этого нужно воспользоваться командой вида `bcdedit /set [содержимое поля identifier данного элемента меню] description <новое название элемента меню>`. Если вы не укажете содержимое поля `identifier`, то будет переименован элемент меню, имеющий значение `{current}` поля `identifier`. Например, `bcdedit /set description "Vista Build 5384"` или `bcdedit /set {default} description "Vista Build 5384 (TEST)"`.

Обратите внимание на то, что в предыдущей команде после содержимого поля `identifier` идет ключевое слово `description`. Если еще раз перечитать описание вывода команды `bcdedit`, то можно заметить, что такое же слово встреча-

ется среди полей блоков данных (см. листинг 2.1). Это не просто совпадение — именно название поля и нужно указывать в данной команде. Например, вы можете изменить значение поля `systemroot` с помощью команды `bcdedit /set [содержимое поля identifier данного элемента меню] systemroot <новый каталог, содержащий файлы Windows>`.

Изменение запускаемой по умолчанию операционной системы и таймаута. Еще одной возможностью, которая может вам пригодиться, является изменение операционной системы, запускаемой по умолчанию. Для этого нужно воспользоваться командой `bcdedit /default <содержимое поля identifier данного элемента меню>`. Например, команда `bcdedit /default {ntldr}` устанавливает по умолчанию загрузку файла `boot.ini` для выбора операционной системы более ранней версии, чем Windows Vista.

Можно также изменить время ожидания выбора операционной системы пользователем (содержимое поля `timeout` блока данных `Windows Boot Manager`). Для этого нужно воспользоваться командой `bcdedit /timeout <новое время ожидания в секундах>`.

Удаление и создание элемента загрузочного меню. Если же вы хотите удалить какой-либо элемент загрузочного меню, то это можно сделать с помощью команды `bcdedit /delete <содержимое поля identifier данного элемента меню>`. Например, чтобы удалить элемент Microsoft Windows из загрузочного меню (см. листинг 2.1), нужно воспользоваться командой `bcdedit /delete {default}`.

Естественно, что, кроме удаления элемента загрузочного меню, вы можете создать свой элемент меню. Проще всего для этого выполнить копирование уже существующего элемента меню. Чтобы это сделать, нужно воспользоваться командой `bcdedit /copy <содержимое поля identifier элемента меню, который вы будете копировать> /d <значение поля description нового элемента загрузочного меню>`.

Изменение порядка загрузочного меню. И последней командой, которую мы рассмотрим, будет команда изменения порядка отображения элементов загрузочного меню Windows Vista: `bcdedit /displayorder <дальнейшие параметры>`. Она имеет несколько разновидностей, поэтому рассмотрим каждую из них отдельно.

- `bcdedit /displayorder <содержимое поля identifier 1> <содержимое поля identifier 2> … <содержимое поля identifier N>` — с помощью данной команды вы полностью изменяете порядок отображения элементов загрузочного меню. Например, `bcdedit /displayorder {current} {default} {ntldr}`.
- `bcdedit /displayorder <содержимое поля identifier> /addfirst` — команда перемещает на первое место загрузочного меню элемент с указанным значением поля `identifier`. Например, `bcdedit /displayorder {ntldr} /addfirst`.

- `bcdedit /displayorder <содержимое поля identifier> /addlast` — перемещает на последнее место загрузочного меню элемент с указанным значением поля `identifier`.
- `bcdedit /displayorder <содержимое поля identifier> /remove` — команда удаляет из загрузочного меню элемент с указанным значением поля `identifier`.

Дополнительные параметры команды bcdedit.exe

В общем, вы поняли принцип работы с программой `bcdedit.exe`, а теперь вкратце опишу остальные команды этой программы, которые вам могут понадобиться.

- `/enum` — отображает настройки элемента меню, содержимое поля `identifier` которого указано в параметре команды. Фактически команда выводит сведения о конкретном блоке данных, также отображаемые при вводе команды `bcdedit` без параметров. Однако с помощью данной команды можно просмотреть сведения о любом идентификаторе, даже если он не отображается в загрузочном меню. Например, об идентификаторе `{memdiag}` или `{dbgsettings}`.
- `/create` — позволяет создать новый элемент загрузочного меню.
- `/toolsdisplayorder` — дает возможность изменять последовательность отображения элементов нижнего загрузочного меню (по умолчанию в нем используется только один элемент — Windows Memory Diagnostic). Параметры данной команды аналогичны параметрам команды `/displayorder`.

Более подробную информацию о командах можно просмотреть, воспользовавшись синтаксисом вида `bcdedit <команда> -?`.

ПРИМЕЧАНИЕ

На сайте компании Microsoft можно найти файл BCD.doc, содержащий описание работы с новым загрузочным меню (на английском языке). Если эта информация вам интересна, то попытайтесь воспользоваться ссылкой http://download.microsoft.com/download/a/f/7/af7777e5-7dcd-4800-8a0a-b18336565f5b/BCD.doc.

Классы репозитария CIM

Работать с новым загрузочным меню операционной системы Windows Vista можно и с помощью набора новых классов, хранящихся в пространстве имен `\\.\root\wmi`. Непосредственно к свойствам описанных ниже классов обратиться нельзя, однако можно выполнять методы данных классов — результаты некоторых из них возвращают экземпляры на другие классы, свойства которых разрешено модифицировать.

ПРИМЕЧАНИЕ

В книге предполагается, что вы уже имеете представление о WMI и репозитарии CIM. Если это не так, то в приложении 2 описаны некоторые примеры работы с пространствами имен, классами и их свойствами и методами.

Класс BcdStore

Данный класс представляет собой коллекцию объектов загрузочного меню. Он поддерживает одно свойство, доступное только для чтения, — `FilePath`, тип: `string`. Свойство является ключевым. Оно уникально идентифицирует путь к объекту.

Класс также поддерживает следующие методы.

- `CopyObject` — копирует объект.

  Входящие параметры.

  - Строковый параметр, определяющий файл загрузочного меню.
  - Строковый параметр, определяющий идентификатор загрузочного меню.
  - Флаг копирования. Имеет тип `uint32`. Если значение флага равно `1`, то будет создан новый идентификатор для копируемого объекта. Если значение флага равно `2`, то существующий объект будет удален. Если же значение данного флага равно `3`, то существующий объект будет удален, а создаваемому объекту будет присвоен новый идентификатор.

  Возвращаемый параметр: указатель на класс `BcdObject`.

- `CopyObjects` — копирует несколько объектов.

  Входящие параметры.

  - Первый — строковый — параметр, определяющий файл загрузочного меню.
  - Второй параметр определяет тип объекта. Он имеет тип `uint32`.
  - Флаги копирования. Имеет тип `uint32`. Если значение флага равно `1`, то будет создан новый идентификатор для копируемого объекта. Если значение флага равно `2`, то существующий объект будет удален. Если же значение данного флага равно `3`, то существующий объект будет удален, а создаваемому объекту будет присвоен новый идентификатор.

  Возвращаемый параметр: строковый.

- `CreateObject` — создает объект.

  Входящие параметры.

  - Строковый параметр, определяющий идентификатор объекта.
  - Второй параметр определяет тип объекта. Он имеет тип `uint32`.

  Возвращаемый параметр: указатель на класс `BcdObject`.

- `CreateStore` — создает новую коллекцию объектов (загрузочное меню).

  Входящий параметр: строковый параметр, определяющий путь к файлу.

  Возвращаемый параметр: указатель на класс `BcdStore`.

- `DeleteObject` — удаляет объект.

  Входящий параметр: строковый параметр, определяющий идентификатор объекта.

  Возвращаемые параметры: нет.

- `DeleteSystemStore` — удаляет основную коллекцию объектов загрузочного меню.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

- `EnumerateObjects` — возвращает пути ко всем объектам, находящимся в данном хранилище объектов загрузочного меню.

  Входящий параметр: определяет тип объекта. Он имеет тип `uint32`.

  Возвращаемый параметр: массив указателей на класс `BcdObject`.

- `ExportStore` — выполняет экспорт содержимого загрузочного меню в файл.

  Входящий параметр: путь к файлу, в который нужно экспортировать данное хранилище объектов загрузочного меню.

  Возвращаемые параметры: нет.

- `GetSystemDisk` — возвращает название системного раздела.

  Входящий параметр: строковый параметр, который содержит название системного раздела.

  Возвращаемые параметры: нет.

- `GetSystemPartition` — возвращает номер партиции, которая соответствует системному разделу.

  Входящие параметры: нет.

  Возвращаемый параметр: строковый параметр, содержащий номер партиции диска, которая соответствует системному разделу.

- `ImportStore` — импортирует загрузочное меню из файла.

  Входящий параметр: путь к файлу, из которого нужно импортировать хранилище объектов загрузочного меню.

  Возвращаемые параметры: нет.

- `OpenObject` — возвращает указатель на класс `BcdObject`, хранящий сведения о данном объекте.

  Входящий параметр: строковый параметр, определяющий идентификатор объекта.

  Возвращаемый параметр: указатель на класс `BcdObject`.

- `OpenStore` — открывает хранилище объектов загрузочного меню.

  Входящий параметр: строковый параметр, определяющий путь к файлу.

  Возвращаемый параметр: указатель на класс `BcdStore`.

Класс BcdObject

Данный класс включает в себя описание объекта из коллекции объектов загрузочного меню. Он поддерживает следующие свойства, доступные только для чтения.

- `Id`, тип: `string` — свойство является ключевым. Оно определяет CLSID-номер, уникально идентифицирующий объект.

- `StoreFilePath`, тип: `string` — является ключевым. Оно определяет путь к хранилищу, содержащему данный объект.
- `Type`, тип: `uint32` — определяет тип объекта.

Класс также поддерживает следующие методы.

- `DeleteElement` — удаляет элемент.

  Входящий параметр: данный параметр определяет тип объекта. Он имеет тип `uint32`.

  Возвращаемые параметры: нет.
- `EnumerateElements` — отображает список доступных элементов загрузочного меню.

  Входящие параметры: нет.

  Возвращаемый параметр: массив элементов, представленных указателями на класс `BcdElement`.
- `EnumerateElementTypes` — отображает список типов доступных элементов загрузочного меню.

  Входящие параметры: нет.

  Возвращаемый параметр: массив элементов, имеющих тип `uint32`.
- `GetElement` — возвращает элемент.

  Входящий параметр: данный параметр определяет тип объекта. Он имеет тип `uint32`.

  Возвращаемый параметр: указатель на объект `BcdElement`.
- `SetBooleanElement` — устанавливает элемент типа `Boolean`.

  Входящий параметр: данный параметр определяет тип объекта. Он имеет тип `uint32`.

  Возвращаемый параметр: `Boolean`. Имеет тип `Boolean`.
- `SetDeviceElement` — устанавливает элемент типа `Device`.

  Входящие параметры.

  - Данный параметр определяет тип объекта. Он имеет тип `uint32`.
  - Определяет тип устройства. Данный параметр имеет тип `uint32`. Если значение флага равно `1`, то это загрузочный раздел. Если значение флага равно `2`, то это партиция. Если же значение флага равно `3`, то это файл. Ну, а если значение данного параметра равно `5`, то данный элемент устройства неизвестен.

  Возвращаемый параметр: строковый параметр, определяющий дополнительные настройки.
- `SetFileDeviceElement` — устанавливает элемент типа `FileDevice`.

  Входящие параметры.

  - Данный параметр определяет тип объекта. Он имеет тип `uint32`.
  - Определяет тип устройства. Данный параметр имеет тип `uint32`. Если значение флага равно `1`, то это загрузочный раздел. Если значение флага

равно 2, то это партиция. Если же значение флага равно 3, то это файл. Ну, а если значение данного параметра равно 5, то данный элемент устройства неизвестен.

- Строковый параметр, определяющий дополнительные настройки.
- Строковый параметр, определяющий путь.
- Определяет тип родительского устройства. Имеет тип `uint32`.
- Строковый параметр, определяющий дополнительные настройки родительского устройства.
- Строковый параметр, определяющий родительский путь.

Возвращаемые параметры: нет.

- `SetIntegerElement` — устанавливает элемент типа `Integer`.

  Входящие параметры.

  - Данный параметр определяет тип объекта. Он имеет тип `uint32`.
  - Имеет тип `uint64` и определяет устанавливаемое значение.

  Возвращаемые параметры: нет.

- `SetObjectElement` — устанавливает элемент типа `Object`.

  Входящие параметры.

  - Данный параметр определяет тип объекта. Он имеет тип `uint32`.
  - Строковый параметр, определяющий идентификатор объекта.

  Возвращаемые параметры: нет.

- `SetObjectListElement` — устанавливает список элементов типа `Object`.

  Входящие параметры.

  - Данный параметр определяет тип объекта. Он имеет тип `uint32`.
  - Массив строковых параметров, определяющих идентификаторы объектов.

  Возвращаемые параметры: нет.

- `SetPartitionDeviceElement` — устанавливает элемент типа `PartitionDevice`.

  Входящие параметры.

  - Данный параметр определяет тип объекта. Он имеет тип `uint32`.
  - Определяет тип устройства. Данный параметр имеет тип `uint32`. Если значение флага равно 1, то это загрузочный раздел. Если значение флага равно 2, то это партиция. Если же значение флага равно 3, то это файл. Ну, а если значение данного параметра равно 5, то данный элемент устройства неизвестен.
  - Строковый параметр, определяющий дополнительные настройки.
  - Строковый параметр, определяющий путь.

  Возвращаемые параметры: нет.

- `SetStringElement` — устанавливает элемент типа `String`.

  Входящие параметры.

  - Данный параметр определяет тип объекта. Он имеет тип `uint32`.
  - Строковый параметр, определяющий устанавливаемую строку.

  Возвращаемые параметры: нет.

Класс BcdElement

Содержит описание элементов загрузочного меню. Он поддерживает следующие свойства, доступные только для чтения:

- `ObjectId`, тип: `string` — хранит идентификатор элемента;
- `StoreFilePath`, тип: `string` — содержит путь к хранилищу объектов (загрузочному меню), которому принадлежит данный элемент;
- `Type`, тип: `uint32` — определяет подтип элемента.

Класс BcdDeviceData

Этот класс содержит дополнительное описание элементов устройства. Он поддерживает следующие свойства, доступные только для чтения.

- `AdditionalOptions`, тип: `string` — содержит дополнительные параметры элемента.
- `DeviceType`, тип: `uint32` — идентифицирует тип элемента устройства. Например, если значение данного свойства равно `1`, то данный элемент является загрузочным. Если значение равно `2`, то элемент является партицией. Если же значение свойства равно `3`, то элемент является файлом. Ну, а если значение этого свойства равно `5`, то элемент устройства неизвестен.

Класс BcdDeviceElement

Содержит описание элементов устройства. Он поддерживает следующие свойства, доступные только для чтения:

- `Device`, тип: указатель на класс `BcdDeviceData` — определяет тип элемента устройства;
- `ObjectId`, тип: `string` — хранит идентификатор элемента устройства;
- `StoreFilePath`, тип: `string` — включает в себя путь к хранилищу объектов (загрузочному меню), которому принадлежит данный элемент устройства;
- `Type`, тип: `uint32` — определяет подтип элемента.

Класс BcdDeviceUnknownData

Класс включает в себя описание данных неизвестного элемента устройства. Эти данные представлены в двоичном виде.

- `AdditionalOptions`, тип: `string` — доступно как для чтения, так и для записи. Содержит дополнительные параметры элемента.
- `Data`, тип: массив значений `uint8` — определяет данные элемента.

- `DeviceType`, тип: `uint32` — доступно как для чтения, так и для записи. Свойство идентифицирует тип элемента устройства. Например, если значение данного свойства равно `1`, то элемент является загрузочным. Если значение равно `2`, то элемент является партицией. Если же значение данного свойства равно `3`, то элемент является файлом. Ну, а если значение равно `5`, то элемент устройства неизвестен.

Класс BcdDeviceFileData

Этот класс содержит описание данных элемента устройства — файла. Если не сказано об обратном, то свойства данного класса доступны только для чтения.

- `Parent`, тип: указатель на класс `BcdDeviceData` — содержит указатель на родительский элемент.
- `Path`, тип: `string` — хранит путь к устройству.
- `AdditionalOptions`, тип: `string` — доступно как для чтения, так и для записи. Содержит дополнительные параметры элемента.
- `DeviceType`, тип: `uint32` — доступно как для чтения, так и для записи. Свойство идентифицирует тип элемента устройства. Например, если значение данного свойства равно `1`, то элемент является загрузочным. Если значение равно `2`, то элемент является партицией. Если же значение свойства равно `3`, то элемент является файлом. Ну, а если значение данного свойства равно `5`, то элемент устройства неизвестен.

Класс BcdDevicePartitionData

Класс содержит описание данных элемента устройства — партиции. Если не сказано об обратном, то свойства данного класса доступны только для чтения.

- `Path`, тип: `string` — включает в себя путь к устройству.
- `AdditionalOptions`, тип: `string` — доступно как для чтения, так и для записи. Содержит дополнительные параметры элемента.
- `DeviceType`, тип: `uint32` — доступно как для чтения, так и для записи. Свойство идентифицирует тип элемента устройства. Например, если значение данного свойства равно `1`, то элемент является загрузочным. Если значение равно `2`, то элемент является партицией. Если же значение свойства равно `3`, то элемент является файлом. Ну, а если значение данного свойства равно `5`, то элемент устройства неизвестен.

Класс BcdStringElement

Содержит описание строкового элемента. Если не сказано об обратном, то свойства данного класса доступны как для чтения, так и для записи:

- `ObjectId`, тип: `string` — содержит идентификатор элемента;
- `StoreFilePath`, тип: `string` — включает в себя путь к хранилищу объектов (конкретному загрузочному меню), в которое входит данный элемент;
- `String`, тип: `string` — доступно только для чтения, содержит значение данного элемента;
- `Type`, тип: `uint32` — определяет подтип элемента.

Класс BcdObjectElement

Включает в себя описание элемента, указывающего на объект. Если не сказано об обратном, то свойства данного класса доступны как для чтения, так и для записи:

- `Id`, тип: `string` — свойство доступно только для чтения, оно определяет CLSID-номер, уникально идентифицирующий объект, на который указывает данный элемент;
- `ObjectId`, тип: `string` — хранит идентификатор элемента;
- `StoreFilePath`, тип: `string` — содержит путь к хранилищу объектов (конкретному загрузочному меню), в которое входит данный элемент;
- `Type`, тип: `uint32` — определяет подтип элемента.

Класс BcdObjectListElement

Класс содержит описание элемента, указывающего на массив объектов. Если не сказано об обратном, то свойства данного класса доступны как для чтения, так и для записи:

- `Ids`, тип: массив значений строкового типа — включает в себя массив CLSID-номеров, уникально идентифицирующих объекты, на которые указывает данный элемент;
- `ObjectId`, тип: `string` — хранит идентификатор элемента;
- `StoreFilePath`, тип: `string` — содержит путь к хранилищу объектов (конкретному загрузочному меню), в которое входит данный элемент;
- `Type`, тип: `uint32` — определяет подтип элемента.

Класс BcdIntegerElement

Этот класс содержит описание числового элемента. Если не сказано об обратном, то свойства данного класса доступны как для чтения, так и для записи.

- `ObjectId`, тип: `string` — хранит идентификатор элемента.
- `StoreFilePath`, тип: `string` — содержит путь к хранилищу объектов (конкретному загрузочному меню), в которое входит данный элемент.
- `Type`, тип: `uint32` — определяет подтип элемента.
- `Integer`, тип: `uint64` — включает в себя значение данного элемента. Несмотря на то что оно имеет тип `uint64`, его нужно передавать как строку.

Класс BcdBooleanElement

Хранит описание булевого элемента. Если не сказано об обратном, то свойства данного класса доступны как для чтения, так и для записи:

- `ObjectId`, тип: `string` — хранит идентификатор элемента;
- `StoreFilePath`, тип: `string` — содержит путь к хранилищу объектов (конкретному загрузочному меню), в которое входит данный элемент;
- `Type`, тип: `uint32` — определяет подтип элемента;
- `Boolean`, тип: `boolean` — содержит значение данного элемента.

Программа VistaBootPRO

Как вы, наверное, заметили из предыдущей главы, использование программы `bcdedit.exe` является довольно сложным занятием. Именно для облегчения этой процедуры сторонними разработчиками и была создана программа VistaBootPRO (рис. 2.9).

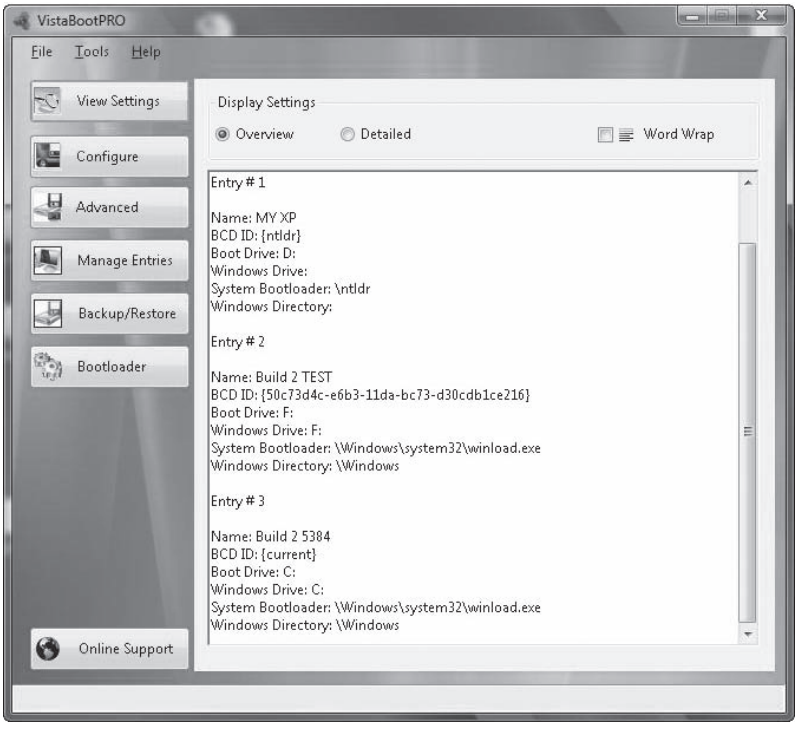


Рис. 2.9. Окно программы VistaBootPRO

Данная программа распространяется бесплатно и занимает 1,41 Мбайт. Ее можно скачать с официального сайта http://www.pro-networks.org/vistabootpro.

Как и рассмотренную ранее программу `bcdedit.exe`, VistaBootPRO нужно запускать только от имени администратора (фактически она является графическим интерфейсом для `bcdedit.exe`).

Окно программы состоит из панели кнопок, расположенной слева, и поля, отображающего информацию о текущих настройках загрузочного меню. При запуске программы это поле отображает ту же информацию, что и вызов команды `bcdedit.exe` без параметров. Рассмотрим основные возможности программы, предоставляемые после нажатия одной из кнопок левой панели.

После нажатия кнопки View Settings можно просмотреть текущие параметры настройки загрузочного меню. Фактически нажатие кнопки View Settings эквивалентно выводу команды `bcdedit.exe` без параметров.

С помощью кнопки Configure можно выполнить следующие действия:

- указать операционную систему, загружаемую по умолчанию, а также таймаут ожидания выбора операционной системы пользователем;
- переименовать один из элементов загрузочного меню, а также изменить букву диска, на котором расположена операционная система, запускаемая при выборе этого элемента меню.

После выбора кнопки Advanced вы сможете настроить дополнительные параметры загрузки определенной операционной системы: параметры режима отладки ядра, возможность запуска операционной системы с минимальной конфигурацией и т. д.

После нажатия кнопки Manage Entries вы сможете создать новый элемент загрузочного меню, удалить уже существующий элемент или упорядочить содержимое загрузочного меню.

С помощью кнопки Backup/Restore можно выполнить архивирование загрузочного меню или восстановление из уже созданного архива.

И, наконец, с помощью кнопки Bootloader можно заново создать загрузочное меню, используемое по умолчанию, или восстановить загрузочное меню, применяемое в ранних версиях операционной системы Windows (на основе файла `boot.ini`).

Программа msconfig.exe

В стандартную поставку Windows Vista входит программа `msconfig.exe`, с помощью которой также можно выполнить настройку некоторых параметров загрузки операционных систем. Для этого нужно запустить данную программу и перейти на вкладку Загрузка (рис. 2.10). Как можно заметить из рисунка, данная программа позволяет настраивать параметры запуска установленных на компьютере операционных систем Windows Vista, а также указывать таймаут ожидания выбора пользователем запускаемой операционной системы.

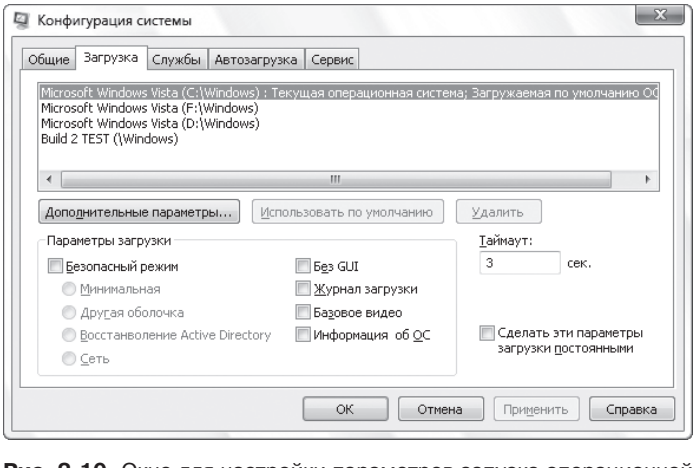


Рис. 2.10. Окно для настройки параметров запуска операционной системы с помощью программы msconfig.exe

С помощью программы `msconfig.exe` можно установить или снять следующие параметры запуска: `/NOGUIBOOT`, `/BOOTLOG`, `/BASEVIDEO`, `/SOS`, `/SAFEBOOT`, `/NUMPROC`, `/MAXMEM`, `/PCILOCK`, `/DETECTHAL`, `/DEBUG`, `/BAUDRATE`, `/CHANNEL`, `/DEBUGPORT`. Более подробно эти параметры описываются далее в подразд. «Файл boot.ini» этого раздела.

Окно Загрузка и восстановление

Некоторые параметры работы загрузочного меню можно изменить и с помощью окна Загрузка и восстановление. К ним относится запускаемая по умолчанию операционная система, таймаут ожидания выбора операционной системы пользователем, а также уникальный параметр — таймаут ожидания перед выбором способа загрузки операционной системы в меню Дополнительные варианты загрузки.

Для отображения окна Загрузка и восстановление сначала нужно вызвать окно Свойства системы. Для этого необходимо выполнить команду `SystemPropertiesAdvanced.exe`. Затем нужно перейти на вкладку Дополнительно окна Свойства системы и в области Загрузка и восстановление нажать кнопку Параметры.

Хранение содержимого загрузочного меню в реестре

Как уже упоминалось ранее, теперь загрузочное меню операционной системы хранится не в файле `boot.ini`, а в реестре. Для этого служит ветвь реестра `HKEY_LOCAL_MACHINE\BCD00000000`. Несмотря на то что способ хранения загрузочного меню в реестре выглядит довольно странно (например, как понять, в реестре какой операционной системы хранится загрузочное меню, ведь на момент его отображения ни одна из операционных систем загружена не была), он работает. Вы можете редактировать загрузочное меню непосредственно из реестра операционной системы, загружаемой по умолчанию.

ПРИМЕЧАНИЕ

Сведения о настройках загрузочного меню также хранятся в каталоге boot, расположенном на системном разделе диска. В этом каталоге хранится файл bcd, который является разделом реестра HKEY_LOCAL_MACHINE\BCD00000000.

Но перед тем как редактировать содержимое ветви `HKEY_LOCAL_MACHINE\BCD00000000`, нужно изменить права доступа к ней. Для этого в контекстном меню данной ветви реестра нужно выбрать команду Разрешения, в появившемся окне выделить свою учетную запись и разрешить ей полный доступ к ветви реестра. Более того, так нужно делать после каждой перезагрузки компьютера, так как после перезагрузки данной ветви присваиваются права доступа по умолчанию.

Вся информация об элементах загрузочного меню хранится в ветви реестра `HKEY_LOCAL_MACHINE\BCD00000000\objects`. Эта ветвь содержит набор подразделов, названных в честь CLSID-номеров поля `identifier` элементов загрузочного меню. При этом в данной ветви реестра содержится намного больше подразделов, чем элементов загрузочного меню — ветвь реестра `HKEY_LOCAL_MACHINE\`

BCD00000000\objects содержит не только настройки элементов загрузочного меню, но и описание различных связей и элементов этого меню, которые никогда в нем не отображаются, но влияют на его работу. Мы рассмотрим только содержимое подразделов, которые определяют отображаемые элементы загрузочного меню. Все они включают в себя дочерний раздел Elements, который, в свою очередь, содержит набор подразделов, определяющих значения полей данного элемента загрузочного меню (например, поля description, locale и т. д.). Например, в ветви реестра HKEY_LOCAL_MACHINE\BCD00000000\objects\{CLSID-номер элемента}\Elements можно встретить такие подразделы.

- 12000002 — хранит значение поля Path.
- 12000004 — содержит значение поля Description.
- 12000005 — хранит значение поля locale.
- 22000002 — содержит значение поля Systemroot.
- 23000003 — если вы переименовывали элемент загрузочного меню, то данный подраздел содержит CLSID-номер предыдущего элемента загрузочного меню (при переименовании элемента загрузочного меню фактически вы делаете копию этого элемента, которая отображается в загрузочном меню). В блоке данных Windows Boot Manager, как и в остальных элементах загрузочного меню, данный подраздел определяет значение поля resumeobject.
- 23000006 — в блоке данных Windows Boot Manager определяет значение поля default.
- 24000001 — хранит значение поля Displayorder блока данных Windows Boot Manager.
- 24000010 — содержит значение поля Toolsdisplayorder блока данных Windows Boot Manager.
- 25000004 — в блоке данных Windows Boot Manager определяет значение поля timeout.
- 12000016 — параметр строкового типа Element данного подраздела определяет название USB-порта, который будет использоваться при передаче отладочной информации на удаленный компьютер.
- 15000007 — параметр REG_BINARY-типа Element данного подраздела определяет количество оперативной памяти, установленной на компьютере, которое будет использоваться при работе в данной операционной системе. Иными словами, его значение эквивалентно значению параметра /MAXMEM.

ПРИМЕЧАНИЕ

Описание параметров запуска операционной системы приведено далее в этом разделе (подразд. «Файл boot.ini»).

- 15000011 — параметр REG_BINARY-типа Element данного подраздела определяет порт, по которому удаленному компьютеру будет передаваться отладочная

информация. Иными словами, его значение эквивалентно значению параметра /DEBUGPORT. Значение 1 определяет порт IEEE 1394. Значение 2 определяет USB-порт. Остальные значения параметра /DEBUGPORT определяются в подразделе 15000013.

- 15000013 — REG_BINARY-параметр Element данного подраздела определяет порт, по которому будет передаваться удаленному компьютеру отладочная информация. Другими словами, его значение эквивалентно значению параметра /DEBUGPORT. Значения от 1 до 4 определяют порты от COM1 до COM4. Остальные значения параметра /DEBUGPORT определяются в подразделе 15000011.
- 15000014 — параметр REG_BINARY-типа Element данного подраздела определяет скорость в бодах, которая будет использоваться при передаче отладочной информации на удаленный компьютер. Иными словами, его значение эквивалентно значению параметра /BAUDRATE.
- 15000015 — REG_BINARY-параметр Element данного подраздела определяет канал порта IEEE 1394, который будет использоваться при передаче отладочной информации на удаленный компьютер. Иначе говоря, его значение эквивалентно значению параметра /CHANNEL.
- 25000061 — параметр REG_BINARY-типа Element данного подраздела определяет количество процессоров, установленных в компьютере, которые будут использоваться при работе в данной операционной системе. Другими словами, его значение эквивалентно значению параметра /NUMPROC.
- 25000080 — параметр REG_BINARY-типа Element данного подраздела определяет значение параметра /BASEVIDEO. Возможны следующие значения:
  - 00 00 00 00 00 00 00 00 — эквивалентно значению MINIMAL параметра /BASEVIDEO;
  - 01 00 00 00 00 00 00 00 — эквивалентно значению NETWORK параметра /BASEVIDEO;
  - 02 00 00 00 00 00 00 00 — эквивалентно значению DSREPAIR параметра /BASEVIDEO.
- 26000081 — если значение параметра REG_BINARY-типа Element этого подраздела равно 01, то данная операционная система будет запускаться со значением MINIMAL(ALTERNATESHELL) параметра /BASEVIDEO. При этом значение параметра Element подраздела 25000080 должно быть равно 00 00 00 00 00 00 00 00.
- 26000010 — если значение REG_BINARY-параметра Element этого подраздела равно 01, то данная операционная система будет запускаться с установленным параметром /DETECTHAL.
- 26000040 — если значение параметра REG_BINARY-типа Element этого подраздела равно 01, то данная операционная система будет запускаться с установленным параметром /BASEVIDEO.
- 26000041 — если значение REG_BINARY-параметра Element этого подраздела равно 01, то операционная система будет запускаться с установленным параметром /NOGUIBOOT.

- 26000070 — если значение параметра REG_BINARY-типа Element указанного подраздела равно 01, то данная операционная система будет запускаться с установленным параметром /PCILOCK.
- 26000090 — если значение REG_BINARY-параметра Element этого подраздела равно 01, то операционная система будет запускаться с установленным параметром /BOOTLOG.
- 26000091 — если значение параметра REG_BINARY-типа Element указанного подраздела равно 01, то операционная система будет запускаться с установленным параметром /SOS.
- 260000a0 — если значение REG_BINARY-параметра Element этого подраздела равно 01, то данная операционная система будет запускаться с установленным параметром /DEBUG.

ПРИМЕЧАНИЕ

Это не все подразделы ветви реестра, определяющей параметры загрузочного меню, но остальные отображают сведения в шестнадцатеричном виде, из-за чего их очень трудно редактировать с помощью реестра.

ВНИМАНИЕ

Выполнение команды rundll32.exe sysdm.cpl, EnableExecuteProtectionSupportW приводит к установке значения параметра REG_BINARY-типа Element, расположенного в ветви реестра HKEY_LOCAL_MACHINE\BCD00000000\Objects\{50c73d4c-e6b3-11da-bc73-d30cdb1ce216}\Elements\25000020, равным 00 00 00 00.

В ветви реестра HKEY_LOCAL_MACHINE\BCD00000000 также содержится подраздел description. Он определяет глобальные настройки загрузочного меню и хранит два интересных параметра REG_DWORD-типа: System и TreatAsSystem. Значения обоих этих параметров по умолчанию равны 1. Если вы присвоите им значения 0, то программа bcdedit.exe больше не сможет редактировать настройки загрузочного меню, а ветвь реестра HKEY_LOCAL_MACHINE\BCD00000000 будет удалена. Тем не менее загрузочное меню будет и дальше отображаться и работать корректно.

Команда Windows Memory Diagnostic

В нижней части нового загрузочного меню Windows Vista появилась команда Windows Memory Diagnostic, с помощью которой вы сможете выполнить диагностику оперативной памяти компьютера (чтобы перейти на эту команду, нужно нажать клавишу Tab). Если в процессе выполнения диагностики система определила, что оперативная память содержит поврежденные ячейки данных, то она запретит доступ к этим ячейкам. Это единственный способ прекратить возникновение ошибок работы программ или экранов BSOD, если оперативная память повреждена. Конечно, после запрета доступа к памяти количество доступной в операционных системах Windows Vista оперативной памяти сократится, но зато работа операционной системы будет более стабильной.

Если после диагностики оперативной памяти доступ к определенным ячейкам был заблокирован, то вы сможете воспользоваться командой `bcdedit /enum {badmemory}`, чтобы просмотреть список заблокированных ячеек.

ПРИМЕЧАНИЕ

Сведения о результатах диагностики оперативной памяти заносятся в журнал Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ MemoryDiagnostics-Results.

Программу диагностики оперативной памяти вы также можете запустить непосредственно из операционной системы. Для этого нужно воспользоваться программой `MdSched.exe`, расположенной в каталоге `%systemroot%\system32`. После запуска данной программы перед вами отобразится окно Средство диагностики памяти Windows, которое позволяет выбрать одну из следующих возможностей.

- Выполнить перезагрузку и проверку — после выбора данной команды будут завершены все программы, открытые в данный момент, и компьютер перезагрузится. При этом вместо отображения загрузочного меню будет автоматически запущена программа проверки оперативной памяти.
- Выполнить проверку при следующем включении компьютера — если вы выберете данную команду, то при следующей перезагрузке компьютера вместо отображения загрузочного меню будет автоматически запущена программа проверки оперативной памяти.

Можно также воспользоваться параметром `/rn` программы `MdSched.exe`. В этом случае никаких окон выводиться не будет, операционная система автоматически завершит все программы, открытые в данный момент, и перезагрузит компьютер. При этом вместо отображения загрузочного меню будет автоматически запущена программа проверки оперативной памяти.

Дополнительные варианты загрузки

Как и в предыдущих версиях операционной системы Windows, в загрузочном меню Windows Vista можно нажать клавишу F8, чтобы перейти к меню дополнительных вариантов загрузки операционной системы. Теперь это меню содержит намного больше команд запуска операционной системы, среди которых можно встретить следующие.

- Безопасный режим — при загрузке операционной системы запускаются только основные драйверы и службы, без которых запуск Windows просто невозможен. Если вы подозреваете, что система не загружается из-за испорченного драйвера или ошибки службы, то можно попробовать загрузить ее в безопасном режиме.
- Безопасный режим с загрузкой сетевых драйверов — кроме стандартных драйверов и служб, при запуске операционной системы выполняется попытка запуска всех служб, реализующих доступ к сети.
- Безопасный режим с поддержкой командной строки — при загрузке операционной системы запускаются только основные драйверы и службы, без которых запуск

Windows просто невозможен. Кроме того, вместо графической оболочки запускается командная строка `cmd.exe`. Если ошибка возникает при загрузке графической оболочки операционной системы, то можно попробовать воспользоваться этим режимом.

- Ведение журнала загрузки — при запуске операционной системы создается файл `ntbtlog.txt` (в каталоге %systemroot%), содержащий сведения обо всех драйверах и службах, которые были запущены или, наоборот, запуск которых не произошел из-за ошибок.
- Включение видеорежима с низким разрешением (640 × 480) — операционная система запускается при разрешении монитора равном 640 × 480 пикселов. Если ошибка возникает при загрузке графической оболочки операционной системы, то можно попробовать воспользоваться этим режимом.
- Последняя удачная конфигурация (дополнительно) — операционная система запускается с использованием заведомо работоспособной ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00N`. При каждом успешном запуске операционной системы создается копия ветви `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00N`, ссылка на которую используется при выборе данного элемента меню, если загрузка с использованием текущей версии данной ветви реестра приводит к ошибке. Это может пригодиться, если вы только что установили какой-нибудь драйвер или службу, а после перезагрузки компьютера операционная система больше не запускается.
- Режим восстановления служб каталогов — при запуске операционной системы происходит восстановление службы каталогов контроллера домена Active Directory.
- Режим отладки — при запуске операционной системы активизируется отладчик ядра операционной системы. При возникновении ошибки BSOD сведения отладчика передаются на удаленный компьютер через подключенный нуль-модемный кабель или службу RAS (с помощью модема).
- Отключить автоматическую перезагрузку при отказе системы — выбор данного элемента меню приводит к стандартному запуску операционной системы, но при возникновении ошибки операционная система не перезагружается, а отображается «синий экран смерти» со сведениями о произошедшей ошибке.
- Отключение обязательной проверки подписи драйверов — выбор этого элемента меню приводит к запрещению проверки сигнатуры драйверов во время их запуска.
- Обычная загрузка Windows — выполняется стандартный запуск операционной системы.

Файл boot.ini

Несмотря на то что файл `boot.ini` больше не используется в Windows Vista, знание его формата может понадобиться, если на вашем компьютере установлены предыдущие версии операционной системы Windows. Файл `boot.ini` является обычным текстовым файлом, расположенным на системном диске. По умолчанию данному файлу присвоено разрешение только на чтение, поэтому перед редактированием ему нужно присвоить права на полный доступ. Следует также учитывать,

что данный файл является скрытым и системным, поэтому по умолчанию его не увидит даже администратор. Перед редактированием данного файла с помощью окна Свойства папки нужно разрешить отображение скрытых и суперскрытых файлов и папок.

В листинге 2.2 показан пример файла `boot.ini`.

Листинг 2.2. Формат файла boot.ini

```
[boot loader]
timeout=0
default=multi(0)disk(0)rdisk(0)partition(3)\WINDOWS

[operating systems]
multi(0)disk(0)rdisk(0)partition(3)\WINDOWS="Microsoft Windows XP Professional RU
Test" /NOEXECUTE=OPTIN /FASTDETECT
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional RU Recent"
/FASTDETECT /NOEXECUTE=OPTIN
c:\CMDCONS\BOOTSECT.DAT="Microsoft Windows XP Recovery Console" /CMDCONS
```

Раздел [boot loader]

Файл `boot.ini` состоит из двух разделов — `[boot loader]` и `[operating systems]`. Первый раздел должен содержать два параметра. Параметр `timeout` определяет интервал (в секундах) ожидания выбора загружаемой операционной системы пользователем. А параметр `default` определяет операционную систему, которая будет загружаться в том случае, если пользователь так и не выбрал операционной системы для загрузки (в виде пути ARC к ядру операционной системы).

Раздел [operating system]

Раздел `[operating system]` включает в себя список элементов загрузочного меню и определяет путь к системным файлам операционных систем, загружаемых с помощью этих элементов. Каждая строка данного раздела определяет один элемент загрузочного меню. Синтаксис строк данного раздела следующий: `ARC-имя\системная папка операционной системы="название элемента загрузочного меню" [параметры запуска операционной системы]`.

ПРИМЕЧАНИЕ

Как говорится, из каждого правила бывают исключения. Исключением из предыдущего правила является способ определения элемента загрузочного меню, с помощью которого запускается консоль восстановления (третья строка раздела [operating system] в листинге 2.2). В этом случае ARC-имя заменяется обычным путем к файлу.

ARC-именем называется часто применяемый способ идентификации раздела жесткого диска. Он применяется в том случае, когда нужно однозначно определить конкретный раздел диска на определенном жестком диске, подключенном к определенному контроллеру. ARC-имя состоит из номера контроллера жесткого дис-

ка, номера жесткого диска, подключенного к этому контроллеру, и номера раздела на этом жестком диске. В приведенном листинге 2.2 ARC-именем является строка `multi(0)disk(0)rdisk(0)partition(3)`.

ПРИМЕЧАНИЕ

ARC-имя раздела, из которого была запущена данная операционная система Windows Vista, содержится в параметре строкового типа SystemBootDevice ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control.

Первая часть ARC-имени. Первая часть строки (`multi(0)`) определяет тип и номер контроллера жесткого диска. Нумерация контроллеров начинается с нуля, а тип контроллера может принимать значения `multi` или `scsi`.

Значение `scsi` говорит о том, что жесткий диск, подключенный к контроллеру, является диском SCSI с отключенной BIOS. В этом случае на системном диске должен храниться файл `ntbootdd.sys`, который при загрузке будет выполнять функции BIOS данного жесткого диска.

В остальных случаях, если BIOS компьютера поддерживает прерывание INT 13, первая часть ARC-имени должна быть равна `multi(*)`.

Если же BIOS компьютера не поддерживает прерывание INT 13, а размер загрузочного тома больше 8 Гбайт, то используется значение `signature(*)`. В этом случае операционная система ищет раздел по сигнатуре, которая представляет собой GUID-номер раздела.

Вторая и третья части ARC-имени. Вторая и третья части строки (`disk(0)` и `rdisk(0)`) определяют номер жесткого диска, подключенного к данному контроллеру. Нумерация жестких дисков также начинается с нуля. Особенностью определения жесткого диска является то, что одна из частей строки ARC-имени всегда должна быть равна нулю. Если первая часть ARC-имени равна `multi(*)`, то вторая часть ARC-имени всегда должна быть равна `disk(0)`, а третья часть должна определять номер жесткого диска. Если первая часть ARC-имени равна `scsi(*)` или `signature(*)`, то третья часть ARC-имени всегда должна быть равна `rdisk(0)`, а вторая часть должна определять номер жесткого диска.

ПРИМЕЧАНИЕ

Если первая часть ARC-имени равна multi(*), то вместо rdisk(*) в третьей части может использоваться значение cdrom(*). В этом случае загрузчик будет пытаться загрузить операционную систему с диска, расположенного в приводе компакт-дисков.

Четвертая часть ARC-имени. Четвертая часть ARC-имени (`partition(3)`) определяет раздел жесткого диска, на котором хранятся системные файлы Windows. Обратите внимание, что нумерация разделов жесткого диска начинается с единицы, а не с нуля, как у предыдущих частей ARC-имени.

Параметры запуска операционной системы

Теперь рассмотрим назначения параметров запуска операционной системы, которые могут указываться в файле `boot.ini`. Большинство из этих параметров можно также использовать и при запуске операционной системы Windows Vista. В этом случае будет указана команда, с помощью которой можно установить соответствующий параметр запуска.

ПРИМЕЧАНИЕ

Все параметры запуска, с которыми была запущена операционная система Windows Vista, хранятся в параметре строкового типа SystemStartOptions ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control.

- `/3GB` — позволяет увеличить пользовательскую часть адресного пространства, выделяемого для одного процесса, с 2 до 3 Гбайт. Естественно, что увеличение данного пространства происходит не просто так — оно достигается путем уменьшения системного адресного пространства с 2 до 1 Гбайт. Повышение размера пользовательского адресного пространства позволяет ускорить работу приложений, которые интенсивно обращаются к виртуальной памяти (если эти приложения поддерживают увеличенное адресное пространство).

  Данный параметр влияет только на 32-разрядные системы. В 64-разрядных системах по умолчанию пользовательское и системное пространство равны по 8 Тбайт.

- `/BASEVIDEO` — при указании данного параметра операционная система будет загружаться с использованием стандартного графического драйвера `vga.sys`. Если вы подозреваете, что операционная система не может загрузиться именно из-за драйвера графической карты, то можно попробовать загрузить ее с помощью стандартного драйвера.

  В операционной системе Windows Vista значение данного параметра можно изменить с помощью команды `bcdedit.exe /set <элемент загрузочного меню> VGA <TRUE или FALSE>`.

- `/BAUDRATE=<количество бод>` — определяет скорость обмена данными, которая будет применяться во время отладки запуска операционной системы. Он должен использоваться только вместе с параметром `/DEBUG`. По умолчанию используется скорость 9600 бод для модемного соединения (с помощью службы RAS) и 19 200 бод для нуль-модемного кабеля.

  В операционной системе Windows Vista значение данного параметра можно изменить с помощью команды `bcdedit.exe /set <элемент загрузочного меню> BAUDRATE <скорость>`.

- `/BOOTLOG` — при использовании данного параметра во время загрузки операционной системы в каталоге %systemroot% будет создаваться файл `NTBTLOG.TXT`, хранящий сведения обо всех удачно загруженных драйверах, а также о драйверах, которые загрузить не удалось. При этом сначала все сведения о загрузке помещаются в ветвь реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\`

BootLog, и лишь потом, после загрузки Диспетчера сеансов (smss.exe) и проверки целостности файловой системы, создается файл NTBTLOG.TXT.

Параметр /BOOTLOG используется по умолчанию при безопасной загрузке операционной системы.

В Windows Vista значение данного параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> BOOTLOG <TRUE или FALSE>.

- /BOOTLOGO — при использовании данного параметра во время запуска операционной системы будет отображаться не стандартная заставка операционной системы Windows, а заставка, представленная файлом boot.bmp, расположенным в каталоге %systemroot%. Этот файл должен представлять собой растровое 16-цветное изображение размером 640 × 480 пикселов.
- /BREAK — в процессе инициализации операционной системы вызывает остановку HAL на точке прерывания. Это может быть необходимо при работе отладчика (с установленным параметром /DEBUG). При использовании параметра /BREAK без запуска отладчика будет появляться «синий экран смерти».

  В операционной системе Windows Vista значение данного параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> HALBREAKPOINT <TRUE или FALSE>.
- /BURNMEMORY=<количество мегабайт оперативной памяти> — определяет объем оперативной памяти, который операционная система не будет использовать в своей работе (будет считать его несуществующим).

  В Windows Vista значение данного параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> REMOVEMEMORY <объем неиспользуемой памяти>.
- /CHANNEL — определяет канал порта IEEE 1394, по которому будет передаваться отладочная информация, если значение параметра /DEBUGPORT равно 1394 и используется параметр /DEBUG.

  Параметр /CHANNEL может принимать значения от 0 до 62. По умолчанию используется канал 0.

  В операционной системе Windows Vista значение данного параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> CHANNEL <канал>.
- /CLKLVL — если используется многопроцессорная версия HAL для систем x86 (halmps.dll), то установка данного параметра говорит о том, что распознавание сигналов системного таймера будет выполняться не по фронту, а по потенциалу.
- /CRASHDEBUG — при использовании этого параметра во время загрузки операционной системы в память будет загружаться отладчик ядра, который перейдет в активное состояние только в случае возникновения ошибки запуска операционной системы. До возникновения ошибки отладчик ядра будет неактивен, а это значит, что он не будет постоянно использовать последовательный порт.

- /DEBUG — загружает отладчик, который активируется основным отладчиком при возникновении ошибки запуска операционной системы. В этом случае сведения об ошибке будут передаваться по COM-порту на удаленный компьютер для выполнения отладки операционной системы.

  В Windows Vista значение данного параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> BOOTDEBUG TRUE. Можно также воспользоваться командой bcdedit.exe /set <элемент загрузочного меню> DEBUG <TRUE или FALSE>.

- /DEBUGPORT=<COM-порт> — позволяет указать номер COM-порта, по которому будет передаваться отладочная информация на удаленный компьютер. По умолчанию используется порт COM1. Кроме COM-портов (с первого по четвертый), можно использовать значения USB и 1394 этого параметра.

  В операционной системе Windows Vista значение данного параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> DEBUGPORT <номер порта>. Можно также воспользоваться командой bcdedit.exe /set <элемент загрузочного меню> DEBUGTYPE <тип порта, например, SERIAL, 1394 или USB>, чтобы определить тип порта, по которому происходит процесс отладки.

- /DETECTHAL — разрешает при загрузке определять HAL и файл ядра операционной системы.

  В ОС Windows Vista значение данного параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> DETECTHAL <TRUE или FALSE>.

- /EXECUTE — после установки этого параметра защита DEP будет отключена.

- /FASTDETECT — при использовании данного параметра во время загрузки операционной системы не будет запускаться файл ntdetect.com для определения оборудования, установленного на компьютере и подключенного к последовательным и параллельным портам. Вместо этого оборудование будет определяться системой Plug and Play.

  Параметр используется при загрузке по умолчанию.

- /INTAFFINITY — применяется при использовании многопроцессорной версии HAL для x86-совместимых компьютеров (halmps.dll). По умолчанию прерывания может обрабатывать любой из процессоров многопроцессорной системы. Если же этот параметр будет установлен, то прерывания будет разрешено обрабатывать только одному процессору (с наибольшим порядковым номером).

- /KERNEL=<файл ядра операционной системы> — с его помощью можно изменить файл ядра операционной системы, используемый для ее загрузки. По умолчанию используется файл ntoskrnl.exe из каталога %systemroot%\system32.

  В операционной системе Windows Vista значение этого параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> KERNEL <имя файла>.

- /HAL=<файл HAL> — позволяет загрузить операционную систему на основе файла HAL, отличного от используемого по умолчанию.

  В Windows Vista значение этого параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> HAL <имя файла>.

  Файл HAL позволяет определить основные возможности, которые доступны операционной системе. Именно от него зависит, может ли операционная система поддерживать работу с несколькими процессорами, механизм энергосбережения ACPI и т. д.

  При обновлении операционной системы версия HAL, применяемая в предыдущей операционной системе, будет применяться и в новой системе.

  По умолчанию в 32-рязрядной операционной системе Windows Vista доступны следующие HAL:

  - Hal.dll — представляет собой HAL для стандартного компьютера, используется по умолчанию;
  - Halacpi.dll — HAL для компьютеров, поддерживающих ACPI (ACPI PIC HAL);
  - Halmacpi.dll — представляет собой HAL для многопроцессорных систем с поддержкой спецификации ACPI.

- /LASTKNOWNGOOD — загружает операционную систему в режиме запуска последней удачной конфигурации.

  В операционной системе Windows Vista значение данного параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> LASTKNOWNGOOD <TRUE или FALSE>.

- /MAXMEM=<количество мегабайт оперативной памяти> — определяет максимальное количество оперативной памяти, которое будет доступно операционной системе.

- /MAXPROCPERCLUSTER=<количество процессоров> — может применяться при использовании многопроцессорной версии HAL для x86-совместимых компьютеров. В этом случае она разрешает кластерный режим адресации контроллера прерываний APIC.

  В ОС Windows Vista значение этого параметра можно изменить с помощью следующей команды: bcdedit.exe /set <элемент загрузочного меню> CLUSTERMODEADDRESSING <количество процессоров>.

- /MININT — при установке этого параметра раздел реестра SYSTEM будет загружаться в систему как изменяемый. При этом все изменения в нем будут храниться в памяти, а не заноситься на жесткий диск (то есть после перезагрузки все изменения будут потеряны). Параметр используется операционной системой Windows PE.

  В операционной системе Windows Vista значение этого параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> WINPE <TRUE или FALSE>.

- /NODEBUG — при использовании данного параметра на экран компьютера не будет выводиться отладочная информация, а отладочные параметры (/DEBUG и т. д.) будут игнорироваться.
- /NOEXECUTE=<уровень работы DEP> — позволяет включить работу механизма DEP, а также настроить способ его работы. Существует четыре способа работы механизма DEP, которые включаются установкой определенного значения данного параметра:
  - OptIn — механизм DEP защищает только основные системные файлы;
  - OptOut — он включен для всех программ, запускаемых пользователем, при этом пользователь может указать программы-исключения;
  - AlwaysOn — механизм DEP включен для всех программ, запускаемых пользователем, при этом нельзя указать программы-исключения;
  - AlwaysOff — он всегда отключен, даже если аппаратно поддерживается процессором.

  В Windows Vista значение параметра /NOEXECUTE=<уровень работы DEP> можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> nx <значение параметра>. Например, bcdedit.exe /set {current} nx AlwaysOff.
- /NOGUIBOOT — во время запуска операционной системы вместо графической заставки будет отображаться информация о текущих действиях системы.

  В ОС Windows Vista значение данного параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> GRAPHICSMODEDISABLED <TRUE или FALSE>.

  Отключить загрузочную заставку можно и с помощью команды bcdedit.exe /set <элемент загрузочного меню> QUIETBOOT TRUE.
- /NOLOWMEM — может применяться только вместе с параметром /PAE и только на компьютерах, которые имеют более 4 Гбайт оперативной памяти. В этом случае все драйверы, приложения и пулы оперативной памяти будут загружаться в область памяти за пределами первых 4 Гбайт. Иными словами, этот параметр используется для проверки совместимости установленных в операционную систему драйверов с таким большим объемом оперативной памяти.

  В Windows Vista значение этого параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> NOLOWMEM <TRUE или FALSE>.
- /NOSERIALMICE=<COM-порт> — позволяет запретить поиск мыши на указанных COM-портах (COM-порты пишутся через запятую). Все дело в том, что некоторые устаревшие источники бесперебойного питания, подключаемые к COM-порту, могут посчитать переданный на порт сигнал как сигнал к отключению компьютера.
- /NOPAE — запрещает запуск версии ядра операционной системы, поддерживающего механизм PAE.

В операционной системе Windows Vista значение данного параметра можно изменить с помощью команды `bcdedit.exe /set <элемент загрузочного меню> pae ForceDisable`.

- `/NUMPROC=<количество процессоров>` — определяет количество процессоров, установленных на компьютере, которые будут использоваться в данной операционной системе.

  В Windows Vista значение этого параметра можно изменить с помощью команды `bcdedit.exe /set <элемент загрузочного меню> NUMPROC <количество процессоров>`.

- `/ONECPU` — может использоваться в многопроцессорных системах для того, чтобы заставить операционную систему работать только с одним процессором.

  В операционной системе Windows Vista значение этого параметра можно изменить с помощью команды `bcdedit.exe /set <элемент загрузочного меню> ONECPU <TRUE или FALSE>`.

- `/PAE` — при использовании данного параметра будет запускаться версия ядра операционной системы, использующего механизм PAE. Механизм PAE позволяет драйверам устройств использовать 64-разрядную адресацию, что повышает максимальный объем оперативной памяти, доступный в операционной системе (до 64 Гбайт для 32-разрядных систем и до 1024 Гбайт для 64-разрядных систем).

  Файл ядра, использующего механизм PAE, называется `ntkrnlpa.exe`.

  В ОС Windows Vista значение параметра `/PAE` можно изменить с помощью команды `bcdedit.exe /set <элемент загрузочного меню> pae <значение параметра, которое может быть равно Default, ForceEnable или ForceDisable>`.

- `/PCILOCK` — при использовании этого параметра операционной системе будет запрещено динамически назначать IRQ и другие ресурсы ввода-вывода доступным PCI-устройствам. В этом случае все данные о работе PCI будут браться из настроек BIOS.

- `/RDPATH=<путь к файлу SDI>` — с его помощью можно указать путь к образу среды предустановки, который будет использоваться для загрузки операционной системы. Указанный файл может храниться как на локальном, так и на удаленном компьютере.

  В операционной системе Windows Vista значение данного параметра можно изменить с помощью команды `bcdedit.exe /set <элемент загрузочного меню> RAMDISKSDIPATH <путь к файлу>`.

  Кроме `RAMDISKSDIPATH <путь к файлу>`, вы можете воспользоваться следующими параметрами команды:

  - `RAMDISKIMAGELENGTH <длина>` — определяет длину образа в файле SDI;
  - `RAMDISKIMAGEOFFSET <смещение>` — указывает смещение, по которому начинается образ нужной операционной системы в файле SDI;

  - RAMDISKSDIDEVICE <устройство> — определяет устройство, на котором находится файл SDI;
  - RAMDISKTFTPCLIENTPORT <номер порта> — указывает порт, по которому клиент TFTP будет взаимодействовать с компьютером, где хранится файл WIM.

- /SAFEBOOT:<режим> — с его помощью можно определить режим запуска операционной системы. Доступны следующие значения.
  - MINIMAL — обычный безопасный режим. При этом список драйверов, загружаемых в данном режиме, определяется дочерними разделами ветви HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal.
  - MINIMAL(ALTERNATESHELL) — безопасный режим с поддержкой командной строки. При этом файл оболочки, используемый в данном режиме (по умолчанию cmd.exe), определяется параметром строкового типа AlternateShell, расположенным в ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot.
  - NETWORK — безопасный режим с загрузкой сетевых драйверов. При этом список драйверов, загружаемых в данном режиме, определяется дочерними разделами ветви системного реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network.
  - DSREPAIR — безопасный режим для восстановления каталога Active Directory.

  В операционной системе Windows Vista значение параметра /SAFEBOOT:<режим> можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> SAFEBOOT <Minimal, Network или DsRepair>. Можно также воспользоваться командой bcdedit.exe /set <элемент загрузочного меню> SAFEBOOTALTERNATESHELL <TRUE или FALSE> для указания запуска в безопасном режиме с загрузкой командой строки.

- /SCSIORDINAL:<идентификатор> — позволяет явным образом указать идентификатор SCSI-контроллера для операционной системы.
- /SDIBOOT=<путь к файлу SDI> — используется в операционных системах класса Embedded и указывает путь к образу среды предустановки, с помощью которого запускается операционная система.
- /SOS — при его использовании во время запуска операционной системы на экран монитора будет выводиться информация обо всех драйверах, загружаемых в данный момент.

  В ОС Windows Vista значение этого параметра можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> SOS <TRUE или FALSE>.

- /USERVA=<от 2048 до 3072> — позволяет определить использование большего объема адресного пространства (до 3072 Мбайт). Назначение этого параметра сходно с назначением параметра /3GB.

В Windows Vista значение параметра /USERVA=<от 2048 до 3072> можно изменить с помощью команды bcdedit.exe /set <элемент загрузочного меню> INCREASEUSERVA <объем неиспользуемой памяти>.

- /YEAR=<год> — позволяет переопределить год, который будет использоваться операционной системой. Значение, определенное в данном параметре, подменяет год, определенный в BIOS.

Перенос настроек из другой операционной системы

Еще одной важной задачей, к которой вы, возможно, захотите перейти сразу же после установки новой операционной системы Windows Vista, является перенос настроек из предыдущей операционной системы в новую. Специально для этого установочный диск Windows Vista содержит в себе мастер для переноса настроек.

Использование установочного диска Windows Vista

Как уже упоминалось ранее, чтобы отобразить этот мастер, нужно запустить установочный диск Windows Vista в старой операционной системе и выбрать ссылку Перенос файлов и параметров настройки с другого компьютера, отображаемую в начальном окне мастера установки. После этого перед вами отобразится окно мастера Средство переноса данных Windows (рис. 2.11).

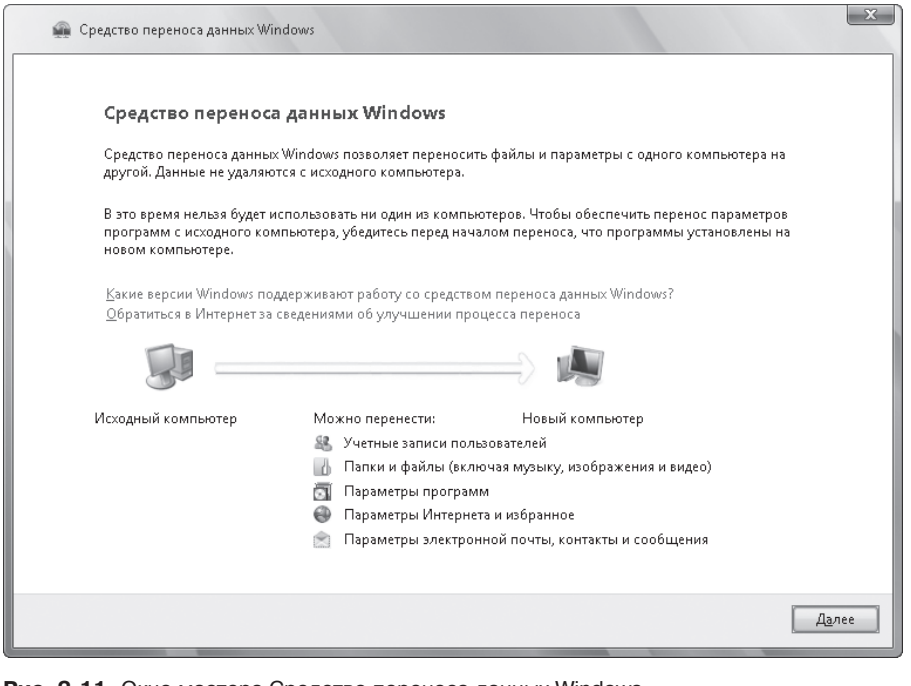


Рис. 2.11. Окно мастера Средство переноса данных Windows

Как сказано в окне мастера, с его помощью вы сможете перенести настройки учетных записей пользователей, подключения к Интернету, почтового клиента, программные

настройки, содержимое стандартных папок Windows (Мои рисунки, Моя музыка и т. д.), а также любые другие файлы или файлы с определенным расширением, которые вы потом выберете. После нажатия кнопки Далее мастер может попросить вас закрыть все запущенные в данный момент приложения, затем отобразит окно, в котором вы должны выбрать способ переноса данных в новую операционную систему (рис. 2.12). Можно выполнить перенос между компьютерами как по USB-кабелю, с помощью которого синхронизированы два компьютера, как с помощью компакт-диска, DVD, «флэшки» или внешнего диска, так и с помощью общего сетевого ресурса. Здесь, наверное, стоит пояснить: мастер считает, что вы переносите настройки между операционными системами, расположенными на двух разных компьютерах, а не на одном. Если это не так, то лучшим выбором можно назвать перенос настроек с помощью съемных устройств (третья кнопка окна мастера). После нажатия этой кнопки можно будет выбрать перенос с помощью съемного жесткого диска, после чего указать, чтобы мастер сохранил переносимые файлы настроек на локальном диске.

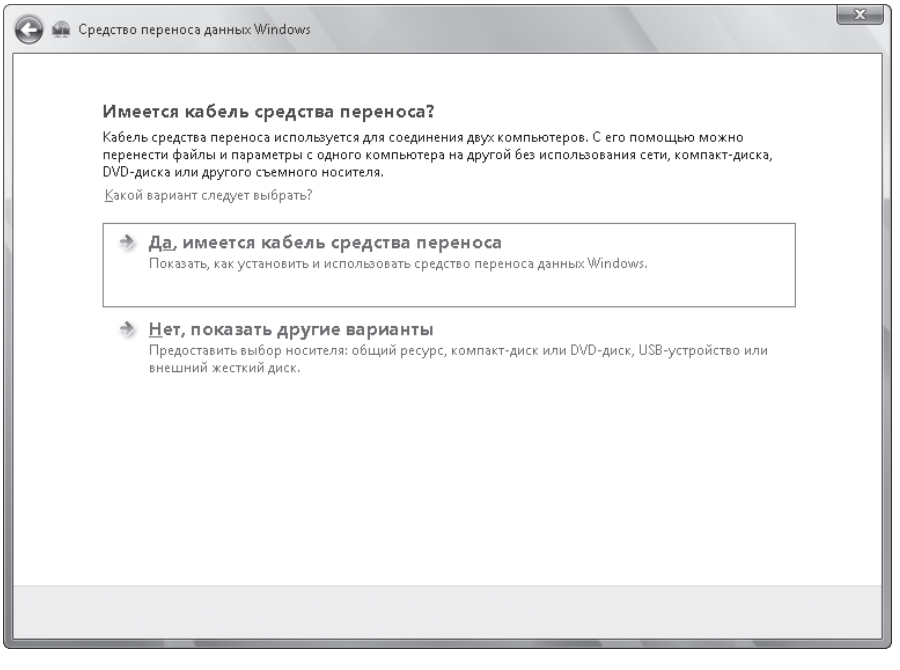


Рис. 2.12. Окно выбора способа переноса данных

Следующим шагом мастера будет вопрос о том, что именно вы будете переносить. Можно выбрать либо перенос настроек текущего пользователя, либо перенос настроек всех пользователей, либо выборочный перенос настроек. Конечно, лучше выбрать выборочный перенос, после чего мастер просмотрит содержимое вашего жесткого диска на наличие файлов, которые нужно перенести, а затем отобразит список тех файлов и параметров, которые можно перенести (рис. 2.13). Обратите внимание на три кнопки, расположенные под списком переносимых настроек. С помощью кнопок Добавить файлы и Добавить папки вы можете добавить

файлы и папки к списку переносимых данных. С помощью кнопки Выбрать диски можно определить диски, на которых мастер будет искать файлы настроек для переноса.

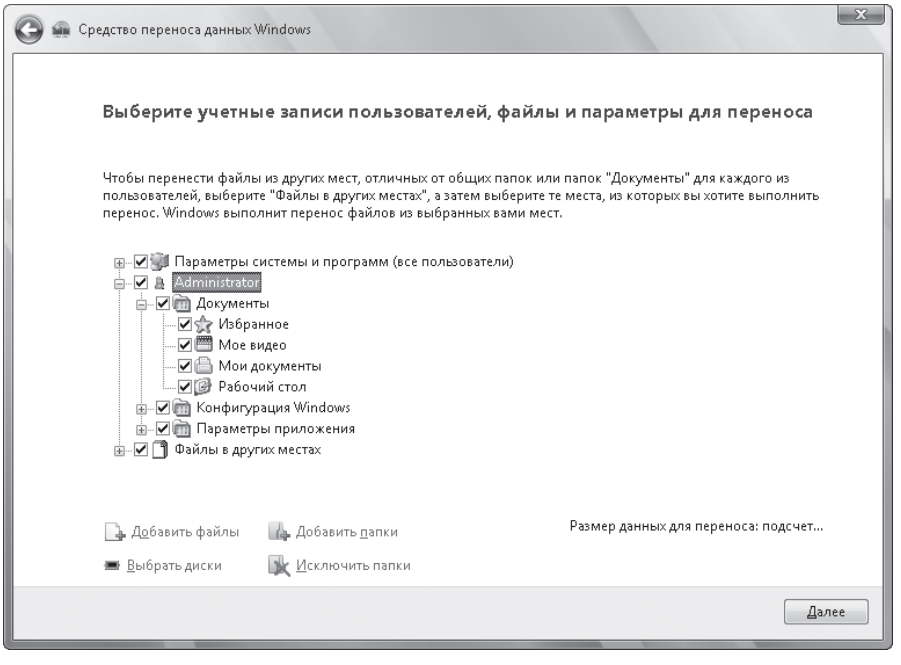


Рис. 2.13. Список переносимых параметров

После того как вы подготовите список переносимых данных, достаточно нажать кнопку Передача, чтобы начать их перенос. В процессе переноса на указанном носителе будет создан файл `SaveData.mig`.

Следующим шагом переноса будет загрузка новой операционной системы Windows Vista и повторный запуск мастера Средство переноса данных Windows с установочного диска операционной системы. На этот раз перед вами отобразится окно мастера, в котором можно выбрать, начать новый процесс переноса данных или продолжить старый (рис. 2.14). Чтобы окончательно перенести уже записанные настройки в новую операционную систему, нужно выбрать Продолжить выполнение переноса. После этого мастер спросит, где хранятся необходимые настройки: на компьютере в сети или на съемном устройстве. В данном случае, если вы сохранили настройки на локальном диске, нужно выбрать второй вариант, то есть на съемном устройстве.

После этого перед вами появится окно, в котором нужно выбрать созданный на прошлом шаге файл, и наконец-то начнется процесс переноса настроек.

Можно поступить и проще. Чтобы начать процесс переноса, достаточно дважды щелкнуть кнопкой мыши на файле, созданном мастером Средство переноса данных Windows.

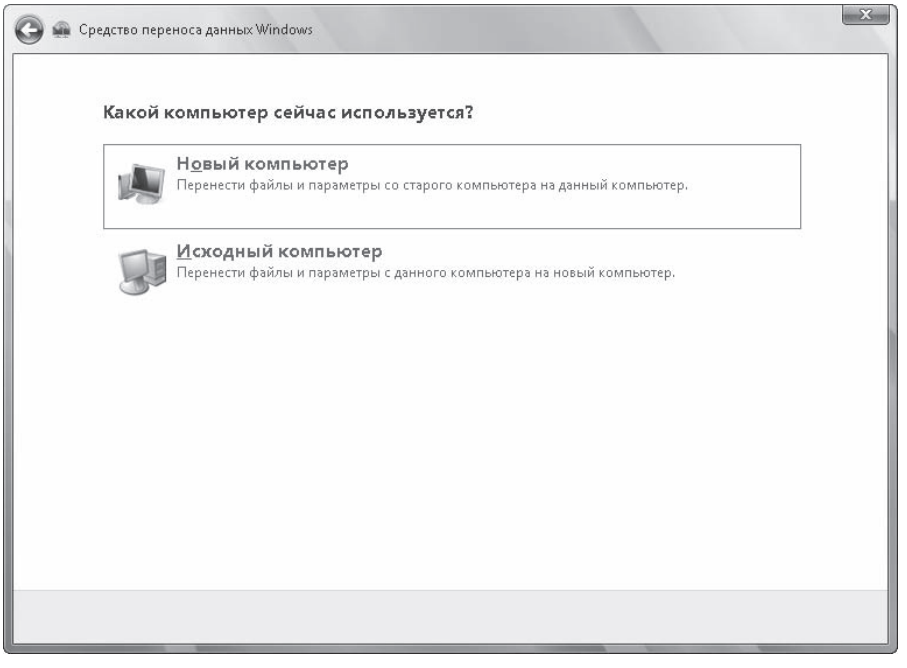


Рис. 2.14. Записываем перенесенные данные в новую операционную систему

Использование стандартной программы Windows Vista

Но что делать, если по каким-то причинам вы не имеете в данный момент установочного диска Windows Vista? На самом деле, это не проблема, ведь мастер Средство переноса данных Windows входит в стандартную поставку Windows Vista. Чтобы его запустить, нужно выбрать в меню Пуск ▸ Все программы операционной системы Windows Vista подпапку Стандартные ▸ Служебные, а в ней выбрать элемент Средство переноса данных Windows. Или просто запустить файл `migwiz.exe`, расположенный по адресу `%systemroot%\system32\migwiz`.

Также можно запустить программу `MigAutoPlay.exe`, расположенную в каталоге `%systemroot%\system32`. Если вы загрузите данную программу с параметром `/service`, то она запустится в режиме службы. Без указания параметров программа запускает мастер Средство переноса данных Windows.

После этого перед вами отобразится уже знакомый мастер, но в последующих своих окнах он предложит вам выбрать, на каком компьютере в данный момент запущен мастер Средство переноса данных Windows. Если вы выберете вариант Новый компьютер, то мастер задаст вам несколько новых вопросов. Их целью будет создание съемного диска, который бы содержал копию мастера Средство переноса данных Windows.

Когда вы создадите копию мастера на съемном диске, достаточно зайти в старую операционную систему и запустить мастер со съемного диска. Все остальные шаги аналогичны описанному выше созданию переносимых настроек с помощью установочного диска.

ПРИМЕЧАНИЕ

Мастер Средство переноса данных Windows после своей работы создает файл журнала, содержащий сведения о том, что именно он сделал. Этот файл называется setupact.txt и находится в каталоге %userprofile%\AppData\Local\MigWiz.

Активация Windows Vista

Если вы обладаете дистрибутивом Windows Vista одной из следующих редакций: Windows Vista Starter Edition, Windows Vista Home Basic Edition, Windows Vista Home Premium Edition или бета-версией операционной системы, то после того как установите операционную систему, ее еще нужно будет активировать.

Методы активации операционной системы

Если в процессе установки при вводе кода продукта вы не снимали флажок Автоматически активировать Windows при подключении к Интернету, то операционная система автоматически выполнит активацию при первом подключении к Интернету. Если же вы сняли флажок активации, то ее можно выполнить вручную. Для этого нужно вызвать окно Система и выбрать ссылку Осталось N дн. для выполнения активации. Активируйте Windows сейчас. Проще всего вызвать это окно с помощью комбинации клавиш Windows+Pause Break.

После выбора указанной ссылки будет запущена программа `slui.exe`, расположенная в каталоге `%systemroot%\system32`. Сначала она пытается выполнить активацию с помощью Интернета. Если у нее это не получается, например в данный момент нет подключения к Интернету, то можно будет выполнить активацию по телефону или модему. Настройки всех этих способов активации хранятся в файлах `migip.dun`, `phone.inf` и `reg.isp`, расположенных в каталоге `%systemroot%\system32\SLUI`.

Если вам нужно выполнить активацию сразу нескольких операционных систем на разных компьютерах, то для этого можно воспользоваться сценарием `slmgr.vbs`, расположенным в каталоге `%systemroot%\system32`.

ПРИМЕЧАНИЕ

С помощью данного файла можно также выполнить одно интересное действие — сбросить счетчик активации до начального количества дней (до 30 дней). Для этого достаточно ввести команду slmgr.vbs -rearm.

Можно также выполнить активацию на основе файла лицензии, для чего нужно воспользоваться командой `rundll32 slcc.dll, OpenPackage <путь к файлу с лицензией>`.

И последним способом активации является использование методов классов `SoftwareLicensingService` и `SoftwareLicensingProduct` пространства имен `\\root\cimv2` инструментария управления Windows.

Механизм активации

Активация операционной системы Windows Vista основана на новом механизме Software Protection Platform (SPP). Если пользователь не активирует операционную систему после определенного количества дней, то запуск оболочки операционной системы Windows Vista будет запрещен — вместо нее будет отображаться мастер активации операционной системы. Заметьте, что с помощью данного мастера можно запустить браузер Internet Explorer, а уже с его помощью — запустить как окно Проводника, так и любую другую программу. Другими словами, фактически работать с операционной системой можно, однако оболочку операционной системы запустить нельзя.

Параметры работы механизма Software Protection Platform можно настроить с помощью параметров REG_DWORD-типа, расположенных в подразделах ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL.

- SkipRearm — позволяет определить, разрешен ли сброс счетчика активации операционной системы.
- NotificationDisabled — по умолчанию операционная система периодически отображает уведомление о необходимости активации операционной системы. Если же данному параметру, расположенному в подразделе Activation ветви реестра, присвоить значение 1, то уведомление о необходимости активации отображаться не будет.
- ActivationInterval — данный параметр, расположенный в подразделе Activation ветви реестра, позволяет указать интервал отображения напоминания о необходимости активации.

Классы репозитария CIM

Как было сказано выше, репозитарий CIM операционной системы Windows Vista содержит несколько классов, с помощью которых можно управлять активацией операционной системы и других установленных программ. Все эти классы хранятся в пространстве имен \\.\root\cimv2.

Класс SoftwareLicensingService

Этот класс содержит сведения о службе Лицензирование программного обеспечения, установленной в операционной системе. Он поддерживает следующие свойства, доступные только для чтения.

- ClientMachineID, тип: string — содержит уникальный идентификатор клиента данного компьютера. Этот идентификатор помещается во все запросы к серверу на обслуживание (KMS).
- IsKeyManagementServiceMachine, тип: uint32 — определяет, включена ли служба обслуживания на данном компьютере. Если свойство имеет значение 0, то служба отключена. Если же свойство имеет значение 1, то служба запущена.
- KeyManagementServiceCurrentCount, тип: uint32 — указывает количество активных в данный момент клиентов службы обслуживания запросов на активацию. Если значение свойства равно 0xFFFFFFFF, то служба обслуживания отключена.

- KeyManagementServiceMachine, тип: string — определяет название службы обслуживания запросов на активацию, если она установлена и имеет название.
- KeyManagementServiceProductKeyID, тип: string — указывает уникальный идентификатор службы обслуживания запросов на активацию, если она установлена.
- PolicyCacheRefreshRequired, тип: uint32 — представляет собой флаг, указывающий состояние кэша политики лицензирования. Если значение данного свойства равно 0, то обновление кэша не требуется. Если же значение равно 1, то необходимо обновление кэша.
- RequiredClientCount, тип: uint32 — определяет максимальное количество поддерживаемых службой обслуживания запросов на активацию соединений с клиентами.
- Version, тип: string — является ключевым и определяет версию службы Software Licensing.
- VLActivationInterval, тип: uint32 — указывает частоту соединения (в минутах) клиента со службой обслуживания запросов на активацию для выполнения лицензирования.
- VLRenewalInterval, тип: uint32 — определяет то, как часто (в минутах) данный компьютер будет связываться со службой обслуживания запросов на активацию для возобновления лицензии.

Данный класс также поддерживает множество методов, позволяющих работать со службами активации.

- ClearKeyManagementServiceMachine — удаляет имя службы управления запросами активации.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.
- ClearProductKeyFromRegistry — удаляет сведения о ключе продукта из реестра.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.
- InstallLicense — устанавливает лицензию для текущего продукта.

  Входящий параметр: строковый параметр, определяющий лицензию.

  Возвращаемые параметры: нет.
- InstallLicensePackage — устанавливает пакет с лицензией для текущего продукта.

  Входящий параметр: строковый параметр, определяющий пакет лицензии.

  Возвращаемые параметры: нет.
- InstallProductKey — устанавливает ключ продукта.

  Входящий параметр: строковый параметр, определяющий ключ продукта.

  Возвращаемые параметры: нет.

- `SetKeyManagementServiceMachine` — устанавливает новое имя для службы управления запросами активации.

  Входящий параметр: строковый параметр, определяющий новое имя службы.

  Возвращаемые параметры: нет.

- `SetVLActivationInterval` — устанавливает новую частоту соединения компьютера со службой управления запросами активации для лицензирования.

  Входящий параметр: указывает новую частоту соединения в минутах. Значение этого параметра может находиться в интервале от `15` до `43 200`. Имеет тип `uint32`.

  Возвращаемые параметры: нет.

- `SetVLRenewalInterval` — устанавливает новую частоту соединения компьютера со службой управления запросами активации для возобновления лицензии.

  Входящий параметр: указывает новую частоту соединения в минутах. Значение этого параметра может находиться в интервале от `15` до `43 200`. Имеет тип `uint32`.

  Возвращаемые параметры: нет.

Класс SoftwareLicensingProduct

Экземпляры данного класса содержат сведения о лицензируемых продуктах. Он поддерживает следующие свойства, доступные только для чтения.

- `ApplicationID`, тип: `string` — хранит идентификатор продукта.
- `Description`, тип: `string` — содержит описание продукта.
- `EvaluationEndDate`, тип: `datetime` — определяет срок действия ключа продукта.
- `GracePeriodRemaining`, тип: `uint32` — указывает оставшееся время, после которого необходимо обновить лицензию продукта.
- `ID`, тип: `string` — является ключевым, содержит идентификатор продукта.
- `LicenseStatus`, тип: `uint32` — определяет статус лицензирования данного продукта. Возможны следующие значения: `0` — продукт нелицензирован, `1` — продукт лицензирован, `2` — состояние продукта: `OOBGrace`, `3` — состояние продукта: `OOTGrace`.
- `MachineURL`, тип: `string` — хранит URL-адрес службы лицензирования, которая предоставляет лицензии данному продукту. Например, для операционной системы Windows Vista это свойство равно `go.microsoft.com/fwlink/?LinkId=N`.
- `Name`, тип: `string` — определяет имя продукта.
- `OfflineInstallationId`, тип: `string` — указывает идентификатор автономного инсталляционного ключа продукта. Если значение данного свойства равно `NULL`, то ключ продукта не установлен.

- PartialProductKey, тип: string — определяет последние ключи продукта. Если значение равно NULL, то ключ продукта не установлен.
- ProcessorURL, тип: string — содержит URL-адрес службы лицензирования, которая предоставляет лицензии данному продукту.
- ProductKeyID, тип: string — определяет идентификатор ключа продукта.
- ProductKeyURL, тип: string — хранит URL-адрес службы лицензирования.
- UseLicenseURL, тип: string — содержит URL-адрес службы лицензирования, используемой для лицензирования.

Этот класс также поддерживает несколько методов, позволяющих работать с активацией продукта.

- Activate — выполняет активацию продукта.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.
- DepositOfflineConfirmationId — выполняет активацию продукта с помощью телефонного звонка на основе автономного идентификатора подтверждения.

  Входящие параметры:

  - параметр строкового типа, определяющий идентификатор активации;
  - параметр строкового типа, определяющий идентификатор подтверждения.

  Возвращаемые параметры: нет.
- UninstallProductKey — удаляет ключ продукта.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

Автоматизация установки с помощью файла ответа

Как и в предыдущих версиях этой операционной системы, Windows Vista поддерживает файл ответов, содержимое которого будет использоваться при установке операционной системы. Однако теперь файл ответов имеет расширение XML (как и раньше, он называется unattend) и создается в этом формате. Кроме того, теперь в файле ответов unattend.xml хранится не только информация, используемая при обычной установке операционной системы, но и информация, используемая программой sysprep.exe (раньше данная информация хранилась в отдельном файле sysprep.inf).

Файл ответов содержит следующие полезные теги (как правило, в открывающем теге также отображает параметр ShowUI="yes|no", который определяет, будет ли в процессе установки перед пользователем отображаться соответствующее окно для изменения значения, указанного в теге).

- AcceptEula — если значение между открывающим и закрывающим тегом равно Yes, то вы автоматически принимаете с лицензионное соглашение.

- `FullName` — содержит имя пользователя, работающего с операционной системой.
- `Organization` — определяет организацию, в которой устанавливается операционная система.
- `ComputerName` — указывает имя компьютера.
- `ProductKey` — определяет ключ продукта.
- `DiskConfig` — содержит вложенные теги для выбора раздела диска, в который будет автоматически устанавливаться операционная система.
- `JoinDomain` — тег не закрывается. Его параметры определяют имя домена, пользователя и пароль, если ваш компьютер должен входить в домен.
- `Accounts` — может содержать множество вложенных тегов `Account` (не закрываются), параметры которых определяют имя создаваемых учетных записей и пароли.
- `AutoLogon` — может хранить вложенный тег `Logon` (не закрывается). Его параметры определяют учетную запись, под именем которой будет выполняться автоматический вход в систему.
- `Hardware` — может содержать вложенный тег `DisplayAdapter` (не закрывается), параметры которого определяют используемое по умолчанию разрешение экрана, глубину цвета и частоту развертки.
- `RunOnce` — может включать в себя множество вложенных тегов `Executable` (не закрываются), параметры которых определяют команды, которые будут выполнены при первом входе пользователей в систему.

Кроме файла `unattend.xml`, при установке операционной системы Windows Vista также можно применять файл `oobe.xml`. Он позволяет настроить окно приветствия Windows, добавить к нему свой логотип, указать дополнительные языковые параметры или дополнительный текст.

Глава 3

Интерфейс Windows Vista

- **Краткий обзор интерфейса**
- **Настройка оболочки Windows**

3.1. Краткий обзор интерфейса

Опытный пользователь, не первый год работающий с операционной системой Windows XP, при переходе на новую операционную систему Windows Vista может немного растеряться. Действительно, несмотря на то что ничего революционного и кардинально нового в интерфейсе Windows Vista нет, большинство стандартных элементов оболочки операционной системы были переделаны так, что в первое время чувствуется легкий дискомфорт при работе с операционной системой. Например, был модернизирован такой, казалось бы, вечный элемент операционной системы, как Проводник. Или новое меню Пуск, не похожее на своих предшественников.

Чтобы вы более комфортно чувствовали себя при работе с новой операционной системой, вкратце опишу ее обновленный интерфейс, после чего перейду непосредственно к возможностям настройки оболочки Windows Vista.

Окно входа в систему

Особенностью Windows Vista является то, что больше не существует возможности изменить режим отображения окна входа в систему. В Windows XP присутствовало два режима: экран приветствия и стандартный режим Windows 2000. В Windows Vista остался только экран приветствия, который включен по умолчанию (рис. 3.1). Хотя, если ваш компьютер будет подключен к домену, установится стандартный режим входа в систему.

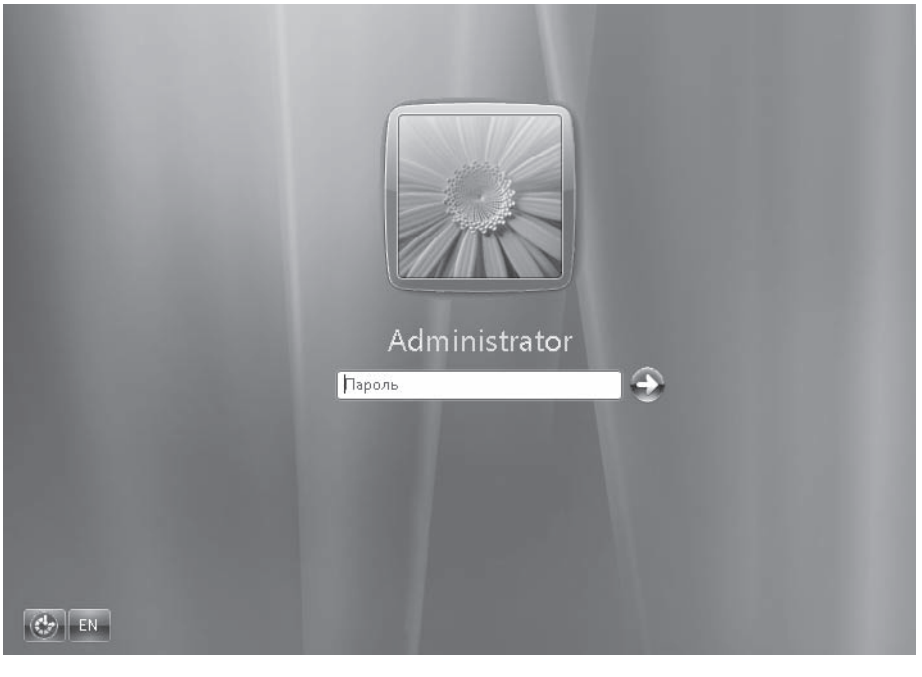


Рис. 3.1. Экран приветствия Windows Vista

Кнопка специальных возможностей

Особенностью нового экрана приветствия Windows Vista является не только изменившийся рисунок, а отображаемая в нижнем левом углу кнопка. Она позволяет настроить специальные возможности оболочки Windows, предназначенные для людей с ослабленным зрением или ограниченными физическими возможностями. После нажатия данной кнопки отобразится окно Специальные возможности (рис. 3.2), с помощью которого можно выполнить следующие операции:

- задействовать модуль чтения команд (Narrator);
- запустить программу, увеличивающую часть экрана (Magnifier);
- отобразить на экране монитора клавиатуру (On-Screen Keyboard);
- установить залипание клавиш;
- увеличить контрастность выводимого изображения;
- отключить функцию повторения зажатой клавиши клавиатуры.

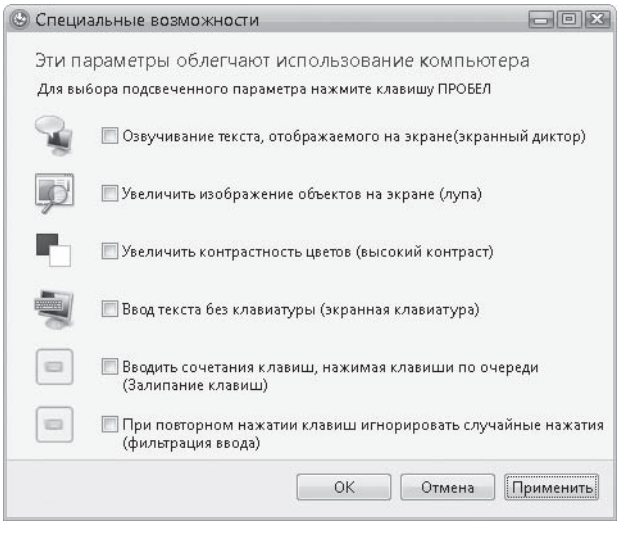


Рис. 3.2. Окно Специальные возможности

Изменение раскладки клавиатуры

Обратите также внимание на название раскладки клавиатуры, отображаемое в нижней части окна входа в систему. Пусть его вид не введет вас в заблуждение. Это не просто название текущей раскладки — если вы щелкнете кнопкой мыши на данной надписи, то перед вами отобразится список языков, с помощью которого можно сменить текущую раскладку клавиатуры.

Ссылка Сменить пароль

Если вы неправильно введете пароль для учетной записи, то под полем ввода отобразится ссылка Сменить пароль, с помощью которой можно вызвать мастер сброса пароля.

Этот мастер работает на основе данных, которые вы ранее записали на дискету. Чтобы вызвать мастер записи данных для сброса пароля, нужно воспользоваться мастером Учетные записи пользователей, который отображается после щелчка кнопкой мыши либо на одноименном значке папки Панель управления, либо на вашем изображении в меню Пуск. После отображения мастера Учетные записи пользователей выберите в нем ссылку Создание дискеты восстановления пароля, что приведет к открытию окна Мастер забытых паролей. Его работа состоит всего из двух шагов: сначала он просит вас вставить чистую дискету в дисковод, а потом — ввести пароль для текущей учетной записи.

ПРИМЕЧАНИЕ

Вызывать мастер сброса паролей можно с помощью команды rundll32.exe KEYMGR.dll, PRShowRestoreWizardExW.

Вызвать мастер забытых паролей также можно с помощью команды rundll32.exe KEYMGR.dll, PRShowSaveFromMsginaW.

Меню Пуск

Еще одним изменившимся элементом оболочки, который следует описать перед тем как более подробно заняться настройкой операционной системы, является меню Пуск (рис. 3.3). Благодаря интерфейсу Aero оно стало прозрачным, а благодаря новому механизму поиска теперь из этого меню можно искать программы (рис. 3.4), расположенные в меню Пуск ▸ Все программы, в пользовательских папках, в списках MRU и т. д.

Кстати, теперь меню Пуск ▸ Все программы отображается непосредственно как часть самого меню Пуск, а не как раскрывающийся список.

Стоит признать, что по сравнению с меню Пуск операционной системы Windows XP новое меню стало намного удобнее. Теперь непосредственно из него можно выключить или заблокировать компьютер (кнопки со значками выключения и замка в нижней части меню напротив строки поиска). Из меню Пуск вы также можете выполнить дополнительные операции выключения: переключиться на другого пользователя (Windows Vista при использовании экрана приветствия так же, как и Windows XP, поддерживает возможность быстрого переключения пользователей без завершения работы программ), завершить сеанс данного пользователя, перезагрузить компьютер, перейти в режим сна или спящий режим. Все эти возможности скрываются за стрелкой вправо, отображенной напротив кнопки блокирования компьютера.

Обратите внимание, что теперь все стандартные папки Windows лишились приставки Мой (например, вместо Мой компьютер просто Компьютер), а в меню Пуск появилась папка перехода в каталог пользователя (в каталог %userprofile%). Она названа по имени пользователя.

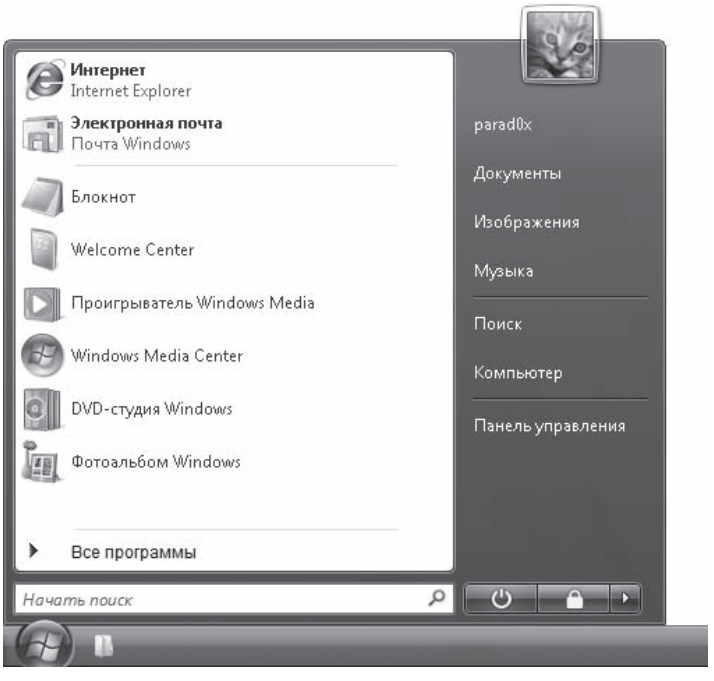


Рис. 3.3. Новое меню Пуск

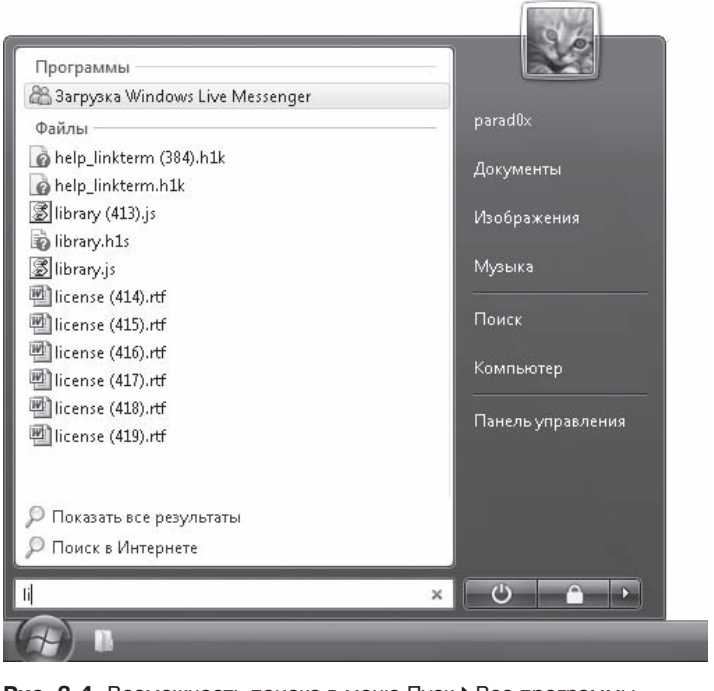


Рис. 3.4. Возможность поиска в меню Пуск ▸ Все программы

Как видно из рис. 3.4, если вы воспользуетесь панелью поиска меню Пуск, то в меню Пуск ▸ Все программы останутся только те программы (при этом не важно, находятся ли они непосредственно в меню Пуск ▸ Все программы или в одной из его подпапок), которые удовлетворяют введенному вами критерию. Обратите также внимание, что вывод результатов начинается непосредственно после того, как вы введете первую букву искомого слова.

Иными словами, когда вы введете первую букву, отобразятся все программы из меню Пуск ▸ Все программы, начинающиеся с этой буквы (если название программы состоит из нескольких слов, то поиск выполняется сразу по всем словам, а не по первому). Когда вы введете вторую букву искомого слова, то список программ сузится еще больше и т. д.

Как можно заметить из рис. 3.4, после выполнения поиска в меню Пуск ▸ Все программы отображаются также две ссылки: Поиск в Интернете и Показать все результаты. Выбор первой выполняет поиск с помощью поискового механизма сайта http://search.live.com, а выбор второй — среди содержимого файловой системы компьютера.

Проводник

Если вы удивлены новым меню Пуск, то Проводник Windows Vista вас удивит еще больше — он очень сильно отличается от знакомого вам по предыдущим версиям Windows Проводника (рис. 3.5).

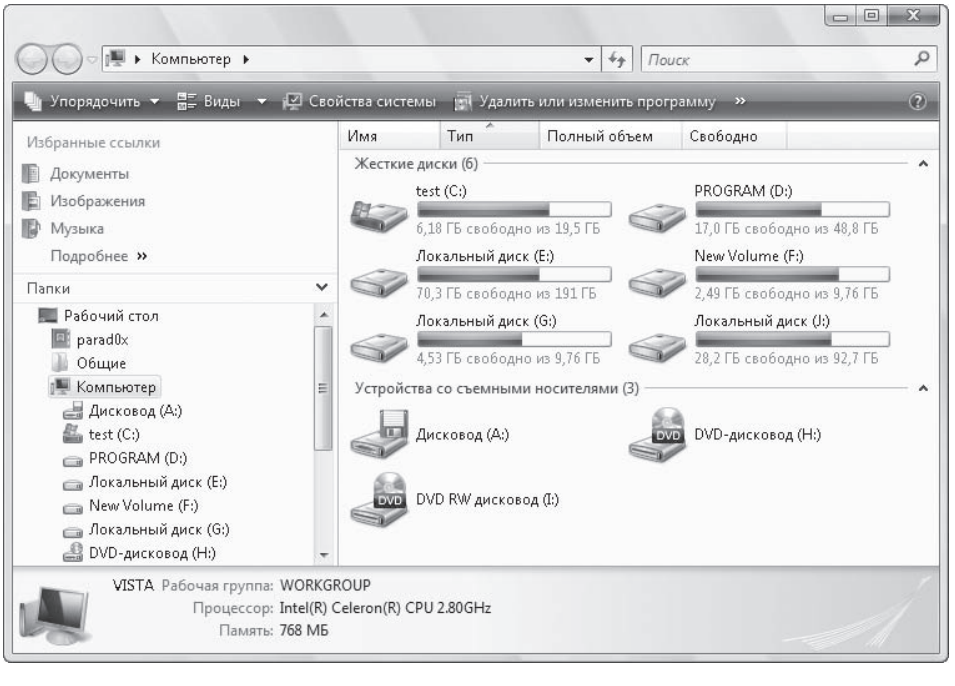


Рис. 3.5. Окно Проводника Windows Vista

Во-первых, как и многие другие элементы операционной системы, он содержит строку поиска. Во-вторых, по умолчанию в Проводнике больше не отображается стандартная строка меню. А в-третьих, теперь появилась возможность отображения в Проводнике больших значков (вплоть до 256 пикселов), что можно увидеть на рис. 3.6.

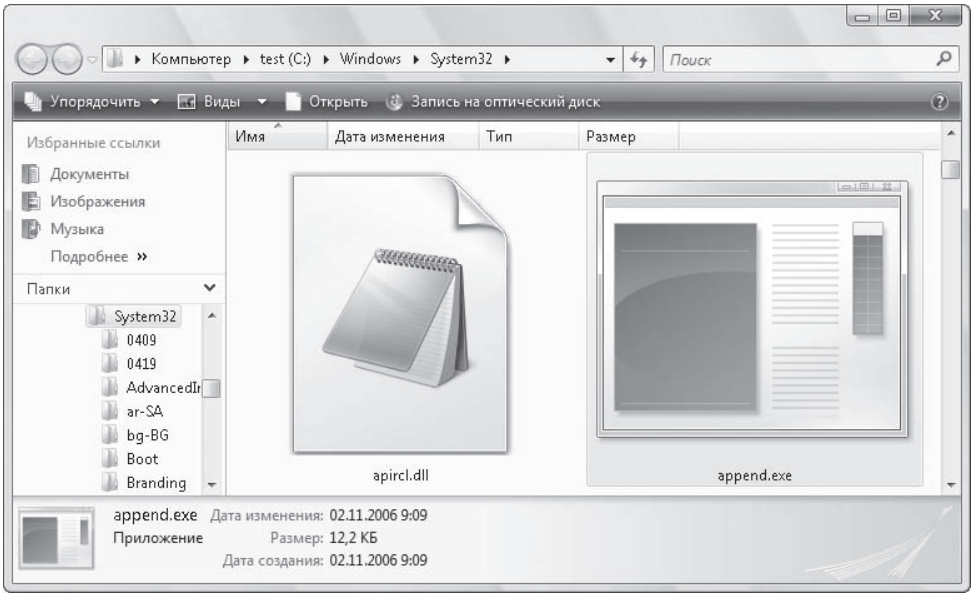


Рис. 3.6. Использование самых крупных значков

Теперь Проводник Windows состоит из шести элементов, каждый из которых заслуживает отдельного описания.

Адресная строка

Если в предыдущих версиях операционной системы Windows адресная строка была всего лишь элементом, содержащим путь к открытому в данный момент каталогу, в Windows Vista она представляет собой еще один способ быстрой навигации по файловой системе компьютера. Теперь в адресной строке напротив каждого элемента пути к каталогу стоит стрелка. Если вы нажмете ее, то Проводник отобразит список каталогов, являющихся дочерними по отношению к данному. Если вы щелкнете кнопкой мыши на одном из каталогов списка, то перейдете непосредственно в этот каталог.

Также с помощью контекстного меню адресной строки можно выполнить копирование пути из адресной строки в буфер обмена.

Панель поиска

С помощью панели поиска вы можете выполнить быстрый поиск папок и файлов в текущем каталоге и всех его подкаталогах. При этом если вы щелкнете кнопкой мыши на стрелке вниз, расположенной справа от изображения увеличительного стекла, то сможете выполнить настройку параметров поиска.

Панель основных операций

С помощью панели основных операций, которая расположена под адресной строкой, можно выполнить следующие часто применяемые операции:

- выбор способа отображения содержимого каталога (список Виды);
- выбор способа группировки содержимого каталога (список Упорядочить);
- открытие файла или папки (команда Открыть);
- добавление файла или папки к списку данных, которые будут записаны на DVD или компакт-диск (команда Запись на оптический диск).

Панель Избранные ссылки

В левой части окна Проводника можно встретить панель (при уменьшении ширины окна Проводника она скрывается), с помощью которой можно перейти к наиболее часто используемым каталогам, а также к результатам недавно выполненного поиска. Особенностью этой панели является то, что ее содержимое можно редактировать, добавляя свои каталоги или удаляя уже существующие.

Панель Папки

Данная панель является стандартной панелью Проводника, присутствовавшей еще в предыдущих версиях операционной системы Windows. Она отображает дерево каталогов файловой системы и позволяет выполнить быстрый переход к нужному вам каталогу. Никаких существенных изменений в этой панели замечено не было.

Строка описания

Еще одна интересная строка нового Проводника. Она отображает самые необходимые сведения либо о каталоге, содержимое которого в данный момент открыто (например, размер занимаемого им места), либо о файле или папке, которая в данный момент выделена (размер, дату создания, владельца).

Как было сказано ранее, теперь Проводник по умолчанию не содержит строки меню. Это объясняется довольно просто: наиболее часто используемые операции строки меню можно выполнить с помощью других элементов Проводника. Однако если вам потребуется выполнить те команды, которые есть только в меню, то строку меню можно просто отобразить, нажав клавишу Alt (рис. 3.7).

Кстати, обратите внимание, что на рис. 3.7 в правом нижнем углу программы `tcmsetup.exe` отображается щит. В Windows Vista это говорит о том, что данную программу можно запустить только с правами администратора. Теперь возле всех программ и возможностей операционной системы, которые требуют для своей работы права администратора, отображается такой щит.

Панель управления

Последним рассмотренным нами элементом оболочки является папка Панель управления (рис. 3.8). Точнее, в данной главе мы вкратце рассмотрим назначение всех апплетов и окон, доступ к которым можно получить из Панели управления.

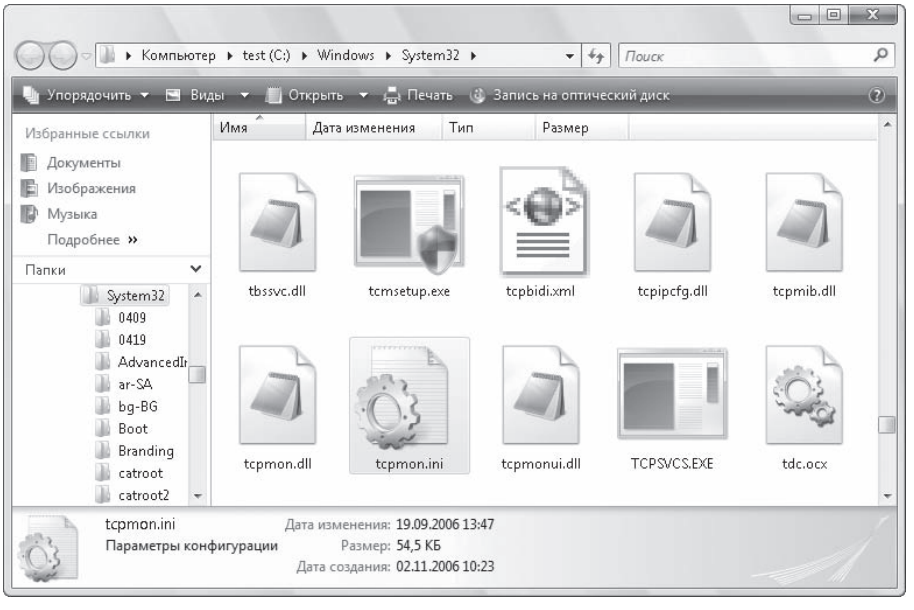


Рис. 3.7. Строка меню Проводника

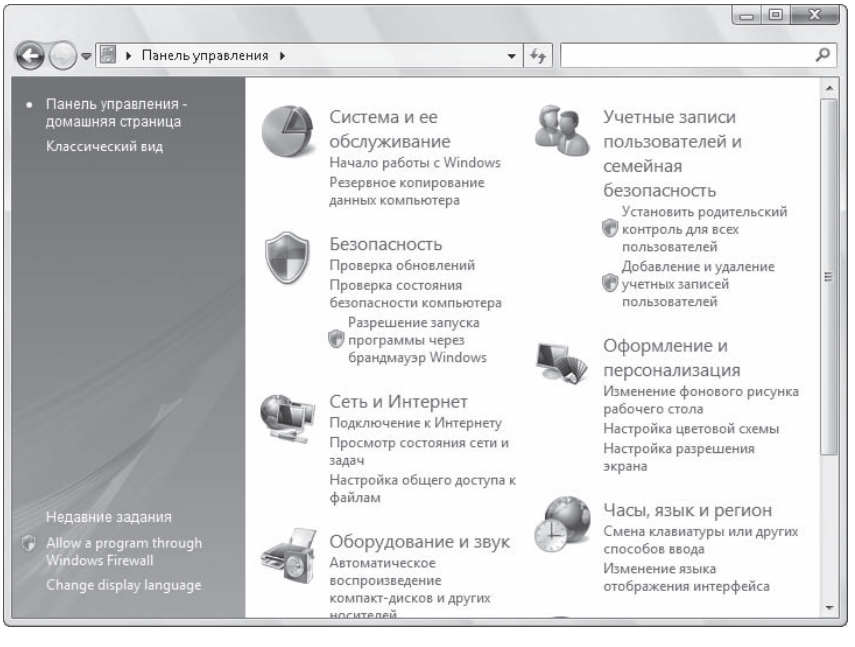


Рис. 3.8. Папка Панель управления при отображении вида по категориям

Чтобы отобразить папку Панель управления, достаточно в меню Пуск выбрать одноименный элемент. По умолчанию используется вид папки по категориям (все содержимое папки сгруппировано по определенному признаку), но вы можете

использовать классический вид, выбрав ссылку Классический вид в окне папки Панель управления. В этом случае папка будет содержать сразу все апплеты и окна.

Значки папки Панель управления

С помощью значков классического вида папки Панель управления можно получить доступ к следующим апплетам, программам и окнам.

Работа с оборудованием

Следующие значки относятся к работе с оборудованием.

- Установка оборудования — позволяет запустить программу `hdwwiz.exe`, расположенную в каталоге `%systemroot%\system32`, которая, в свою очередь, запускает апплет `hdwwiz.cpl`. С помощью этой программы можно установить драйверы для нового оборудования, которое по каким-то причинам не смогло установиться с помощью подсистемы Plug and Play.

  Если используется вид по категориям, то доступ к данному значку получить нельзя.

ПРИМЕЧАНИЕ

Вы можете отдельно вызвать мастер установки модема (Мастер установки оборудования). Для этого достаточно воспользоваться командой rundll32.exe modemui.dll, InvokeControlPanel.

  Данная возможность операционной системы Windows Vista ничем не отличается от возможности предыдущих версий Windows.

  - Внутреннее имя приложения: Microsoft.AddHardware.
  - ActiveX-объект: `{7A979262-40CE-46ff-AEEE-7884AC3B6136}`.

- Диспетчер устройств — дает возможность запустить оснастку `devmgmt.msc`, с помощью которой можно просмотреть свойства и параметры установленного на компьютере оборудования, а также установить, переустановить или выполнить откат драйверов, используемых этим оборудованием.

  Если используется вид по категориям, то доступ к этому значку можно получить с помощью одноименного элемента категорий Оборудование и звук и Система и ее обслуживание.

  - Внутреннее имя приложения: Microsoft.DeviceManager.
  - ActiveX-объект: `{74246bfc-4c96-11d0-abef-0020af6b0b7a}`.

- Игровые устройства — позволяет запустить апплет `joy.cpl`. С его помощью можно настроить параметры работы имеющихся у вас игровых контроллеров (джойстики, рули и т. д.), а также установить новый контроллер.

  Если используется вид по категориям, то доступ к данному значку можно получить с помощью одноименного элемента категории Оборудование и звук.

ПРИМЕЧАНИЕ

Это окно можно отобразить и с помощью команды rundll32.exe joy.cpl, ShowJoyCPL.

- Клавиатура — позволяет запустить апплет `main.cpl` для настройки параметров работы клавиатуры.

  Когда используется вид по категориям, доступ к данному значку можно получить с помощью одноименного элемента категории Оборудование и звук.

- Мышь — дает возможность запустить апплет `main.cpl` для настройки параметров работы мыши.

  Данный апплет ничем не отличается от одноименного апплета предыдущих версий операционных систем семейства Windows. Однако обратите внимание на один интересный параметр, о назначении которого знали немногие пользователи Windows XP. Он настраивается с помощью элементов области Залипание кнопки мыши, расположенной на вкладке Кнопки мыши окна Свойства: Мышь. Область содержит флажок Включить залипание, установка которого позволяет включить функцию «залипания» левой кнопки мыши. Если, установив данную функцию, вы нажмете и станете удерживать левую кнопку мыши, то после ее отпускания через некоторое время операционная система все равно будет считать, что кнопка еще нажата, пока вы не выполните щелчок левой кнопкой мыши. При этом время, в течение которого нужно зажимать левую кнопку перед тем как она «залипнет», можно изменить с помощью кнопки Параметры области Залипание кнопки мыши.

ПРИМЕЧАНИЕ

С помощью апплета main.cpl можно изменить скорость мигания каретки. Это же можно сделать, выполнив команду rundll32.exe user32.dll, SetCaretBlinkTime "значение в миллисекундах".

С помощью апплета main.cpl можно также поменять назначение кнопок мыши местами. Это же можно сделать, выполнив команду rundll32.exe user32.dll, SwapMouseButton. Однако с помощью данной команды можно изменить назначение кнопок мыши в одну сторону. Обратно же поменять назначение кнопок мыши с ее помощью нельзя.

  Если используется вид по категориям, то доступ к этому значку можно получить с помощью одноименного элемента категории Оборудование и звук.

- Перо и устройства ввода — позволяет запустить апплет `tabletpc.cpl`. С его помощью можно настроить параметры касания пером поверхности монитора. Возможности данного апплета напоминают возможности другого апплета — `mouse.cpl`.

  Если используется вид по категориям, то доступ к данному значку можно получить с помощью одноименного элемента категорий Оборудование и звук и Мобильные ПК.

- Телефон и модем — позволяет запустить апплет `telephon.cpl`, с помощью которого можно настроить параметры удаленного доступа (через модемное подключение).

ПРИМЕЧАНИЕ

Апплет можно запустить и с помощью команды rundll32.exe TAPI32.dll, internalConfig.

Когда используется вид по категориям, доступ к данному значку можно получить с помощью одноименного элемента категории Оборудование и звук.

- Принтеры — дает возможность отобразить список доступных в операционной системе принтеров, сканеров или факсов. В этом списке могут присутствовать как локальные принтеры, так и сетевые. Даже если вы не устанавливали ни одного принтера, данный список будет содержать два элемента (Fax и Microsoft XPS Document Writer), устанавливаемых по умолчанию. Первый из них позволяет передать документы через Интернет на удаленный факсимильный аппарат, а второй позволяет преобразовать документ в новый формат документов XPS, впервые появившийся в операционной системе Windows Vista.

  Если используется вид по категориям, то доступ к этому значку можно получить с помощью одноименного элемента категории Оборудование и звук.

  - Внутреннее имя приложения: Microsoft.Printers.
  - ActiveX-объект: `{2227A280-3AEA-1069-A2DE-08002B30309D}`.

- Сканеры и камеры — позволяет запустить программу `imagingDevices.exe`, расположенную в каталоге `%systemroot%\system32`. С ее помощью можно установить драйверы для новой камеры или сканера, а также настроить параметры уже установленного оборудования.

  Когда используется вид по категориям, доступ к данному значку можно получить с помощью одноименного элемента категории Оборудование и звук.

  - Внутреннее имя приложения: Microsoft.ScannersAndCameras.
  - ActiveX-объект: `{00f2886f-cd64-4fc9-8ec5-30ef6cdbe8c3}`.

- Звук — дает возможность запустить апплет `mmsys.cpl`, с помощью которого можно просмотреть свойства и настроить устройства для воспроизведения звука (вкладка Воспроизведение), настроить устройства записи (вкладка Запись), а также отредактировать список событий, которые будут озвучиваться операционной системой (вкладка Звуки). Рассмотрим вкладки апплета:

  - Воспроизведение — здесь вы можете установить используемое по умолчанию устройство воспроизведения звука (если у вас установлено несколько устройств), отключить устройство, определить используемые устройством аудиоканалы (две колонки, четыре колонки, система 5.1 и т. д.), изменить значок, отображаемый при наведении указателя мыши на значок звука в области уведомления, указать общий уровень звука, а также отдельные уровни для различных колонок, указать частоту, с которой будет выдаваться звук (качество звучания), и т. д.;

- Запись — на этой вкладке можно установить используемое по умолчанию устройство записи звука (если у вас установлено несколько устройств), отключить устройство, изменить значок, отображаемый при наведении указателя мыши на значок звука в области уведомления, указать общий уровень записи, указать частоту, с которой будет записываться звук (качество звучания), и т. д.;
- Звуки — здесь можно выполнить те же действия, что и в предыдущих операционных системах семейства Windows.

ПРИМЕЧАНИЕ

В операционной системе Windows Vista изменилось не только содержимое окна Sound, но и сам способ работы операционной системы со звуковыми устройствами и драйверами. Например, теперь драйверы звуковых устройств, как и видеокарт, работают не на уровне ядра, а на уровне пользователя. Это позволяет повысить не только стабильность работы операционной системы, но и скорость работы драйвера звукового устройства.

Если используется вид по категориям, то доступ к этому значку можно получить с помощью одноименного элемента категории Оборудование и звук.

- Текст в речь — позволяет запустить апплет `sapi.cpl`, расположенный по адресу `%systemroot%\system32\speech\speechux` (все остальные апплеты расположены в каталоге `%systemroot%\system32`). С его помощью можно настроить параметры работы микрофона.

  При использовании вида по категориям доступ к значку получить нельзя.

Настройка интерфейса

С помощью перечисленных далее значков можно установить настройки интерфейса.

- Автозапуск — с помощью данного значка можно перейти к новому окну Windows Vista, которое позволяет отредактировать поведение системы при помещении в привод компакт-дисков диска с определенным содержанием. Список содержимого дисков, для которых можно настроить отдельные действия, довольно большой. К нему относятся аудио- и видеодиски различных форматов, диски, содержащие файлы программ, рисунки, музыку или фильмы, а также пустые записываемые диски.

  Когда используется вид по категориям, доступ к этому значку можно получить с помощью одноименного элемента категории Оборудование и звук.

  - Внутреннее имя приложения: Microsoft.AutoPlay.
  - ActiveX-объект: `{9C60DE1E-E5FC-40f4-A487-460851A8D915}`.
- Управление цветом — после выбора данного значка будет запущена программа `colorcpl.exe`, расположенная в каталоге `%systemroot%\system32`. С ее помощью можно выбрать цветовой профиль для таких устройств передачи графики, как монитор, факс, сканер или принтер.

Если используется вид по категориям, то доступ к данному значку можно получить с помощью одноименного элемента категории Оборудование и звук.

- Внутреннее имя приложения: Microsoft.ColorManagement.
- ActiveX-объект: {B2C761C6-29BC-4f19-9251-E6195265BAF1}.

■ Свойства папки — выбор этого значка вызывает окно Свойства папки, с помощью которого можно настроить некоторые параметры оболочки операционной системы, а также параметры поиска в Windows Vista.

Когда используется вид по категориям, доступ к значку можно получить с помощью одноименного элемента категории Оформление и персонализация.

- Внутреннее имя приложения: Microsoft.FolderOptions.
- ActiveX-объект: {6DFD7C5C-2451-11d3-A299-00C04F8EF6AF}.

■ Персонализация — позволяет запустить мастер, с помощью которого можно настроить многие параметры интерфейса операционной системы Windows Vista. В основном данный мастер выполняет функции окна Свойства: Экран, присутствовавшего в предыдущих версиях операционной системы Windows.

Если используется вид по категориям, то доступ к этому значку можно получить с помощью одноименного элемента категорий Оформление и персонализация, Оборудование и звук, Мобильные ПК.

- Внутреннее имя приложения: Microsoft.Personalization.
- ActiveX-объект: {ED834ED6-4B5A-4bfe-8F11-A626DCB6A921}.

■ Язык и региональные стандарты — дает возможность запустить апплет `intl.cpl`. С помощью данного апплета можно настроить используемый формат даты и времени, денежный формат, а также настроить используемый операционной системой по умолчанию язык и параметры переключения языков.

При использовании вида по категориям доступ к данному значку можно получить с помощью одноименного элемента категории Часы, язык и регион.

ПРИМЕЧАНИЕ

Сведения об изменении языковых настроек заносятся в журнал Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ International.

Сведения об устанавливаемых или удаляемых языках заносятся в журнал Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ LanguagePackSetup.

Сведения о работе с языковыми возможностями операционной системы (например, сведения о библиотеках, функции которых изменяли язык) заносятся в журнал Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ MUI.

Кроме того, обратите внимание на кнопку Копировать в зарезервированные учетные записи, расположенную на вкладке Дополнительно окна Язык и региональные стандарты. С ее помощью вы сможете копировать все языковые настройки вашей учетной записи в другую учетную запись (учетную запись, используемую

по умолчанию, и служебную учетную запись (системную запись, LOCAL SERVICE и NETWORK SERVICE)).

Обратите также внимание на кнопку Установить или удалить язык, расположенную на вкладке Языки и клавиатуры окна Язык и региональные стандарты. С ее помощью можно установить дополнительные языковые пакеты или удалить уже существующие. В Windows Vista больше не нужно покупать отдельную операционную систему, если необходимо изменить ее локализацию (язык). Теперь для смены локализации достаточно установить дополнительный языковой пакет.

Большинство настроек, которые можно изменить с помощью данного апплета, хранятся в ветви реестра HKEY_CURRENT_USER\Control Panel\International. При этом их можно переопределить с помощью групповых политик, расположенных в разделе Конфигурация пользователя ▸ Административные шаблоны ▸ Панель управления ▸ Язык и региональные стандарты. Эти политики изменяют значения параметров REG_DWORD-типа, расположенных в ветви системного реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Control Panel\International.

А с помощью групповых политик, расположенных в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Службы языковых стандартов, можно изменить системные языковые настройки.

ПРИМЕЧАНИЕ

Используя команду rundll32.exe MSCTF.dll, TF_RunInputCPL, можно вызвать окно Text Services and Input Languages.

Еще одна команда, позволяющая вызвать данное окно, — rundll32.exe shell32.dll, Control_RunDLL Input.dll.

- Speech Recognition Options — нововведением операционной системы Windows Vista является возможность диктовки сообщений или управления компьютером голосом. Эту функцию можно настроить с помощью именно этого значка.

  Если используется вид по категориям, то доступ к значку можно получить с помощью одноименного элемента категории Специальные возможности.

  - Внутреннее имя приложения: Microsoft.SpeechRecognitionOptions.
  - ActiveX-объект: {58E3C745-D971-4081-9034-86E34B30836A}.

- Параметры планшетного компьютера — позволяет запустить апплет TabletPC.cpl, с помощью которого можно настроить параметры работы модуля Tablet PC.

  Когда используется вид по категориям, доступ к значку можно получить с помощью одноименного элемента категорий Оборудование и звук и Мобильные ПК.

- Панель задач и меню "Пуск" — дает возможность отобразить одноименное окно, с помощью которого можно настроить параметры отображения меню Пуск, а также Панели задач операционной системы.

При использовании вида по категориям доступ к данному значку можно получить с помощью одноименного элемента категории Оформление и персонализация.

- Внутреннее имя приложения: Microsoft.TaskbarAndStartMenu.
- ActiveX-объект: {0DF44EAA-FF21-4412-828E-260A8728E7F1}.

■ Центр начальной настройки — после выбора значка запускается одноименный мастер, с помощью которого можно выполнить основные действия по настройке операционной системы и ее компонентов, а также просмотреть конфигурацию компьютера и количество оставшихся до активации операционной системы дней. По умолчанию этот мастер отображается при каждом входе в операционную систему.

ПРИМЕЧАНИЕ

Данный мастер можно отобразить и с помощью команды rundll32.exe oobefldr.dll, ShowWelcomeCenter.

Если используется вид по категориям, то доступ к значку можно получить с помощью одноименного элемента категории Система и ее обслуживание.

- Внутреннее имя приложения: Microsoft.WelcomeCenter.
- ActiveX-объект: {CB1B7F8C-C50A-4176-B604-9E24DEE8D4D1}.

■ Свойства боковой панели Windows — позволяет запустить программу sidebar.exe, расположенную по адресу %programfiles%\Windows Sidebar. С ее помощью можно настроить параметры отображения боковой панели, а также просмотреть список мини-приложений, которые будут отображаться на боковой панели.

Когда используется вид по категориям, доступ к этому значку можно получить с помощью одноименного элемента категорий Программы и Оформление и персонализация.

- Внутреннее имя приложения: Microsoft.WindowsSidebarProperties.
- ActiveX-объект: {37efd44d-ef8d-41b1-940d-96973a50e9e0}.

■ Windows Sideshow — дает возможность отобразить мастер, с помощью которого можно просмотреть и отредактировать список мини-приложений, отображаемых на специальной панели ноутбука или другого устройства (например, новые ноутбуки будут поставляться со специальным маленьким экраном на передней панели, на котором можно отобразить такую информацию, как заряд батареи, количество непрочитанных писем и т. д.).

Если используется вид по категориям, то доступ к значку можно получить с помощью одноименного элемента категории Оборудование и звук.

- Внутреннее имя приложения: Microsoft.WindowsSideShow.
- ActiveX-объект: {E95A4861-D57A-4be1-AD0F-35267E261739}.

Администрирование операционной системы

Для администрирования ОС используются следующие значки.

- Администрирование — этот значок позволяет перейти в каталог `%programdata%\microsoft\windows\start menu\programs\Administrative Tools`, содержащий набор часто применяемых администратором программ и оснасток консоли управления Microsoft. По умолчанию в данном каталоге расположены следующие оснастки.
  - Управление компьютером — отображает оснастку `compmgmt.msc`, предоставляющую основные возможности по настройке параметров работы компьютера.
  - Источники данных (ODBC) — позволяет вызвать окно настройки ODBC. Данный ярлык запускает программу `odbcad32.exe`.
  - Просмотр событий — дает возможность просмотреть содержимое стандартных журналов Windows с помощью оснастки `eventvwr.msc`.
  - Инициатор iSCSI — отображает окно настройки протокола iSCSI. Данный ярлык запускает программу `iscsicpl.exe`.
  - Локальная политика безопасности — запускает оснастку `secpol.msc`, с помощью которой можно определить текущие значения настроек параметров безопасности компьютера.
  - Средство диагностики памяти — позволяет перезагрузить компьютер для выполнения диагностики оперативной памяти. Данный ярлык запускает программу `MdSched.exe`.
  - Управление печатью — отображает оснастку `printmanagement.msc`, предназначенную для работы с принтерами, доступными локальному или удаленному компьютеру.
  - Монитор производительности и стабильности — выводит оснастку `perfmon.msc`, которая позволяет создавать объекты, собирающие сведения от компонентов операционной системы.
  - Службы — отображает оснастку `services.msc`, которая предоставляет доступ к настройкам работы служб, установленных в операционной системе.
  - Конфигурация системы — позволяет запустить стандартную программу операционных систем семейства Windows `msconfig.exe`.
  - Планировщик заданий — отображает оснастку `taskschd.msc`, предназначенную для работы с назначенными заданиями.
  - Брандмауэр Windows в режиме повышенной безопасности — отображает оснастку `WF.msc`, которая позволяет настраивать стандартный брандмауэр операционной системы.

  При установке вида по категориям доступ к этому значку можно получить с помощью одноименного элемента категории Система и ее обслуживание.

  Значок имеет следующие характеристики.

  - Внутреннее имя приложения: Microsoft.AdministrativeTools.
  - ActiveX-объект: `{D20EA4E1-3957-11d2-A40B-0C5020524153}`.

- Центр архивации и восстановления — с помощью этого значка можно перейти к новому мастеру Windows Vista, который позволяет заархивировать или восстановить файлы (или настройки операционной системы), а также создать точки восстановления. Благодаря ему можно также запустить уже известный мастер Средство переноса данных Windows, а также программу Восстановление системы.

  Если используется вид по категориям, то доступ к данному значку можно получить с помощью одноименного элемента категории Система и ее обслуживание.

  - Внутреннее имя приложения: Microsoft.BackupAndRestoreCenter.
  - ActiveX-объект: `{335a31dd-f04b-4d76-a925-d6b47cf360df}`.

- Шифорование диска BitLocker — с помощью мастера (его можно запустить только с правами администратора), вызываемого с использованием этого значка, можно включить или отключить механизм шифрации содержимого определенных разделов жесткого диска. С его помощью можно также запустить оснастку Управление дисками.

  Когда используется вид по категориям, доступ к данному значку можно получить с помощью одноименного элемента категории Безопасность.

  - Внутреннее имя приложения: Microsoft.BitLockerDriveEncryption.
  - ActiveX-объект: `{D9EF8727-CAC2-4e60-809E-86F80A666C91}`.

- Дата и время — позволяет запустить апплет `timedate.cpl` (он отображает окно Дата и время), который дает возможность изменить текущую дату и время, а также используемый системой часовой пояс.

  При использовании вида по категориям доступ к данному значку можно получить с помощью одноименного элемента категории Часы, язык и регион.

ПРИМЕЧАНИЕ

Сведения о настройке времени заносятся в журнал Журналы приложений служб ▸ Microsoft ▸ Windows ▸ DateTimeControlPanel.

Операционная система Windows Vista имеет новую уникальную возможность — установку отображения времени сразу в нескольких часовых поясах. Для выполнения этой операции достаточно воспользоваться новой вкладкой Дополнительные часы окна Дата и время. С ее помощью можно указать два дополнительных часовых пояса (достаточно установить флажок Показать эти часы, выбрать часовой пояс и ввести название дополнительных часов), после чего, если вы наведете и задержите указатель мыши над отображением часов в области уведомления, перед вами отобразится время сразу в нескольких часовых поясах.

ПРИМЕЧАНИЕ

Как и раньше, текущую дату и время можно узнать с помощью репозитария CIM. Для этого применяется класс Win32 CurrentTime, расположенный в пространстве имен

root\cimv2. Например, данный класс поддерживает следующие свойства: Day (определяет текущее число), DayOfWeek (определяет текущий день недели), Hour (определяет час), Minute (определяет количество минут), Month (определяет текущий месяц), Quarter (определяет текущий квартал), Second (определяет количество секунд), WeekInMonth (определяет номер текущей недели в месяце), Year (определяет текущий год).

- Программы по умолчанию — позволяет выполнить такие действия, как выбор программ, используемых по умолчанию, ассоциирование файлов определенного расширения программам, настройки вызова окна Автозапуск.

ПРИМЕЧАНИЕ

Запретить доступ к окну Настройка доступа программ и умолчаний можно с помощью параметра REG-DWORD-типа NoDefaultPrograms, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs. Данному параметру нужно присвоить значение 1.

Если используется вид по категориям, то доступ к этому значку можно получить с помощью одноименного элемента категории Программы.

ПРИМЕЧАНИЕ

Окно Настройка доступа программ и умолчаний можно отобразить с помощью команды rundll32.exe appwiz.cpl, RunSPADW.

Значок имеет следующие характеристики.

- Внутреннее имя приложения: Microsoft.DefaultPrograms.
- ActiveX-объект: `{17cd9488-1228-4b2f-88ce-4298e93e0966}`.

- Центр специальных возможностей — позволяет отобразить мастер специальных возможностей, предназначенный для людей с ослабленным зрением или с физическими недостатками. Он является расширенным вариантом окна, которое можно вызвать при входе пользователя в систему, и с его помощью можно дополнительно настроить параметры работы монитора, мыши, клавиатуры и многие другие параметры.

  Если используется вид по категориям, то доступ к этому значку можно получить с помощью одноименного элемента категорий Оформление и персонализация и Специальные возможности.

  - Внутреннее имя приложения: Microsoft.EaseOfAccessCenter.
  - ActiveX-объект: `{D555645E-D4F8-4c29-A827-D93C859C4F2A}`.

- Шрифты — дает возможность отобразить содержимое каталога `%systemroot%\system32\fonts`. Этот каталог хранит файлы шрифтов, которые зарегистрированы в системе. С помощью значка можно также зарегистрировать новые

шрифты. Для этого достаточно вызвать контекстное меню папки и выбрать команду Установить новый шрифт.

При использовании вида по категориям доступ к данному значку можно получить с помощью одноименного элемента категории Оформление и персонализация.

ПРИМЕЧАНИЕ

Данную папку можно также отобразить с помощью команды rundll32.exe shell32.dll, SHHelpShortcuts_RunDLL FontsFolder.

Значок имеет следующие характеристики.

- Внутреннее имя приложения: Microsoft.Fonts.
- ActiveX-объект: `{D20EA4E1-3957-11d2-A40B-0C5020524152}`.

- Параметры индексирования — позволяет запустить окно, с помощью которого можно настроить параметры индексации файлов и папок для поисковой службы Windows Vista.

  Когда используется вид по категориям, доступ к значку можно получить с помощью одноименного элемента категории Система и ее обслуживание.

ПРИМЕЧАНИЕ

Это окно можно вызвать и с помощью команды rundll32.exe shell32.dll, Control_RunDLL Srchadmin.dll.

- Родительский контроль — дает возможность отобразить мастер, с помощью которого можно ограничить возможности определенных учетных записей пользователей операционной системы (нельзя ограничивать учетные записи, имеющие административные права).

  Если используется вид по категориям, то доступ к значку можно получить с помощью одноименного элемента категорий Безопасность и Учетные записи пользователей и семейная безопасность.

  - Внутреннее имя приложения: Microsoft.ParentalControls.
  - ActiveX-объект: `{96AE8D84-A250-4520-95A5-A47A7E3C548B}`.

- Счетчики и средства производительности — позволяет отобразить мастер, с помощью которого вы сможете протестировать свой компьютер и узнать оценку его производительности, выданную операционной системой.

  При использовании вида по категориям доступ к этому значку можно получить с помощью одноименного элемента категории Система и ее обслуживание.

  - Внутреннее имя приложения: Microsoft.PerformanceInformationAndTools.
  - ActiveX-объект: `{78F3955E-3B90-4184-BD14-5397C15F1EFC}`.

- Электропитание — позволяет вывести окно настройки параметров энергопотребления компьютера. С его помощью можно выбрать определенную схему энергопотребления, изменить настройки схем или создать свою собственную схему. По умолчанию присутствует три схемы энергопотребления: Сбалансированный (используется по умолчанию и определяет средние значения энергопотребления компьютера и его производительности), Экономия энергии (компьютер настраивается на максимальное энергопотребление, и, соответственно, максимально снижается его производительность) и Высокая производительность (компьютер настраивается на максимальную производительность).

ПРИМЕЧАНИЕ

Данное окно можно также отобразить с помощью команды rundll32.exe shell32.dll, Control_RunDLL PowerCfg.cpl @0.

Если используется вид по категориям, то доступ к значку можно получить с помощью одноименного элемента категорий Система и ее обслуживание, Оборудование и звук, Мобильные ПК.

  - Внутреннее имя приложения: Microsoft.PowerOptions.
  - ActiveX-объект: `{025A5937-A6BE-4686-A844-36FE4BEC8B6D}`.

- Отчеты о проблемах и их решениях — выбор этого значка запускает программу `wercon.exe`, расположенную в каталоге `%systemroot%\system32`. Она позволяет просмотреть список проблем, возникших при работе с Windows Vista (под проблемами понимается как отсутствие драйвера оборудования, так и возникшие ошибки и аварийные остановы операционной системы), просмотреть предлагаемые операционной системой решения этих проблем, а также очистить список проблем или настроить параметры данной программы.

  Когда используется вид по категориям, доступ к данному значку можно получить с помощью одноименного элемента категории Система и ее обслуживание.

  - Внутреннее имя приложения: Microsoft.ProblemReportsAndSolutions.
  - ActiveX-объект: `{FCFEECAE-EE1B-4849-AE50-685DCF7717EC}`.

- Программы и компоненты — предоставляет следующие возможности: просмотр установленных в операционной системе программ и обновлений, запуск программы `optionalfeatures.exe`, предназначенной для установки и удаления компонентов операционной системы, а также получение доступа к сайту Microsoft, содержащему список новых программ для операционной системы, которые вы можете купить или скачать.

ПРИМЕЧАНИЕ

Запустить программу optionalfeatures.exe можно и с помощью команды rundll32.exe appwiz.cpl, RunOCMW.

Если используется вид по категориям, то доступ к значку можно получить с помощью одноименного элемента категории Программы.

- Внутреннее имя приложения: Microsoft.ProgramsAndFeatures.
- ActiveX-объект: `{7b81be6a-ce2b-4676-a29e-eb907a5126c5}`.

■ Система — позволяет отобразить новое окно Система. С его помощью можно просмотреть и изменить параметры настройки системы Windows Vista, а также узнать оставшееся время до активации операционной системы или запустить программу активации.

ПРИМЕЧАНИЕ

Данное окно можно также отобразить с помощью команды rundll32.exe emdmgmt.dll, EMDMgmtLaunchPropertiesW.

Если используется вид по категориям, то доступ к значку можно получить с помощью одноименного элемента категории Система и ее обслуживание.

- Внутреннее имя приложения: Microsoft.System.
- ActiveX-объект: `{BB06C0E4-D293-4f75-8A90-CB05B6477EEE}`.

■ Учетные записи пользователей — позволяет отобразить мастер, с помощью которого можно управлять учетными записями пользователей: изменять пароли к ним, создавать новые учетные записи или удалять старые, изменять имя учетной записи или группу, к которой она принадлежит. С помощью этого мастера можно также подготовить дискету с паролем пользователя (если вы забудете пароль, то при входе в систему можно будет воспользоваться дискетой, чтобы его сменить), отредактировать параметры использования сертификата пользователя, а также изменить сетевые пароли, которые запомнила операционная система. И не стоит забывать о ссылке Изменение своего рисунка данного мастера, которая является единственным способом изменения рисунка пользователя, отображаемого в меню Пуск.

При использовании вида по категориям доступ к данному значку можно получить с помощью одноименного элемента категории Учетные записи пользователей и семейная безопасность.

- Внутреннее имя приложения: Microsoft.UserAccounts.
- ActiveX-объект: `{60632754-c523-4b62-b45c-4172da012619}`.

■ Windows CardSpace — выбор значка запускает апплет `infocardcpl.cpl`, который позволяет создать что-то вроде электронной пластиковой карты. С ее помощью можно более безопасно выполнять покупки в Интернете (если интернет-магазин поддерживает данную возможность). При этом при оформлении покупки вам больше не придется вводить дополнительные сведения и свои реквизиты — вся эта информация будет храниться в электронной пластиковой карте.

Для работы данного апплета необходим компонент операционной системы Windows Foundation Components for WinFX 3.0, который устанавливается по умолчанию.

Если используется вид по категориям, то доступ к значку можно получить с помощью одноименного элемента категории Учетные записи пользователей и семейная безопасность.

- Внутреннее имя приложения: Microsoft.CardSpace.
- ActiveX-объект: {78CB147A-98EA-4AA6-B0DF-C8681F69341C}.

Настройка безопасности

Для настройки безопасности вы можете использовать следующие значки.

- Центр обеспечения безопасности Windows — позволяет запустить апплет `wscui.cpl`, с помощью которого можно настроить параметры службы обновления компьютера, брандмауэра операционной системы, программы Защитник Windows, а также настройки браузера Internet Explorer.

  Если используется вид по категориям, то доступ к этому значку можно получить с помощью одноименного элемента категории Безопасность.

- Защитник Windows — дает возможность запустить программу `MSASCui.exe`, расположенную в каталоге `%programfiles%\Windows Defender`. С ее помощью можно настроить параметры защиты операционной системы от вирусов и других злонамеренных программ.

  При использовании вида по категориям доступ к данному значку можно получить с помощью одноименного элемента категорий Безопасность и Программы.

  - Внутреннее имя приложения: Microsoft.WindowsDefender.
  - ActiveX-объект: {D8559EB9-20C0-410E-BEDA-7ED416AECC2A}.

- Брандмауэр Windows — запускает программу `FirewallControlPanel.exe`, которая расположена в каталоге `%systemroot%\system32`. С ее помощью можно настроить некоторые параметры работы стандартного брандмауэра операционной системы Windows Vista, направленные на блокирование входящих подключений.

  Когда используется вид по категориям, доступ к этому значку можно получить с помощью одноименного элемента категории Безопасность.

  - Внутреннее имя приложения: Microsoft.WindowsFirewall.
  - ActiveX-объект: {4026492F-2F69-46B8-B9BF-5654FC07E423}.

- Центр обновления Windows — дает возможность отобразить мастер, с помощью которого можно проверить на сайте Microsoft новые обновления для операционной системы Windows Vista, изменить параметры работы службы Windows Update, а также просмотреть историю установки обновлений системы.

  Если используется вид по категориям, то доступ к данному значку можно получить с помощью одноименного элемента категорий Безопасность и Система и ее обслуживание.

  - Внутреннее имя приложения: Microsoft.WindowsUpdate.
  - ActiveX-объект: {36eef7db-88ad-4e81-ad49-0e313f0c35f8}.

Работа с сетью

Перечисленные ниже значки используются при работе с сетью.

- Свойства обозревателя — позволяет запустить апплет `inetcpl.cpl`, настраивающий параметры работы браузера Internet Explorer.

  Если установлен вид по категориям, то доступ к этому значку можно получить с помощью одноименного элемента категории Сеть и Интернет.

- Инициатор iSCSI — дает возможность запустить программу `iscsicpl.exe`, расположенную в каталоге `%systemroot%\system32`. С ее помощью можно более тонко настроить параметры работы устройств, подключенных к контроллеру SCSI.

  При использовании вида по категориям доступ к данному значку получить нельзя.

  - Внутреннее имя приложения: Microsoft.iSCSIInitiator.
  - ActiveX-объект: `{A304259D-52B8-4526-8B1A-A1D6CECC8243}`.

- Центр управления сетями и общим доступом — позволяет запустить мастер, с помощью которого в Windows Vista выполняется большая часть работы, направленной на создание, администрирование или настройку сети.

  Если используется вид по категориям, то доступ к значку можно получить с помощью одноименного элемента категории Сеть и Интернет.

  - Внутреннее имя приложения: Microsoft.NetworkAndSharingCenter.
  - ActiveX-объект: `{8E908FC9-BECC-40f6-915B-F4CA0E70D03D}`.

- Автономные файлы — после выбора этого значка отображается одноименное окно, с помощью которого можно настроить параметры работы механизма автономных файлов, а также просмотреть текущий список автономных файлов или открыть Центр синхронизации.

  Когда используется вид по категориям, доступ к данному значку можно получить с помощью одноименного элемента категории Сеть и Интернет.

ПРИМЕЧАНИЕ

Данное окно можно также отобразить с помощью команды rundll32.exe shell32.dll, Control_RunDLL Cscui.dll.

- Соседние пользователи — позволяет запустить апплет `collab.cpl`.

  При использовании вида по категориям доступ к значку можно получить с помощью одноименного элемента категории Сеть и Интернет.

- Центр синхронизации — позволяет запустить программу `mobsync.exe`, расположенную в каталоге `%systemroot%\system32`. С ее помощью можно настроить параметры синхронизации данного компьютера с любым устройством, которое ее поддерживает, синхронизировать устройство с компьютером, а также просмотреть список синхронизированных в данный момент устройств или список конфликтов, из-за которых синхронизация устройства невозможна.

ПРИМЕЧАНИЕ

Сведения о диагностике работы мастера Центр синхронизации хранятся в журнале Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Sync Center.

Если используется вид по категориям, то доступ к данному значку можно получить с помощью одноименного элемента категорий Сеть и Интернет и Мобильные ПК.

- Внутреннее имя приложения: Microsoft.SyncCenter.
- ActiveX-объект: `{9C73F5E5-7AE7-4E32-A8E8-8D23B85255BF}`.

- Центр устройств Windows Mobile — позволяет запустить программу для настройки параметров подключения к компьютеру таких устройств, как, например, коммуникаторы.

ПРИМЕЧАНИЕ

Вы можете запретить доступ к данному значку, если установите значение параметра REG_DWORD-типа NoMobilityCenter, расположенного в ветви системного реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\MobilityCenter, равным 1.

Когда используется вид по категориям, доступ к данному значку можно получить с помощью одноименного элемента категорий Сеть и Интернет, Оборудование и звук, Мобильные ПК.

- Внутреннее имя приложения: Microsoft.MobilityCenter.
- ActiveX-объект: `{5ea4f148-308c-46d7-98a9-49041b1dd468}`.

Работа с программой control.exe

Вы, наверное, заметили, что выше для некоторых значков папки Панель управления также приводилось их внутреннее имя. С его помощью вы можете самостоятельно вызвать соответствующее окно, не пользуясь папкой Панель управления. Для этого достаточно воспользоваться командой `control /Name <внутреннее имя приложения>`. Собственно, вы можете использовать программу `control.exe` для вызова самой папки Панель управления.

Программа `control.exe` также поддерживает следующие параметры.

- `/name Microsoft.GetProgramsOnline` — подключается к Интернету для отображения страницы Microsoft, содержащей доступные для скачивания программы.
- `USERPASSWORDS2` — отображает окно Учетные записи пользователей. Особенностью данного окна является то, что с его помощью вы можете указать учетную запись, которая будет автоматически загружаться при запуске компьютера (не нужно будет выбирать учетную запись для входа и вводить ее пароль). Благодаря этому же окну можно переименовать учетную запись Администратор.
- `UPDATE` — выводит окно Центр обновления Windows.

- SYSTEM — отображает окно Система.
- SCANNERCAMERA — выводит окно Сканеры и камеры.
- USERPASSWORDS — отображает мастер Учетные записи пользователей.
- INFRARED — выводит окно настройки параметров инфракрасного подключения.
- NETCONNECTIONS — отображает доступные в данный момент сетевые подключения.
- SCHEDTASKS — выводит оснастку Планировщик задач.
- ADMINTOOLS — отображает каталог Администрирование.
- TELEPHONY — выводит окно Телефон и модем.
- FOLDERS — отображает окно Свойства папки.
- FONTS — выводит каталог Шрифты.
- PRINTERS — отображает каталог Принтеры.
- KEYBOARD и MOUSE — выводят окно Свойства: Мышь.
- INTERNATIONAL — отображает окно Язык и региональные стандарты.
- PORTS — выводит окно Свойства системы, открытое на вкладке Оборудование.
- DATE/TIME — отображает окно Дата и время.
- COLOR — выводит окно Параметры оформления.

ПРИМЕЧАНИЕ

Окно Параметры оформления можно отобразить и с помощью команды rundll32.exe shell32.dll, Control_RunDLL desk.cpl desk,@Appearance.

- DESKTOP — отображает окно Параметры дисплея.

ПРИМЕЧАНИЕ

Окно Параметры дисплея можно отобразить и с помощью команды rundll32.exe shell32.dll, Control_RunDLL desk.cpl desk,@Settings.

Как же хранятся в реестре внутренние имена апплетов? Они находятся в параметре System.ApplicationName ветвей реестра HKEY_CLASSES_ROOT\CLSID\<CLSID-номер ActiveX-объекта>.

Но есть еще одна ветвь реестра, которая хранит все внутренние имена апплетов, — HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\Extended Properties\System.ApplicationName. В ней содержатся параметры строкового типа, имена которых определяют путь к апплету, а значения — внутреннее имя апплета. Стоит заметить, что именно содержимое

этой ветви используется программой control.exe для определения внутреннего имени апплета. Например, в данной ветви реестра есть параметр %SystemRoot%\system32\wscui.cpl, который хранит значение Microsoft.SecurityCenter. Если вы измените значение этого параметра, например, на MS, то сможете запустить окно Windows Security Center с помощью более простой команды control /name ms.

Работа с ActiveX-объектами

При описании значков папки Панель управления были приведены также названия ActiveX-объектов, которые создают данные значки. Но что можно сделать с этими названиями?

Во-первых, с их помощью можно отобразить или скрыть соответствующие значки ActiveX-объектов на Рабочем столе, в папке Компьютер или, собственно, в папке Панель управления. Как это сделать, будет описано далее в этой главе.

Во-вторых, некоторые из приведенных ActiveX-объектов можно использовать в конструкциях вида ::{21EC2020-3AEA-1069-A2DD-08002B30309D}\::{CLSID-номер соответствующего ActiveX-объекта} для запуска соответствующего окна или мастера.

И, в-третьих, с их помощью можно отобразить или скрыть соответствующие значки ActiveX-объектов в любой папке файловой системы. Для этого достаточно создать папку и приписать к ее имени значение .{CLSID-номер соответствующего ActiveX-объекта}.

Окно Программы и компоненты

Напоследок опишу работу с окном, которое рано или поздно понадобится любому пользователю, — окном, с помощью которого можно удалить или переустановить программы и обновления операционной системы. В Windows Vista это окно было существенно доработано и изменено, хотя принцип его построения не изменился.

ПРИМЕЧАНИЕ

Список установленных в операционной системе программ можно просмотреть и с помощью экземпляров класса Win32_Product, принадлежащего пространству имен root\cimv2. Например, данный класс поддерживает следующие свойства: IdentifyingNumber (ключевое свойство, содержащее CLSID-номер данного установленного продукта), InstallDate2 (определяет дату установки продукта в формате datetime), Name (определяет название продукта), PackageCache (определяет путь к папке или MSI-файлу, который хранит архивную копию установочного пакета продукта).

Кроме того, класс Win32_Product позволяет воспользоваться следующими методами: Admin (устанавливает на компьютере от имени администратора указанный в атрибуте продукт), Install (устанавливает на компьютере указанный в атрибуте продукт), Reinstall (переустанавливает продукт), Uninstall (удаляет продукт, описываемый данным экземпляром класса), Upgrade (обновляет продукт, описываемый данным экземпляром класса).

Окно Программы и компоненты представляет собой аналог окна Установка и удаление программ операционной системы Windows XP. С его помощью можно просмотреть список установленных программ или обновлений, а также удалить определенную программу или обновление. Кроме того, с помощью данного окна можно установить или удалить стандартные компоненты операционной системы.

Основное окно представлено на рис. 3.9. Оно состоит из панели ссылок, содержащей следующие элементы.

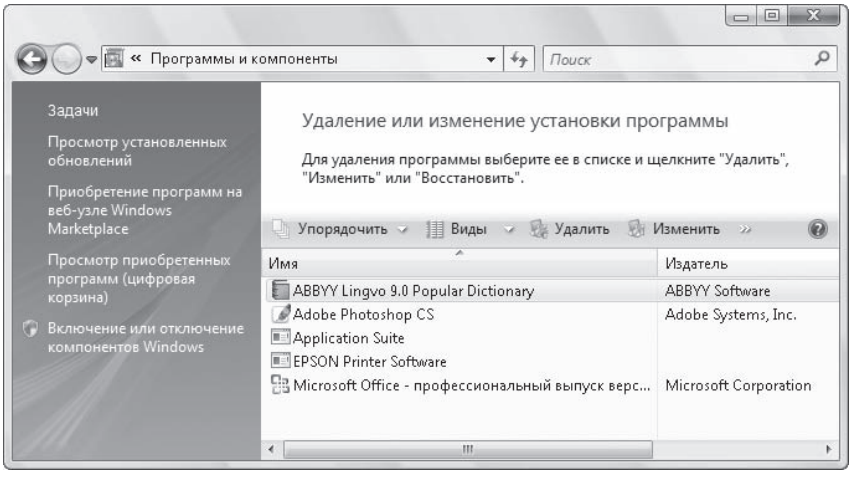


Рис. 3.9. Окно Программы и компоненты

- Просмотр установленных обновлений или Удаление программы — позволяет отобразить список всех установленных в системе программ (Удаление программы) или обновлений (Просмотр установленных обновлений). При этом обратите внимание на элементы контекстного меню установленной программы/обновления или на панель инструментов окна Программы и компоненты. Они будут содержать те операции, которые можно выполнить с установленной программой или обновлением.
  - Удалить — удалить программу или обновление.
  - Изменить — изменить список компонентов программы, которые должны быть установлены.
  - Восстановить — переустановить программу, если по каким-то причинам она не работает.

  Обратите также внимание на панель колонок в списке установленных программ или обновлений. По умолчанию на ней находится только одна колонка — Имя. Однако если вы отобразите контекстное меню панели колонок и выберете команду Больше, то перед вами отобразится окно, где можно определить колонки, которые будут находиться на панели колонок в окне Программы и компоненты. Например, можно отобразить такие сведения об установленной программе, как ее издатель, размер, версия, дата установки, каталог, в который была установлена программа, и многое другое.

- Приобретение программы на веб-узле Windows Marketplace — отображает страницу http://g.msn.com/WMHFUSEN в браузере Internet Explorer. Сайт содержит список программ от разработчиков Microsoft, которые можно скачать и установить.
- Просмотр приобретенных программ (цифровая корзина) — запускает программу Digitall Locker Assistant, которая была описана ранее.
- Включение или отключение компонентов Windows — позволяет запустить программу `optionalfeatures.exe`, с помощью которой можно удалить или установить компоненты операционной системы Windows Vista. Описание данной программы и компонентов операционной системы будет приведено в разд. 9.1.

Хранение сведений об установленных в системе программах и обновлениях

Как и раньше, сведения о программах, установленных в операционной системе Windows, хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`. Каждая установленная вами программа должна создавать свой собственный раздел в данной ветви реестра, название которого не имеет значения. Содержимое этого раздела определяет параметры отображения сведений о программе в окне Программы и компоненты, а также команду, выполняемую при удалении программы, и сами возможности удаления, доступ к которому можно получить с помощью окна Программы и компоненты. Рассмотрим наиболее интересные параметры, которые можно встретить в данной ветви реестра.

- `DisplayName` — параметр строкового типа содержит название, которое будет отображаться в списке установленных программ окна Программы и компоненты и идентифицировать данную программу. Значение этого параметра может переопределяться значением нового параметра реестра `DisplayName_Localized`, который также может находиться в данной ветви реестра.
- `InstallLocation` — строковый параметр хранит путь к каталогу, в который была установлена данная программа. Значение этого параметра может переопределяться значением нового параметра реестра `InstallLocation_Localized`, который также может находиться в данной ветви реестра.
- `UninstallString` — этот параметр строкового типа содержит команду, которая будет выполняться при попытке удаления программы. Значение этого параметра может переопределяться значением нового параметра реестра `UninstallString_Localized`, который также может находиться в данной ветви реестра.
- `ModifyPath` — строковый параметр хранит команду, которая будет выполняться после нажатия кнопки Изменить для данной программы.
- `NoRemove` — если значение этого параметра `REG_DWORD`-типа равно `1`, то кнопка Удалить исчезнет из окна Программы и компоненты для данной программы, то есть вы не сможете ее удалить.
- `NoModify` — при установке значения данного параметра `REG_DWORD`-типа равным `1` кнопка Изменить исчезнет из окна Программы и компоненты для данной программы.

- NoRepair — если значение данного параметра REG_DWORD-типа равно 1, то кнопка Восстановить исчезнет из окна Программы и компоненты для данной программы.
- LogFile — параметр строкового типа хранит путь к файлу журнала, создаваемому при установке или удалении данной программы.

А вот сведения об установленных обновлениях больше не хранятся в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall. Теперь они расположены в ветвях реестра следующего формата: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\<SID>\Products\<номер программы>\Patches\<номер обновления для нее>. Например, в данных ветвях реестра можно встретить следующие параметры.

- DisplayName — параметр строкового типа содержит название, которое будет отображаться в списке установленных обновлений окна Программы и компоненты и идентифицировать данное обновление.
- State — если значение этого параметра REG_DWORD-типа равно 1, то обновление будет отображаться в окне Программы и компоненты. Если же значение равно 0, то обновление в окне Программы и компоненты отображаться не будет.
- Uninstallable — при установке значения данного параметра REG_DWORD-типа равным 1 для данного обновления в окне Программы и компоненты отобразится кнопка Удалить, и вы сможете удалить обновление.

Настройка окна с помощью групповых политик

Возможности окна Программы и компоненты можно ограничить с помощью групповых политик, описанных в файле Programs.admx и расположенных в разделе Конфигурация пользователя ▸ Административные шаблоны ▸ Панель управления ▸ Программы.

Данные групповые политики изменяют значения параметров REG_DWORD-типа, расположенных в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Programs:

- NoInstalledUpdates — если значение параметра равно 1, то страница установленных обновлений отображаться не будет;
- NoDefaultPrograms — при установке значения этого параметра равным 1 страница доступа к программам и параметрам по умолчанию отображаться не будет;
- NoProgramsAndFeatures — если значение данного параметра равно 1, то страница установленных программ отображаться не будет;
- NoGetPrograms — при установке значения этого параметра равным 1 страница установки опубликованных программ отображаться не будет;
- NoProgramsCPL — если значение параметра равно 1, то все возможности, кроме работы с Windows Marketplace, будут запрещены;
- NoWindowsFeatures — при установке значения этого параметра равным 1 страница компонентов операционной системы отображаться не будет;

- `NoWindowsMarketplace` — если значение параметра равно `1`, то ссылка Приобретение программ на веб-узле Windows Marketplace работать не будет.

3.2. Настройка оболочки Windows

Теперь, после того как новый интерфейс и новые возможности Windows Vista вас не пугают, займемся подробным описанием нового интерфейса операционной системы Windows Vista и возможностей его настройки.

Настройка меню Пуск и Панели задач

Новые меню Пуск и Панель задач — это сразу бросается в глаза пользователю, в первый раз вошедшему в операционную систему Windows Vista. Эти элементы оболочки ОС стали намного красивее благодаря появившейся прозрачности и новому общему интерфейсу Windows Vista. Однако найдутся многие пользователи, которым по каким-то причинам не понравится новое меню Пуск и Панель задач. Либо они захотят чего-то большего, либо их компьютер просто слишком слаб для идеального отображения этих элементов. Именно для них операционная система должна предоставлять возможности по настройке меню Пуск или Панели задач. И операционная система Windows Vista такие возможности предоставляет.

ПРИМЕЧАНИЕ

В предыдущих версиях операционной системы Windows репозитарий CIM поддерживал класс Win32_ProgramGroup, принадлежащий пространству имен root\cimv2. С помощью данного класса можно было просмотреть содержимое меню Пуск ▸ Все программы. Больше этот класс не поддерживается.

Работа с меню Пуск

Основным способом настройки меню Пуск является окно Свойства панели задач и меню "Пуск", которое можно отобразить несколькими способами.

- Выбрав команду Свойства из контекстного меню Панели задач.
- Выбрав значок Свойства панели задач и меню "Пуск" в окне Панели управления.
- С помощью команды `rundll32 shell32.dll, Options_RunDLL 3` (при вводе команды обязательно нужно учитывать регистр символов в имени функции, которую вы запускаете; в данной команде названием функции является `Options_RunDLL`). Особенностью данного способа является то, что окно при запуске отображает вкладку Меню "Пуск", которая нам как раз и нужна.

Вкладка Меню "Пуск" окна Свойства панели задач и меню "Пуск"

После отображения окна нужно перейти на вкладку Меню "Пуск", которая как раз и содержит функции настройки меню Пуск (рис. 3.10).

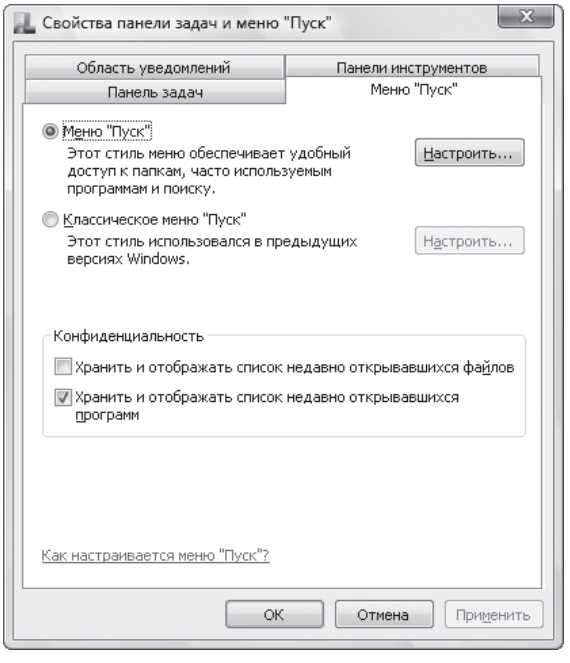


Рис. 3.10. Вкладка Меню "Пуск" окна Свойства панели задач и меню "Пуск"

С помощью данной вкладки можно переключиться между новым интерфейсом меню Пуск и классическим, используемым еще в Windows 2000, а также снять или установить следующие флажки.

- Хранить и отображать список недавно открывавшихся файлов — по умолчанию флажок установлен. Это говорит о том, что операционная система будет хранить и отображать список недавно открывавшихся файлов. Если вы снимете данный флажок, то из меню Пуск исчезнет команда Недавние документы, отображающая список недавно открываемых файлов.
- Хранить и отображать список недавно открывавшихся программ — по умолчанию этот флажок установлен. Это говорит о том, что в меню Пуск будет отображаться список недавно запущенных программ. Этот список отображается в левой части меню Пуск, и, если вы снимете этот флажок, список часто используемых программ исчезнет, и на его место вы сможете поместить ссылки на нужные вам программы (эти ссылки называются фиксированным списком программ).

Настройка нового меню Пуск. Чтобы настроить параметры нового меню Пуск, нужно нажать кнопку Настроить напротив переключателя Меню "Пуск" окна Свойства панели задач и меню "Пуск". После этого отобразится окно Настройка меню "Пуск", с помощью которого можно выполнить следующие операции.

- Указать, сколько элементов будет отображаться в списке Недавние документы, если вы его не отключили. Для этого нужно воспользоваться полем Размер меню "Пуск".

- Указать, будут ли в меню Пуск отображаться ссылки на используемый по умолчанию браузер и почтовый клиент. Для этого нужно воспользоваться флажками области Отображать в меню "Пуск".
- Определить команды, которые будут отображаться в меню Пуск, для чего нужно воспользоваться списком окна Настройка меню "Пуск". С помощью данного списка можно добавить или удалить следующие команды (а также отобразить их как список того, что содержится в папках, на которые они ссылаются): Компьютер, Подключение, Панель управления, Игры, Избранное, Программы по умолчанию, Документы, Справка и поддержка, Музыка, Сеть, Изображения, Поиск, Администрирование, а также команду, ссылающуюся на каталог %userprofile%.

  С помощью этого списка можно также отредактировать следующие настройки меню Пуск.

  - Разрешить контекстное меню и перетаскивание объектов — по умолчанию флажок установлен, и это говорит о том, что вы можете пользоваться операциями Drag & Drop для перемещения ярлыков в меню Пуск ▸ Все программы. После снятия флажка вы больше не сможете самостоятельно редактировать меню Пуск ▸ Все программы.
  - Выделять недавно установленные программы — по умолчанию установлен, и это говорит о том, что ссылки на недавно установленные программы, расположенные в меню Пуск ▸ Все программы, будут отображаться другим цветом. Как правило, это только мешает ориентированию в меню Пуск ▸ Все программы, особенно если вы привыкнете пользоваться встроенным в меню Пуск поисковиком.
  - Раскрывать меню при наведении и задержке указателя мыши — флажок по умолчанию установлен. Это говорит о том, что операционная система будет раскрывать списки меню Пуск, если вы задержите на некоторое время над ними указатель мыши.
  - Флажки Поиск в избранном и журнале обзора и Поиск программ — по умолчанию встроенный поисковик меню Пуск производит поиск в меню Пуск ▸ Все программы, среди сетевых подключений, а также в списках Избранного и недавно открытых документах, однако, сняв эти флажки, можно исключить поиск в определенной категории меню Пуск.
  - Сортировка меню "Все программы" по именам — по умолчанию флажок установлен, и это говорит о том, что содержимое списка Пуск ▸ Все программы будет сортироваться по названиям.
  - Крупные значки — флажок по умолчанию установлен. Это говорит о том, что в меню Пуск будут отображаться большие значки программ. Снятие флажка приведет к использованию в меню Пуск (в фиксированном списке программ и в списке часто используемых программ) маленьких значков, однако размер меню Пуск от этого не изменится. Хотя увеличится количество программ, которые вы сможете поместить в фиксированный список меню Пуск.

Настройка классического меню Пуск. Если вам больше нравится классическое меню Пуск, то для перехода на него нужно в окне Свойства панели задач и меню "Пуск"

установить переключатель в положение Классическое меню "Пуск". К сожалению, классическое меню Пуск не поддерживает прозрачности интерфейса Windows Aero (рис. 3.11).

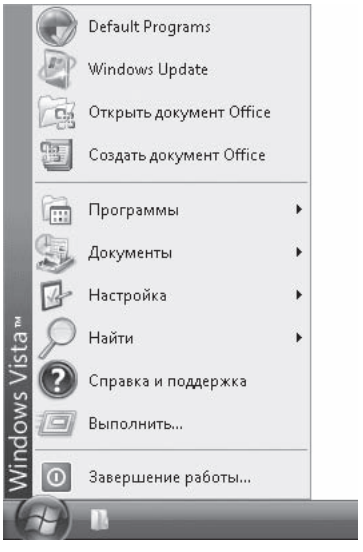


Рис. 3.11. Классическое меню Пуск

Чтобы настроить параметры классического меню Пуск, нужно нажать кнопку Настроить напротив переключателя Классическое меню "Пуск". После этого отобразится окно Настройка классического меню "Пуск", с помощью которого можно выполнить следующие операции.

- Отредактировать и отсортировать содержимое списка Пуск ▸ Все программы. Для этого применяются кнопки области Меню "Пуск".

ПРИМЕЧАНИЕ

Область Меню "Пуск" содержит кнопку Удалить, с помощью которой можно быстро удалить ненужные элементы меню. Непонятно, почему эта кнопка доступна только при использовании классического меню Пуск, ведь найдутся пользователи, которые с удовольствием пользовались бы ей и при работе с новым меню Пуск.

Если вы используете новое меню Пуск и при этом желаете пользоваться окном для быстрого удаления содержимого меню, то вам может быть полезно знание команды rundll32.exe appwiz.cpl, ConfigStartMenu. Она отображает именно это окно.

- Очистить список недавно открывавшихся документов (меню Пуск ▸ Документы). Для этого нужно нажать кнопку Очистить.
- Отредактировать содержимое меню Пуск. Для этого нужно воспользоваться списком Дополнительные параметры меню "Пуск". С его помощью можно настроить отображение следующих элементов классического меню Пуск: Администра-

тивные шаблоны, Избранное, Завершение сеанса, Выполнить. Также с его помощью можно отобразить в виде ссылок такие элементы классического меню Пуск, как Панель управления, Документы, Сетевые подключения, Изображения, Принтеры.

С помощью данного списка можно также настроить следующие параметры классического меню Пуск: поддержку операций Drag & Drop меню Пуск ▸ Все программы, отображение маленьких значков, а также использование персонализированного меню Пуск ▸ Все программы (это когда из меню скрываются все элементы, которыми вы долго не пользовались, а в самом низу меню отображается стрелка, с помощью которой скрытые элементы можно отобразить) и прокрутки, если меню не помещается на экране компьютера.

Настройка меню Пуск с помощью групповых политик

Еще одним компонентом операционной системы Windows Vista, с помощью которого можно настроить меню Пуск, является оснастка `gpedit.msc`. Благодаря ей осуществляется доступ к групповым политикам, которые можно применить к компьютеру. Групповые политики — это набор параметров реестра, ограничивающих или более тонко настраивающих интерфейс операционной системы или входящих в нее компонентов. Более подробно групповые политики будут рассматриваться в гл. 5, а пока перечислю те из них, которые влияют на параметры работы меню Пуск.

Все они хранятся в файле `StartMenu.admx` и расположены в подразделе Конфигурация пользователя ▸ Административные шаблоны ▸ Меню «Пуск» и панель задач оснастки `gpedit.msc` (рис. 3.12). Чтобы изменить настройки какой-нибудь групповой политики, нужно дважды щелкнуть на ней кнопкой мыши и в появившемся окне задать значение групповой политики. Как правило, можно задать следующие значения групповой политики: Не задана, Включена, Отключена. Значение Не задана приводит к удалению параметра, который изменяется с помощью данной политики, из реестра. Значение Включена, как правило, приводит к установке политики (присвоение соответствующему параметру реестра значения `1`). Значение Отключена, как правило, приводит к противоположному действию (присвоение соответствующему параметру реестра значения `0`).

В окне Редактор объектов групповой политики можно также прочитать подробное описание того, что делает данная групповая политика (на вкладке Расширенный).

Все эти политики изменяют значения параметров `REG_DWORD`-типа, расположенных в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`. Рассмотрим наиболее интересные из этих параметров.

- `ClearRecentDocsOnExit` — если значение параметра равно `1`, то при выходе пользователя из системы список недавно открывавшихся документов будет очищаться.
- `NoSMBalloonTip` — при установке значения равным `1` не будут отображаться всплывающие подсказки области уведомлений и некоторые подсказки меню Пуск.
- `NoClose` — если значение этого параметра равно `1`, то из меню Пуск, а также из окна завершения работы Windows будут удалены команды Завершение работы, Перезагрузка, Сон, Гибернация.

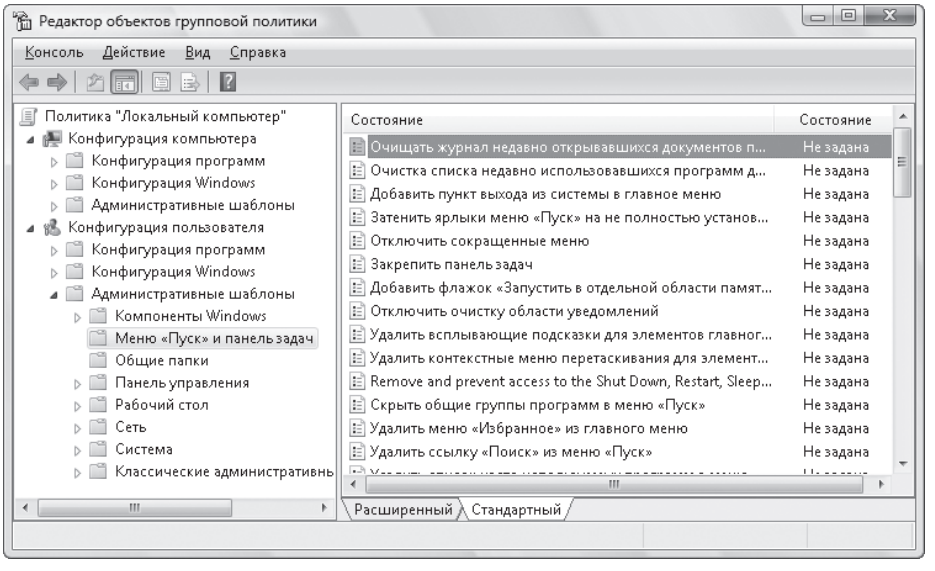


Рис. 3.12. Меню Пуск, настроенное с помощью оснастки gpedit.msc

- `NoCommonGroups` — при установке значения равным `1` в меню Пуск не будет отображаться содержимое, определенное в общей для всех папке. Также из контекстного меню, отображаемого при нажатии кнопки Пуск, будут удалены команды Открыть общее для всех меню и Проводник в общее для всех меню.
- `NoStartMenuMorePrograms` — если значение параметра равно `1`, то из меню Пуск будет удален список Все программы.
- `NoStartMenuPinnedList` — при установке значения равным `1` из меню Пуск будет удален список закрепленных программ. Например, к ним относятся отображаемые по умолчанию ссылки на почтовый клиент и браузер.
- `NoSetFolders` — если значение этого параметра равно `1`, то кнопки Панель управления, Принтеры и Подключение из меню Пуск будут удалены.
- `NoSimpleStartMenu` — при установке значения равным `1` пользователю будет разрешено использовать только классическое меню Пуск.
- `NoStartMenuEjectPC` — если значение данного параметра равно `1`, то кнопка Отстыковка ПК не будет отображаться в меню Пуск. Эта кнопка отображается при использовании операционной системы на ноутбуке, который в данное время подключен к док-станции (специальное оборудование, которое идет в поставку ноутбуков и расширяет их возможности).

Настройка меню Пуск с помощью реестра и других малоизвестных возможностей

Мы рассмотрели все стандартные возможности настройки меню Пуск, присутствующие в операционной системе Windows Vista. Но поскольку эта книга рассчитана на опытных пользователей, стандартные возможности являются лишь вершиной айсберга, в которой вы, без сомнения, разбирались и до приобретения этой книги.

Сейчас же рассмотрим возможности Windows Vista, о которых IT-специалисты корпорации Microsoft говорят мало либо вообще не говорят, считая их внутренним механизмом работы операционной системы.

Данная глава, как и все остальные главы этой книги, предназначенные для опытных пользователей, будет сформирована как справочник по возможностям настройки меню Пуск. Иначе говоря, сначала будет описываться сама возможность настройки, а потом то, как это сделать.

Скрытие кнопки блокирования компьютера. Как вы уже знаете, в новом меню Пуск напротив панели поиска присутствуют две кнопки: выключения компьютера и его блокирования. Как правило, домашним пользователям ни к чему возможность блокирования компьютера, поэтому ее можно отключить. После этого исчезнет как кнопка из меню Пуск, так и сама возможность блокировки с помощью списка выключения компьютера, что не намного, но повышает производительность работы с меню Пуск. При этом сама функциональность операционной системы нисколько не снижается — вы и дальше сможете выполнять блокирование компьютера с помощью комбинации клавиш Windows+L.

Чтобы скрыть кнопку блокировки компьютера из меню Пуск, нужно присвоить параметру `REG_DWORD`-типа `DisableLockWorkstation`, расположенному в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`, значение равное `1`. Следует признать, что этот параметр можно изменять и с помощью групповых политик, но перед этим его пришлось бы там еще найти. Но из-за большого количества политик в последнее время это является довольно сложной задачей.

Изменение задержки перед сменой изображений команд в новом меню Пуск. Не всем пользователям понравится механизм изменения изображения, расположенного сверху меню Пуск операционной системы Windows Vista, — оно меняется при наведении указателя мыши на какую-нибудь команду. Кому-то этот механизм покажется довольно медленным, кому-то — слишком неуклюжим или затормаживающим и без того слабый компьютер, а кому-то просто понравится картинка пользователя, располагающаяся в новом меню Пуск в качестве изображения по умолчанию (кстати, если щелкнуть на ней кнопкой мыши, то откроется окно Учетные записи пользователей). Если вы один из таких пользователей, то сейчас узнаете, как можно изменить механизм вывода изображения меню Пуск.

Для этого придется изменить три параметра типа `REG_DWORD` (по умолчанию они не существуют, поэтому их нужно создать), расположенные в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage`. Это следующие параметры: `StartPanel_FadeDelay`, `StartPanel_FadeIn` и `StartPanel_FadeOut`.

Параметр `StartPanel_FadeDelay` определяет задержку перед сменой изображений. Например, если вы не хотите, чтобы изображения вообще сменялись, то этому параметру нужно присвоить значение `0xffffffff`. После перезагрузки оболочки в новом меню Пуск всегда будет выводиться изображение вашей картинки. В противном случае укажите в этом параметре время в миллисекундах, на которое

пользователь должен задержать указатель мыши на команде из меню Пуск, чтобы изображение окончательно изменилось.

Остальные два параметра определяют время перехода одного изображения в другое. Вы, наверное, заметили, что при изменении изображения новая картинка как бы проступает среди старого изображения (последовательно изменяется прозрачность старого и нового изображений). На первых этапах работы с операционной системой этот эффект может восхищать пользователя, но потом его просто не замечаешь. Чтобы не загружать операционную систему лишними эффектами, параметрам `StartPanel_FadeIn` и `StartPanel_FadeOut` можно присвоить значение `0`. После этого одно изображение будет сменяться другим немедленно (точнее, после истечения времени, указанного в параметре `StartPanel_FadeDelay`). А можно и более тонко настроить время перехода, добившись более четкого и красивого эффекта. В этом случае в этих параметрах нужно указать время перехода в миллисекундах.

Отключение индексирования содержимого меню Пуск. По умолчанию содержимое меню Пуск индексируется для возможности выполнения в нем поиска. Вообще, это довольно спорная возможность. Зачем вообще искать в меню Пуск, если там хранятся одни ярлыки?

Чтобы не загружать операционную систему лишними действиями, возможность индексации меню Пуск можно отключить. Для этого нужно присвоить параметру `REG_DWORD`-типа `StartMenuIndexed`, расположенному в ветви системного реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage`, значение равное `0`.

Редактирование списка программ меню Пуск, которые никогда не попадут в список часто используемых. Иногда бывает необходимо запретить добавление программы, которой вы часто пользуетесь, в список нового меню Пуск. В Windows Vista это делается так же, как и в ее предшественнице Windows XP.

Для этого нужно обратиться к ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileAssociation`. Она хранит два параметра строкового типа: `AddRemoveApps` и `AddRemoveNames`. Первый из них определяет названия программ, которые не будут отображаться в меню Пуск, а второй — слова, которые не должны содержаться в названиях, отображаемых в меню Пуск.

Запретить отображение определенной программы в меню Пуск можно и с помощью ветви реестра `HKEY_CLASSES_ROOT\Applications\<имя программы>`. Для этого в ней нужно создать параметр строкового типа `NoStartPage`, не содержащий никакого значения.

Изменение команд меню Пуск. Если вам надоело, что команда, отображающая, например, папку Мой компьютер, всегда называется Компьютер, то можно попробовать изменить название некоторых команд, расположенных в новом меню Пуск, с помощью реестра. Стоит только учесть, что названия этих команд изменятся не только в меню Пуск, но и во всей оболочке Windows Vista.

Чтобы это сделать, нужно изменить значение параметра (По умолчанию), введя в него то название, которое вам нужно. При этом следует учесть, что в соответствующей ветви системного реестра не должно быть параметра REG_EXPAND_SZ-типа LocalizedString. В противном случае этот параметр нужно удалить, так как он переопределяет значение параметра (По умолчанию) (или просто изменить значение не параметра (По умолчанию), а параметра LocalizedString). Итак, изменить значение параметра (По умолчанию) можно в следующих ветвях реестра, определяющих значки, отображающиеся в меню Пуск:

- HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D} — изменяет название значка Компьютер;
- HKEY_CLASSES_ROOT\CLSID\{ED228FDF-9EA8-4870-83b1-96b02CFE0D52} — изменяет название значка Игры.

Изменение команд Свойства Интернета контекстного меню значков почтового клиента и браузера в меню Пуск. Раз уж мы решили полностью настроить содержимое меню Пуск, то нельзя упустить такой возможности как изменение команды, которая выполняется при выборе элемента Свойства Интернета контекстного меню значков нового меню Пуск, указывающих на почтовый клиент и браузер. Действительно, уже то, что по умолчанию эти команды отображают одно и то же окно — Свойства: Интернет, должно вызвать недовольство.

Чтобы изменить название элемента Свойства Интернета и команду, которую он вызывает, нужно воспользоваться следующими параметрами реестра, имеющими строковый тип: Propertiestext и Properties. Первый параметр изменяет название элемента Свойства Интернета, а второй — запускаемую программу. Оба параметра находятся в следующих ветвях реестра:

- HKEY_CLASSES_ROOT\CLSID\{2559a1f4-21d7-11d4-bdaf-00c04f60b9f0}\Instance\InitPropertyBag — определяет команду значка браузера;
- HKEY_CLASSES_ROOT\CLSID\{2559a1f5-21d7-11d4-bdaf-00c04f60b9f0}\Instance\InitPropertyBag — определяет команду значка почтового клиента.

Но и это еще не все. Вы можете добавить свои собственные команды к контекстному меню значков нового меню Пуск, указывающих на почтовый клиент и браузер. Для этого достаточно воспользоваться ветвями реестра HKEY_CLASSES_ROOT\CLSID\{2559a1f4-21d7-11d4-bdaf-00c04f60b9f0} и HKEY_CLASSES_ROOT\CLSID\{2559a1f5-21d7-11d4-bdaf-00c04f60b9f0} (соответственно, для добавления команд к контекстному меню браузера и почтового клиента). В этих ветвях нужно создать подраздел shell, а в нем — дочерние подразделы, название которых не важно. Сколько подразделов вы создадите, столько новых команд и появится в контекстном меню. Параметру (По умолчанию) созданных подразделов нужно присвоить название нового элемента контекстного меню. После этого в созданных подразделах нужно создать подраздел command, а его параметр (По умолчанию) должен содержать команду, которая будет запускаться при

выборе этого элемента контекстного меню. Для примера в листинге 3.1 приведена часть REG-файла, определяющего контекстное меню, представленное на рис. 3.13.

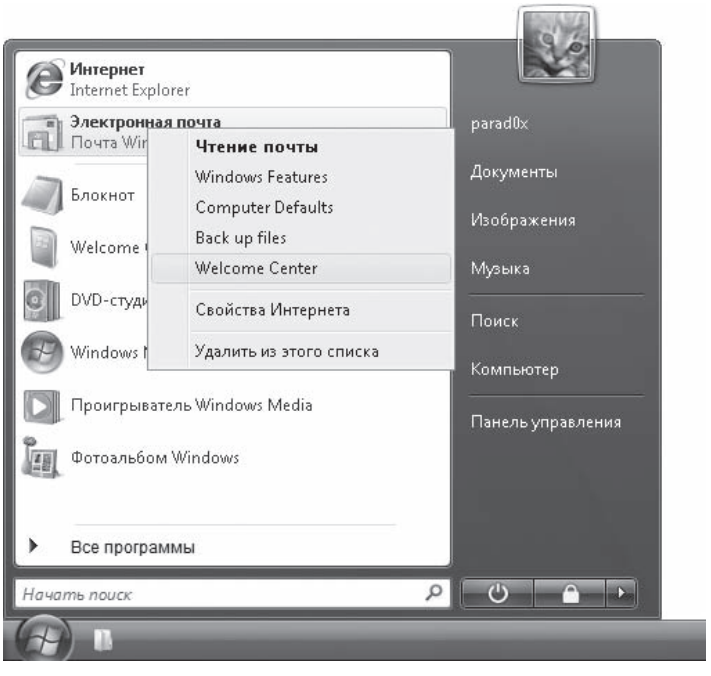


Рис. 3.13. Создаем контекстное меню для значка почтового клиента, а также изменяем названия команд меню Пуск

Листинг 3.1. Контекстное меню, представленное на рис. 3.13

```
REGEDIT4

[HKEY_CLASSES_ROOT\CLSID\{2559a1f5-21d7-11d4-bdaf-00c04f60b9f0}\shell]

[HKEY_CLASSES_ROOT\CLSID\{2559a1f5-21d7-11d4-bdaf-00c04f60b9f0}\shell\1]
@="Windows Features"

[HKEY_CLASSES_ROOT\CLSID\{2559a1f5-21d7-11d4-bdaf-00c04f60b9f0}\shell\1\command]
@="rundll32.exe appwiz.cpl, RunOCMW"

[HKEY_CLASSES_ROOT\CLSID\{2559a1f5-21d7-11d4-bdaf-00c04f60b9f0}\shell\2]
@="Computer Defaults"

[HKEY_CLASSES_ROOT\CLSID\{2559a1f5-21d7-11d4-bdaf-00c04f60b9f0}\shell\2\command]
@="rundll32.exe \"appwiz.cpl\", RunSPADW"

[HKEY_CLASSES_ROOT\CLSID\{2559a1f5-21d7-11d4-bdaf-00c04f60b9f0}\shell\3]
```

```
@="Back up files"

[HKEY_CLASSES_ROOT\CLSID\{2559a1f5-21d7-11d4-bdaf-00c04f60b9f0}\shell\3\command]
@="rundll32.exe \"brcpl.dll\", ExecuteBackupAppTask RunBackup"

[HKEY_CLASSES_ROOT\CLSID\{2559a1f5-21d7-11d4-bdaf-00c04f60b9f0}\shell\4]
@="Welcome Center"

[HKEY_CLASSES_ROOT\CLSID\{2559a1f5-21d7-11d4-bdaf-00c04f60b9f0}\shell\4\command]
@="rundll32.exe \"oobefldr.dll\", ShowWelcomeCenter"
```

Настройка Панели задач

Как и меню Пуск, Панель задач настраивается с помощью окна Свойства панели задач и меню "Пуск". Для этого оно содержит вкладки Область уведомлений, Панели инструментов и Панель задач.

ПРИМЕЧАНИЕ

Переходить между задачами, отображаемыми в Панели задач, можно с помощью комбинации клавиш Windows+T.

Окно Свойства панели задач и меню "Пуск"

С помощью вкладки Панель задач можно изменить следующие параметры работы Панели задач.

ПРИМЕЧАНИЕ

Окно Свойства панели задач и меню "Пуск", открытое на вкладке Панели инструментов, можно отобразить с помощью команды rundll32.exe shell32.dll, Options_RunDLL 6.

- Закрепить панель задач — установка этого флажка блокирует возможность изменения размера и местоположения находящихся на Панели задач стандартных панелей инструментов. После его установки вы также не сможете изменить высоту Панели задач.
- Автоматически скрывать панель задач — после установки данного флажка Панель задач будет автоматически скрываться с экрана, если на нее не наведен указатель мыши.
- Отображать панель задач поверх остальных окон — установив этот флажок, вы дадите команду всегда располагать Панель задач поверх всех окон.
- Группировать сходные кнопки панели задач — после установки данного флажка все кнопки Панели задач, определяющие окна одной и той же программы, при нехватке места на Панели задач будут объединяться в одну.

- Отображать панель быстрого запуска — позволяет отобразить на Панели задач область уведомлений (отображается справа от кнопки Пуск и содержит ярлыки для часто используемых программ).
- Отображать образцы окон (эскизы) — позволяет управлять использованием новой функции Windows Vista (эта функция называется технологией Live Taskbar). По умолчанию (флажок установлен) при удерживании указателя мыши над кнопкой Панели задач перед вами отобразится эскиз страницы, которую можно вывести после нажатия данной кнопки (рис. 3.14). Если снять этот флажок, то эскиз страницы отображаться не будет.

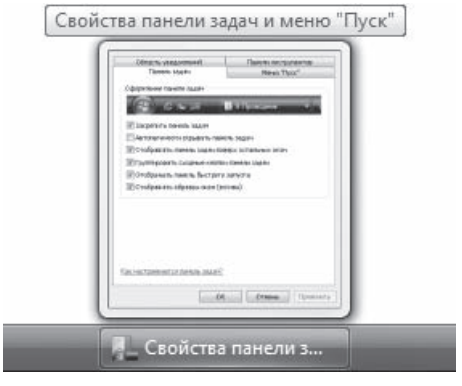


Рис. 3.14. Эскиз окна

С помощью вкладки Область уведомлений можно выполнить следующие действия.

ПРИМЕЧАНИЕ

Окно Свойства панели задач и меню "Пуск", открытое на вкладке Меню "Пуск", можно отобразить с помощью команды rundll32.exe shell32.dll, Options_RunDLL 4.

- Включить механизм скрытия долго не используемых значков области уведомлений. После его включения на данной вкладке активизируется кнопка Настроить. С ее помощью можно определить значки области уведомлений, которые всегда будут отображаться, независимо от того, как долго они не используются. Это же окно можно отобразить, воспользовавшись командой `rundll32 shell32.dll, Options_RunDLL 5`.
- Указать, будут ли в области уведомлений отображаться значки часов, звука, сетевой активности и питания компьютера (только для ноутбуков).

С помощью вкладки Панели инструментов можно определить, какие стандартные панели инструментов будут отображаться на Панели задач. В Windows Vista доступны следующие панели инструментов: Адрес (отображает адресную строку), Проигрыватель Windows Media (отображает панель управления проигрывателем), Связи (отображает содержимое каталога `%userprofile%\Favorites\Links`),

Планшетный ПК — панель ввода (отображает соответствующую кнопку), Рабочий стол (отображает содержимое Рабочего стола пользователя) и Быстрый запуск (панель быстрого запуска).

Используемые панели инструментов можно указать с помощью списка Панели инструментов контекстного меню Панели задач. Кроме того, с помощью данного списка можно создать свою собственную панель инструментов на основе содержимого определенной папки.

Настройка с помощью групповых политик

Вторым шагом настройки Панели задач может быть использование возможностей групповых политик. Большинство из этих возможностей описаны в файле `Taskbar.admx` и хранятся в уже известном вам разделе групповых политик Конфигурация пользователя ▸ Административные шаблоны ▸ Меню «Пуск» и панель задач.

Политики данного раздела изменяют параметры `REG_DWORD`-типа, расположенные в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`. Рассмотрим основные из них.

- `NoAutoTrayNotify` — если значение данного параметра равно `1`, то будет запрещена возможность скрытия неиспользуемых значков в области уведомлений.
- `NoSetTaskbar` — при установке значения этого параметра равным `1` будет запрещено отображать окно Свойства панели задач и меню "Пуск".
- `NoToolbarsOnTaskbar` — если значение параметра равно `1`, то на Панели задач будет запрещено отображение панелей инструментов.
- `NoTrayContextMenu` — при установке значения этого параметра равным `1` не будет отображаться контекстное меню для Панели задач и ее элементов.
- `NoTrayItemsDisplay` — если значение параметра равно `1`, то в области уведомлений не будут отображаться уведомления — останутся только часы.
- `TaskbarNoAddRemoveToolbar` — при установке значения этого параметра равным `1` на Панели задач будут отображаться уже добавленные панели инструментов, однако добавление дополнительных или удаление уже отображаемых панелей инструментов будет запрещено.
- `TaskbarNoDragToolbar` — если значение параметра равно `1`, то пользователю будет запрещено перетаскивать на Панель задач панели инструментов.
- `TaskbarNoNotification` — при установке значения этого параметра равным `1` в области уведомлений не будут выводиться всплывающие уведомления.
- `TaskbarNoRedock` — если значение параметра равно `1`, то пользователю будет запрещено выполнять перемещение Панели задач в другой угол экрана.

Настройка Панели задач с помощью реестра и других малоизвестных возможностей

Поговорим о малоизвестных возможностях настройки Панели задач и стандартных панелей инструментов.

Изменение названия папки, содержимое которой отображает панель инструментов Связи. С помощью панели инструментов Связи на Панели задач можно создать еще один раскрывающийся список, содержащий, например, ярлыки для запуска программ или команд `rundll32` (новые команды `rundll32.exe` операционной системы Windows Vista приведены в приложении 1). Единственное, что может огорчить пользователя, который очень рьяно следит за свободным местом на Панели задач, так это само слово Связи, которое отображается на ней и занимает намного больше места, чем сама панель инструментов. К счастью, с помощью реестра можно изменить название каталога, содержимое которого отображается панелью Связи, а следовательно, и название, которое отображается на Панели задач.

Для этого нужно создать параметр строкового типа `LinkFolderName`, расположенный в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion`, и присвоить ему название новой панели инструментов. Например, данному параметру можно присвоить значение `'`. После этого будет создана новая папка (с названием, которое вы указали в параметре `LinkFolderName`) в каталоге `%userprofile%\Favorites`. Теперь осталось только заполнить ее содержимым и отобразить панель инструментов Связи. На рис. 3.15, *слева*, приведен вариант такого примера.

Но если вы не хотите создавать раскрывающийся список на Панели задач и при этом не очень сильно дорожите свободным местом на ней, то всегда можно написать там для себя ободряющее сообщение. При этом, чтобы в каталоге `%userprofile%\Favorites` не создавалось никакой папки, нужно присвоить параметру `REG_DWORD`-типа `ShowTaskFolder`, расположенному в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar`, значение `1` (рис. 3.15, *справа*).

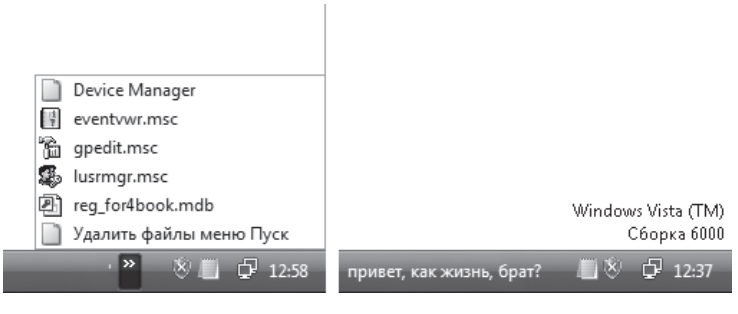


Рис. 3.15. Варианты использования панели инструментов Связи

Использование языковой панели. В операционной системе Windows XP список Панели инструментов контекстного меню Панели задач содержал возможность создания еще одной панели инструментов — Языковой панели. В Windows Vista по умолчанию отсутствует этот элемент списка. Он появится, лишь когда вы добавите языковую панель. Языковую панель по-прежнему можно отобразить с помощью окна Язык и региональные стандарты, доступ к которому можно получить с помощью Панели управления. В данном окне нужно перейти на вкладку Языки и клавиатуры и нажать кнопку Настройки, после чего отобразится еще одно окно — Языки и службы

текстового ввода. В нем нужно перейти на вкладку Языковая панель и переключатель Языковая панель установить в положение Располагается в произвольном месте рабочего стола, чтобы языковая панель отобразилась на Рабочем столе (рис. 3.16, *слева*).

ПРИМЕЧАНИЕ

Диалоговое окно Языки и службы текстового ввода можно вызвать и с помощью команды rundll32.exe MSCTF.dll, TF_RunInputCPL.

Теперь поговорим о возможностях дополнительной настройки языковой панели с помощью реестра. Все параметры языковой панели хранятся в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\CTF` и ее подразделах.

Непосредственно в этой ветви содержится параметр `REG_DWORD`-типа `ShowTipbar`. Если его значение равно `0`, то вы не сможете отобразить языковую панель, а также значок языка в области уведомлений.

Остальные параметры, доступ к которым нельзя получить с помощью контекстного меню языковой панели, хранятся в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\CTF\MSUTB`. Среди них наиболее интересными являются параметры `REG_DWORD`-типа `ShowDebugMenu` и `NewLook`.

Если значение первого параметра равно `1`, то вместо обычного контекстного меню языковой панели сначала будет отображаться отладочное. Оно содержит две команды. С помощью команды `Close cicload` можно завершить работу программы `ctfmon.exe` (она как раз и отвечает за отображение языковой панели и значка языка в области уведомлений). А с помощью команды Отмена можно отобразить стандартное контекстное меню языковой панели.

Если значение второго параметра равно `0`, то цвет языковой панели изменится на белый, что красиво смотрится на белом фоне (рис. 3.16, *справа*).



Рис. 3.16. Две версии языковой панели

Если вы и дальше будете использовать языковую панель, то можно добавить команду Языковая панель в список Панели инструментов контекстного меню Панели задач. Для этого достаточно создать в ветви реестра `HKEY_CLASSES_ROOT\CLSID\{540D8A8B-1C3F-4E32-8132-530F6A502090}` раздел `Implemented Categories`, а в этом разделе — подраздел `{00021492-0000-0000-C000-000000000046}`.

Раз уж мы затронули вопрос добавления языковой панели к списку Панели инструментов контекстного меню Панели задач, то нужно еще упомянуть, что вы

можете изменить ее название. Для этого достаточно в параметре строкового типа MenuTextPUI, расположенном в ветви реестра HKEY_CLASSES_ROOT\CLSID\{540D8A8B-1C3F-4E32-8132-530F6A502090}, указать новое название.

Удаление элементов списка Панели инструментов контекстного меню Панели задач. Закрепим полученные в предыдущем разделе знания. Чтобы удалить из списка Панели инструментов определенный элемент, нужно в ветви реестра HKEY_CLASSES_ROOT\CLSID\{CLSID-номер ActiveX-объекта, отображаемого в списке}\Implemented Categories удалить подраздел {00021492-0000-0000-C000-000000000046}. По умолчанию в списке Панели инструментов отображаются следующие ActiveX-объекты.

- {01E04581-4EEE-11D0-BFE9-00AA005B4383} — определяет отображение панели инструментов Адрес.
- {0A4286EA-E355-44FB-8086-AF3DF7645BD9} — определяет отображение панели инструментов Проигрыватель Windows Media.
- {0E5CBF21-D15F-11D0-8301-00AA005B4383} — определяет отображение панели инструментов Связи.
- {8B4A02DB-97BB-4C1B-BE75-8827A7358CD0} — определяет отображение панели инструментов Планшетный ПК — панель ввода.

Настройка Рабочего стола пользователя

Возможности настройки Рабочего стола в Windows Vista не сильно изменились по сравнению с Windows XP. Тем не менее, изменился способ доступа к этим возможностям. Теперь, если вы выберете контекстное меню Рабочего стола, то больше не увидите в нем команды Свойства. Ее место заняла команда Персонализация, после выбора которой перед вами отобразится одноименное окно.

ПРИМЕЧАНИЕ

Как и в предыдущих версиях операционной системы Windows, настройки Рабочего стола можно изменить с помощью класса Win32_Desktop, принадлежащего пространству имен root\cimv2. Например, данный класс поддерживает следующие свойства: BorderWidth (определяет ширину границы окна), CursorBlinkRate (определяет частоту мигания курсора при работе с текстом (в миллисекундах)), DragFullWindows (определяет, отображается ли содержимое окна при перетаскивании), IconSpacing (определяет расстояние между значками), IconTitleFaceName (определяет название шрифта значков), Name (ключевое свойство, определяющее компьютер и имя пользователя, которому принадлежат данные настройки Рабочего стола), ScreenSaverActive (определяет, включено ли отображение заставки), ScreenSaverExecutable (определяет путь к файлу заставки), Wallpaper (определяет путь к файлу обоев Рабочего стола).

Раз уж мы заговорили о контекстном меню Рабочего стола, то нельзя не упомянуть о новой возможности Windows Vista. Теперь с помощью команды Вид контекстного меню можно изменять размер значков, расположенных на Рабочем столе.

Окно Персонализация

Окно Персонализация представлено на рис. 3.17.

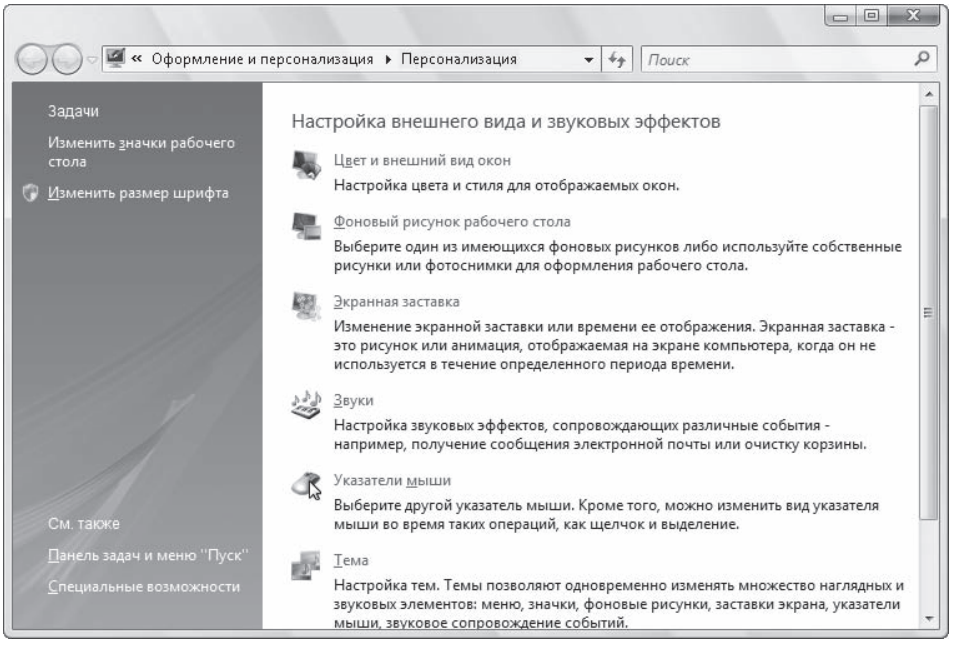


Рис. 3.17. Окно Персонализация

ПРИМЕЧАНИЕ

Если значение параметра REG_DWORD-типа NoDispCPL, расположенного в ветви HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System, равно 1, то окно Персонализация будет содержать только две работающие ссылки: Звуки и Указатели мыши.

Параметры дисплея

Отображает вкладку Параметры (в Windows Vista она называется Монитор) окна Свойства: Экран, известного пользователям операционных систем Windows XP. С помощью данной вкладки вы сможете выбрать используемый по умолчанию монитор, а также настроить разрешение экрана и глубину цвета. Если же вы нажмете кнопку Дополнительно данного окна, то также сможете выполнить следующие действия:

- отобразить окно Свойства для установленной графической карты;
- просмотреть все режимы (сочетания разрешения экрана, глубины цвета и частоты обновления экрана), которые доступны для вашей графической карты и монитора;
- изменить частоту обновления экрана;

- выполнить другие настройки, которые предоставляет драйвер вашей видеокарты и монитора.

ПРИМЕЧАНИЕ

Если значение параметра REG_DWORD-типа NoDispSettingsPage, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System, равно 1, то данная возможность окна Персонализация работать не будет.

Операционная система Windows Vista поддерживает команду rundll32.exe IEAKENG.dll, ShowDeskCpl. Она вызывает окно Специальные возможности. Перед вызовом данного окна команда устанавливает в 1 параметры ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System, тем самым запрещая доступ к окну. После своей работы команда восстанавливает значения этих параметров.

Цвет и внешний вид окна

Это единственное окно, с помощью которого можно управлять настройками нового интерфейса Windows Aero. К сожалению, оно содержит не очень много настроек. Единственное, что можно сделать с его помощью, — изменить цвет окантовки окон Проводника, а также их прозрачность. Для этого служит специальный ползунок, изменяющий прозрачность, а также несколько предопределенных цветовых решений интерфейса Windows Vista.

ПРИМЕЧАНИЕ

Если значение параметра REG_DWORD-типа NoDispAppearancePage, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System, равно 1, то данная возможность окна Персонализация работать не будет.

Предопределенные цвета, которые можно использовать в окне Персонализация, хранятся в подразделах ветви реестра HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\Glass Colorization\Swatches. Вы можете изменить их с помощью параметра REG_DWORD-типа Color. А с помощью параметра REG_DWORD-типа PreviewId можно изменить порядок следования предопределенных цветов. Например, только так можно изменить цвет, используемый операционной системой по умолчанию.

Кроме того, если вы нажмете кнопку Показать настройку цветов окна, то сможете самостоятельно задать цвет окон Проводника.

Окно также содержит ссылку Открыть свойства классического внешнего вида для выбора других возможностей. С ее помощью можно открыть окно Параметры оформления. Оно напоминает стандартную вкладку Оформление окна Свойства: Экран операционной системы Windows XP. С его помощью можно решить следующие задачи.

- Изменить цветовую схему оформления оболочки. Особо следует обратить внимание на первые четыре схемы. По умолчанию используется схема Windows

Аэро, которая включает интерфейс Aero Glass. Но если вы не хотите использовать этот интерфейс, то можно воспользоваться другими цветовыми схемами. Например, схемой Windows Vista — упрощенный стиль, которая отключает интерфейс Aero Glass и все его возможности, но оставляет стандартное оформление Windows Vista. Или схемой Стандартная, которая не только отключает интерфейс Aero Glass, но и изменяет цветовое оформление, преобразуя интерфейс Windows Vista в интерфейс предыдущих операционных систем семейства Windows. Также можно воспользоваться цветовой схемой Классическая, которая аналогична схеме Стандартная, но использует более темный цвет окон.

- Изменить следующие дополнительные эффекты.
  - Определить метод сглаживания экранных шрифтов (без сглаживания, сглаживание Обычный, предназначенное для ЭЛТ-мониторов, или сглаживание ClearType, предназначенное для TFT-мониторов). Операционная система Windows Vista поддерживает следующие шрифты, специально созданные для применения сглаживания ClearType: Constantia, Cambria, Corbel, Calibri, Candara и Consolas.
  - Убрать тени вокруг раскрывающихся списков меню. Прорисовка теней также загружает компьютер и занимает определенное время перед отображением списка меню, поэтому их можно отключить с целью повышения быстродействия работы оболочки Windows Vista.
  - Указать, чтобы при перемещении окна не отображалось его содержимое. Благодаря этому существенно снижается нагрузка на процессор компьютера, но следует обратить внимание, что в Windows Vista при перемещении не будет отображаться даже рамка окна (в Windows XP при перемещении окна без отображения его содержимого была видна рамка окна, что было очень удобно).
- Изменить цвет, шрифт, начертание и размер основных элементов оболочки операционной системы. Например, таких как активный и неактивный заголовок окна, кнопки заголовка окна, строка меню, расстояние между значками и т. д.

Фоновый рисунок рабочего стола

Благодаря этой ссылке можно изменить цвет или изображение, расположенное на Рабочем столе. После щелчка кнопкой мыши на ссылке перед вами отобразится мастер, содержащий список стандартных обоев Рабочего стола. Если вы дважды щелкнете кнопкой мыши на элементе этого списка, то файл обоев откроется в стандартном редакторе изображений. Чтобы установить обои на Рабочем столе, достаточно одинарного щелчка кнопкой мыши (или просто навести указатель мыши на элемент списка, если применяется возможность открытия файлов и папок одинарным щелчком кнопкой мыши).

ПРИМЕЧАНИЕ

Окно Фоновый рисунок рабочего стола можно отобразить и с помощью команды rundll32.exe shell32.dll, Control_RunDLL desk.cpl desk,@Desktop.

Если значение параметра REG_DWORD-типа NoDispBackgroundPage, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System, равно 1, то данная возможность окна Персонализация работать не будет.

Таких же действий можно добиться, если присвоить параметру REG_DWORD-типа NoChangingWallPaper, расположенному в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop, значение 1.

Мастер также содержит раскрывающийся список — в нем можно выбрать направление, в котором сделаны обои Рабочего стола. Например, по умолчанию раскрывающийся список содержит такие элементы:

- Общие изображения — список рисунков, хранящихся в специальной пользовательской папке Windows Vista Общие изображения (расположена по адресу `%systemdrive%\users\public`);
- Сплошные цвета — позволяет установить фоновый цвет Рабочего стола.

Все эти элементы соответствуют названиям папок каталога `%systemroot%\web\wallpaper`.

Раскрывающийся список может также содержать до десяти ваших каталогов. Ссылки на них хранятся в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\Images`. Для этого используются параметры строкового типа с именами от `0` до `9`.

ПРИМЕЧАНИЕ

В Windows Vista осталась возможность установки изображения в качестве фона Рабочего стола с помощью его контекстного меню. Для этого достаточно выбрать команду Сделать фоновым рисунком Рабочего стола контекстного меню файла изображения (поддерживаются как BMP-, так и JPG-файлы).

Экранная заставка

Отображает окно, хорошо знакомое пользователям предыдущих версий операционной системы. С его помощью можно настроить параметры заставки Windows Vista, которая будет отображаться после определенного времени бездействия компьютера. Благодаря этому окну можно также перейти к мастеру настройки параметров питания компьютера (ссылка Изменить параметры электропитания).

ПРИМЕЧАНИЕ

Если значение параметра REG_DWORD-типа NoDispScrSavPage, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System, равно 1, то данная возможность окна Персонализация работать не будет.

С помощью параметра строкового типа ScreenSaveActive, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\

Desktop, можно включить или отключить использование заставки. А с помощью параметра строкового типа SCRNSAVE.EXE можно указать путь к файлу заставки. При этом соответствующие возможности окна Экранная заставка будут заблокированы.

Изменить заставку можно с помощью команды rundll32.exe desk.cpl, InstallScreenSaver "путь к заставке".

Операционная система Windows Vista содержит в своей поставке следующие заставки.

ПРИМЕЧАНИЕ

Все заставки представляют собой файлы с расширением SCR, расположенные в каталоге %systemroot%\system32. С помощью контекстного меню данных файлов вы можете просмотреть заставку (команда Test), настроить параметры ее работы (команда Настроить) или установить ее (команда Установить).

- Объемный текст (файл `ssText3d.scr`) — выводит произвольный текст, который вы можете указать, нажав кнопку Параметры окна Параметры экранной заставки (или выбрав команду Настроить в контекстном меню файла `ssText3d.scr`).
- Северное сияние (файл `Aurora.scr`) — отображает заставку, которая использовалась при установке операционной системы. Ее настройки нельзя изменить с помощью кнопки Параметры окна Параметры экранной заставки, однако их можно изменить непосредственно с помощью реестра. Все они имеют тип `REG_DWORD` и расположены в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Screensavers\Aurora`.
  - `Speed` — скорость передвижения линий.
  - `Brightness` — яркость заставки. При значениях `0` и `0xffffffff` заставка аналогична заставке Пустой экран. В остальных случаях яркость заставки меняется незначительно.
  - `NumLayers` — количество отображаемых в заставке слоев передвигающихся линий. Чем больше слоев, тем более монотонным становится центр экрана — наиболее заметны изменения при установке значения данного параметра равным `0x100`.
- Пустой экран (файл `scrnsave.scr`) — просто отображает черный экран.
- Мыльные пузыри (файл `Bubbles.scr`) — отображает летающие по экрану монитора мыльные пузыри. Настройки данной заставки нельзя изменить с помощью кнопки Параметры окна Параметры экранной заставки, однако их можно изменить непосредственно с помощью реестра. Все они расположены в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Screensavers\Bubbles`.
  - `ShowShadows` — определяет, будет ли под мыльными пузырями отображаться тень (по умолчанию отображается).
  - `MaterialGlass` — если значение данного параметра равно `0`, то мыльные пузыри не будут прозрачными.

- `ShowBubbles` — при установке значения равным `0` мыльные пузыри будут передвигаться по черному экрану (по умолчанию они передвигаются по изображению экрана, которое выводилось при активировании заставки).
- `TurbulenceForce` — если значение параметра равно `0`, то будут отображаться мыльные пузыри белого цвета. А если значение этого параметра больше нуля, то отображаются серо-белые мыльные пузыри. По умолчанию пузыри цветные.
- `TurbulenceSpeed` — определяет среднюю скорость перемещения шариков.
- `Radius` — определяет размер мыльных шариков. Чем меньше размер шариков, тем больше их будет на экране.
- `SphereDensity` — если данный параметр присутствует в реестре, то по экрану будет передвигаться только один шарик.

- Геометрический вальс (файл `Mystify.scr`) — отображает полет постоянно изменяющейся линии, за которой тянется след. Настройки данной заставки нельзя изменить с помощью кнопки Параметры окна Параметры экранной заставки, однако их можно изменить непосредственно с помощью реестра. Все они расположены в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Screensavers\Mystify`.
  - `CameraFOV` — максимальное приближение линий к экрану. Чем больше это значение, тем ближе будут казаться летающие линии.
  - `LineWidth` — максимальная ширина следа от летающих линий.
  - `NumLines` — количество летающих по экрану монитора линий (по умолчанию одна).
- Фотографии (файл `PhotoScreensaver.scr`) — отображает на экране изображения, хранящиеся в каталоге Изображения профиля пользователя. Настройки данной заставки можно изменить с помощью кнопки Параметры окна Параметры экранной заставки.
- Ленты (файл `Ribbons.scr`) — выводит разноцветные ленты, которые летают по экрану. Настройки данной заставки нельзя изменить с помощью кнопки Параметры окна Параметры экранной заставки, однако их можно изменить непосредственно с помощью реестра. Все они расположены в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Screensavers\Ribbons`.
  - `CameraFOV` — максимальное приближение лент к экрану.
  - `RibbonWidth` — максимальная ширина летающих лент.
  - `NumRibbons` — количество летающих по экрану монитора лент (по умолчанию одна).
  - `Blur` — если значение параметра равно `0`, то след от летающей ленты исчезать не будет. В конечном итоге черный экран заставки будет полностью разукрашен цветными лентами.
- Энергия Windows (файл `ssBranded.scr`) — выводит новую заставку Windows Vista.

- Эмблема Windows (файл `logon.scr`) — отображает логотип операционной системы в различных частях экрана.

Звуки

Отображает окно Windows Звуки, с помощью которого можно изменить звуковое сопровождение различных событий операционной системы. Например, событий выключения или включения компьютера. При этом с помощью данного окна можно как изменить музыкальный файл, который будет проигрываться при возникновении данного события, так и полностью отключить звуковое сопровождение события.

После того как вы выполните все изменения, на их основе можно создать звуковую схему, чтобы потом быстро перейти к ее использованию. Для этого нужно нажать кнопку Сохранить как.

Указатели мыши

С помощью данной ссылки можно отобразить окно Свойства: Мышь (апплет `main.cpl`), открытое на вкладке Указатели. Оно предоставляет возможности настройки указателей мыши, которые будут отображаться при возникновении какого-нибудь события. Например, при подведении указателя мыши на границу окна или при необходимости ожидания выполнения какого-нибудь действия. Также на данной вкладке можно отключить отображение тени под указателем мыши. Для этого нужно снять флажок Включить тень указателя.

Тема

Щелчок кнопкой мыши на данной ссылке отображает окно Параметры темы, открытое на вкладке Темы. С ее помощью можно применить созданную ранее тему оформления операционной системы. Обратите внимание, что с помощью данной вкладки можно создать свою тему на основе текущих настроек реестра. Иными словами, вы можете полностью настроить интерфейс операционной системы (цветовое оформление, используемые обои Рабочего стола, используемые файлы указателей и т. д.), а потом сохранить все настройки в теме, которую потом можно легко использовать в другой операционной системе. По умолчанию ваши темы сохраняются в каталоге `%userprofile%\Documents`.

ПРИМЕЧАНИЕ

Установить тему можно с помощью одной из следующих команд.

rundll32.exe shell32.dll, Control_RunDLL desk.cpl desk,@Appearance /Action:OpenTheme /file:"путь к файлу стиля".

rundll32.exe shell32.dll, Control_RunDLL desk.cpl desk,@Appearance /Action:OpenMSTheme /file:"путь к файлу стиля".

rundll32.exe shell32.dll, Control_RunDLL desk.cpl desk,@Themes /Action:OpenTheme /file:"путь к файлу".

Тема представляет собой обычный текстовый файл с расширением THEME, содержащий значения изменяемых темой параметров реестра, хранящихся в корневом разделе HKEY_CLASSES_ROOT или HKEY_CURRENT_USER (рис. 3.18). В Windows Vista присутствуют две стандартные темы (Windows Vista и Классическая), расположенные в каталоге %systemroot%\Resources\Themes.

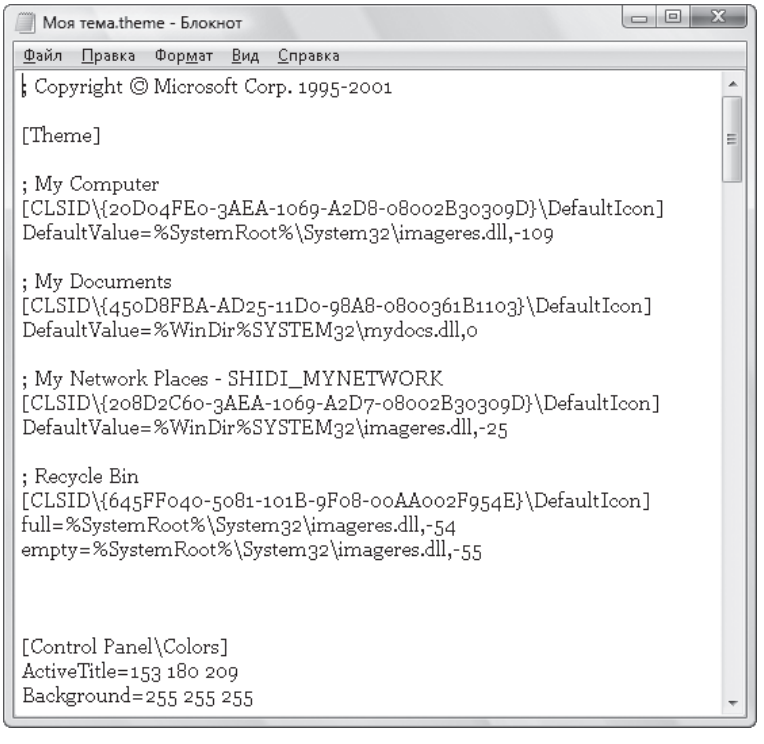


Рис. 3.18. Содержимое файла темы

Тема может содержать следующие настройки.

- Значки ActiveX-объектов — для этого применяется раздел [Theme] файла темы, содержащий значения параметров (По умолчанию) ветвей системного реестра HKEY_CLASSES_ROOT\CLSID\{CLSID-номер ActiveX-объекта}\DefaultIcon.
- Цвета, используемые интерфейсом оболочки, — раздел [Control Panel\Colors] файла темы. Он содержит значения параметров ветви системного реестра HKEY_CURRENT_USER\Control Panel\Colors. Значения этих параметров представлены строкой RGB-формата (сначала определяется красная компонента цвета, потом зеленая и синяя, все компоненты могут иметь значение от 0 до 255 и пишутся через пробел).
- Путь к файлам указателей, используемых оболочкой, — раздел [Control Panel\Cursors] файла темы, содержащий значения параметров ветви реестра HKEY_CURRENT_USER\Control Panel\Cursors.

- Содержимое ветви системного реестра HKEY_CURRENT_USER\Control Panel\Desktop — соответственно, для этого применяется раздел файла [Control Panel\Desktop].
- Используемую заставку — раздел [Boot].
- Воспроизводимые при возникновении определенных событий музыкальные файлы — для этого применяется раздел [VisualStyles].

Изменить значки рабочего стола

С помощью данной ссылки можно отобразить окно Параметры значков рабочего стола, позволяющее указать, будут ли отображаться на Рабочем столе такие элементы, как значки Компьютер, Файлы пользователя, Сеть, Корзина, Internet Explorer, Панель управления. С помощью данного окна можно изменить стандартные значки Корзины, папки Компьютер, Сеть и Файлы пользователя. Для этого нужно выбрать элемент, значок которого нужно изменить, а потом нажать кнопку Сменить значок. После этого отобразится список значков, хранящихся в библиотеке imageres.dll.

Изменить размер шрифта

После выбора данной ссылки запустится программа DliScaling.exe, расположенная в каталоге %systemroot%\system32. С ее помощью можно изменить используемое монитором количество точек на дюйм (dpi). Чем большим вы установите это значение, тем более читабельным будет текст и более увеличенными будут символы. По умолчанию используется значение 96 точек на дюйм.

Боковая панель

Одним из нововведений операционной системы Windows Vista является боковая панель, содержащая различные мини-приложения. Боковая панель является обычной программой и по умолчанию не отображается на Рабочем столе.

Windows Sidebar

Для настройки боковой панели можно воспользоваться значком Свойства боковой панели Windows, отображаемым в Панели управления. После его запуска перед вами появится окно, представленное на рис. 3.19.

С его помощью можно выполнить следующие действия.

- Определить, будет ли боковая панель отображаться поверх всех окон (флажок Боковая панель всегда поверх остальных окон). Если боковая панель будет отображаться поверх всех окон, то она будет занимать фиксированное место на Рабочем столе и никакая программа не сможет перекрыть ее. При этом боковая панель будет отображаться одним цветом, тогда как при снятии данного флажка она станет градиентной.
- Определить, будет ли она загружаться при запуске операционной системы (флажок Запускать боковую панель при запуске Windows). После установки данного флажка будет создан параметр в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run, запускающий файл sidebar.exe, расположенный в каталоге %programfiles%\Windows Sidebar, при каждой загрузке операционной системы.

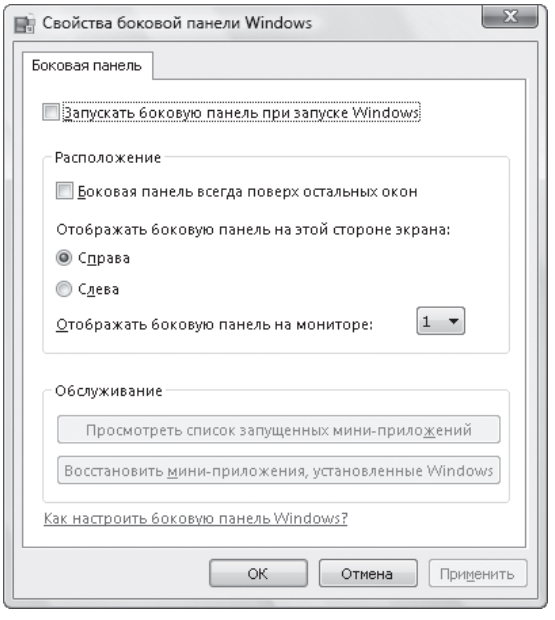


Рис. 3.19. Окно Свойства боковой панели Windows

- Определить сторону экрана, на которой будет отображаться боковая панель (на левой или правой стороне). Для этого служит переключатель Отображать боковую панель на этой стороне экрана.
- Можно также определить монитор, на котором она будет отображаться (если используются системы с несколькими одновременно подключенными мониторами). Для этого служит раскрывающийся список Отображать боковую панель на мониторе.
- Если боковая панель в данный момент отображается, то будет активна кнопка Просмотреть список запущенных мини-приложений, с помощью которой можно просмотреть список запущенных в данный момент мини-приложений, а также удалить ненужные.

Sidebar.exe

Если боковая панель в данный момент не запущена, то описанное в предыдущем разделе окно вам не поможет. Для ее запуска нужно запустить программу `sidebar.exe`, расположенную в каталоге `%programfiles%\Windows Sidebar`.

Изображение боковой панели представлено на рис. 3.20.

Настроек как таковых боковая панель не содержит. Единственное, что можно сделать, — вызвать рассмотренное нами окно Свойства боковой панели Windows. Для этого нужно выбрать команду Свойства из контекстного меню боковой панели.

С помощью контекстного меню боковой панели можно выполнить и такие операции, как скрытие боковой панели в область уведомлений (команда Скрыть боковую панель), а также добавление новых мини-приложений (команда Добавить мини-приложения).



Рис. 3.20. Боковая панель и мини-приложения Часы и Заметки

После выбора команды Добавить мини-приложения перед вами отобразится окно, содержащее список всех имеющихся на компьютере мини-приложений (все они хранятся в каталоге `%programfiles%\Windows Sidebar\Gadgets`). По умолчанию с операционной системой Windows Vista поставляются следующие мини-приложения.

- Календарь — календарь, позволяющий узнать текущий день и год.
- Часы — часы, приведенные на рис. 3.20.
- Контакты — строка поиска по контактам адресной книги Почты Windows. С ее помощью вы сможете не только просмотреть список доступных контактов, но и определить телефон или электронный адрес контакта.
- Индикатор ЦП — текущая загруженность процессора, а также процент использования оперативной памяти.
- Валюта — позволяет выполнить конвертирование одних денежных валют в другие. Для этого используется специальный сайт, поэтому для работы данного мини-приложения необходим доступ к Интернету.
- Заголовки новостей веб-каналов — дает возможность отображать на боковой панели RSS-ленты, на которые вы подписаны.
- Заметки — позволяет быстро записывать некоторый текст без необходимости запускать какой-нибудь текстовый редактор. Изображение этого мини-приложения приведено на рис. 3.20.
- Головоломка — еще одна игра от программистов Microsoft. В ней вы должны сложить картинку из разрозненных кусков.
- Показ слайдов — отображает содержимое стандартной папки Изображения в виде слайд-шоу.

- Ценные бумаги — позволяет следить за падением акций на бирже. Для этого используется специальный сайт, поэтому для работы данного мини-приложения необходим доступ к Интернету.
- Погода — дает возможность просматривать прогноз погоды. Для этого используется специальный сайт, поэтому для работы данного мини-приложения необходим доступ к Интернету.

Чтобы добавить мини-приложение на боковую панель, нужно дважды щелкнуть на нем кнопкой мыши.

Контекстное меню мини-приложений выглядит более интересно. С его помощью можно изменить прозрачность мини-приложения (команда Непрозрачность), вынести мини-приложение за рабочее пространство боковой панели, после чего его можно расположить в любом месте Рабочего стола (команда Загрузить на боковую панель), а также изменить настройки мини-приложения (команда Параметры).

Вынести мини-приложение за рабочее пространство боковой панели можно и с помощью мыши. Достаточно воспользоваться операцией Drag & Drop. Как правило, после этого мини-приложение увеличивается в размерах. Кроме того, если вы вынесете его за боковую панель, то после ее скрытия он так и останется на Рабочем столе.

Каждое мини-приложение имеет индивидуальные настройки, доступ к которым можно получить с помощью команды Настройки контекстного меню мини-приложения. Например, в Калькуляторе можно указать, чтобы на его экране отображались предыдущие ваши действия (они будут отображаться, только когда Калькулятор вынесен за пределы боковой панели), в часах можно указать, чтобы также отображалась секундная стрелка, в мини-приложениях для доступа к RSS можно указать RSS-ленты, содержимое которых будет отображаться, в мини-приложении Показ слайдов можно определить переходной эффект между картинками, а также интервал их смены.

Все настройки мини-приложений и самой боковой панели сохраняются в файле `Settings.ini`, расположенном по адресу `%userprofile%\AppData\Local\Microsoft\Windows Sidebar`.

Мини-приложения

Как уже было сказано, все мини-приложения хранятся в каталоге `%programfiles%\Windows Sidebar\Gadgets`. Мини-приложение представляет собой набор PNG-изображений, как правило, расположенных во вложенной папке images, а также набор HTML-файлов, определяющих поведение и работу мини-приложения. Они расположены во вложенной папке en-US (для англоязычной версии мини-приложения). Если вы разбираетесь в HTML-программировании и знакомы с языком JavaScript, то можете самостоятельно изменить код мини-приложения по своему усмотрению или создать собственное мини-приложение.

Настройка Рабочего стола с помощью групповых политик

Большая часть параметров настройки Рабочего стола описана в файле `Desktop.admx` и расположена в разделе Конфигурация пользователя ▸ Административные шаблоны ▸ Рабочий стол и во вложенных в него подразделах (Рабочий стол и Active Directory).

Политики данного раздела изменяют значения параметров REG_DWORD-типа ветви HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.

- Запретить пользователям вручную перенаправлять папки профилей — установка данной политики запрещает пользователям перемещать стандартные пользовательские папки операционной системы Windows Vista (например, Изображения, Документы, Видео и т. д.). После применения политики из окна Свойства пользовательских папок исчезнет вкладка Папка. Данная политика влияет на значение параметра DisablePersonalDirChange.
- Удалить пункт 'Свойства' из контекстного меню значка 'Компьютер' — после установки этой политики скрывается элемент Свойства из контекстного меню значка Компьютер. Данная политика влияет на значение параметра NoPropertiesMyComputer.
- Удалить пункт 'Свойства' из контекстного меню значка 'Документы' — установка данной политики приводит к скрытию элемента Свойства из контекстного меню значка Документы. Политика влияет на значение параметра NoPropertiesMyDocuments.
- Удалить пункт 'Свойства' из контекстного меню компонента 'Корзина' — после установки этой политики скрывается элемент Свойства из контекстного меню значка Корзина. Политика влияет на значение параметра NoPropertiesRecycleBin.
- Не сохранять параметры при выходе — после установки данной политики перестанут сохраняться новые настройки расположения окон и значков Рабочего стола и т. д. Политика влияет на значение параметра NoSaveSettings.
- Не добавлять общие папки, из которых открыты документы в 'Сеть' — установка данной политики приводит к запрещению добавления ярлыков на недавно используемые сетевые ресурсы в папку Сеть. Политика влияет на значение параметра NoRecentDocsNetHood.

Еще одним разделом групповых политик (описан в файле DWM.admx), который можно использовать для настройки Рабочего стола, является раздел Конфигурация пользователя ▸ Административные шаблоны ▸ Компоненты Windows ▸ Диспетчер окна рабочего стола. Он позволяет настроить параметры работы нового интерфейса Aero Glass.

Политики данного раздела изменяют параметры REG_DWORD-типа ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\DWM.

- DisallowFlip3d — позволяет запретить отображение окна Flip 3D.
- DisallowAnimations — дает возможность запретить эффекты анимации окон.
- DisallowComposition — позволяет запретить работу интерфейса Aero.
- DisallowColorizationColorChanges — дает возможность запретить изменение цветового оформления окон с помощью ссылки Цвет и внешний вид окон окна Персонализация.
- DefaultColorizationColorState — если значение параметра равно 1, то стандартный цвет рамки окон будет заменен цветом, указанным в параметрах DefaultColorizationColorAlpha, DefaultColorizationColorBlue, DefaultColorizationColorGreen и DefaultColorizationColorRed.

ПРИМЕЧАНИЕ

Механизм Flip 3D можно активизировать комбинацией клавиш Windows+Tab либо Ctrl+Windows+Tab. При этом вторая комбинация клавиш запускает механизм Flip 3D в режиме залипания, то есть после нажатия данной комбинации для перехода между окнами вам достаточно будет просто нажимать клавишу Tab. Когда же вы выберете нужное окно, необходимо нажать клавишу Enter.

Групповая политика также позволяет настроить некоторые параметры доступа к возможностям боковой панели Windows. Для этого применяются параметры, описанные в файле `Sidebar.admx` и расположенные в разделе Конфигурация пользователя ▸ Административные шаблоны ▸ Компоненты Windows ▸ Боковая панель.

Политики данного раздела изменяют параметры `REG_DWORD`-типа ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar`.

- `OverrideMoreGadgetsLink` — имеет строковый тип. Значение этого параметра определяет сайт, на котором программа будет искать дополнительные мини-приложения. По умолчанию поиск ведется на сайте Microsoft.
- `TurnOffSidebar` — если значение данного параметра равно `1`, то запуск боковой панели будет запрещен.
- `TurnOffUnsignedGadgets` — когда значение параметра равно `1`, боковой панели будет запрещено выполнять установку и запуск неподписанных мини-приложений.
- `TurnOffUserInstalledGadgets` — если значение данного параметра равно `1`, то боковой панели будет запрещено запускать мини-приложения, установленные пользователем.

Малоизвестные настройки Рабочего стола

Продолжим изучение возможностей настройки операционной системы, которые нельзя выполнить с помощью стандартных окон Windows Vista.

Скрытие и отображение версии операционной системы с рабочего стола

Операционная система Windows Vista по умолчанию не отображает на Рабочем столе свою версию. К сожалению, в ней нет стандартных способов отобразить или скрыть версию с Рабочего стола. Однако это можно сделать с помощью реестра. Для этого достаточно параметру `REG_DWORD`-типа `PaintDesktopVersion`, расположенному в ветви реестра `HKEY_CURRENT_USER\Control Panel\Desktop`, присвоить значение `0`.

Изменение минимального расстояния для перемещения значков и окон

Вы случайно никогда не перемещали значок вместо того, чтобы выполнить двойной щелчок кнопкой мыши на нем? Как правило, когда пользователь торопится или просто очень быстро выполняет двойной щелчок кнопкой мыши, вместо того

чтобы запустить приложение, происходит перемещение самого значка. Операционная система Windows, еще начиная с Windows 95, имела возможности по устранению таких неприятностей. Но они до сих пор не имеют стандартного способа изменений.

Как обычно, воспользуемся реестром. Нужно изменить значения параметров строкового типа `DragHeight` и `DragWidth`, расположенных в ветви реестра `HKEY_CURRENT_USER\Control Panel\Desktop`. По умолчанию они равны `4`.

Эти параметры определяют количество пикселов (первый параметр определяет количество пикселов сверху и снизу от значка, а второй — справа и слева), перемещение на которые не будет считаться перемещением, и значок (или окно) вернется на свое место. Как правило, используемые по умолчанию четыре пиксела являются очень маленькой величиной, особенно если вы работаете с разрешением экрана выше 1024 × 768 пикселов. Поэтому желательно изменить значения этих параметров хотя бы на `10`.

Изменение расположения обоев на Рабочем столе

Windows Vista поддерживает еще одну интересную возможность — можно сдвинуть рисунок обоев относительно верхней или левой стороны экрана. С помощью этого эффекта очень часто можно добиться довольно интересной композиции Рабочего стола.

Расположением обоев на Рабочем столе управляют два параметра `REG_DWORD`-типа, расположенные в ветви реестра `HKEY_CURRENT_USER\Control Panel\Desktop`. Параметр `WallpaperOriginX` позволяет указать количество пикселов, на которые будет сдвинут вниз рисунок обоев. А параметр `WallpaperOriginY` позволяет указать количество пикселов, на которые будет сдвинут влево рисунок обоев Рабочего стола.

Скрытие и отображение ActiveX-объектов на Рабочем столе

Возможность скрытия и отображения ActiveX-объектов на Рабочем столе в Windows Vista реализована так же, как и в предыдущих версиях операционной системы.

Чтобы отобразить элемент на Рабочем столе, нужно в ветви системного реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace` создать подраздел с названием, соответствующим CLSID-номеру необходимого ActiveX-объекта.

Если же необходимо удалить определенный элемент с Рабочего стола конкретного пользователя, то нужно воспользоваться ветвью реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons`. Данная ветвь реестра содержит два дочерних подраздела: `ClassicStartMenu` и `NewStartPanel`. Нужно создать параметр `REG_DWORD`-типа в одном из этих подразделов в зависимости от того, какой вид меню Пуск вы используете. Название параметра должно соответствовать CLSID-номеру ActiveX-объекта, а значение должно быть равно `1`. Например, чтобы скрыть ActiveX-объект с Рабочего стола при использовании нового вида меню Пуск, нужно создать параметр в подразделе `NewStartPanel`.

Редактирование списка Создать контекстного меню Рабочего стола и Проводника

Список Создать позволяет вам быстро создавать файлы различного расширения, а также папки и ярлыки к файлам и папкам. Этот список является действительно удачной и удобной возможностью операционных систем семейства Windows. Однако уже после установки операционной системы он содержит множество элементов, которые обычному пользователю никогда не понадобятся. А с установкой дополнительных программ этот список только увеличивается.

К счастью, с помощью реестра можно удалить из списка Создать те элементы, которые вам не нужны. Для этого нужно удалить подраздел ShellNew из ветвей реестра HKEY_CLASSES_ROOT\<расширение, файлы которого вы не хотите создавать с помощью списка Создать>. Например, рассмотрим некоторые расширения, файлы которых по умолчанию отображаются в списке Создать.

- Briefcase — элемент Портфель списка Создать.
- .bmp — Точечный рисунок.
- .contact — Контакт.
- .jnt\jntfile — Документ Журнала.
- .lnk — Ярлык.
- .zip\CompressedFolder — Сжатая ZIP-папка.
- Folder — Папка.

Вы также можете сформировать свой элемент списка Создать. Для этого нужно использовать подраздел ShellNew в каталоге HKEY_CLASSES_ROOT\<расширение, файлы которого вы хотите создавать с помощью списка Создать>. После этого в подразделе нужно установить один из следующих параметров:

- Command — строковый параметр, содержит команду, которая будет выполняться при выборе данного элемента списка Создать;
- Data — этот параметр REG_BINARY-типа хранит данные в двоичном виде, которые будет содержать созданный файл;
- FileName — строковый параметр, хранит путь к файлу, на основе которого будет создаваться новый файл (фактически будет создаваться копия этого файла);
- NullFile — создать пустой файл.

Подраздел ShellNew может содержать параметр строкового типа IconPath, определяющий путь к значку, который будет отображаться в списке Создать вместо стандартного значка файла данного расширения. Этот подраздел может также включать в себя параметр строкового типа MenuText, определяющий название библиотеки и идентификатор ресурса, содержимое которого будет заменять собой стандартное название, отображаемое в меню Создать.

Подраздел ShellNew может содержать вложенный подраздел Config. Он, в свою очередь, может включать в себя следующие параметры строкового типа:

- NoExtension — присутствие данного параметра говорит о том, что созданный файл не будет иметь расширения;
- DontRename — наличие этого параметра говорит о том, что имя созданного файла не будет автоматически выделяться, чтобы вы могли сразу переименовать этот файл.

Удаление элементов списка только для папок или разделов диска

Нововведением операционной системы Windows Vista является возможность использования разного списка элементов меню Создать для папок компьютера, разделов диска и Рабочего стола. Для этого применяется параметр строкового типа NewMenuAllowedTypes.

Содержимым данного параметра является список расширений через точку с запятой, элементы которых будут отображаться в списке Создать. Например, чтобы определить, что для каталога или раздела диска должны отображаться только элементы списка Создать, которые позволяют создавать текстовый документ или документ Microsoft Word, достаточно данному параметру присвоить значение .txt;.doc. Учтите только, что в качестве значения данного параметра можно указывать лишь те из расширений, которые отображаются в списке Создать контекстного меню Рабочего стола.

Параметр NewMenuAllowedTypes можно использовать в следующих ветвях реестра.

- HKEY_CLASSES_ROOT\Drive — в этом случае значение параметра определяет список расширений, файлы которых можно создать с помощью списка Создать контекстного меню корневого каталога раздела диска (например, с помощью контекстного меню каталога C:\).
- HKEY_CLASSES_ROOT\Directory — в этом случае значение параметра определяет список расширений, файлы которых можно создать с помощью списка Создать контекстного меню любого каталога, кроме корневых каталогов разделов диска.

Настройка окна, вызываемого нажатием Alt+Tab

Всем известное окно перехода между открытыми окнами, вызываемое нажатием комбинации клавиш Alt+Tab, теперь также можно настроить. Для этого применяются параметры ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AltTab. Эта ветвь хранит следующие параметры типа REG_DWORD.

ПРИМЕЧАНИЕ

Сведения о диагностике работы механизма Alt+Tab заносятся в журнал Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Alt-Tab.

- `MaxIconSizePx` — определяет максимальный размер значка, отображаемого в окне Alt+Tab при отключенном интерфейсе Windows Aero.
- `TopMarginPx` — указывает дополнительную высоту (в пикселах) окна, отображаемого после нажатия комбинации клавиш Alt+Tab. Иначе говоря, он определяет, насколько выше станет указанное окно. При этом дополнительные пикселы добавляются к верхней стороне окна. Значение этого параметра не влияет на количество значков, которые смогут отображаться в окне.
- `SideMarginPx` — определяет дополнительную ширину (в пикселах) окна, отображаемого после нажатия комбинации клавиш Alt+Tab. Определенное в данном параметре количество пикселов будет добавляться к левой и правой сторонам окна. Значение этого параметра не влияет на количество значков, которые смогут отображаться в окне.
- `BottomMarginPx` — указывает дополнительную высоту (в пикселах) окна, отображаемого после нажатия комбинации клавиш Alt+Tab. Иными словами, он определяет, насколько выше станет окно. При этом дополнительные пикселы добавляются к нижней стороне. Значение этого параметра не влияет на количество значков, которые смогут отображаться в окне.
- `ThumbSpacingXPx` — определяет расстояние в пикселах между значками указанного окна по горизонтали.
- `ThumbSpacingYPx` — указывает расстояние в пикселах между значками окна по вертикали.
- `OverlayIconPx` — при отключенном интерфейсе Windows Aero данный параметр определяет размытие значков, отображаемых в окне. При включенном интерфейсе Windows Aero данный параметр определяет размер значков в пикселах.
- `MinWidthPx` — определяет минимальную ширину окна (в пикселах), отображаемого после нажатия комбинации клавиш Alt+Tab. Ширина окна никогда не будет меньше, чем указано в этом параметре.
- `MinThumbSizePcent` — указывает размер эскизов страниц, отображаемых в окне, в процентах относительно максимального размера. Поскольку при отключенном интерфейсе Windows Aero эскизы страниц не отображаются в окне, вызываемом нажатием клавиш Alt+Tab, данный параметр влияет только на окно при включенном интерфейсе Windows Aero. Параметр может принимать значения от `0` до `10`. Чем больше его значение, тем больше эскиз страниц.
- `MaxThumbSizePx` — определяет размер эскизов страниц, отображаемых в окне, в пикселах.
- `OverlayIconDXPx` — указывает смещение (в пикселах) вправо значков относительно эскизов страниц окна. Параметр может принимать значения от `0` до используемого в окне размера значков.
- `OverlayIconDYPx` — определяет смещение (в пикселах) вниз значков относительно эскизов страниц окна, вызываемого нажатием клавиш Alt+Tab. Параметр может принимать значения от `0` до используемого в окне размера значков.
- `Columns` — указывает количество значков, отображаемых в одной строке окна. Изменение данного параметра вступает в силу только после перезагрузки оболочки.

- `Rows` — определяет количество строк значков окна, вызываемого нажатием клавиш Alt+Tab. Изменение данного параметра вступает в силу только после перезагрузки оболочки.
- `StartAlpha` — указывает начальную прозрачность окна, отображаемого после нажатия комбинации клавиш Alt+Tab.
- `FinalAlpha` — определяет конечную прозрачность окна, отображаемого после нажатия комбинации клавиш Alt+Tab. Фактически присутствие данного параметра делает окно максимально прозрачным.
- `FadeOut_ms` — указывает количество миллисекунд, которое должно пройти перед тем, как окно полностью исчезнет. При этом на протяжении данного времени окно будет изменять прозрачность от полной видимости до исчезновения.

Для примера на рис. 3.21 приведено измененное окно, отображаемое после нажатия комбинации клавиш Alt+Tab.



Рис. 3.21. Измененное окно перехода между открытыми окнами

Активация замедления эффекта минимизации с помощью клавиши Shift

По умолчанию при минимизации или восстановлении размеров окна (если включен интерфейс Aero), используются специальные эффекты. Если вы их еще не отключили, то существует возможность замедления выполнения этих эффектов. Для этого достаточно в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\DWM` создать параметр `REG_DWORD`-типа `AnimationsShiftKey` и присвоить ему значение `1`. Если после перезагрузки компьютера вы нажмете и удержите клавишу Shift и начнете сворачивать/восстанавливать окно, данный процесс будет выполняться замедленно.

Настройка Проводника

После интерфейса Windows Aero вторым значимым изменением в оболочке операционной системы можно назвать новый обновленный Проводник. Он больше не отображает строку меню (но ее можно отобразить, нажав клавишу Alt), тем не менее, работать с ним стало удобнее.

Теперь основные функции строки меню хранятся в подменю Раскладка (рис. 3.22). С его помощью можно создать папку, выполнить копирование, удаление или перемещение файла или папки, а также отобразить окно Свойства открытой в данный момент в Проводнике папки. Также с помощью данного подменю можно отобразить окно Свойства папки или скрыть/отобразить различные части окна Проводника (список команды Раскладка). Кстати, с помощью команды Раскладка можно закрепить строку меню в Проводнике, чтобы она отображалась всегда, а не только при нажатии клавиши Alt. Для этого нужно установить флажок напротив элемента Строка меню списка Раскладка.

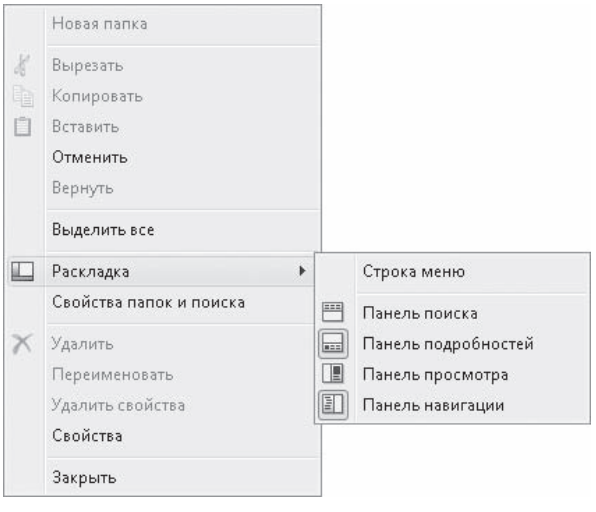


Рис. 3.22. Список Раскладка

Строка меню нового Проводника в основном содержит те же команды, что и строка меню Проводника операционной системы Windows XP. Особо стоит выделить меню Сервис, с помощью команд которого можно подключить или отключить сетевой диск, а также вызвать окна Центр синхронизации и Свойства папки.

Строка состояния нового Проводника также изменилась. По сравнению со своей предшественницей она стала больше и теперь содержит как описание некоторых атрибутов файла или папки, так и изображение этого файла или папки.

Если вы считаете, что новая строка состояния выглядит слишком большой, то можете ее уменьшить. Для этого в контекстном меню строки состояния нужно раскрыть список Размер и выбрать в нем один из предопределенных размеров строки состояния (рис. 3.23).

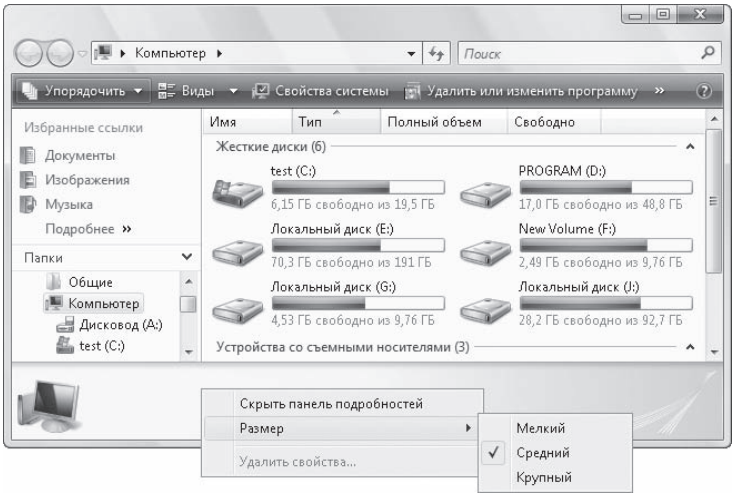


Рис. 3.23. Изменение размера строки состояния

Проводник Windows Vista поддерживает еще одну строку состояния. Она использует меньше места, не отображает значок выделенного файла, а также не использует эффектов анимации, что может быть важно пользователям, заботящимся о повышении производительности операционной системы. Чтобы отобразить эту строку состояния, нужно в меню Вид Проводника установить флажок Строка состояния.

На рис. 3.24 представлено окно Проводника, отображающего сразу две строки состояния.

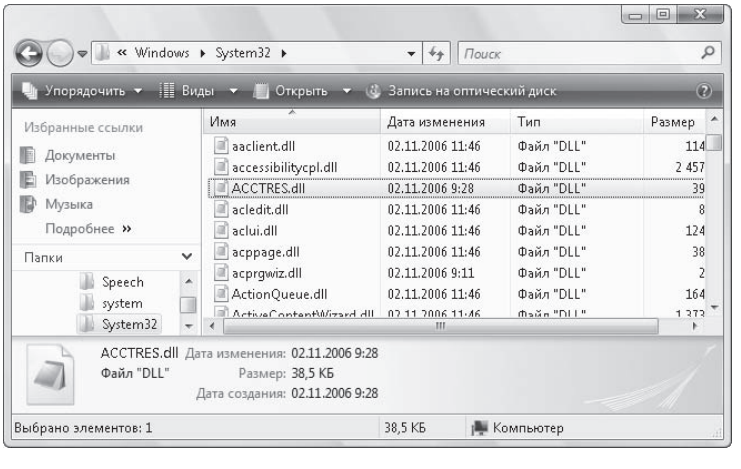


Рис. 3.24. Две строки состояния

Панель Избранные ссылки

Достоинством нового Проводника можно с уверенностью назвать панель Избранные ссылки, с помощью которой можно быстро перейти в предопределенные каталоги

файловой системы. По умолчанию данная панель отображает следующие ссылки: Документы, Изображения, Музыка, Недавно измененные, Поиски.

Особо стоит рассказать о новом каталоге Поиски. Он содержит набор предопределенных условий поиска, а также все сохраненные вами условия. Каждое условие поиска хранится в виде отдельного файла с расширением SEARCH. Если вы запустите этот файл, то начнется поиск с заданными условиями. Например, по умолчанию данная папка содержит следующие файлы поиска:

- `Недавняя электронная почта` — отображает все электронные сообщения, полученные за последние дни;
- `Недавние документы` — выводит все документы из соответствующей папки, созданные за последние дни;
- `Недавние изображения и видео` — отображает все файлы папок Изображения и Видео, созданные за последние дни;
- `Мои файлы с общим доступом` — выводит все файлы, для которых открыт общий доступ;
- `Индексированные места` — отображает все файлы, находящиеся в индексированных каталогах.

Особенностью данной панели является то, что вы можете самостоятельно редактировать ее содержимое. Для этого в контекстном меню панели Избранные ссылки нужно выбрать команду Открыть папку. После этого отобразится содержимое папки `%userprofile%\Links`.

Контекстное меню панели Избранные ссылки содержит команду Восстановить список избранного по умолчанию. С ее помощью можно восстановить используемые по умолчанию ярлыки данной панели (Документы, Поиски и т. д.), если вы их удалили.

Окно Свойства папки

Окно Свойства папки является основным окном настройки параметров работы Проводника Windows Vista. Для этого оно содержит две вкладки: Общие и Вид.

ПРИМЕЧАНИЕ

Окно Свойства папки можно отобразить с помощью команды rundll32.exe shell32.dll, Options_RunDLL 0.

Содержимое вкладки Общие совершенно не изменилось. Как и в предыдущих операционных системах, с ее помощью можно убрать панель навигации Проводника (также это можно сделать с помощью списка Раскладка меню Упорядочить), указать, будет ли открываться каждая папка в отдельном окне, а также определить, будет ли файл или папка открываться после одинарного щелчка кнопкой мыши или только после двойного.

Вкладка Вид также не изменилась. Она по-прежнему содержит список настроек, с помощью которых можно отобразить скрытые и суперскрытые (у которых одно-

временно установлены атрибуты Системный и Скрытый) файлы и папки, отобразить известные расширения файлов, запретить поиск сетевых принтеров, запретить использование окна простого общего доступа и т. д. Но, кроме того, список на вкладке Вид имеет дополнительные настройки, наиболее интересны из которых следующие.

- Всегда отображать значки, а не эскизы — после установки данного флажка использование вида Эскизы страниц будет запрещено, то есть вместо содержимого таких документов, как изображения, будет отображаться значок файла.
- Отображать буквы дисков — после снятия этого флажка напротив значков дисков в папке Компьютер больше не будет отображаться буква диска. Останется только его метка.
- Использовать флажки для выбора элементов — после установки данного флажка возле выделенного значка будет отображаться флажок, установка которого приведет к закреплению выделения. Таким способом вы сможете выделить сразу несколько значков, не удерживая при этом клавишу Ctrl.

Окно Свойства папки также содержит вкладку Поиск, с помощью которой можно настроить параметры поиска, но об этой вкладке мы поговорим позже. Обратите внимание, что окно Свойства папки больше не содержит вкладок, с помощью которых раньше можно было настроить параметры работы автономных файлов, а также команды контекстного меню файлов различного расширения.

Настройка Проводника с помощью групповых политик

Групповые политики, предназначенные для настройки Проводника, описаны в файле `WindowsExplorer.admx` и расположены в разделе Конфигурация пользователя ▸ Административные шаблоны ▸ Компоненты Windows ▸ Проводник Windows и во вложенных в него подразделах (Область кадра проводника, Предыдущие версии и Общее диалоговое окно открытия файлов).

Политики данного раздела изменяют значения параметров `REG_DWORD`-типа ветви системного реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`.

- Отключить кэширование эскизов изображений — установка данной политики приводит к запрещению создания файлов `Thumbs.db`. Они содержат эскизы страниц для всех файлов каталога и создаются для ускорения отображения эскизов страниц. Эта политика оказывает влияние на значение параметра `NoThumbnailCache`.
- Скрыть выбранные диски из окна "Мой компьютер" — с помощью этой политики вы можете указать буквы дисков, которые не будут отображаться в папке Компьютер. Несмотря на то что они не отображаются в этой папке, к ним все равно можно будет получить доступ с помощью команды Выполнить. Эта политика влияет на значение параметра `NoDrives`.
- Удалить меню "Файл" из проводника Windows — установка данной политики удаляет меню Файл из окна Проводника и браузера Internet Explorer. Она влияет на значение параметра `NoFileMenu`.

- Удалить команды "Подключение сетевого диска" и "Отключение сетевого диска" — после установки этой политики удалятся соответствующие команды меню Сервис Проводника. Она влияет на значение параметра NoNetConnectDisconnect.
- Запретить вывод контекстного меню по умолчанию для проводника Windows — установка данной политики запрещает отображение контекстного меню Проводника. Она влияет на значение параметра NoViewContextMenu.
- Отключить область сведений — после установки данной политики будет запрещено отображать панель состояния Проводника. Она влияет на значение параметра NoPreviewPane.
- Отключить область просмотра — установка этой политики запрещает отображение панели Просмотр Проводника. Она влияет на значение параметра NoReadingPane.

Настройка Проводника с помощью реестра и других малоизвестных возможностей

Попробуем настроить Проводник с помощью реестра.

Изменение расположения значка диска в папке Мой компьютер

В Windows Vista по умолчанию используется следующий порядок именования томов диска: имя диска или метка диска, буква диска. В некоторых случаях такой порядок именования бывает неудобен. Например, когда из-за длинной метки или имени диска не отображается его буква.

К счастью, с помощью реестра можно управлять расположением буквы диска. Для этого применяется параметр REG_DWORD-типа ShowDriveLettersFirst, расположенный в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer. По умолчанию значение данного параметра равно 0, однако его можно изменить на 4. В этом случае буква диска будет отображаться перед его меткой. Также значение данного параметра можно изменить на 2, что приведет к скрытию буквы диска из его имени.

Добавление команд Зашифровать/Расшифровать к контекстному меню файлов

Если вы часто пользуетесь стандартной возможностью операционной системы по шифрованию файлов, то к контекстному меню файла или папки можно добавить команду Зашифровать, с помощью которой легко выполняется шифрование файлов. Для этого достаточно в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced создать параметр REG_DWORD-типа EncryptionContextMenu и присвоить ему значение 1.

Скрытие и отображение ActiveX-объектов в папке Мой компьютер

Как и в предыдущих версиях, в Windows Vista можно добавить к содержимому папки Компьютер свой ActiveX-объект либо удалить уже существующий.

Чтобы отобразить элемент в папке Компьютер, нужно в ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\NameSpace создать подраздел с названием, соответствующим CLSID-номеру необходимого ActiveX-объекта.

Если же необходимо удалить определенный элемент из папки Компьютер конкретного пользователя, то нужно воспользоваться ветвью реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\HideMyComputerIcons. В данной ветви достаточно создать параметр REG_DWORD-типа, название которого должно соответствовать CLSID-номеру ActiveX-объекта, а значение параметра должно быть равно 1.

Изменение значка определенного раздела диска, а также метки, используемой им по умолчанию

Другой возможностью, которую предоставляет пользователям операционная система Windows Vista, является изменение значка для определенного диска, а также метки, отображаемой для данного диска, если метка не задана с помощью окна Свойства данного диска.

Для этих задач применяется ветвь реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\DriveIcons\<буква диска>.

Чтобы изменить значок диска, нужно в параметре (По умолчанию) подраздела DefaultIcon данной ветви реестра указать путь к новому значку.

Чтобы изменить метку диска, нужно в параметре (По умолчанию) подраздела DefaultLabel данной ветви реестра указать название метки.

Например, на рис. 3.25 отображен результат изменения значка и метки диска с помощью подразделов DefaultIcon и DefaultLabel ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\DriveIcons\c.

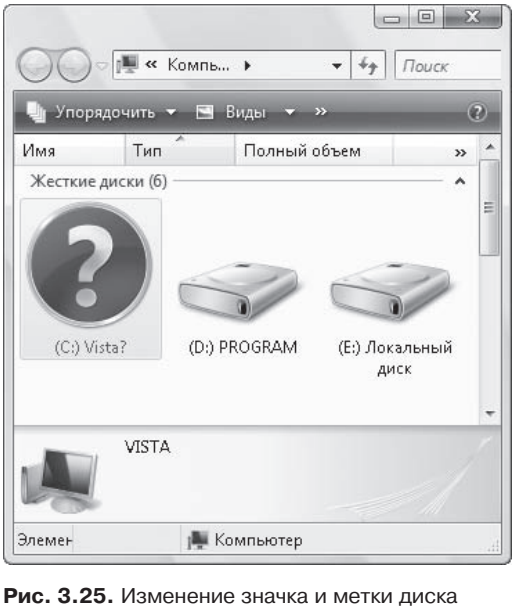


Рис. 3.25. Изменение значка и метки диска

Изменение действия, выполняемого при перемещении файла между папками

По умолчанию при перемещении файла любого расширения между папками выполняется его перемещение. Однако вы можете самостоятельно настроить действие, которое будет выполняться при перемещении файла между папками. Для этого необходимо воспользоваться параметром `REG_DWORD`-типа `DEFAULTDROPEFFECT`. Он может принимать следующие значения:

- `1` — при перемещении файла между папками выполнить его копирование;
- `2` — выполнить перемещение файла;
- `4` — выполнить создание его ярлыка.

Но где же создавать этот параметр? Если вы хотите изменить действие по умолчанию для файлов всех известных расширений, то параметр нужно создать в ветви реестра `HKEY_CLASSES_ROOT\*`. Если же вы хотите изменить действие по умолчанию для файлов конкретного расширения, то его нужно создавать в ветви реестра `HKEY_CLASSES_ROOT\<идентификатор расширения>`.

Изменение значка, отображаемого напротив кнопки группировки окон Проводника в Панели задач

В операционной системе Windows вы можете настроить даже такую мелочь, как значок кнопки группировки окон Проводника, отображаемый в Панели задач, когда определенное количество окон Проводника не помещается на ней и операционная система группирует все кнопки окон в одну. Для этого нужно указать путь к новому значку в параметре строкового типа `TaskbarGroupIcon`, расположенном в ветви реестра `HKEY_CLASSES_ROOT\Applications\explorer`.

Кстати, также вы можете изменить изображение, отображаемое напротив кнопки окна Проводника в Панели задач. Для этого нужно указать путь к новому значку в параметре строкового типа `OpenIcon` ветви реестра `HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\DefaultIcon`.

Изменение содержимого вкладки Подробно окна свойств файлов и папок, а также подсказок к файлам

В операционных системах семейства Windows каждый файл имеет набор метаданных, описывающих такие его свойства, как размер, дата создания, автор и т. д. Это очень удобная возможность, но ей не хватает гибкости. Например, на вкладке Подробно окна Свойства для DLL-файлов нет сведений об описании библиотеки, хотя они могут понадобиться администраторам. К счастью, благодаря реестру существует возможность определения метаданных, которые будут отображаться на вкладке Подробно или при выводе описания файла.

Для этого служат параметры строкового типа `FullDetails` и `InfoTip`. Первый из них определяет метаданные, которые будут отображаться на вкладке Подробно окна Свойства, а второй — метаданные, которые будут отображаться при выделении файла или папки (и при удержании указателя мыши над файлом). Оба этих

параметра имеют одинаковый формат значений: сначала идет слово `prop:`, а после него через точку с запятой пишутся метаданные. Никаких пробелов в значении параметров быть не должно. Ниже приведен список самых часто используемых метаданных:

- `System.Attributes` — присвоенные файлу или папке атрибуты (поле Атрибуты);
- `System.Author` — имя автора файла (поле Автор);
- `System.Capacity` — общий объем папки или диска (поле Размер);
- `System.ComputerName` — имя компьютера (поле Компьютер);
- `System.Comment` — комментарий к файлу (поле Комментарий);
- `System.Copyright` — данные об авторских правах на файл (поле Права);
- `System.DateModified` — дата изменения файла (поле Изменен);
- `System.DateCreated` — дата создания файла (поле Создан);
- `System.DateAccessed` — дата последнего доступа к файлу (поле Открыт);
- `System.DisplayName` — имя файла (поле Имя);
- `System.DisplayFolder` — путь к папке, в которой хранится файл (поле Папка);
- `System.DisplayType` — описание типа файла (поле Тип);
- `System.FileCount` — количество файлов в папке или на диске (поле Содержит);
- `System.FreeSpace` — количество свободного места на диске (поле Свободно);
- `System.Keywords` — теги, которые имеет изображение (поле Ключевые слова);
- `System.Language` — язык, на котором создан файл (поле Язык);
- `System.OfflineAvailability` — определяет, доступен ли данный сетевой файл автономно (Автономный доступ);
- `System.PercentFull` — количество использованного на диске места (поле Занято);
- `System.Rating` — рейтинг файла (поле Рейтинг);
- `System.Size` — размер файла (поле Размер);
- `System.TotalFileSize` — общий размер файлов в папке (поле Общий размер);
- `System.Audio.EncodingBitrate` — битрейт звукового файла (поле Скорость потока);
- `System.Document.PageCount` — количество страниц в текстовом файле (поле Количество страниц);
- `System.DRM.IsProtected` — отображает, защищен ли файл с помощью лицензии DRM (поле Защита);
- `System.Link.Target` — путь к файлу, на который указывает ссылка (поле Путь к папке);

- `System.Link.Description` — описание ссылки (поле **Описание**);
- `System.Link.DateVisited` — дата последнего использования ссылки (поле **Дата изменения**);
- `System.File.Owner` — имя владельца файла (поле **Владелец**);
- `System.File.Description` — описание файла (поле **Описание**);
- `System.File.Version` — версия файла (поле **Версия**);
- `System.Image.HorizontalSize` — размер файла изображения по горизонтали (поле **Горизонтальное разрешение**);
- `System.Image.VerticalSize` — размер файла изображения по вертикали (поле **Разрешение по вертикали**);
- `System.Image.BitDepth` — глубина изображения (поле **Глубина цвета**);
- `System.Music.Artist` — исполнитель музыкального файла (поле **Исполнитель**);
- `System.Music.AlbumTitle` — альбом, из которого взят данный музыкальный файл (поле **Альбом**);
- `System.Music.TrackNumber` — номер музыкального файла в альбоме (поле **Номер записи**);
- `System.Music.Genre` — жанр песни (поле **Жанр**).

Теперь определим, где могут находиться параметры `FullDetails` и `InfoTip`. Например, они могут находиться в следующих ветвях реестра.

- `HKEY_CLASSES_ROOT\*` — указывают описание для всех файлов, зарегистрированных в системе. При этом описание может переопределяться непосредственно в ветви реестра, которая указывает описание для файлов данного расширения.
- `HKEY_CLASSES_ROOT\AllFilesystemObjects` — определяют описание для любых объектов файловой системы (диски, папки, файлы и т. д.).

  Например, по умолчанию значение параметра `FullDetails` данной ветви реестра равно `prop:System.PropGroup.FileSystem;System.DisplayName;System.CanonicalType;System.DisplayFolder;System.Size;System.DateCreated;System.DateModified;System.DateAccessed;System.Attributes;*System.OfflineAvailability;*System.OfflineStatus;*System.SharedWith;*System.File.Owner;*System.ComputerName`. Обратите внимание на звездочки перед некоторыми метаданными. Они говорят, что данное поле должно отображаться только в том случае, когда его поддерживает файл.
- `HKEY_CLASSES_ROOT\Drive` — указывает описание для дисков.
- `HKEY_CLASSES_ROOT\Folder` — определяет описание для папок.
- `HKEY_CLASSES_ROOT\Printers` — указывает описание для принтеров.

Если же вам нужно изменить описание для файлов конкретного расширения, то их ветвь реестра нужно еще найти. Для этого нужно посмотреть на параметр `(По умолчанию)` ветви реестра `HKEY_CLASSES_ROOT\<.расширение файла>`.

После этого нужно найти ветвь реестра HKEY_CLASSES_ROOT\<значение параметра (По умолчанию) предыдущей ветви реестра>.

Раз уж мы затронули содержимое вкладки Подробно окна Свойства, то нельзя не заметить, что на этой вкладке появилась новая ссылка: Удаление свойств и личной информации. С ее помощью можно быстро удалить значения тех метаданных, которые доступны пользователю как для чтения, так и для записи. Например, к таким метаданным относятся название артиста, песни и альбома для музыкальных файлов.

После того как вы щелкнете кнопкой мыши на ссылке, перед вами отобразится окно Удаление свойств. В этом окне напротив всех метаданных, значения которых можно удалить, расположен неустановленный флажок. Если флажок установить, после чего нажать кнопку OK окна, то значения соответствующих метаданных будут удалены.

Изменение контекстного меню Проводника и Рабочего стола

По умолчанию контекстное меню Проводника и Рабочего стола содержит лишь такие элементы, как команда создания нового файла, команда отображения окна Свойства (или окна Персонализация для Рабочего стола), команды группировки. Однако, как можно судить по множеству созданных программ, которые заменяют собой стандартное контекстное меню, пользователю нужно намного больше команд этого контекстного меню.

Если вы тоже так считаете, то должны знать, что, кроме использования специальной программы, заменяющей собой стандартное контекстное меню, существует другой способ — самостоятельная настройка контекстного меню Проводника и Рабочего стола.

Сведения о контекстном меню Рабочего стола и Проводника расположены в ветви реестра HKEY_CLASSES_ROOT\Directory\Background. Данный раздел включает в себя два дочерних подраздела.

- Shell — определяет стандартные команды контекстного меню Рабочего стола и Проводника, которые вызывают различные программы.

  Заметьте, что данный подраздел по умолчанию содержит вложенный подраздел cmd, определяющий команду контекстного меню Рабочего стола и Проводника, с помощью которой можно открыть программу cmd.exe. В этой программе будет по умолчанию открыт путь к каталогу, из которого вы вызвали данную команду. Однако, как вы, наверное, уже проверили, такой команды вообще не существует в контекстном меню Рабочего стола и Проводника. Чтобы она отобразилась, нужно в ветви реестра HKEY_CLASSES_ROOT\Directory\Background\Shell\cmd удалить параметр строкового типа Extended.

  Одну новую команду в контекстное меню мы уже добавили. Как видите, это не так сложно. Если же вам нужно добавить собственную команду, которая будет отображаться в контекстном меню Рабочего стола и Проводника, то в данном подразделе нужно создать новый дочерний подраздел, название которого не имеет

значения. Параметру (По умолчанию) данного подраздела нужно присвоить название команды, которое будет отображаться в контекстном меню. После этого в созданном вами подразделе нужно создать дочерний подраздел command, параметр (По умолчанию) которого будет определять команду, выполняемую при выборе созданного вами пункта контекстного меню Рабочего стола и Проводника. После этого новый пункт отобразится в контекстном меню Рабочего стола и Проводника.

- ShellEx — содержит вложенный подраздел ContextMenuHandler. Он определяет команды контекстного меню Рабочего стола и Проводника, действия которых основаны на возможностях ActiveX-объектов.

  По умолчанию данный подраздел включает в себя подраздел New, параметр (По умолчанию) которого определяет CLSID-номер ActiveX-объекта. Если вы удалите данный подраздел, то из контекстного меню Рабочего стола и Проводника исчезнет команда Создать.

  Кроме того, вы можете добавить собственные ActiveX-объекты к контекстному меню Рабочего стола и Проводника. Для этого в подразделе ShellEx нужно создать дочерний подраздел, например с именем New2. В параметре (По умолчанию) подраздела New2 нужно указать CLSID-номер ActiveX-объекта, который нужно добавить к контекстному меню Рабочего стола и Проводника. К сожалению, многие команды ActiveX-объектов замещают собой команды других ActiveX-объектов, поэтому можно указать только один из приведенных далее CLSID-номеров.

  Например, ниже описаны CLSID-номера наиболее интересных стандартных ActiveX-объектов. CLSID-номера остальных ActiveX-объектов, которые также можно добавить к контекстному меню, описаны в приложении 4. После CLSID-номера указано, какую команду он добавляет к контекстному меню Рабочего стола и Проводника.

  - {2559a1f0-21d7-11d4-bdaf-00c04f60b9f0} — Поиск. Данная команда замещает собой команды Справка и поддержка и Выполнить.
  - {2559a1f1-21d7-11d4-bdaf-00c04f60b9f0} — Справка и поддержка. Она замещает собой команды Поиск и Выполнить.
  - {2559a1f3-21d7-11d4-bdaf-00c04f60b9f0} — Выполнить. Данная команда замещает собой команды Справка и поддержка и Поиск.
  - {645FF040-5081-101B-9F08-00AA002F954E} — Очистить Корзину. Данный ActiveX-объект может отображаться вместе с другим ActiveX-объектом, поэтому если вы не хотите из контекстного меню удалять пункт Создать (или любой другой) ради того, чтобы добавить эту команду, то просто создайте в подразделе Shellex дочерний подраздел, например New4, а его параметру (По умолчанию) присвойте данный CLSID-номер.

Изменение содержимого контекстного меню файлов различного расширения

Для выполнения этой операции создавались целые программы, однако опытный пользователь, наверное, знал, что раньше для изменения содержимого контекст-

ного меню файлов различного расширения достаточно было открыть вкладку Типы файлов окна Свойства папки. К сожалению, в Windows Vista разработчики решили вообще убрать эту вкладку из указанного окна. Поэтому теперь для изменения содержимого контекстного меню придется пользоваться реестром.

Многие пользователи вообще не могут понять, зачем нужно изменять контекстное меню файлов различного расширения, однако в некоторых случаях это очень облегчает жизнь. Мало того что вы можете удалить ненужные элементы контекстного меню, так можно еще добавить новые элементы. Например, если вам часто нужно открывать исполняемые файлы в других программах (дизассемблере, редакторе ресурсов или даже в простом Блокноте), то вы, без сомнения, уже думали над тем, как вообще это сделать. Действительно, как быстро открыть исполняемый файл в Блокноте, если в его контекстном меню и в помине нет команды Открыть с помощью? Поэтому для примера попробуем добавить к контекстному меню файлов с расширением EXE именно эту команду.

Чтобы это сделать, сначала нужно в ветви реестра HKEY_CLASSES_ROOT найти подраздел идентификатора для расширения EXE. Это можно сделать двумя способами. Во-первых, можно посмотреть на параметр (По умолчанию) ветви реестра HKEY_CLASSES_ROOT\<расширение файла>, то есть в данном случае ветви HKEY_CLASSES_ROOT\.exe. Значение этого параметра и будет названием раздела идентификатора, к которому нам нужно перейти. Вторым же способом является использование стандартной программы командной строки assoc.exe. Чтобы отобразить с ее помощью идентификатор расширения EXE, достаточно ввести команду assoc.exe.

После этого нужно перейти в ветвь реестра HKEY_CLASSES_ROOT\<идентификатор расширения>\shell. Вы уже обратили внимание, что подраздел с названием shell встречался в предыдущем совете данной главы? Все верно, это один и тот же подраздел с одинаковой структурой и одинаковыми возможностями. Поэтому описывать здесь способ создания нового элемента контекстного меню файлов мы не будем. Он и так был описан ранее.

Итак, чтобы добавить команду Открыть с помощью к контекстному меню файлов с расширением EXE, нужно в ветви реестра HKEY_CLASSES_ROOT\.exe\shell создать новый подраздел, допустим, с названием openWith. А в нем нужно создать вложенный подраздел с названием command. Чтобы добавить команду Открыть с помощью, параметру (По умолчанию) этого подраздела нужно присвоить строку rundll32 shell32.dll, OpenAs_RunDLL %1.

Если же вы хотите открывать исполняемые файлы только с помощью Блокнота, то параметру (По умолчанию) достаточно присвоить значение notepad.exe %1.

Настройка папки Панель управления

К сожалению, нет никаких стандартных способов настройки папки Панель управления. Однако это не значит, что вы не сможете изменить ее содержимое. Как обычно, для этого применяется реестр.

Скрытие апплетов классической папки Панель управления

Скрытие апплетов Панели управления может понадобиться по разным причинам. Но основной из них является оптимизация скорости отображения этой папки. Например, можно скрыть неиспользуемые вами апплеты, чтобы скорость отображения Панели управления увеличилась. Можно также скрыть все апплеты папки, после чего создать свой ActiveX-объект, отображаемый в Панели управления, с помощью контекстного меню которого можно будет запустить необходимый апплет. В этом случае скорость отображения папки будет почти мгновенной. Но эта возможность будет описана в приложении 4, а пока просто рассмотрим ветви реестра, с помощью которых можно скрыть тот или иной апплет.

Стандартной ветвью системного реестра Windows, используемой для этого, является `HKEY_CURRENT_USER\Control Panel\don't load`. Чтобы скрыть определенный апплет, нужно в этой ветви создать параметр строкового типа, название которого соответствует названию скрываемого апплета. Например, чтобы скрыть апплет `main.cpl`, нужно создать в этой ветви реестра параметр `main.cpl`.

Второй ветвью реестра, с помощью которой можно запретить отображение апплетов в Панели управления, является `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\don't load`. Ее формат полностью аналогичен предыдущей ветви, но она определяет те апплеты, которые не будут отображаться в Панели управления для всех учетных записей пользователей, тогда как предыдущая ветвь реестра скрывала апплеты только для текущей учетной записи.

ПРИМЕЧАНИЕ

Любой апплет можно вызвать с помощью команды вида rundll32.exe shell32.dll, Control_RunDLL "апплет или DLL-файл".

Теперь рассмотрим названия всех апплетов, доступных в Windows Vista.

- `Appwiz.cpl` — вызывает окно Установка и удаление программ. По умолчанию данный апплет скрыт с помощью ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\don't load`. Однако он отображается с помощью ActiveX-объекта.
- `Collab.cpl` — открывает окно Соседние пользователи.
- `Desk.cpl` — вызывает окно Параметры дисплея и отображает одноименный значок в Панели управления. По умолчанию апплет скрыт с помощью ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\don't load`.
- `Firewall.cpl` — открывает окно Брандмауэр Windows. По умолчанию апплет скрыт с помощью ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\don't load`. Однако он отображается с помощью ActiveX-объекта.
- `Hdwwiz.cpl` — вызывает окно Установить оборудование. По умолчанию апплет скрыт с помощью ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\`

Windows\CurrentVersion\Control Panel\don't load. Однако он отображается с помощью ActiveX-объекта.

- Inetcpl.cpl — открывает окно Свойства: Интернет.
- Intl.cpl — открывает окно Язык и региональные стандарты.
- Irprops.cpl — вызывает окно работы с устройствами Bluetooth.
- Joy.cpl — вызывает окно Игровые устройства.
- Main.cpl — открывает окна Свойства: Мышь и Свойства: Клавиатура.
- Mmsys.cpl — вызывает окно Звук.
- Ncpa.cpl — открывает окно Сетевые подключения и отображает одноименный значок в Панели управления. По умолчанию апплет скрыт с помощью ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\don't load. Однако он отображается с помощью ActiveX-объекта.
- Powercfg.cpl — вызывает окно Электропитание и отображает одноименный значок в Панели управления. По умолчанию апплет скрыт с помощью ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\don't load. Однако он отображается с помощью ActiveX-объекта.
- Sapi.cpl — открывает окно Свойства речи.
- Sysdm.cpl — вызывает окно Свойства системы. По умолчанию апплет скрыт с помощью ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\don't load. Однако он отображается с помощью ActiveX-объекта.

ПРИМЕЧАНИЕ

На вкладке Дополнительно окна Свойства системы присутствует кнопка Переменные среды, с помощью которой можно отобразить одноименное окно. Он позволяет изменить переменные среды окружения.

Окно Переменные среды можно отобразить и с помощью команды rundll32.exe sysdm.cpl, EditEnvironmentVariables.

- TabletPC.cpl — вызывает окно Перо и устройства ввода.
- Telephon.cpl — открывает окно Телефон и модем.
- Timedate.cpl — вызывает окно Дата и время.
- wmdConn.cpl — открывает окно Центр устройств Windows Mobile.
- Wscui.cpl — вызывает окно Центр обеспечения безопасности Windows.

ПРИМЕЧАНИЕ

Это же окно можно отобразить с помощью команды rundll32.exe shell32.dll, Control_RunDLL wscui.cpl perfnav_alsosecuritycenter.

Добавление и скрытие ActiveX-объектов из классической папки Панель управления

Кроме апплетов, Панель управления может содержать и различные ActiveX-объекты. Их также можно удалить (или добавить новые). Для этого используется ветвь реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace.

Чтобы добавить новый ActiveX-объект в классическую Панель управления, нужно в данной ветви реестра создать подраздел, название которого соответствует CLSID-номеру нового ActiveX-объекта. Соответственно, чтобы удалить один из существующих в классической Панели управления ActiveX-объектов, нужно удалить описывающий его подраздел.

CLSID-номера ActiveX-объектов (и определяемые ими окна), отображаемых по умолчанию в папке Панель управления, можно узнать из приложения 4.

Отображение апплетов в Панели управления при использовании вида по категориям

Еще одной возможностью настройки Панели управления является добавление новых апплетов при использовании вида по категориям. Для этого нужно не только определить добавляемый апплет, но и указать категорию, в которую он будет добавлен.

ПРИМЕЧАНИЕ

Если значение параметра REG_DWORD-типа RecentView, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel, равно 1, то при следующем запуске Панели управления будет использоваться вид по категориям.

Для добавления апплетов используется ветвь реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\Extended Properties\{305CA226-D286-468e-B848-2B2E8E697B74} 2. Чтобы добавить апплет, нужно создать в этой ветви реестра параметр REG_DWORD-типа, название которого должно определять путь к апплету и его наименование. Значение же этого параметра определяет категорию Панели управления, к которой будет добавлен данный апплет. Возможны следующие значения параметра:

- 0x00000001 — Оформление и персонализация;
- 0x00000002 — Оборудование и звук;
- 0x00000003 — Сеть и Интернет;
- 0x00000004 — Оборудование и звук;
- 0x00000005 — Система и ее обслуживание;
- 0x00000006 — Часы, язык и регион;

- 0x00000007 — Специальные возможности;
- 0x00000008 — Программы;
- 0x00000009 — Учетные записи пользователей и семейная безопасность;
- 0x0000000a — Безопасность;
- 0xFFFFFFFF — отображать только в классической Панели управления.

Отображение ActiveX-объектов в Панели управления при использовании вида по категориям

Способ отображения ActiveX-объектов в Панели управления при использовании вида по категориям отличается от применяемого в предыдущих версиях Windows. Теперь, чтобы отобразить ActiveX-объект, нужно в ветви реестра HKEY_CLASSES_ROOT\CLSID\{CLSID-номер ActiveX-объекта} создать параметр строкового типа System.ControlPanel.Category. Его значение определяет категорию (значения категорий описаны выше). При этом один и тот же ActiveX-объект может отображаться в разных категориях. Для этого достаточно написать несколько категорий через запятую. Например, чтобы отобразить ActiveX-объект сразу в категориях Оборудование и звук и Система и ее обслуживание, нужно данному параметру присвоить значение 2,5.

Отображение категории Мобильные ПК при использовании вида по категориям папки Панель управления

Если вы работаете не на ноутбуке, то вид категорий Мобильные ПК в папке Панель управления не используется, однако с помощью реестра можно указать, чтобы он также отображался. Для этого достаточно присвоить значение 1 параметру REG_DWORD-типа ShowCategoryMobilePC, расположенному в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\ControlPanel.

Вход и выход пользователя из системы

Некоторые параметры работы окна входа (и выхода) пользователя в систему также можно настроить. Однако для этого нет ни одного стандартного окна операционной системы Windows Vista, поэтому придется пользоваться другими способами.

ПРИМЕЧАНИЕ

Сведения о работе процесса winlogon.exe заносятся в журнал Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Winlogon.

Настройка с помощью групповых политик

Настроить параметры входа пользователей в систему можно сразу с помощью нескольких разделов групповых политик.

Первым разделом, с помощью которого это можно сделать, является раздел Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Вход в систему. Политики данного раздела определяются файлом `Logon.admx` и изменяют параметры `REG_DWORD`-типа, расположенные в дочерних подразделах ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies`.

- `DefaultLogonDomain` — параметр имеет строковый тип и расположен в дочернем разделе `System` данной ветви реестра. Он определяет домен, используемый по умолчанию при входе пользователя в систему.
- `ExcludedCredentialProviders` — имеет строковый тип и расположен в дочернем разделе `System`. С его помощью можно указать CLSID-номера провайдеров аутентификации, использование которых при аутентификации пользователей будет запрещено. По умолчанию Windows поддерживает провайдеры аутентификации с помощью пароля или смарт-карты.
- `DisableLocalMachineRun` — расположен в дочернем разделе `Explorer`. Если его значение равно `1`, то запуск программ, определенных в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, при входе пользователя в систему будет запрещен.
- `DisableLocalMachineRunOnce` — параметр расположен в дочернем разделе `Explorer`. Установка его значения равным `1` запрещает запуск при входе пользователя в систему программ, определенных в ветви системного реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`.
- `DisableStartupSound` — находится в дочернем разделе `System`. Если его значение равно `1`, то при входе пользователя в систему звук запуска операционной системы воспроизводиться не будет.
- `HideFastUserSwitching` — параметр расположен в дочернем разделе `System`. Если его значение равно `1`, то кнопка перехода между пользователями не будет отображаться в меню Пуск и окне входа в систему.
- `LogonType` — находится в дочернем разделе `System`. Если его значение равно `0`, то всегда будет отображаться классическое окно входа в систему.
- `SyncForegroundPolicy` — параметр расположен в ветви системного реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion\Winlogon`. Если его значение равно `1`, то операционная система будет ожидать полной инициализации сети перед завершением входа пользователя в систему.

С помощью значений параметров строкового типа, расположенных в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run`, можно определить программы, которые будут запускаться при входе пользователей в систему.

Параметры входа пользователя в систему можно изменить и с помощью групповых политик раздела Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Параметры входа Windows. Политики данного раздела определя-

ются файлом WinLogon.admx, изменяют параметры REG_DWORD-типа, расположенные в ветви HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

- Разрешить или запретить программам использование специального сочетания клавиш — изменяет значение параметра SoftwareSASGeneration. Определяет, могут ли службы или программы Центра специальных возможностей симулировать режим SAS.
- Отображать при входе пользователя сведения о предыдущих попытках входа — меняет значение параметра DisplayLastLogonInfo. Если значение данного параметра равно 1, то в окне входа в систему будет отображаться имя пользователя, который входил в систему в последний раз.
- Сообщать, когда сервер входа недоступен при входе пользователя — изменяет значение параметра ReportControllerMissing. Данная политика определяет, будет ли отображаться всплывающее сообщение, если компьютер при входе пользователя не смог соединиться с контроллером домена и из-за этого при входе использовались предыдущие настройки аутентификации.

Изображение пользователя, используемое для всех учетных записей, может быть переопределено с помощью параметра REG_DWORD-типа UseDefaultTile, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer. Это делается с помощью групповой политики раздела Конфигурация компьютера ▸ Административные шаблоны ▸ Панель управления ▸ Учетные записи пользователей.

Малоизвестные возможности

Изменение цвета Рабочего стола, отображаемого перед окном приветствия. Если вы решили полностью настроить интерфейс новой операционной системы Windows Vista, то с помощью параметра строкового типа background, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LogonType, можно указать цвет фона (в RGB-формате), который будет отображаться перед выводом окна приветствия.

Добавление учетной записи администратора к списку окна приветствия. По умолчанию окно приветствия не содержит возможности входа в операционную систему от имени учетной записи Администратор. Тем не менее, эту возможность можно добавить с помощью реестра.

Для этого достаточно воспользоваться ветвью реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList. По умолчанию она отсутствует, поэтому ее нужно создать. Она определяет учетные записи пользователей, которые будут отображаться в окне приветствия. Чтобы отобразить в окне приветствия учетную запись администратора, в этой ветви реестра нужно создать параметр REG_DWORD-типа administrator и присвоить ему значение 1.

Аналогичным образом можно скрывать или отображать другие учетные записи пользователей.

Настройка автоматического входа пользователя в систему. Как и предыдущие версии, Windows Vista поддерживает возможность указания пользователя, профиль которого автоматически будет загружаться при запуске операционной системы. Однако если в Windows XP это окно можно было отобразить только с помощью команды `rundll32.exe` или параметра программы `control.exe`, то в Windows Vista для этого предназначена специальная программа `netplwiz.exe`.

Достаточно запустить данную программу (отобразится окно Учетные записи пользователей), выбрать нужного вам пользователя из списка, снять флажок Требовать ввод имени пользователя и пароля и нажать кнопку OK. После этого отобразится окно, в котором нужно ввести пароль для учетной записи соответствующего пользователя. Теперь (при следующей перезагрузке) система будет автоматически использовать выбранный вами логин и введенный пароль для входа.

ПРИМЕЧАНИЕ

С помощью команды rundll32.exe netplwiz.dll, ClearAutoLogon можно отключить автоматический вход в систему.

Окно Учетные записи пользователей можно отобразить также с помощью команд `rundll32.exe netplwiz.dll, UsersRunDll` или `control USERPASSWORDS2`.

Завершение работы операционной системы с помощью команд rundll32.exe. С помощью некоторых команд программы `rundll32.exe` можно перезагрузить компьютер или сделать вид, что он будет перезагружен:

- `rundll32.exe IEAKENG.dll, DoReboot` — вызывает окно перезагрузки компьютера;
- `rundll32.exe shell32.dll, RestartDialogEx` — выводит окно перезагрузки компьютера;
- `rundll32.exe user32.dll, DisplayExitWindowsWarnings` — вызывает окно перезагрузки компьютера;
- `rundll32.exe user32.dll, LockWorkStation` — блокирует компьютер.

Завершение работы с помощью команды shutdown.exe. В поставку операционной системы Windows Vista входит программа командной строки, с помощью которой можно выполнить завершение работы компьютера. Эта команда поддерживает следующие варианты использования (они были доступны и в предыдущих версиях операционной системы Windows). В каждой из приведенных ниже команд можно использовать параметр `/m \\<IP-адрес компьютера>` для определения сетевого компьютера, работа которого будет завершена.

- `shutdown.exe /l` — выход текущего пользователя из системы.
- `shutdown.exe /s` — выключение компьютера.
- `shutdown.exe /r` — перезагрузка компьютера.

- `shutdown.exe /h` — перевод компьютера в спящий режим. Этот параметр является нововведением Windows Vista.
- `shutdown.exe /i` — отображает окно, с помощью которого можно настроить значения параметров команды. С его помощью можно выбрать компьютеры, которым будет послана команда завершения работы, комментарий, действие, которое произойдет (выход из системы, перезагрузка и т. д.). После того как вы настроите параметры команды и нажмете кнопку OK, команда будет послана всем выбранным компьютерам.

Программа также поддерживает дополнительные параметры, с помощью которых можно указать комментарий, интервал ожидания перед завершением работы компьютера и т. д. Кроме того, программа `shutdown.exe` операционной системы Windows Vista поддерживает три новых параметра: `G`, `P` и `E`. Подробнее об этих и других параметрах можно прочитать, если ввести команду `shutdown.exe /?`.

Настройка механизма поиска

Механизм поиска, используемый в Windows Vista, существенно изменился, поэтому в контексте данной главы о его новых настройках просто нельзя не упомянуть.

Окно Search

Но сначала рассмотрим само окно поиска и способы его использования.

После того как вы нажмете комбинацию клавиш Windows+F, перед вами отобразится окно, приведенное на рис. 3.26. Фактически, это обычное окно Проводника, имеющее дополнительную панель поиска, называемую Панель поиска. Собственно, такую же панель поиска можно отобразить и в Проводнике, если в меню Упорядочить выбрать команду Раскладка ▸ Панель поиска.

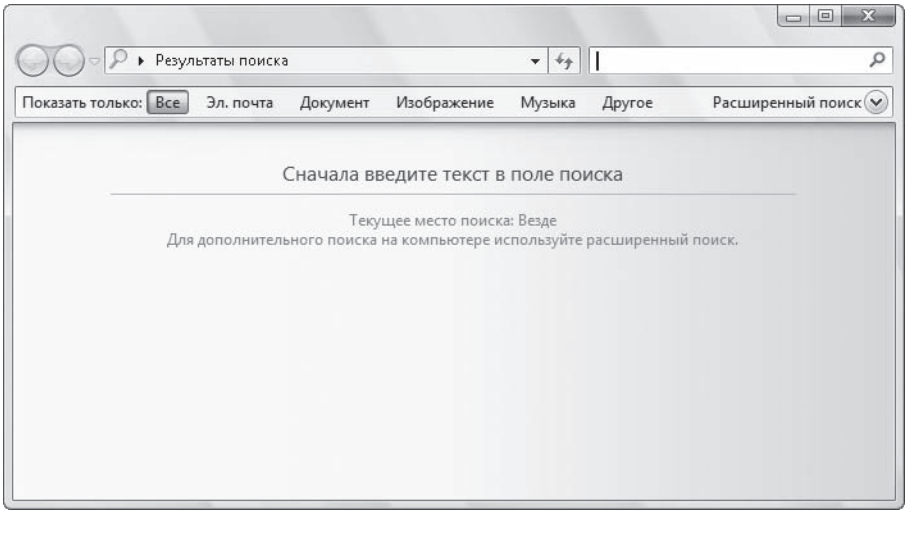


Рис. 3.26. Окно поиска

С помощью дополнительной панели поиска можно определить тип файла, который вы будете искать (кнопки напротив текста Показать только). По умолчанию выбрана кнопка Все, что говорит о том, что поиск будет вестись среди всех файлов. Вы также можете воспользоваться следующими кнопками:

- Изображение — искать среди файлов изображений с расширениями 3DS, A11, AI, ANI, ART, AMF, B1N, B8, BMP, CDR, CMP, CPS, EMF, EPS, GIF, TIF, TIFF, JPEG, JPG и т. д.;
- Музыка — вести поиск среди музыкальных файлов с расширениями AAC, AIF, AIFC, AU, CDA, DFS, DSS, M3U, MIDI, MID, MP3 и т. д.;
- Документ — искать среди файлов с расширениями XML, XLS, XLL, WRI, WPD, WKS, TXT, TEXT, RTF, PPT и т. д.;
- Эл. почта — вести поиск среди файлов с расширениями EML, MSG, NWS, VCS.

ПРИМЕЧАНИЕ

Если вы не знаете, к какой категории поиска относит операционная система Windows Vista файлы с тем или иным расширением, то можно посмотреть содержимое ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\KindMap. Она хранит параметры строкового типа. Название параметра определяет расширение файла, а значение параметра — категорию поиска, с помощью которой можно найти файлы с таким расширением.

Обратите внимание на стрелку вниз, напротив которой написан текст Расширенный поиск. После щелчка кнопкой мыши на ней отобразится дополнительная панель, с помощью которой можно выполнить поиск по метаданным файла или его параметрам. Панель содержит следующие поля.

- Папка — определяет каталог, в котором нужно искать данные.
- Дата — позволяет указать дату создания искомого файла.
- Размер (КБ) — можно указать размер искомого файла в килобайтах.
- Имя — позволяет указать имя искомого файла или шаблон для поиска.
- Ключевые слова — можно указать значения тегов, по которым нужно найти изображение или другой файл.
- Авторы — позволяет указать автора документа, который нужно найти.

На панели также расположен флажок Включая неиндексированные, скрытые и системные файлы (медленно). По умолчанию поиск выполняется только среди индексированных файлов, однако с помощью данного флажка это можно изменить.

Приведенные выше параметры отображаются, если вы выполняете поиск среди всех файлов (установлена кнопка Все поля Показать только). Если же вы выполняете поиск среди определенного типа файлов, то некоторые параметры поиска будут другими.

Сохранение запросов поиска

В Windows Vista присутствует возможность сохранения запросов поиска с целью их дальнейшего использования. Для этого после проведения поиска достаточно нажать кнопку Сохранить условия поиска панели инструментов. Это приведет к сохранению запроса поиска в файле, расположенном в каталоге `%userprofile%\Поиски`. В подразд. «Настройка Проводника» это раздела уже описывалось содержимое данного каталога, сейчас же поговорим о самих создаваемых папках поиска.

Каталог, создаваемый при сохранении поиска, является виртуальным (нововведение Windows Vista). Виртуальные каталоги основаны на запросах к базам данных, и при входе в соответствующий каталог будет выполняться запрос. В нашем случае поиск будет начинаться на основе запроса. Также на основе виртуального каталога создана ссылка Все программы меню Пуск.

ПРИМЕЧАНИЕ

Еще одним новым термином операционной системы Windows Vista является термин «виртуализация файлов и реестра». Данный механизм применяется операционной системой при активном UAC.

Механизм виртуализации используется операционной системой в том случае, если какая-либо программа пытается записать данные в каталог (или изменить значения ветви реестра), доступ на запись к которому ей запрещен. В этом случае запрос программы перенаправляется в каталог вида %userprofile%\AppData\Local\VirtualStore\<путь к реальному каталогу, в который пытается записать данные программа, без буквы диска>, либо в ветвь реестра вида HKEY_CURRENT_USER\Software\Classes\VirtualStore\<путь к реальной ветви реестра, в которую пытается записать данные программа>. Например, если программа пытается записать файл settings.ini в каталог C:\Program Files\this_program, доступ к которому ей запрещен, фактически программа запишет файл в каталог %userprofile%\AppData\Local\VirtualStore\program files\this_program.

Фактически каталог запроса поиска представляет собой текстовый файл в XML-формате с расширением SEARCH. Для примера попробуем создать команду контекстного меню файлов с данным расширением, с помощью которой можно просмотреть содержимое файла в Блокноте. Для этого нужно присвоить значение `notepad.exe %1` параметру (`По умолчанию`) ветви реестра `HKEY_CLASSES_ROOT\SearchFolder\shell\Notepad.exe\command`. Для сохранения целостности контекстного меню файлов запроса нужно также присвоить значение `open` параметру (`По умолчанию`) ветви реестра `HKEY_CLASSES_ROOT\SearchFolder\shell`.

После этого в контекстном меню каталогов запроса поиска отобразится команда `Notepad.exe`, с помощью которой можно просмотреть запрос в Блокноте. Непосредственно в нем вы также сможете изменять запрос поиска.

Вкладка Поиск окна Свойства папки

Основным окном настройки механизма поиска является вкладка Поиск окна Свойства папки. Данная вкладка содержит набор флажков, рассортированных по типу

применения. Флажки изменяют параметры REG_DWORD-типа ветви системного реестра Windows HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Search\Preferences.

Мы же рассмотрим назначения всех этих флажков вместе.

- Включать подпапки при вводе текста в поле поиска — изменяет значение параметра SearchSubFolders. Флажок определяет, будет ли выполняться поиск в содержащихся в каталоге подкаталогах, когда вы используете панели быстрого поиска (например, панель поиска в меню Пуск или в окне Проводника).
- Поиск частичных совпадений — меняет значение параметра AutoWildCard. Флажок определяет, будет по умолчанию выполняться поиск по части слова или для этого нужно использовать символы подстановки.
- Использовать языковой поиск — изменяет значение параметра EnableNaturalQuerySyntax.
- Не использовать индекс при поиске в файловой системе (медленно) — меняет значение параметра WholeFileSystem. Если флажок установлен, то поиск в файловой системе не будет выполняться только в содержимом индекса.
- Включать системные папки — изменяет значение параметра SystemFolders. Флажок определяет, будет ли выполняться поиск в системных каталогах.
- Включать сжатые файлы (ZIP, CAB…) — меняет значение параметра ArchivedFiles. Флажок определяет, будет ли выполняться поиск в заархивированных файлах (если поиск не выполняется в индексе).

На данной вкладке также расположен переключатель, с помощью которого можно определить, где именно по умолчанию будет выполняться поиск. Переключатель изменяет значения параметров REG_DWORD-типа SearchOnly, расположенных в ветвях реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Search\PrimaryProperties\IndexedLocations и HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Search\PrimaryProperties\UnindexedLocations, и может быть установлен в следующие положения.

- Индексированные места: имена файлов и содержимое. Неиндексированные места: только имена файлов — в индексированных каталогах выполнять поиск как по имени файла, так и в его содержимом. Если же каталог не индексирован, то выполнять поиск только в имени файла.
- Всегда искать имена файлов и содержимое (медленно) — выполнять поиск как в имени файла, так и в его содержимом.
- Всегда искать только имена файлов — выполнять поиск только в имени файла.

Окно Параметры индексирования

Окно предназначено для настройки индексирования файлов (рис. 3.27), значок для его запуска расположен в Панели управления. Чтобы его можно было запустить, нужно иметь административные права, а также необходимо, чтобы была запущена служба Поиск Windows.

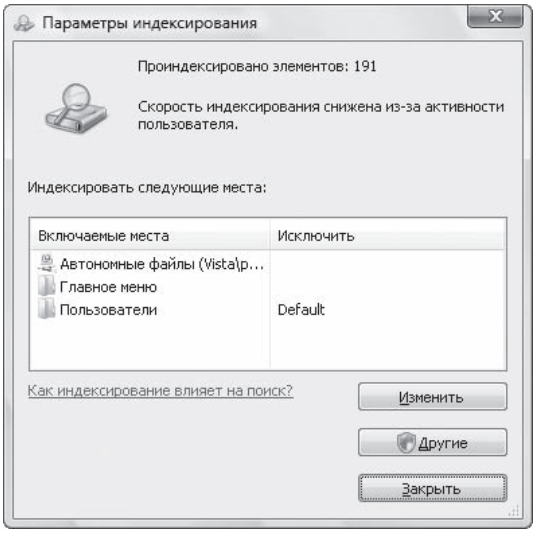


Рис. 3.27. Окно Параметры индексирования

Окно отображает количество файлов, находящихся на данный момент в индексе, а также список папок, содержимое которых разрешено добавлять в индекс. Чтобы добавить папку, содержимое которой будет индексироваться, или удалить уже присутствующую папку, нужно нажать кнопку Изменить. После этого отобразится окно Индексированные места. Чтобы добавить содержимое папки в индекс, достаточно установить напротив нее флажок. В противном случае нужно снять флажок. К сожалению, удалять из индекса автономные папки нельзя.

В окне Параметры индексирования также присутствует кнопка Другие, с помощью которой можно отобразить окно Дополнительно (рис. 3.28). Оно содержит две вкладки: Параметры индексирования и Типы файлов.

С помощью вкладки Параметры индексирования можно установить следующие настройки:

- будут ли индексироваться зашифрованные файлы;
- будут ли отдельно индексироваться похожие слова, но с небольшим отличием в написании;
- где будет находиться каталог, содержащий индекс (кнопка Выбрать новые);
- также можно удалить старый индекс и начать формирование нового, если вы подозреваете, что старый индекс был поврежден (кнопка Перестроить).

После перехода на вкладку Типы файлов перед вами отобразится список всех зарегистрированных в системе расширений файлов. Если флажок напротив расширения установлен, то файлы с данным расширением будут помещаться в индекс. По умолчанию в индекс помещаются очень многие файлы с расширениями, которые могут быть вам совершенно не нужны, поэтому желательно сразу же снять флажки напротив тех расширений, файлы которых вы не хотите видеть в индексе.

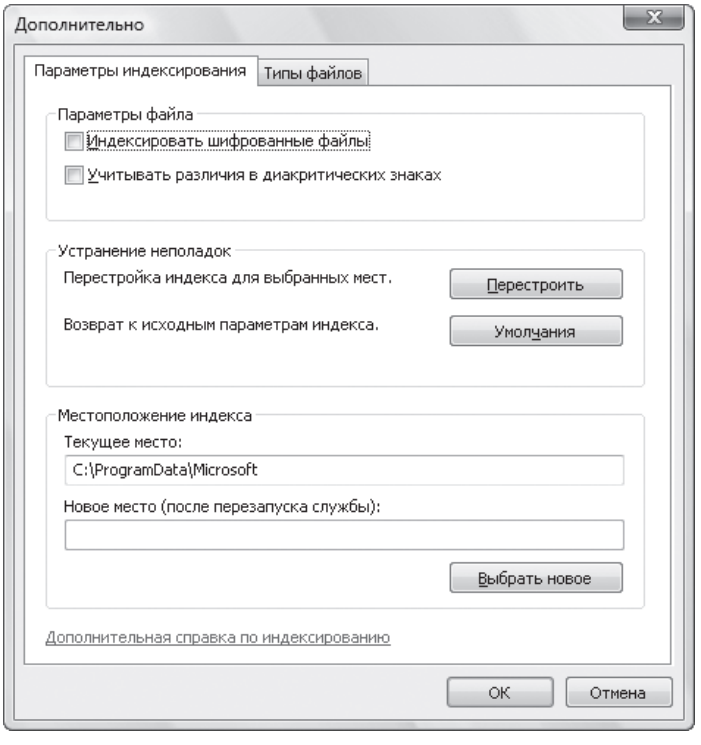


Рис. 3.28. Окно настройки индексируемых каталогов

После этого обратите внимание на второй столбик списка расширений — он определяет, что именно будет индексироваться у файла: все содержимое файла и его свойства или только его свойства. Если вы выделите расширение файла, то с помощью переключателей Индексировать только свойства и Индексировать свойства и содержимое файлов, расположенных внизу окна Дополнительно, сможете изменить индексируемое содержимое файла.

Настройка поиска с помощью групповых политик

Для настройки поиска с помощью групповых политик применяется раздел Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Поиск. Политики данного раздела описаны в файле `search.admx`, изменяют параметры `REG_DWORD`-типа, расположенные в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search`.

- `AllowIndexingEncryptedStoresOrItems` — если значение параметра равно `1`, то индексирование шифрованных файлов будет разрешено.
- `AllowUsingDiacritics` — при установке значения данного параметра равным `1` будет разрешено использование диакритических знаков. В этом случае слова, содержащие в своем составе диакритические знаки, и те же слова, но без диакритических знаков, будут считаться разными. В противном случае такие пары слов будут считаться идентичными.

- DataDirectory — имеет строковый тип. С его помощью можно изменить путь к каталогу, в котором будет храниться база данных индексирования.
- PreventIndexingEmailAttachments — если значение этого параметра равно 1, то индексация почтовых вложений запрещена.
- PreventIndexingOfflineFiles — при установке значения данного параметра равным 1 будет запрещена индексация содержимого каталога автономных файлов.
- PreventIndexingOutlook — если значение параметра равно 1, то индексация сообщений почтового клиента будет запрещена.
- PreventIndexingPublicFolders — при установке значения данного параметра равным 1 будет запрещена индексация содержимого каталога Public.
- PreventIndexingUncachedExchangeFolders — если значение этого параметра равно 1, то индексация некэшируемых каталогов программы Exchange будет запрещена (по умолчанию запрещена).
- PreventUsingAdvancedIndexingOptions — при установке значения данного параметра равным 1 не будет отображаться окно настройки дополнительных возможностей индексирования (отображается с помощью кнопки Другие окна Параметры индексирования).

Настройка дополнительных параметров индексирования

Теперь рассмотрим дополнительные возможности настройки индексирования файлов. Одной из них является изменение свойств файлов, которые будут индексироваться. По умолчанию список свойств хранится в текстовом файле msscolumn.txt, расположенном в каталоге %programdata%\Microsoft\Search\Config. Данный файл хорошо документирован, однако его настоятельно не рекомендуется изменять вручную. Если вы хотите изменить параметры индексирования свойств, необходимо воспользоваться файлом gencolmn.xsl, после чего нужно перезапустить службу индексирования, что приведет к повторному созданию файла msscolumn.txt.

Другим способом дополнительной настройки индексирования является редактирование параметров ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Search и ее подразделов. Эта ветвь содержит следующие наиболее интересные параметры.

- Data Directory — параметр строкового типа позволяет изменить путь к каталогу, в котором служба индексирования будет хранить свои данные. По умолчанию используется каталог %programdata%\Microsoft\Search\Data.
- DefaultColumnFile — имеет строковый тип и позволяет изменить путь к файлу msscolumn.txt, содержащему, как вы знаете, список свойств, которые будут индексироваться.
- UseLowPriorityConfiguration — этот параметр REG_DWORD-типа позволяет определить приоритет работы службы индексирования (то есть количество процессорного времени, которое будет использоваться для создания и проверки индекса).

Следует выделить и ветвь реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Search\CatalogNames\Windows\SystemIndex. Она также содержит несколько интересных параметров:

- IgnoreShortcuts — этот параметр REG_DWORD-типа определяет, будут ли заноситься в индекс ярлыки файлов;
- Pkm:catalog:LastUrlIndex — параметр строкового типа определяет название файла, на котором завершился процесс индексирования файлов.

Еще одной ветвью реестра, которая хранит интересные параметры индексирования, является ветвь HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Search\Gather. Она определяет параметры выполнения индексирования файлов и содержит следующие возможности.

- LowDiskMinimumMBytes — этот параметр REG_DWORD-типа позволяет указать размер свободного места на диске (в мегабайтах), содержащем базу данных индекса, при преодолении которого помещение файлов в индекс будет запрещено. По умолчанию файлы в индекс не помещаются, если на диске осталось меньше 50 Мбайт.
- NotifyQueueFileLimit — позволяет указать максимальное количество файлов, которые можно поместить в индекс. По умолчанию используется значение 49 999 (в десятичной системе счисления).

Поиск с помощью программы where

Поиск можно выполнить и с помощью новой программы командной строки операционной системы Windows Vista. Она позволяет искать нужные файлы на основе шаблонов в указанном каталоге.

У вас, возможно, возникнет вопрос, зачем пользоваться этой программой, если можно использовать стандартное окно Результаты поиска операционной системы Windows Vista. Дело в том, что поиск с помощью программы where примерно в 20 раз быстрее, чем с помощью окна Результаты поиска.

Рассмотрим основные возможности данной программы. Чтобы просмотреть ее подробное описание, в командной строке введите команду where /?.

- where <шаблон имени файла или несколько шаблонов, написанных через пробел> — выполняет поиск файлов на основе указанных шаблонов в текущем каталоге. При этом на экране отображаются только пути к найденным файлам и их имена.

  В шаблонах имен файлов используются стандартные подстановочные символы. Например, символ ? заменяет один любой символ, а символ * заменяет любое количество символов. Например, шаблон test*.* выполняет поиск всех файлов любого расширения, имена которых начинаются с test. А шаблон test?.mp? выполняет поиск файлов, состоящих из пяти символов, первые четыре из которых равны test. Расширение файла должно состоять из трех символов, первые два из которых равны mp.

- where /R <каталог> <шаблон имени файла или несколько шаблонов, написанных через пробел> — искать на основе указанных шаблонов в указанном каталоге и его подкаталогах.
- where /T <каталог> <шаблон имени файла или несколько шаблонов, написанных через пробел> — кроме имени найденных файлов, отображается их размер, а также дата изменения.

Поиск с помощью программы find.exe

Если же вам нужно выполнить поиск в содержимом одного или нескольких файлов каталога, то можно воспользоваться программой командной строки find.exe. Основной синтаксис данной программы следующий: find <строка, по которой ищем> <путь к каталогу и название файла>. Например, с помощью команды find "Windows" C:\download\support.microsoft.com\kb* выполняется поиск файлов, содержащих слово «Windows», среди всех файлов соответствующего каталога.

Перед строкой, которую нужно искать, можно указать дополнительные параметры, изменяющие сам смысл поиска:

- /V — в результате поиска отобразить на экране все строки, которые не содержат той строки, которую мы ищем;
- /C — отобразить на экране все строки, которые содержат ту строку, которую мы ищем;
- /N — в результате поиска отобразить номера строк, которые подходят условиям поиска;
- /I — игнорировать регистр искомого слова при выполнении поиска.

Поиск с помощью программы findstr.exe

Большими возможностями поиска в содержимом файла обладает программа командной строки findstr.exe. Хотя ее основной синтаксис такой же, как и у программы find.exe (findstr <строка, по которой ищем> <путь к каталогу и название файла>), она поддерживает больше параметров поиска.

Просмотреть список параметров данной программы можно с помощью команды findstr /?.

Настройка оболочки

Последней темой, которую мы рассмотрим в контексте данной главы, будет общая настройка оболочки операционной системы Windows Vista. Как и раньше, для этих целей существует несколько стандартных окон.

Окно Параметры быстродействия

С его помощью можно настроить основные параметры оптимизации оболочки Windows Vista. Чтобы его отобразить, нужно сначала вызвать окно Система. Наиболее быстрым способом для этого является нажатие сочетания клавиш Windows+Pause Break.

В появившемся окне нужно выбрать ссылку Дополнительные параметры системы, что приведет к запуску программы `SystemPropertiesAdvanced.exe`, расположенной в каталоге `%systemroot%\system32`. Она представляет собой окно Свойства системы, используемое в предыдущих версиях операционной системы Windows. Чтобы отобразить окно Параметры быстродействия, нужно на вкладке Дополнительно в области Быстродействие нажать кнопку Параметры.

Окно Параметры быстродействия (рис. 3.29) содержит три вкладки: Визуальные эффекты, Дополнительно и Предотвращение выполнения данных.

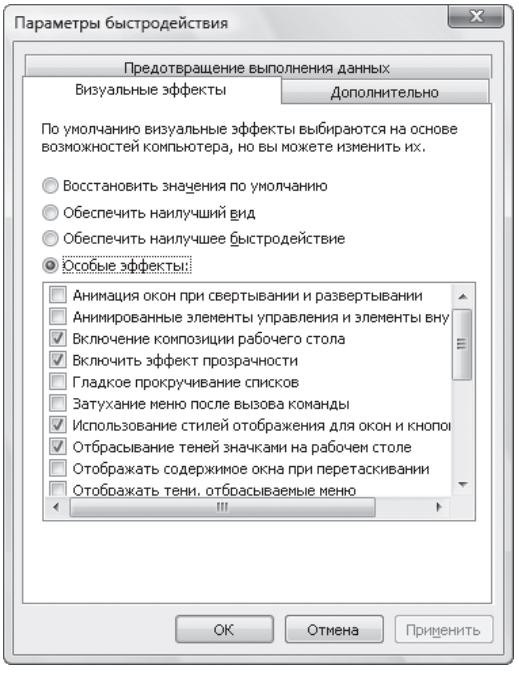


Рис. 3.29. Окно Параметры быстродействия

Вкладка Визуальные эффекты

Вкладка содержит основные настройки оптимизации интерфейса оболочки Windows Vista. Все они расположены в приведенном списке. Рассмотрим наиболее интересные возможности настройки, предоставляемые данным списком.

- Анимация окон при свертывании и развертывании — вы, наверное, заметили, что теперь в Windows Vista применяется особый эффект при максимизации и минимизации окон программ и Проводника. Этот эффект требует много системных ресурсов и, возможно, может просто не понравиться многим пользователям. Поэтому с помощью снятия данного флажка можно отключить и эффект минимизации/максимизации окон.
- Эффекты затухания или скольжения при обращении к меню — определяет, будут ли применяться эффекты затухания или выдвижения при отображении списков

меню. Если необходимо повысить быстродействие работы операционной системы, этот флажок лучше снять.

- Эффекты затухания или скольжения при появлении подсказок — флажок определяет, будут ли применяться эффекты затухания или выдвижения при отображении подсказок в области уведомлений. Если необходимо повысить быстродействие работы операционной системы, то этот флажок лучше снять.
- Затухание меню после вызова команды — определяет, будет ли применяться эффект затухания после того, как вы выберете элемент из списка меню. Если необходимо повысить быстродействие работы операционной системы, этот флажок лучше снять.
- Отображать тени, отбрасываемые меню — флажок определяет, будут ли отображаться тени под списками меню. На тени под окнами этот флажок не влияет. Если необходимо повысить быстродействие работы операционной системы, этот флажок лучше снять.
- Отображение тени под указателем мыши — определяет, будет ли отображаться тень под указателем мыши. Если необходимо повысить быстродействие работы операционной системы, этот флажок лучше снять.
- Отображение прозрачного прямоугольника выделения — флажок определяет, будет ли отображаться полупрозрачный прямоугольник выделения. По умолчанию флажок установлен, что приводит к отображению прямоугольника выделения синим полупрозрачным цветом. Если вы снимете этот флажок, то прямоугольник выделения станет полностью прозрачным.
- Гладкое прокручивание списков — определяет, будет ли использоваться гладкая прокрутка раскрывающихся списков меню. Если необходимо повысить быстродействие работы операционной системы, то этот флажок лучше снять.
- Отбрасывание теней значками на рабочем столе — флажок определяет, будут ли отображаться тени от значков, расположенных на Рабочем столе. Если необходимо повысить быстродействие работы операционной системы, этот флажок лучше снять.
- Использование стилей отображения для окон и кнопок — снятие этого флажка приведет к отключению интерфейса Aero Glass и изменению интерфейса Windows Vista на стандартный интерфейс предыдущих версий операционной системы.

Кроме того, на вкладке Визуальные эффекты расположен переключатель. Если вы установите его в положение Восстановить значения по умолчанию или Обеспечить наилучший вид, то все флажки в описанном выше списке будут установлены, то есть будут использоваться все предоставляемые Windows Vista эффекты интерфейса. Если вы установите переключатель в положение Обеспечить наилучшее быстродействие, то все эффекты операционной системы Windows, описанные в данном списке, будут отключены.

Вкладка Дополнительно

Файл подкачки. Вкладка позволяет изменить размеры файла подкачки операционной системы. Он представляет собой файл на жестком диске, в который

операционная система помещает (из оперативной памяти) давно не используемые данные. Для этого система делит всю оперативную память на страницы. Если к какой-то странице давно не обращались, она помещается в файл подкачки. Если в дальнейшем происходит обращение к странице, которая в данный момент находится в файле подкачки, то она помещается обратно в оперативную память. Общий размер памяти, доступной программе, равен сумме объемов файла подкачки и оперативной памяти.

Для операционных систем семейства x86 размер файла подкачки не может быть больше 4 Гбайт (так как именно такой максимальный размер может быть у общего виртуального пространства), если только для процессора не включен механизм PAE (расширение физических адресов). В этом случае размер файла подкачки может достигать 16 Тбайт.

Несмотря на то что 32-разрядные операционные системы могут использовать до 128 Гбайт физической памяти, максимальный размер любого виртуального пространства пользовательского процесса равен 2 Гбайт (если не используются параметры загрузки операционной системы `/3GB` или `/USERVA`). Если же необходимо расширить максимальный доступный объем виртуальной памяти, то применяются механизмы PAE (функция диспетчера памяти) или AWE (набор API-интерфейсов, позволяющий программам резервировать большие области памяти).

Механизм PAE позволяет адресовать до 64 Гбайт виртуального пространства для 32-разрядных и до 1024 Гбайт для 64-разрядных операционных систем.

ПРИМЕЧАНИЕ

Если вам когда-нибудь будет нужно удалить файл подкачки, то это можно сделать, запустив операционную систему в безопасном режиме с поддержкой командной строки.

По умолчанию операционная система создает файл подкачки, который в полтора раза больше, чем текущий размер установленной в системе оперативной памяти. На данный момент многие компьютеры начинают оснащать более чем 1 Гбайт оперативной памяти, поэтому необходимость в большом файле подкачки становится все меньше и меньше. Более того, в некоторых случаях можно вообще отключить создание файла подкачки, если было определено, что компьютер совершенно нормально справляется и без него.

ПРИМЕЧАНИЕ

Для просмотра сведений о файле подкачки можно использовать два стандартных класса репозитария CIM: Win32_PageFileUsage и Win32_PageFile. Оба этих свойства хранятся в пространстве имен root\cimv2.

С помощью класса Win32_PageFileUsage можно просмотреть сведения о текущем состоянии файла подкачки. Например, класс поддерживает следующие свойства: AllocatedBaseSize (определяет общий размер файла подкачки), CurrentUsage (опре-

деляет текущий размер, используемый файлом подкачки (в мегабайтах)), Name (ключевое свойство, которое определяет путь к файлу подкачки), PeakUsage (определяет максимальный размер (в мегабайтах) файла подкачки за текущий сеанс работы операционной системы).

Используя класс Win32_PageFile, можно узнать параметры настройки файла подкачки. Многие из возможностей данного класса соответствуют возможностям класса Win32_PageFileUsage.

Чтобы определить интенсивность использования файла подкачки, нужно понаблюдать за состоянием следующих счетчиков производительности (описание счетчиков производительности будет приведено в гл. 5, посвященной оснасткам операционной системы).

- `\MEMORY\\Available Mbytes` — определяет доступный в данный момент объем оперативной памяти. Если вы хотите полностью отключить файл подкачки, то значение данного счетчика никогда не должно опускаться ниже 4 Мбайт.
- `\MEMORY\\Pages Input/sec` — указывает количество страниц, которые помещаются в оперативную память за одну секунду. Если значение данного счетчика больше или равно десяти, то вам, скорее всего, нужно думать не о том, отключать файл подкачки или нет, а о том, куда бы перенести его для повышения доступа к нему.

  Если обращение к файлу подкачки происходит слишком интенсивно (десять страниц в секунду или больше), то рекомендуется переместить его на отдельный жесткий диск или даже набор RAID-дисков.
- `\Paging File(_Total)\\%Usage` — определяет процент использования файла подкачки. Если значение данного счетчика постоянно больше 70 %, то файл подкачки рекомендуется перенести на отдельный диск.
- `\Paging File(_Total)\\%Usage Peak` — указывает пиковый процент использования файла подкачки. Если значение данного счетчика постоянно больше 70 %, то файл подкачки рекомендуется перенести на отдельный диск.
- `\Process(_Total)\\Page File Bytes Peak` — пиковый порог использования файла подкачки процессами в байтах. Значение данного счетчика не должно быть слишком большим.

Направление оптимизации. На вкладке также можно указать, для каких операций будет оптимизироваться работа операционной системы Windows Vista. Для этого применяется переключатель, расположенный в области Распределение времени процессора. По умолчанию переключатель установлен в положение программ. Если вы установите его в положение служб, работающих в фоновом режиме, то распределение времени работы процессора изменится — количество тактов, которые предоставляются процессу, расположенному на переднем плане, на один такт, предоставляемый процессам заднего плана, уменьшится. Иными словами, больше тактов процессора будут предоставляться различным службам и программам, которые не имеют в данный момент фокус.

Вкладка Предотвращение выполнения данных

С помощью вкладки Предотвращение выполнения данных можно определить, будет включен механизм защиты от неправомерного изменения содержимого оперативной памяти (DEP) для всех программ или только для основных системных модулей. Если вы выбрали использование механизма DEP для всех программ, то с помощью данной вкладки также можно указать программы-исключения, проверка работы которых выполняться не будет.

Основным назначением механизма DEP является предотвращение запуска вредоносного кода из области данных, стека и кучи (как правило, эти области никогда не должны содержать исполняемый код). Благодаря этому предотвращаются некоторые виды атак, которые помещают исполняемый код в область памяти, не содержащую его изначально и не предназначенную для запуска кода (стек, куча и т. д.), и запускают этот код.

Операционная система Windows Vista поддерживает как программную, так и аппаратную реализацию механизма DEP.

Аппаратная реализация. Аппаратная реализация механизма DEP должна поддерживаться процессором компьютера (у AMD она называется NX, а у Intel — XD). При ее использовании определенные области памяти помечаются специальным атрибутом, который запрещает запуск кода из этих областей памяти (изменяется один бит элемента таблицы страниц виртуальной памяти (PTE)) и вызывает исключение при попытке запуска. Если данное исключение остается необработанным, то запуск такого исполняемого кода запрещается.

Чтобы аппаратная реализация DEP могла работать, механизм PAE процессора должен быть включен. Операционная система включает его автоматически, если процессор поддерживает аппаратную реализацию DEP.

Аппаратная реализация DEP может не работать в том случае, если она запрещена в BIOS. Некоторые BIOS хранят параметр, который может называться так: `Data Execution Prevention`, `XD`, `Execute Disable` или `NX`. С его помощью можно отключить аппаратную реализацию DEP.

Программная реализация. По умолчанию в операционных системах Windows Vista включена программная реализация механизма DEP. Именно ею можно управлять с помощью вкладки Предотвращение выполнения данных. Программная реализация механизма DEP не зависит от того, поддерживает или нет процессор аппаратную реализацию DEP. Она блокирует программы, которые пытаются воспользоваться механизмом обработки исключений операционной системы Windows.

ПРИМЕЧАНИЕ

В 64-разрядных версиях операционной системы механизм DEP всегда включен для всех программ и драйверов устройств. Отключить его нельзя.

Варианты работы DEP. Как программная, так и аппаратная реализация DEP поддерживает четыре варианта работы.

- `OptIn` — используется по умолчанию. Механизм DEP защищает только основные системные файлы, например стеки потоков и страницы пользовательского режима.
- `OptOut` — механизм DEP включен для всех программ, запускаемых пользователем. При этом вы можете указать программы-исключения с помощью вкладки Предотвращение выполнения данных. Программы-исключения заносятся в реестр в виде параметров строкового типа, названия которых определяют путь к программам-исключениям. Значение же параметров равно `DisableNXShowUI`. Эти параметры хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers`.
- `AlwaysOn` — механизм DEP включен для всех программ, запускаемых пользователем. При этом нельзя указать программы-исключения с помощью вкладки Предотвращение выполнения данных. Даже те программы, для которых запрещен запуск с включенным DEP, загружаются с ним.
- `AlwaysOff` — механизм DEP всегда отключен, даже если он аппаратно поддерживается процессором.

Чтобы изменить вариант работы механизма DEP, нужно указать новый вариант с помощью программы `bcdedit.exe`. Синтаксис этой программы был описан в первых главах данной книги.

Окно Загрузка и восстановление

Сразу же хотелось бы рассмотреть еще одно окно, доступ к которому можно получить с помощью вкладки Дополнительно окна Свойства системы. Оно не влияет на интерфейс операционной системы Windows Vista, но позволяет настроить поведение операционной системы при возникновении ошибок.

ПРИМЕЧАНИЕ

В операционной системе Windows XP можно было самостоятельно сгенерировать «синий экран» с кодом 0x000000E2. Для этого нужно было присвоить параметру REG_DWORD-типа CrashOnCtrlScroll, расположенному в ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters, значение 1. После этого (после перезагрузки компьютера) можно будет вызвать «синий экран», дважды нажав клавишу Scroll Lock, удерживая при этом нажатой правую клавишу Ctrl.

Данная возможность поддерживается только клавиатурами, использующими стандартный драйвер операционной системы i8042prt.sys. Как правило, это клавиатуры, работающие через порт PS/2.

Операционная система Windows Vista также содержит данный драйвер, и он тоже поддерживает параметр CrashOnCtrlScroll.

Чтобы отобразить окно Загрузка и восстановление, нужно нажать кнопку Параметры в области Загрузка и восстановление. Окно содержит два основных поля: Загрузка

операционной системы и Отказ системы. Первую область мы рассмотрели, когда настраивали параметры загрузочного меню Windows Vista, поэтому сейчас обратим внимание только на вторую.

Область Отказ системы содержит три флажка, установленных по умолчанию:

- Записать событие в системный журнал — определяет, будет ли записываться сообщение об ошибке в системный журнал Windows Vista;
- Выполнить автоматическую перезагрузку — указывает, будет ли выполняться автоматическая перезагрузка компьютера при отображении «синего экрана смерти»;
- Заменять существующий файл дампа — определяет, будет ли выполняться перезапись файла дампа содержимого оперативной памяти (`memory.dmp`), если он уже существует.

Виды дампов памяти. С помощью области Отказ системы можно определить, будет ли вообще создаваться дамп содержимого оперативной памяти при возникновении ошибки, и если будет, то какой. Для этого используется раскрывающийся список области Запись отладочной информации. Он содержит следующие элементы.

- (отсутствует) — не создавать дамп памяти.
- Малый дамп памяти (64 КБ) — создает малый дамп памяти размером 64 Кбайт, содержащий только информацию об ошибке. Все малые дампы памяти хранятся в каталоге `%systemroot%\Minidump` (в виде отдельных файлов с именами в формате `mini<месяц><день><год>-<порядковый номер файла>.dmp`).

  Малый дамп памяти включает в себя следующие данные:

  - список драйверов, загруженных во время возникновения ошибки;
  - контекст процессора (PRCB), который привел к возникновению ошибки;
  - сведения о процессе, вызвавшем ошибку, и контекст его ядра (EPROCESS);
  - сведения о процессе, поток которого вызвал ошибку, и его контекст ядра (ETHREAD);
  - стек вызовов в режиме ядра для потока, который привел к ошибке.

  Следует обратить внимание на то, что малый дамп памяти можно создавать только в том случае, если размер используемого операционной системой файла подкачки (расположенного на загрузочном томе) равен как минимум 2 Мбайт.

  Данный вид дампа памяти можно загружать с помощью программы `Dumpchk.exe`. Она анализирует дамп памяти, выводит его содержимое в удобочитаемом виде, а также указывает на секции, в которых, возможно, и возникла ошибка. Основной синтаксис данной программы: `Dumpchk.exe <параметры> <имя файла малого дампа>`.
- Дамп памяти ядра — создает только дамп оперативной памяти, содержащей ядро операционной системы. Данный тип дампа используется по умолчанию. При этом в каталоге `%systemroot%` будет создаваться файл `memory.dmp`. Размер

файла `memory.dmp` будет равен примерно одной трети от всего объема оперативной памяти компьютера.

Дамп памяти ядра хранит содержимое памяти, выделенное для:

- ядра;
- HAL;
- драйверов режима ядра и других программ режима ядра.

Данный вид дампа памяти можно загружать в стандартные символьные отладчики операционной системы.

- Полный дамп памяти — вместо дампа ядра операционной системы создается полный дамп оперативной памяти. При этом создается файл `memory.dmp`, расположенный в каталоге `%systemroot%`, который хранит содержимое всей оперативной памяти компьютера на момент возникновения ошибки. При следующем возникновении ошибки содержимое файла `memory.dmp` будет перезаписано.

  Следует обратить внимание на то, что полный дамп памяти можно создавать только в том случае, если размер используемого операционной системой файла подкачки как минимум на 1 Мбайт больше объема всей оперативной памяти компьютера. Кроме того, полный дамп памяти нельзя создавать на компьютерах с 32-битной операционной системой, на которых установлено более 2 Гбайт оперативной памяти.

  Данный вид дампа памяти можно загружать в стандартные символьные отладчики операционной системы.

ПРИМЕЧАНИЕ

Параметры работы с дампами памяти можно просмотреть и с помощью свойств класса Win32_OSRecoveryConfiguration, принадлежащего пространству имен root\cimv2. Например, данный класс поддерживает следующие свойства: AutoReboot (определяет, будет ли выполняться автоматическая перезагрузка компьютера при возникновении критической ошибки), DebugFilePath (определяет путь к файлу, в который будут помещаться данные при создании полного дампа памяти), DebugInfoType (определяет тип создаваемого при возникновении ошибки дампа памяти), KernelDumpOnly (определяет, будет ли выполняться только создание дампа памяти ядра), Name (ключевое свойство, определяющее операционную систему, настройки которой хранятся в экземпляре класса), OverwriteExistingDebugFile (определяет, будет ли новый дамп памяти перезаписывать старый), SendAdminAlert (определяет, будет ли при возникновении ошибки отправляться сообщение на административную консоль), WriteToSystemLog (определяет, будет ли при возникновении ошибки информация о ней записываться в стандартный журнал операционной системы).

В операционной системе Windows Vista вы можете самостоятельно создать дамп памяти запущенного в данный момент процесса. Для этого достаточно запустить программу Windows Task Manager (комбинация клавиш Ctrl+Shift+Esc), перейти на вкладку Процессы, найти нужный процесс и в его контекстном меню выбрать команду Create Dump File. После этого начнется создание дампа памяти, по завершении

которого перед вами отобразится путь к каталогу, в котором был создан дамп памяти данного процесса.

Использование групповых политик

Для настройки оболочки можно применять групповые политики, расположенные в подразделе Конфигурация пользователя ▸ Административные шаблоны ▸ Меню «Пуск» и панель задач.

Все описанные далее групповые политики изменяют значения параметров типа REG_DWORD ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.

- Отключить слежение за действиями пользователя — установка этой политики позволяет отключить стандартный механизм операционных систем семейства Windows, направленный на слежение за действиями пользователя. Например, именно с помощью этого механизма возможна работа персонализированного меню Пуск и персонализированных меню различных программ. Если вы не пользуетесь этой возможностью, то для увеличения быстродействия компьютера ее можно отключить.

  Политика влияет на значение параметра NoInstrumentation.

- Не использовать сопоставление ярлыков оболочки на основе поиска — установка данной политики позволяет отключить стандартный механизм операционных систем семейства Windows, направленный на восстановление ярлыков, не работающих из-за перемещения файла, на которые они указывали. После установки данной политики система не будет выполнять поиск перемещенного файла на томах NTFS.

  Эта политика влияет на значение параметра NoResolveSearch.

- Не использовать метод на основе отслеживания для сопоставления ярлыков — установка этой политики позволяет отключить стандартный механизм операционных систем семейства Windows, направленный на восстановление ярлыков, не работающих из-за перемещения файлов, на которые они указывали. После установки данной политики система не будет выполнять поиск перемещенного файла на основе его идентификатора на томах NTFS. Вместо этого будет выдаваться сообщение о том, что ярлык указывает на несуществующий файл.

Политика влияет на значение параметра NoResolveTrack.

Настройка оболочки с помощью реестра

Теперь рассмотрим, как можно настроить оболочку, используя параметры реестра.

Установка активации окон при перемещении на них указателя

В Windows Vista, как и в остальных операционных системах семейства Windows, присутствует возможность активации окна при перемещении на него указателя мыши без дополнительного щелчка кнопкой мыши на нем. Это может быть очень полезно для портативных компьютеров (ноутбуков или Tablet PC), где не слишком удобно пользоваться левой и правой кнопками мыши.

Для включения активации применяется два бита (это битовая маска) параметра REG_DWORD-типа UserPreferencesMask, расположенного в ветви реестра HKEY_CURRENT_USER\Control Panel\Desktop.

ПРИМЕЧАНИЕ

Этот параметр может иметь тип REG_BINARY. Не забывайте, что параметры такого типа отличаются от параметров типа REG_DWORD направлением чтения байтов. Например, если нужно установить битовую маску 0x00000001, то нужно добавить к значению параметра типа REG_DWORD значение 1 (то есть изменить последний байт значения параметра). Однако, если нужно добавить эту битовую маску к параметру типа REG_BINARY, то значение 1 нужно добавить к первому байту значения параметра (например, чтобы добавить 1 к значению параметра 00 00 00 00, нужно изменить значение параметра на 01 00 00 00).

- 0x00000001 — установка данного бита приводит к активации окна при наведении на него указателя. При этом само окно не переходит на передний план.
- 0x00000040 — установка этого бита приводит к тому, что активированные окна будут переходить на передний план.

Можно также определить время удержания указателя мыши над окном перед тем, как оно станет активным. Для этого необходимый интервал времени (в миллисекундах) нужно указать в параметре REG_DWORD-типа ActiveWndTrkTimeout, расположенном в ветви реестра HKEY_CURRENT_USER\Control Panel\Desktop.

Изменение времени отображения списков меню

По умолчанию Windows Vista выполняет задержку перед отображением содержимого меню (приблизительно в половину секунды). Однако существует возможность ее отключения или изменение самой величины задержки.

Для этого применяется параметр строкового типа MenuShowDelay, расположенный в ветви реестра HKEY_CURRENT_USER\Control Panel\Desktop. Он содержит величину задержки в миллисекундах.

Изменение цвета, которым выделяются сжатые и зашифрованные файлы и папки

По умолчанию названия сжатых файлов операционная система Windows Vista выделяет синим цветом, а зашифрованных — зеленым. Однако можно самостоятельно указать цвета, которыми будут отображаться сжатые и зашифрованные файлы. Для этого нужно воспользоваться ветвью реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer.

Чтобы изменить цвет названия сжатых файлов, нужно указать новый цвет в параметре REG_BINARY-типа AltColor. Этот параметр имеет следующий формат значения: 0×R 0×G 0×B 00, где 0×R представляет красную компоненту цвета, 0×G — зеленую, а 0×B — синюю.

Чтобы изменить цвет названия сжатых файлов, нужно указать новый цвет в параметре REG_BINARY-типа AltEncryptionColor.

Изменение назначения клавиш мультимедийной клавиатуры

Если вы обладаете мультимедийной клавиатурой, имеющей такие дополнительные клавиши, как, например, Back, E-Mail, Media, Calculator и т. д., то с помощью реестра можно изменить их назначение. Для этого нужно указать новую команду в параметре строкового типа Shell Execute в одном из подразделов ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\AppKey.

Эта ветвь реестра может содержать следующие подразделы, каждый из которых определяет команду отдельной клавиши:

- 1 — Back;
- 2 — Forward;
- 3 — Refresh;
- 4 — Stop;
- 5 — Search;
- 6 — Favorites;
- 7 — Home;
- 15 — E-mail;
- 16 — Media;
- 17 — My Computer;
- 18 — Calculator.

Вместо параметра Shell Execute можно воспользоваться еще одним параметром строкового типа: Association. Его значение должно представлять собой расширение файла (вместе с точкой), ассоциированная с которым программа будет запускаться после нажатия данной мультимедийной клавиши.

Настройка параметров работы файловой системы NTFS

Настройки файловой системы NTFS также влияют на производительность как оболочки, так и всей операционной системы в целом. Чтобы не разбрасывать описание настроек файловой системы по всей книге, опишем их в данном подразделе.

Для настройки большинства возможностей файловой системы Windows Vista можно пользоваться как реестром, так и командой fsutil behavior. Рассмотрим оба этих способа.

Все настройки файловой системы NTFS хранятся в параметрах типа REG_DWORD-ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem. При этом некоторые из них, возможно, уже будут вам известны, так как они присутствовали и в предыдущих версиях Windows.

Чтобы изменить какой-нибудь параметр работы файловой системы, доступный с помощью программы `fsutil.exe`, нужно воспользоваться командой `Fsutil behavior set <параметр> <значение>`. Список же всех возможных параметров можно отобразить с помощью команды `Fsutil Behavior query`. Можно также просмотреть текущее значение параметра. Для этого применяется команда `Fsutil Behavior query <параметр>`.

Итак, далее приведены команды программы `fsutil.exe`, с помощью которых можно изменить значения определенных параметров реестра.

- `Allowextchar` — команда изменяет значение параметра системного реестра `NtfsAllowExtendedCharacterIn8dot3Name`. Она позволяет разрешить или запретить отображение символов, не относящихся к числовым символам или буквам алфавита, в именах файлов формата 8.3 (имена в формате MS-DOS).

  Возможные значения: `0` или `1`.

- `disable8dot3` — изменяет значение параметра системного реестра Windows `NtfsDisable8dot3NameCreation`. Она позволяет разрешить или запретить возможность создания имен файлов в формате 8.3. По умолчанию значение данного параметра равно `0`.

  Возможные значения: `0` или `1`.

- `Disablecompression` — нововведение операционной системы Windows Vista. Эта команда изменяет значение параметра `NtfsDisableCompression`, с помощью которого можно запретить использование стандартных возможностей сжатия операционной системы. По умолчанию его значение равно `0`.

  Возможные значения: `0` или `1`.

- `Disableencryption` — это также нововведение операционной системы Windows Vista. Команда изменяет значение параметра `NtfsDisableEncryption`, с помощью которого можно запретить использование стандартных возможностей шифрования (EFS) операционной системы. По умолчанию значение параметра равно `0`.

  Возможные значения: `0` или `1`.

- `disablelastaccess` — команда изменяет значение параметра системного реестра `NtfsDisableLastAccessUpdate`. Она позволяет включить или отключить механизм обновления меток последнего доступа к папкам. По умолчанию обновление меток включено, что снижает скорость открытия каталогов. Поэтому лучше установить значение данного параметра равным `1`.

  Возможные значения: `0` или `1`.

- `Encryptpagingfile` — нововведение операционной системы Windows Vista. Команда изменяет значение параметра `NtfsEncryptPagingFile`, с помощью которого можно указать, будет ли выполняться шифрование содержимого файла подкачки. По умолчанию значение данного параметра равно `0`.

  Возможные значения: `0` или `1`.

- `quotanotify` — команда изменяет значение параметра системного реестра `NtfsQuotaNotifyRate`. Она позволяет указать интервал (в секундах) возникновения событий записи информации о квоте в стандартный журнал Windows. Слишком большое значение частоты приводит к подвисанию компьютера во время записи в журнал, так как ко времени возникновения события запросов на запись в журнал может накопиться очень много. По умолчанию значение равно 3600 секунд.

  Возможные значения: от `0` до `4294967295`.

- `Memoryusage` — нововведение операционной системы Windows Vista. Команда изменяет значение параметра `NtfsMemoryUsage`. Она позволяет определить общий размер оперативной памяти, выделяемой для нужд файловой системы. По умолчанию значение данного параметра равно `0`.

  Возможные значения: `1` или `2`.

- `mftzone` — изменяет значение параметра реестра `NtfsMftZoneReservation`. Она позволяет определить формат главной таблицы тома (MFT). При использовании значения `1` таблица MFT будет подстраиваться под хранение малого количества файлов большого размера. При использовании значения `4` таблица MFT будет подстраиваться под хранение большого количества файлов малого размера. Промежуточные значения `2` и `3` подстраивают таблицу MFT под хранение файлов среднего размера с уклоном, соответственно, в ту или иную сторону. По умолчанию значение параметра вообще равно `0`.

  Возможные значения: `1` или `4`.

- `SymlinkEvaluation` — нововведение операционной системы Windows Vista. Данная команда изменяет значения следующих параметров системного реестра: `SymlinkLocalToLocalEvaluation`, `SymlinkLocalToRemoteEvaluation`, `SymlinkRemoteToLocalEvaluation`, `SymlinkRemoteToRemoteEvaluation`. С их помощью можно определить, разрешены ли соответствующие символьные ссылки (локальная ссылка на локальную, локальная ссылка на удаленную и т. д.). По умолчанию значения данных параметров соответственно равны `1`, `1`, `0`, `0`.

  Возможные значения: `0` или `1`.

Настройка работы с эскизами страниц

Операционная система Windows Vista предоставляет больше возможностей для настройки работы с эскизами страниц, чем ее предшественницы.

Основной ветвью реестра, в которой содержатся сведения о настройках хранения кэша эскизов страниц для данной учетной записи пользователя, является ветвь `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Software\Microsoft\Windows\CurrentVersion\ThumbnailCache`. В ней могут находиться следующие параметры.

- `Location` — параметр хранит путь к каталогу, в котором находятся файлы, содержащие кэш эскизов страниц. В данном каталоге расположены следующие файлы кэша эскизов страниц с расширением DB: `thumbcache_32`,

thumbcache_96, thumbcache_256, thumbcache_1024, thumbcache_idx и thumbcache_sr.

По умолчанию кэш эскизов страниц хранится в каталоге %userprofile%\AppData\Local\Microsoft\Windows\Explorer.

- MaxCacheFileSize32 — определяет максимальный размер файла кэша эскизов страниц thumbcache_32.
- MaxCacheFileSize96 — указывает максимальный размер файла кэша эскизов страниц thumbcache_96.
- MaxCacheFileSize256 — определяет максимальный размер файла кэша эскизов страниц thumbcache_256.
- MaxCacheFileSize1024 — указывает максимальный размер файла кэша эскизов страниц thumbcache_1024.
- MaxPercentageOfFreeSpaceForRebalancing — определяет процент свободного места на диске, при котором может происходить процесс ребалансировки файлов кэша эскизов.
- ShrinkIfGreaterThanPercentageOfFreeSpace — указывает, будет ли происходить сжатие файлов кэша эскизов при уменьшении свободного места на диске.
- MinCacheFilesSizesWhenShrinking32 — определяет размер файла кэша эскизов thumbcache_32, при преодолении которого начнется процесс сжатия.
- MinCacheFilesSizesWhenShrinking96 — указывает размер файла кэша эскизов thumbcache_96, при преодолении которого начнется процесс сжатия.
- MinCacheFilesSizesWhenShrinking256 — определяет размер файла кэша эскизов thumbcache_256, при преодолении которого начнется процесс сжатия.
- MinCacheFilesSizesWhenShrinking1024 — указывает размер файла кэша эскизов thumbcache_1024, при преодолении которого начнется процесс сжатия.

На этом закончим рассмотрение способов настройки оболочки Windows.

Глава 4

Работа со стандартными программами Windows Vista

- Проигрыватель Windows Media
- DVD-студия Windows
- Windows Media Center
- Internet Explorer
- Почта Windows
- Защитник Windows
- Фотоальбом Windows
- Другие программы

Операционная система Windows Vista славится не только новым интерфейсом. В ней существенно изменились стандартные, а также были добавлены новые программы, которые мы рассмотрим в этой главе книги.

4.1. Проигрыватель Windows Media

Расположение: `%programfiles%\Windows Media Player\wmplayer.exe`.

Операционная система Windows Vista включает в себя не только новые программы и компоненты, но и улучшенные возможности хорошо известных всем программ. В частности, новая операционная система содержит новый вариант Проигрывателя Windows Media — 11 версию. Существенным отличием данной версии является отсутствие возможностей работы с интернет-радиостанциями. В остальном же новая версия проигрывателя отличается только улучшенным дизайном, а также некоторыми общими нововведениями операционной системы Windows Vista.

При первом запуске Проигрывателя Windows Media (или при первом запуске музыкального файла) перед вами отобразится мастер настройки. С его помощью вы можете установить основные параметры работы Проигрывателя Windows Media, а также расширения музыкальных и видеофайлов, ассоциированные с данным проигрывателем. Например, с помощью данного окна вы можете указать, будет ли проигрыватель пытаться получать информацию о проигрываемых в данный момент песнях из Интернета, обновлять теги находящихся в библиотеке музыкальных файлов на основе данных, получаемых из Интернета, автоматически скачивать из Интернета права для найденного защищенного содержимого.

Но все эти возможности присутствовали и в предыдущих версиях Проигрывателя Windows Media. Нововведением же новой версии является возможность автоматического предоставления общего доступа ко всем музыкальным и видеофайлам для всех компьютеров, находящихся в сети. Эту возможность вы также можете включить с помощью окна конфигурации проигрывателя.

После конфигурирования музыкального проигрывателя перед вами отобразится его главное окно, открытое на вкладке Библиотека (рис. 4.1).

Как и окно Проводника, оно больше не имеет строки меню в стандартном его понимании. Однако ее можно отобразить, нажав комбинацию клавиш Ctrl+M. Теперь строка меню объединила в себе функции строки меню и панели ссылок из предыдущих версий проигрывателя. Данная строка включает следующие элементы: Проигрывается, Библиотека, Копировать с диска, Запись, Синхронизация, Интернет-магазины. Если вы щелкнете кнопкой мыши на верхней части одного из этих элементов, то откроется соответствующая его названию вкладка проигрывателя. Если же вы щелкнете кнопкой мыши на нижней части этого элемента, то перед вами отобразится раскрывающийся список с дополнительными действиями.

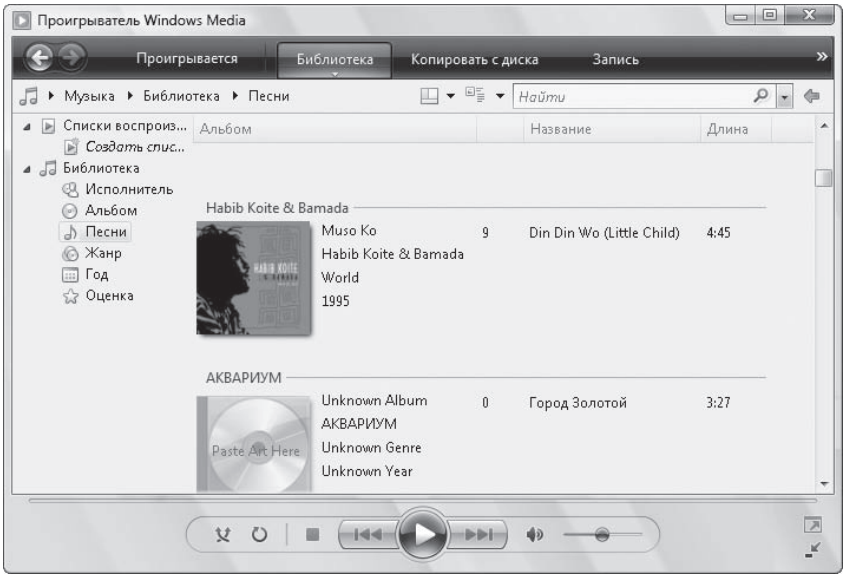


Рис. 4.1. Окно проигрывателя, открытое на вкладке Библиотека

Проигрывание файлов

Создание библиотеки

Чтобы прослушать песню, нужно сначала выбрать ее на вкладке Библиотека. Вместе с Проигрывателем Windows Media поставляется несколько песен, сведения о которых вы сможете увидеть в библиотеке при его запуске. Однако остальные песни, которые, возможно, хранятся на вашем жестком диске, в библиотеке не отображаются. Чтобы добавить их в библиотеку проигрывателя, нужно в раскрывающемся списке элемента Библиотека выбрать команду Добавить в библиотеку. После этого Проигрыватель Windows Media предложит вам выбрать каталоги, в которых нужно искать музыкальные файлы, после чего начнет поиск.

Поиск в библиотеке

Но добавить файлы в библиотеку — это только половина дела. Еще нужно найти интересующие вас файлы в содержимом библиотеки, что бывает довольно сложно сделать при большом количестве треков различных исполнителей.

Для облегчения этой задачи Проигрыватель Windows Media предоставляет два средства.

Первым является хорошо знакомая многим пользователям возможность сортировки по артисту, названию альбома, году создания, жанру песни. По умолчанию отображаются только эти способы сортировки (в списке Библиотека панели, расположенной слева от содержимого библиотеки), но с помощью контекстного меню списка Библиотека можно добавить все возможные способы сортировки, среди которых особо стоит отметить сортировку по папкам, в которых находятся песни.

Иногда ориентирование в названиях папок бывает намного удобнее, чем поиск по названию исполнителя, жанру и т. д.

Вторым же средством является пресловутая строка поиска, которую в Windows Vista можно найти практически в любой стандартной программе. В проигрывателе же строка поиска особенно полезна. С ее помощью можно найти песни по названию исполнителя.

Для облегчения поиска в библиотеке, кроме названия песни и исполнителя, отображается рисунок, идентифицирующий альбом, из которого эта песня была получена (если такого рисунка нет, то отображается предопределенное изображение). Рисунок может облегчить не только поиск песни, но и работу с проигрывателем. С помощью контекстного меню изображения можно прослушать соответствующие ему песни, добавить их в один из существующих листов проигрывания или создать новый лист, удалить соответствующие песни и, конечно, указать путь к новому изображению.

Прослушивание песен

После того как вы выберете из библиотеки необходимые песни, они будут загружены в список на вкладке Проигрывается, а затем начнется их воспроизведение. Управлять воспроизведением песен можно с помощью панели, расположенной в нижней части экрана проигрывателя (рис. 4.2).



Рис. 4.2. Панель управления воспроизведением песен

Панель включает следующие возможности (перечислены слева направо):

- определяет, включен ли режим Shuffle, при котором песни будут воспроизводиться в случайном порядке (по умолчанию песни воспроизводятся последовательно, о чем говорят три вертикально расположенные палочки);
- определяет, разрешено ли повторение песен, которое по умолчанию отключено;
- остановить воспроизведение песни;
- воспроизвести предыдущую песню;
- воспроизведение/пауза;
- воспроизвести следующую песню;
- регулятор громкости.

Копирование содержимого диска

С помощью Проигрывателя Windows Media можно выполнить конвертирование аудиофайлов с расширением CDA в музыкальные файлы. При этом наконец-то

музыкальный проигрыватель поддерживает не только собственный формат WMA, но и используемый многими пользователями MP3-формат (рис. 4.3).

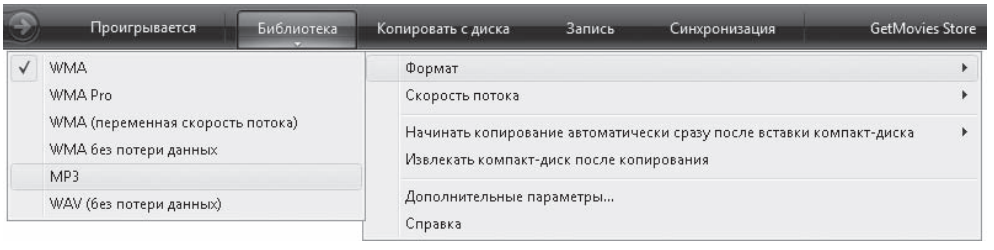


Рис. 4.3. Меню конвертирования музыкальных файлов

Для начала процесса конвертирования аудиофайлов нужно вставить музыкальный компакт-диск и перейти на вкладку Копировать с диска. Но если вы делаете это впервые, то сначала нужно выполнить настройку механизма конвертирования. Проще всего это сделать с помощью раскрывающегося списка элемента Копировать с диска. Он содержит следующие элементы.

- Формат — позволяет изменить формат получаемого при конвертировании музыкального файла. Возможны такие форматы, как WMA, MP3 и WAV.
- Скорость потока — позволяет изменить битрейт получаемого после конвертирования музыкального файла. Чем больше битрейт, тем лучше качество звука и, естественно, больше размер получаемого музыкального файла. Например, Проигрыватель Windows Media поддерживает битрейт музыкальных файлов MP3-формата вплоть до 340 Кбит/с.
- Начинать копирование автоматически сразу после вставки компакт-диска — позволяет указать проигрывателю, что он должен автоматически начинать конвертирование файлов при обнаружении компакт-диска в приводе.
- Извлекать компакт-диск после копирования — определяет, будет ли автоматически открываться привод компакт-дисков после выполнения конвертирования содержимого диска.
- Дополнительные параметры — с помощью данной команды можно отобразить вкладку Копирование музыки с компакт-диска окна Параметры. Благодаря этому окну можно выполнить настройку всех описанных выше параметров конвертирования, а также выбрать папку, в которую будут конвертироваться аудиофайлы.

Если в данный момент отображается вкладка Копировать с диска, то конвертирование файлов выполняется автоматически при обнаружении аудиодиска в приводе. Если же конвертирование не началось, то достаточно нажать кнопку Начать копирование с компакт-диска. Вы также можете определить треки аудиодиска, которые нужно конвертировать.

После того как все указанные файлы будут конвертированы, музыкальный проигрыватель попытается подключиться к Интернету, чтобы найти сведения о конвертируемых файлах: название альбома, песен, год создания и т. д.

Изменение битрейта при кодировании в MP3-файлы

При кодировании аудиофайлов с помощью MP3-кодека музыкального проигрывателя вам доступны только следующие битрейты: 128, 192, 256 и 320 Кбит/с. Но этого может быть недостаточно. Например, когда вы слушаете музыку в основном на переносном проигрывателе или мобильном телефоне, для вас главное не качество записи песни, а ее как можно меньший размер. В этом случае вы можете самостоятельно указать битрейт, в котором будут кодироваться новые MP3-файлы, например битрейт 64 Кбит/с. Хотя можно изменить битрейт на любой, меньший стандартных 128 Кбит/с или больший 320 Кбит/с. Главное, чтобы указанный вами битрейт поддерживался стандартным MP3-кодеком операционной системы Windows Vista (`l3codecp.acm`).

Для этого нужно воспользоваться ветвью реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MediaPlayer\Settings\MP3Encoding`. Она хранит следующие параметры `REG_DWORD`-типа.

- `LowRate` — определяет минимальный битрейт композиции. По умолчанию равен 128 Кбит/с.
- `MediumRate` — указывает средний битрейт композиции. По умолчанию равен 192 Кбит/с.
- `MediumHighRate` — определяет хороший битрейт композиции. По умолчанию равен 256 Кбит/с.
- `HighRate` — указывает самый лучший битрейт композиции. По умолчанию равен 320 Кбит/с.

Значения битрейта в этих параметрах хранятся в шестнадцатеричном счислении. При этом они хранятся не в формате Кбит/с, а в формате бит/с. Например, чтобы присвоить битрейт 64 Кбит/с одному из этих параметров, нужно при записи значения в редакторе реестра переключиться в десятичное счисление и ввести значение `64000`.

Запись диска

Еще одной возможностью, которую вам предоставляет Проигрыватель Windows Media, является запись музыкальных дисков на съемный носитель. Для этого используется вкладка Запись, раскрывающийся список которой позволяет вам настроить следующие параметры записи: будет создан аудиодиск или обычный диск с данными, будет ли автоматически открываться привод после окончания процесса записи. С помощью этого списка вы также можете вывести на экран окно Options, открытое на вкладке Запись. Эта вкладка предоставляет несколько дополнительных возможностей настройки записи, к которым относятся: выбор скорости записи, возможность определения, будет ли выполняться конвертирование музыкальных файлов перед записью, а также формат листа проигрывания, добавляемого на создаваемый диск.

Процесс записи довольно прост. Сначала вы выбираете необходимые файлы из библиотеки, перенося их в список, расположенный справа от поля библиотеки. А после этого просто нажимаете кнопку Начать запись.

Синхронизация со съемными носителями

Кроме записи музыкальных файлов на диск, проигрыватель позволяет выполнить их синхронизацию с уже содержащимися на съемном диске файлами. Для этого применяется вкладка Синхронизация.

Основные настройки синхронизации можно изменить, нажав кнопку Дополнительно на вкладке Устройства окна Параметры. После этого отобразится окно, приведенное на рис. 4.4.

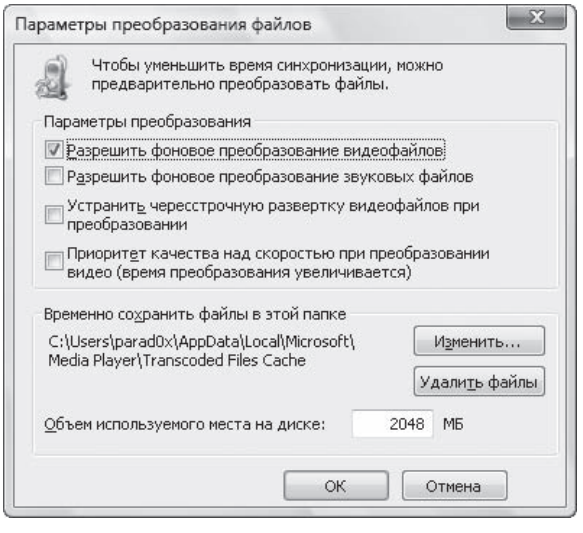


Рис. 4.4. Окно настройки параметров синхронизации

Использование групповых политик

Настроить работу Проигрывателя Windows Media можно с помощью групповых политик, описанных в файле `WindowsMediaPlayer.admx` и расположенных в разделе Конфигурация пользователя ▸ Административные шаблоны ▸ Компоненты Windows ▸ Проигрыватель Windows Media.

Данные политики изменяют параметры `REG_DWORD`-типа, расположенные в ветви системного реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\WindowsMediaPlayer` и ее подразделах.

- `PreventCDDVDMetadataRetrieval` — если значение параметра равно `1`, то музыкальному проигрывателю будет запрещено автоматически получать из Интернета данные о воспроизводимых файлах.
- `PreventMusicFileMetadataRetrieval` — при установке значения этого параметра равным `1` музыкальному проигрывателю будет запрещено автоматически получать из Интернета данные о воспроизводимых MP3- и WMA-файлах.

- EnableScreenSaver — если значение данного параметра равно 0, то запуск заставки при просмотре фильмов будет запрещен.
- PreventCodecDownload — при установке значения этого параметра равным 1 музыкальному проигрывателю будет запрещено автоматически загружать из Интернета недостающие при воспроизведении файла кодеки.
- HidePrivacyTab — если значение параметра равно 1, то вкладка Конфиденциальность в окне Параметры музыкального проигрывателя отображаться не будет.
- HideSecurityTab — при установке значения этого параметра равным 1 не будет отображаться вкладка Безопасность в окне Параметры музыкального проигрывателя.
- HideNetworkTab — если значение параметра равно 1, то вкладка Сеть в окне Параметры музыкального проигрывателя отображаться не будет.
- SetAndLockSkin — при установке значения этого параметра равным 1 при отображении проигрывателя в режиме обложки будет использоваться обложка, указанная в параметре DefaultSkin.
- DefaultSkin — параметр имеет строковый тип. Он содержит путь к обложке музыкального проигрывателя, которая будет применяться по умолчанию при использовании режима обложки, если значение параметра SetAndLockSkin равно 1.

ПРИМЕЧАНИЕ

Список кодеков для просмотра DVD можно определить, введя команду dvdupgrd /detect. При этом отображается библиотека кодека, ее издатель, версия, код CRC, а также определяется, существует ли обновление данного кодека на сайте производителя. Если обновление существует, то скачать его можно будет с помощью команды dvdupgrd /upgrade.

Настройка дополнительных параметров реестра

Как и предыдущие версии Проигрывателя Windows Media, данная версия имеет несколько параметров реестра, доступ к которым нельзя получить с помощью стандартных окон. Рассмотрим эти параметры.

Основной ветвью реестра, которая хранит параметры работы музыкального Проигрывателя Windows Media, является ветвь HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Preferences. Она содержит следующие дополнительные параметры реестра.

- AcceptedPrivacyStatement — если присвоить данному параметру типа REG_DWORD значение 0, то при следующем запуске проигрывателя отобразится мастер его установки, который обычно отображается только при первом запуске.

- `AlwaysOnTopVTenApp` — с помощью настроек музыкального проигрывателя можно заставить его отображаться поверх всех окон (нужно установить флажок Отображать проигрыватель поверх основных окон). При этом проигрыватель будет отображаться поверх всех окон как в стандартном режиме, так и в режиме обложки, что не всегда является удобным, ведь в стандартном режиме окно проигрывателя закрывает практически весь экран. К счастью, с помощью данного параметра `REG_DWORD`-типа можно отдельно настроить, будет ли отображаться поверх всех окон окно проигрывателя в стандартном режиме.
- `AlwaysOnTopVTenSkin` — а с помощью этого параметра типа `REG_DWORD` можно отдельно настроить, будет ли отображаться поверх всех окон окно проигрывателя в режиме обложки.
- `AppColorAux2` — этот параметр строкового типа определяет цвет стандартной строки меню проигрывателя. Формат его значения следующий: `#RGB`, где `R` определяет красный компонент цвета (в шестнадцатеричной системе счисления, значения от `00` до `ff`), `G` определяет зеленый компонент цвета, а `B` — синий. Не забудьте поставить знак # перед цветом, как показано в формате значения данного параметра.

  Можно также настроить цвет основного окна проигрывателя. Для этого применяется параметр строкового типа `AppColorLightV11`. Дополнительно подстроить цвет основного окна (его теней) можно с помощью параметра строкового типа `AppColorDarkV11`.

  Конечно, цветовую грамму проигрывателя можно настроить и с помощью меню Вид ▸ Дополнительные возможности ▸ Выбор цвета. Однако в этом случае вы сможете настроить общие цвета проигрывателя, а не цвета отдельных его элементов.
- `BackgroundScanCompleteDate` — этот параметр строкового типа определяет дату последнего фонового сканирования.
- `CurrentBackgroundScanFolder` — параметр имеет строковый тип и определяет каталог, содержимое которого будет сканироваться при работе проигрывателя в фоновом режиме (будет выполняться поиск новых музыкальных файлов).
- `ForceDisableTerminateOnHeapCorruption` — параметр `REG_DWORD`-типа определяет, будет ли музыкальный проигрыватель продолжать работу при повреждении своих данных.
- `ForceBiDi` — если вам надоело стандартное расположение элементов управления музыкального проигрывателя, то вы можете присвоить данному параметру `REG_DWORD`-типа значение `1`. После этого все элементы проигрывателя будут отображаться с противоположной стороны. Например, кнопки закрытия и минимизации окна проигрывателя будут отображаться не с правой стороны, а с левой. Также переместится поле листа проигрывания. Сразу можно сказать, что зрелище непривычное.
- `GDIPlusStretching` — если значение данного параметра `REG_DWORD`-типа будет равно `0`, то все графические элементы проигрывателя (плавные перехо-

ды и тени) будут отображаться упрощенными — напоминает работу маслом начинающего художника. Это позволит ускорить работу музыкального проигрывателя.

- `LibraryDatabasePath` — этот параметр строкового типа определяет путь к каталогу, в котором Проигрыватель Windows Media будет хранить свою библиотеку (файл `CurrentDatabase_346.wmdl`).
- `LibraryLastAddTime` — параметр имеет строковый тип и определяет дату последнего добавления песен в библиотеку.
- `MediaLibraryCreateNewDatabase` — если данному параметру `REG_DWORD`-типа присвоить значение `1`, то при следующем запуске музыкального проигрывателя будет заново создана его библиотека.
- `SearchOnlyMyPersonalFolder` — если значение данного параметра типа `REG_DWORD` будет равно `1`, то автоматически добавлять файлы в библиотеку можно будет только в том случае, если они находятся в профиле пользователя.

С помощью групповых политик можно также настроить параметры работы музыкального проигрывателя с подписями DRM. Для этого применяются политики, описанные в файле `WindowsMediaDRM.admx` и расположенные в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Управление цифровыми правами Windows Media. Пока что данный раздел содержит только одну политику — Запретить доступ к Интернету для Windows Media DRM. Она позволяет запретить доступ музыкального проигрывателя в Интернет для обновления подписи DRM. Для этого она присваивает параметру `REG_DWORD`-типа `DisableOnline`, расположенному в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WMDRM`, значение `1`.

4.2. DVD-студия Windows

Расположение: `%programfiles%\Movie Maker\DVDMaker.exe`.

Очень долгое время в стандартную поставку операционной системы Windows входила программа для создания видеоклипов — Windows Movie Maker. Однако только сейчас к этой программе добавилась еще одна, с помощью которой созданные материалы можно записать на DVD с возможностью проигрывания на бытовых проигрывателях DVD.

Пользоваться программой DVD-студия Windows очень просто. После ее запуска отобразится окно, приведенное на рис. 4.5 (перед запуском программы необходимо поместить записываемый диск в привод).

С помощью данного окна определяются те файлы, которые будут помещены на записываемый DVD. Для этого нужно выбрать команду Добавить, после чего отобразится стандартное окно выбора файлов.

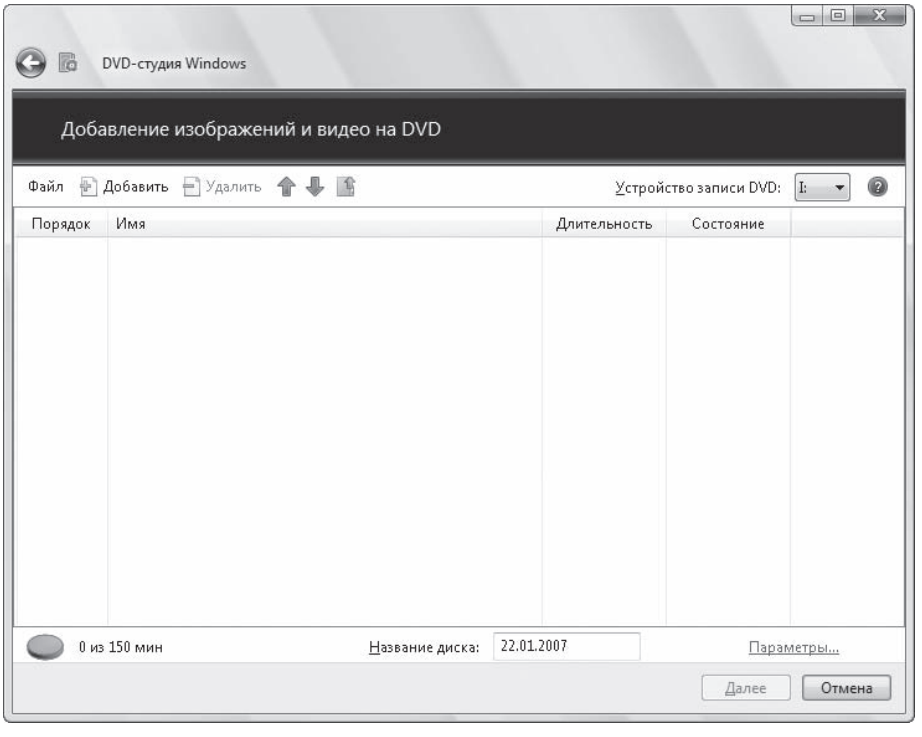


Рис. 4.5. Начальное окно мастера создания DVD

С помощью окна, приведенного на рис. 4.5, можно определить настройки создаваемого диска. Для этого нужно выбрать ссылку Параметры, после чего отобразится окно Параметры DVD, с помощью которого можно определить, будет ли создаваться меню для содержимого создаваемого DVD, а также формат создаваемого видео (PAL или NTSC) и соотношение сторон (широкоформатное соотношение 16:9 или обычное 4:3). Благодаря этому окну можно указать путь к временному каталогу, используемому программой DVD-студия Windows. Изменение временного каталога может понадобиться в том случае, если на используемом по умолчанию диске осталось мало места (часто временный каталог занимает больше нескольких гигабайт).

Когда вы выберете материалы, которые будут записаны на DVD, необходимо нажать кнопку Далее, после чего отобразится окно создания меню (если вы решили, что меню будет создаваться). Вместе с программой DVD-студия Windows поставляется множество предопределенных вариантов меню, в большинстве основанных на теме цветов. Все они отображаются в правой панели мастера (рис. 4.6).

Мастер создания меню позволяет отредактировать текст, отображаемый в меню (кнопка Текст меню), а также позиции элементов меню, шрифт, цвет и размер используемого шрифта (кнопка Настройка меню). Если вы уже создали меню, то можно протестировать его с помощью кнопки Просмотр либо сразу же начать процесс записи диска, нажав кнопку Запись.

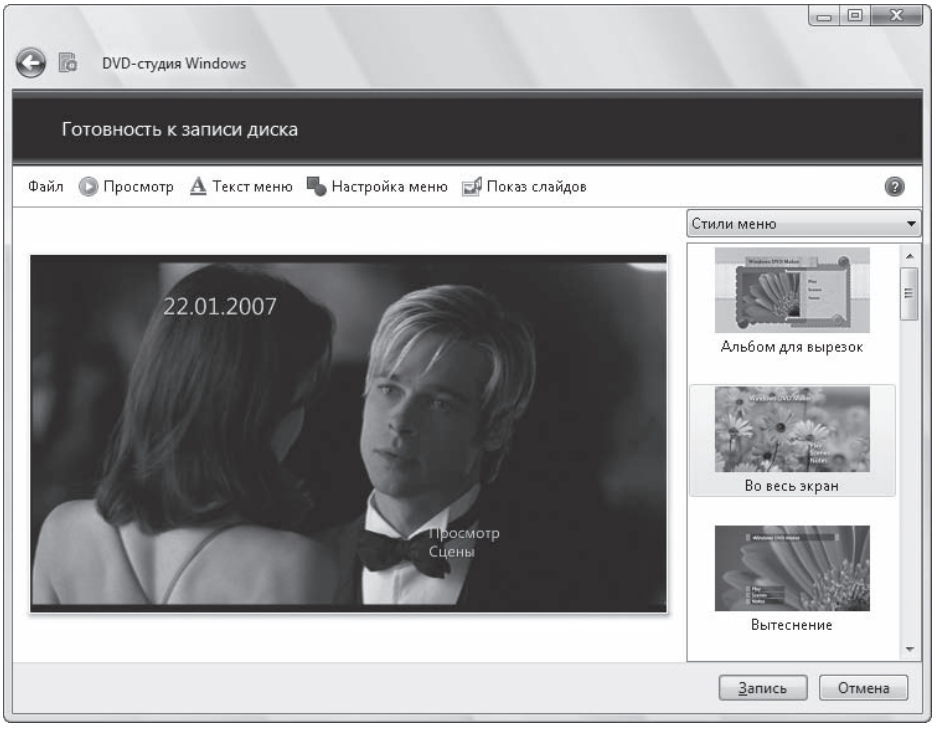


Рис. 4.6. Мастер создания меню

4.3. Windows Media Center

Расположение: `%systemroot%\ehome\`.

Windows Media Center — очень красивая оболочка для всех мультимедийных возможностей операционной системы Windows Vista. Она позволяет быстро получить доступ к мультимедийному контенту и программам, входящим в стандартную поставку операционной системы. Единственное, что может огорчить пользователя, — огромные требования к ресурсам компьютера, которые нужны данной оболочке для комфортной работы.

ПРИМЕЧАНИЕ

Запуск данной программы можно запретить с помощью параметра REG_DWORD-типа MediaCenter, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\WindowsMediaCenter. Для этого достаточно данному параметру присвоить значение 1.

Это же можно сделать с помощью групповой политики Не запускать Windows Media Center, расположенной в разделе Конфигурация пользователя ▸ Административные шаблоны ▸ Компоненты Windows ▸ Windows Media Center. Данная политика описана в файле MediaCenter.admx.

После первого запуска Windows Media Center перед вами отобразится мастер настройки данной оболочки (рис. 4.7). Благодаря ему можно определить, будет ли Windows Media Center использовать возможности Интернета для своей работы, будет ли он взаимодействовать с программой По улучшению качества программного обеспечения Windows (периодически корпорации Microsoft будут отправляться данные о производительности оболочки Windows Media Center). Этот мастер также позволяет настроить параметры работы звуковой подсистемы компьютера и изображение на мониторе.

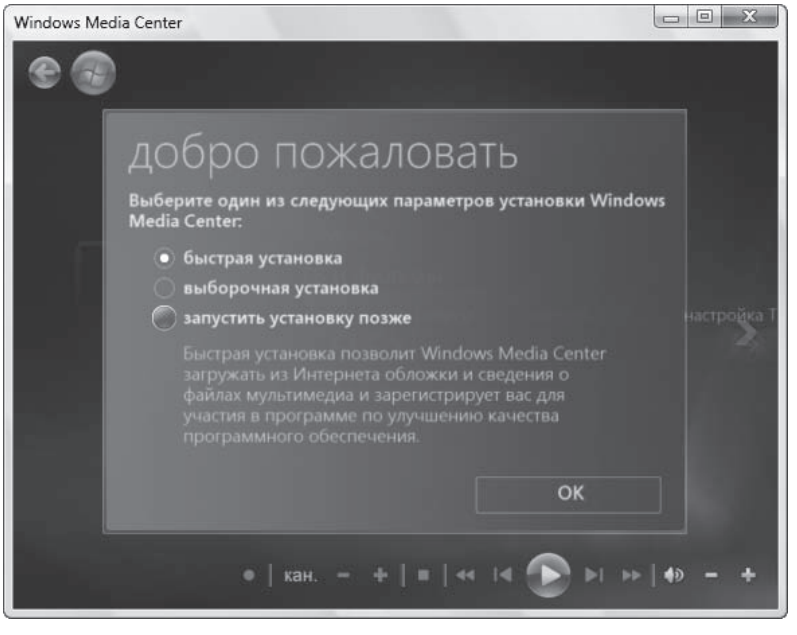


Рис. 4.7. Мастер настройки компонента Windows Media Center

В операционной системе Windows Vista по умолчанию создано пять заданий, которые управляют работой компонента Windows Media Center. Все они расположены в разделе Библиотека планировщика заданий ▸ Microsoft ▸ Windows ▸ Media Center:

- `ehDRMInit` — выполняет команду `%SystemRoot%\ehome\ehPrivJob.exe /DRMInit`;
- `Mcupdate` — `%SystemRoot%\ehome\mcupdate $(Arg0) -gc`;
- `OCURActivate` — `%SystemRoot%\ehome\ehPrivJob.exe /OCURActivate`;
- `OCURDiscovery` — `%SystemRoot%\ehome\ehPrivJob.exe /OCURDiscovery`;
- `UpdateRecordPath` — выполняет следующую команду: `%SystemRoot%\ehome\ehPrivJob.exe /DoUpdateRecordPath $(Arg0)`.

После того как вы настроите оболочку Windows Media Center, перед вами отобразится главное окно программы (рис. 4.8). Его особенностью является то, что им вы можете управлять как с помощью клавиатуры или указателя мыши, так и с по-

мощью пульта дистанционного управления. Благодаря этому управление оболочкой осуществляется только с помощью клавиш управления курсором и клавиши Enter. При нажатии клавиш ↑ или ↓ (если управление осуществляется с помощью мыши, то нужно подвести ее указатель к верхнему или нижнему краю меню, после чего отобразятся стрелки для управления) вы перемещаетесь соответственно вверх и вниз по меню программы. При нажатии клавиш ← и → вы перемещаетесь по содержимому того или иного меню.

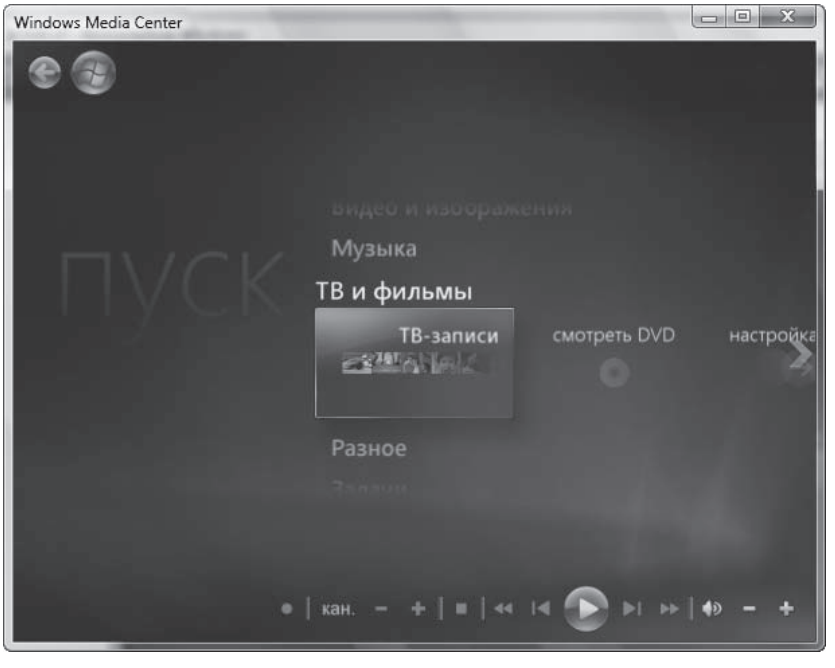


Рис. 4.8. Основное окно оболочки Windows Media Center

Наиболее полно возможности оболочки Windows Media Center можно описать на основе содержимого ее меню, которое состоит из следующих команд.

- Задачи — дает возможность записать мультимедийный контент на записываемый DVD, синхронизировать содержимое стандартных папок Windows (Изображения, Видео, Музыка) с содержимым съемного диска, завершить работу.
- Видео и изображения — позволяет работать с содержимым папок Изображения и Видео, а также просматривать их содержимое в режиме слайд-шоу (при этом применяются различные переходы при смене изображений, что смотрится очень красиво).
- ТВ и фильмы — позволяет просмотреть телепередачу (если установлен ТВ-тюнер), а также записать ее на жесткий диск компьютера.
- Музыка — предоставляет доступ к музыкальным функциям оболочки: работа с библиотекой музыки и поиск в ней (поиск также может осуществляться как с помощью клавиатуры, так и с использованием пульта дистанционного управления

с помощью цифровых клавиш от 0 до 9), прослушивание музыки. Благодаря этой команде вы также можете работать с радиостанциями.

- Разное — предоставляет доступ к Интернету, а также к стандартным играм операционной системы Windows Vista.
- Прослушивание + очередь — если вы уже создали лист воспроизведения, начали его прослушивать (или остановили прослушивание) и перешли к другим возможностям оболочки, то с помощью данного раздела можно вернуться к созданному листу воспроизведения и продолжить его прослушивание.

Не все из этих команд могут присутствовать в Windows Media Center на вашем компьютере. Это скорее связано не с другой версией данной программы, а с содержимым ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Media Center\Start Menu`. Данная ветвь реестра может хранить следующие параметры `REG_DWORD`-типа:

- `HideDVD` — позволяет скрыть раздел ТВ и фильмы ▸ Смотреть DVD программы Windows Media Center.
- `HideTV` — дает возможность скрыть раздел ТВ и фильмы.

4.4. Internet Explorer

Расположение: `%programfiles%\Internet Explorer\iexplore.exe`.

Согласно традициям операционной системы Windows новая версия браузера Internet Explorer входит в каждую новую операционную систему Windows. При этом не просто входит, а является ее неотъемлемой частью. Однако сейчас традиции начинают понемногу меняться. Новая версия браузера Internet Explorer — седьмая — больше не является неотъемлемой частью операционной системы, и вы всегда можете ее удалить абсолютно безболезненно для Windows Vista. Но это не единственное изменение в работе нового браузера.

Перед описанием работы с браузером рассмотрим его основные изменения:

- новый интерфейс, призванный облегчить работу с браузером;
- автоматический поиск RSS-лент, предоставляемых загруженными сайтами;
- поддержка таблиц стилей (CSS) версии 2.1, технологии XMLHTTP для AJAX-приложений, а также поддержка нового формата отображения документов XPS;
- возможность изменения масштабов отдельной загруженной страницы Интернета;
- возможность применения механизма Phishing Filter для определения сайтов, несущих потенциальную угрозу для передаваемых пользователем данных;
- работа браузера от имени пользователя, обладающего минимальными правами в операционной системе.

Интерфейс браузера

При первом запуске браузера (`iexplore.exe`) перед вами отобразится окно, предлагающее включить или отключить Phishing Filter. Что вы ответите, на данный момент не играет большой роли. Впоследствии вы все равно сможете настроить Phishing Filter с помощью специальной команды меню браузера.

Как и большинство окон стандартных программ операционной системы Windows Vista, окно браузера Internet Explorer по умолчанию не содержит строки меню (рис. 4.9), хотя доступ к ней можно получить после нажатия клавиши Alt. Вместо нее теперь используются кнопки, расположенные справа от вкладок. Щелкнув на треугольнике в правой части такой кнопки, вы откроете меню, позволяющее выполнить большинство стандартных действий по работе с браузером.

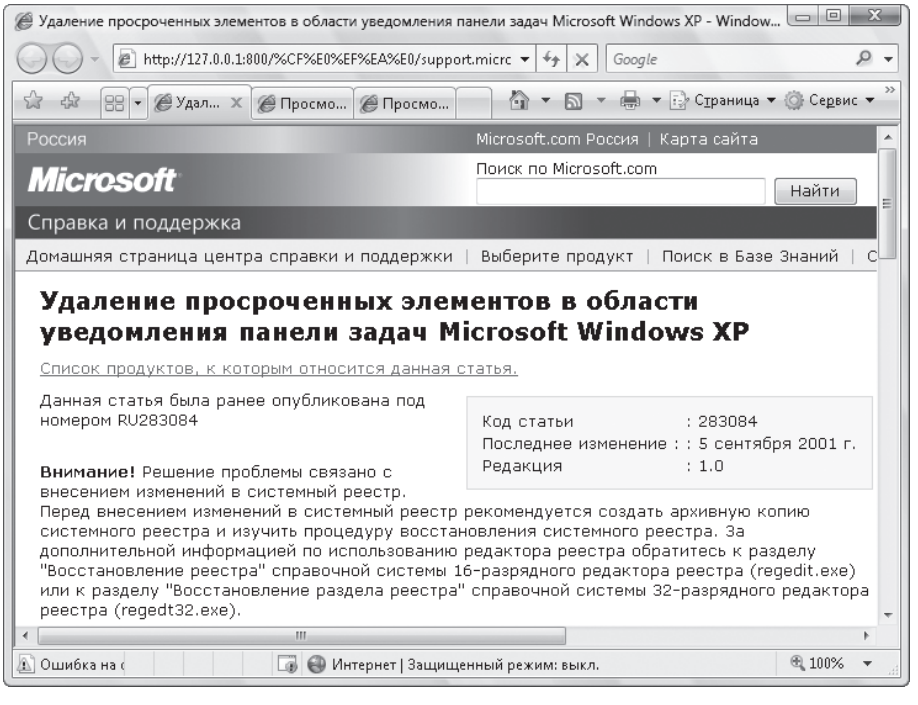


Рис. 4.9. Окно браузера Internet Explorer

Но к ним мы вернемся чуть позже. Сейчас же повнимательнее присмотримся к другим элементам браузера Internet Explorer. Конечно, сразу же бросается в глаза панель вкладок, которая теперь заменила открытие нескольких окон браузера для просмотра нескольких страниц. Обратите внимание, что справа расположена одна пустая вкладка. Она служит для добавления новых вкладок — для этого достаточно просто щелкнуть на ней кнопкой мыши.

Работа с вкладками не представляет никакой сложности, поэтому сразу же рассмотрим еще одну новую функцию браузера — режим предварительного просмотра.

Если вы открыли несколько вкладок, то для быстрой навигации по ним достаточно нажать кнопку слева от панели (изображающую четыре квадратика). После этого все открытые вами вкладки будут отображаться в уменьшенном виде (рис. 4.10). И чтобы перейти на нужную вкладку, достаточно щелкнуть на ней левой кнопкой мыши. С помощью данного режима также можно быстро удалить не нужные вам вкладки.

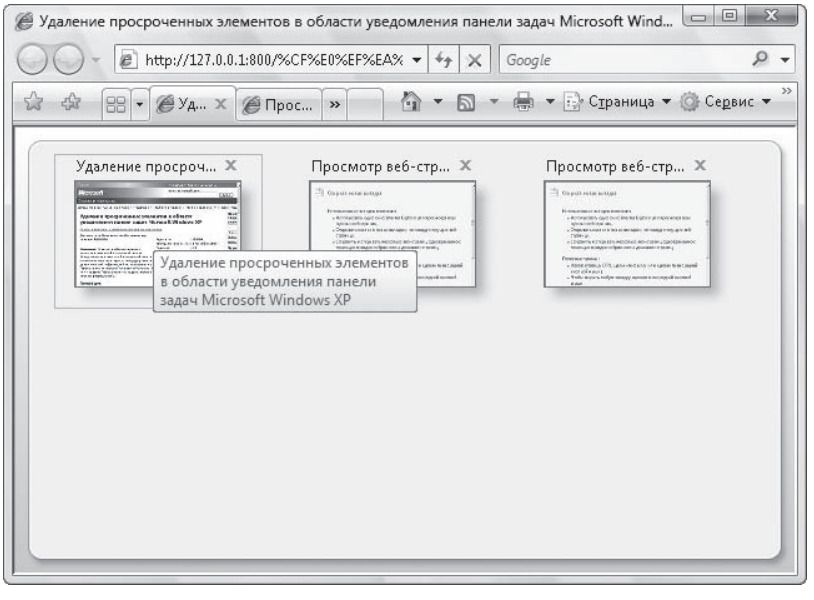


Рис. 4.10. Режим предварительного просмотра в браузере Internet Explorer

Слева от панели вкладок отображается еще одна интересная кнопка. Она является крайней слева и имеет вид звездочки (рис. 4.11). Именно с помощью данной кнопки теперь можно получить доступ к списку избранного (кнопка Избранное). Но, кроме этого, с ее помощью можно получить доступ к запомненным вами RSS-лентам (кнопка Веб-каналы), а также к списку истории ваших путешествий по просторам Интернета (кнопка Журнал).

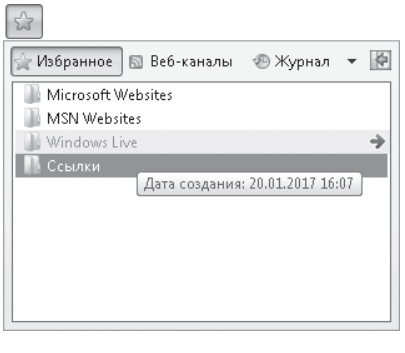


Рис. 4.11. Окно работы с Избранным

Теперь рассмотрим назначение кнопок, отображаемых справа от панели вкладок.

- Домой — нажатие данной кнопки позволяет отобразить домашнюю страницу пользователя. Кроме того, с помощью раскрывающегося списка данной кнопки можно добавить новую домашнюю страницу или удалить уже существующую (браузер Internet Explorer 7.0 поддерживает возможность хранения нескольких адресов домашних страниц).
- Веб-каналы — позволяет управлять RSS-лентами, добавляя ленты, которые есть на открытом в данный момент сайте, к списку избранных. Если браузер обнаруживает, что загружаемая HTML-страница предоставляет один или несколько RSS-каналов, то данная кнопка активируется и, напротив нее появится стрелка вниз (если страница содержит несколько RSS-каналов), с помощью которой можно отобразить список доступных на странице RSS-каналов. После того как вы щелкнете кнопкой мыши на понравившемся RSS-канале, отобразится окно оформления подписки, в котором нужно присвоить имя новому каналу, а также указать папку, в котором он будет храниться.
- Печать — эта кнопка и ее раскрывающийся список предназначены для распечатывания текущей вкладки браузера, а также для настройки параметров печати. Список этой кнопки содержит команду Предварительный просмотр, с помощью которой можно вызвать окно предварительного просмотра того, как текущая веб-страница будет отображаться после печати. С помощью этого окна вы можете запретить вывод заголовков страниц, а также определить (для сложных HTML-страниц), что именно будет распечатано: содержимое всей страницы целиком, отдельного фрейма или содержимое всех фреймов, но распечатанное по отдельности.
- Страница — с помощью раскрывающегося списка этой кнопки можно создать новую закладку, а также сохранить, отправить по электронной почте или просмотреть в Блокноте исходной код открытой в данный момент веб-страницы.

  Как и раньше, существует несколько форматов сохранения веб-страницы. Полное сохранение HTML-страницы и всех изображений и файлов стилей, используемых в ней (Веб-страница, полностью (*.htm, *.html)). Сохранение всего содержимого HTML-страницы в виде отдельного архива (Веб-архив, один файл (*.mht)). Сохранение только HTML-страницы, без рисунков и файлов стилей (Веб-страница, только HTML (*.htm, *.html)). Сохранение только отображаемого текста веб-страницы в текстовом файле (Текстовый файл (*.txt)).

  С помощью этого списка можно увеличить или уменьшить размер используемого на веб-странице шрифта, а также полностью увеличить или уменьшить веб-страницу.
- Сервис — кнопка имеет самое интересное содержимое раскрывающегося списка. С его помощью вы сможете выполнить следующее.
  - Удалить журнал обозревателя — очистить содержимое списка истории вашей навигации по просторам Интернета.
  - Диагностика проблем подключения — вызвать мастер диагностики неисправностей подключения к Интернету, если по какой-то причине вы не можете выполнить подключение.

- Блокирование всплывающих окон — отключить или настроить механизм блокирования всплывающих окон, реализованный в браузере Internet Explorer.
- Фильтр фишинга — настроить механизм Phishing Filter. Именно с его помощью вы можете включить автоматическую проверку загружаемых вебсайтов, настроить механизм Phishing Filter, а также проверить загруженный сайт, если не используется автоматическая проверка.

Вы, наверное, уже так привыкли видеть в каждом окне панель поиска, что совершенно не удивились, увидев ее и в окне браузера. С помощью данной панели можно выполнить поиск введенного слова с помощью поисковой машины MSN. Однако вы можете изменить используемую по умолчанию поисковую машину с помощью команды Изменить параметры поиска по умолчанию контекстного меню строки поиска. Но перед этим нужно воспользоваться командой того же контекстного меню Найти других поставщиков. Она позволяет добавить информацию о новых поисковых машинах, с помощью которых можно выполнять поиск.

ПРИМЕЧАНИЕ

Несмотря на отдельную панель поиска, адресная строка браузера по-прежнему поддерживает функцию автопоиска. По умолчанию функция автопоиска использует поисковую систему MSN.

И последнее, на что нужно обратить внимание в новом интерфейсе браузера, — расположенное справа на строке состояния увеличительное стекло, рядом с которым отображен процент увеличения содержимого данной вкладки. Именно с помощью этого стекла можно увеличивать или уменьшать отображаемую в данный момент веб-страницу. Для этого достаточно щелкнуть кнопкой мыши на увеличительном стекле, после чего раскроется список возможных вариантов увеличения.

После того как вы закончите работу с браузером и попытаетесь закрыть его окно, он задаст вам вопрос, хотите ли вы сохранить открытые в данный момент вкладки для следующего запуска (рис. 4.12). Если вы установите флажок Открыть их при следующем запуске Internet Explorer, то при следующем запуске браузера будут открыты те же вкладки, которые присутствовали при закрытии браузера.

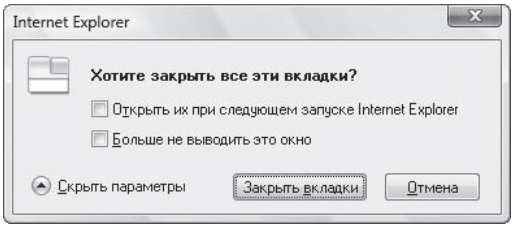


Рис. 4.12. Вопрос сохранения открытых вкладок

Настройка браузера

Теперь поговорим о возможностях настройки новой версии браузера Internet Explorer. Как и раньше, основные возможности настройки данного браузера заключены в окне Свойства: Интернет, доступ к которому можно получить с помощью раскрывающегося списка кнопки Сервис.

Окно свойств Internet Explorer

Большинство возможностей данного окна имелись и в предыдущих версиях браузера Internet Explorer, поэтому их мы затронем только поверхностно.

Как и раньше, окно Свойства: Интернет состоит из семи вкладок (рис. 4.13), каждая из которых содержит набор параметров, сгруппированных по определенному признаку.

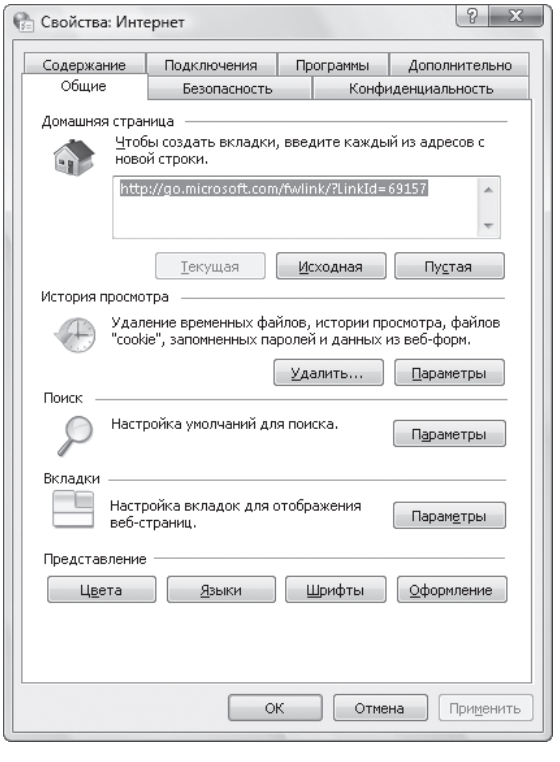


Рис. 4.13. Окно Свойства: Интернет

- Общие — отображается по умолчанию и включает в себя параметры настройки интерфейса браузера, а также возможности очистки временных файлов, файлов cookies, списка истории и т. д. Как и раньше, с помощью данной вкладки можно изменить адрес домашней страницы, используемые цвета ссылок, предпочитаемый язык веб-страницы (если страница содержит дублируемую информацию на нескольких языках, то будет выбран предпочитаемый вами), шрифт, который по умолчанию будет использоваться для отображения текста веб-страницы,

а также параметры пользовательского стиля отображения веб-страниц (соответственно, кнопки Цвета, Языки, Шрифты и Оформление области Представление).

ПРИМЕЧАНИЕ

Обратите внимание на кнопку Языки. С помощью окна Выбор языка, вызываемого данной кнопкой, можно изменить суффикс, который добавляется к адресу при нажатии сочетания клавиш Shift+Ctrl+Enter.

По умолчанию после нажатия этого сочетания клавиш к адресу, введенному в адресную строку, добавляется префикс www и суффикс .com. С помощью поля Настройка префикса и суффикса можно запретить добавление префикса, а также указать суффикс, который будет добавляться вместо суффикса .com.

Но, кроме этого, данная вкладка новой версии браузера содержит возможности настройки параметров панели поиска, а также отображения вкладок браузера Internet Explorer.

Чтобы отобразить параметры настройки поиска, нужно нажать кнопку Параметры области Поиск. После этого отобразится окно работы с поисковыми машинами, доступ к которому также можно было получить с помощью контекстного меню панели поиска.

Чтобы отобразить параметры настройки вкладок, нужно нажать кнопку Параметры поля Вкладки. После этого отобразится окно (рис. 4.14), с помощью которого можно настроить следующие возможности работы вкладок.

- Включить обзор с вкладками (после перезапуска) — позволяет отключить режим использования вкладок браузером Internet Explorer. После этого каждый открываемый вами сайт будет отображаться в отдельном окне.
- Предупреждать при одновременном закрытии вкладок — после снятия данного флажка больше не будет (при закрытии браузера) отображаться окно с вопросом, нужно ли сохранить открытые в данный момент вкладки браузера.
- Всегда переключаться на новую вкладку при ее создании — установив этот флажок, вы всегда будете переключаться на только что созданную вкладку.
- Включить быстрые вкладки (после перезапуска) — быстрыми вкладками называется режим отображения открытых в данный момент вкладок в виде эскизов в отдельном окне браузера. Перейти в режим быстрых вкладок можно либо с помощью комбинации клавиш Ctrl+Q, либо с помощью кнопки слева от первой вкладки поля вкладок браузера.
- Открывать только первую домашнюю страницу при запуске — установка данного флажка приводит к загрузке при старте браузера только первой домашней страницы из списка домашних страниц.
- Открывать новые вкладки справа от текущей — определяет, будет ли новая создаваемая вкладка располагаться справа от текущей (или она будет отображаться самой крайней вкладкой панели).

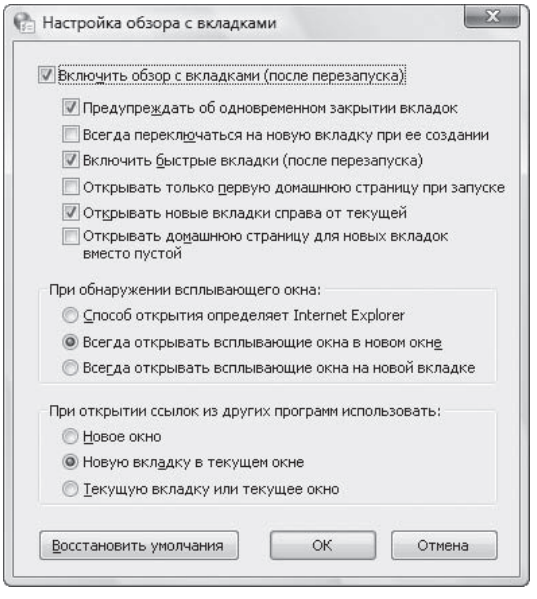


Рис. 4.14. Окно настройки параметров отображения вкладок

- Открывать домашнюю страницу для новых вкладок вместо пустой — после установки данного флажка при создании каждой новой вкладки в нее будет загружаться не пустая страница, а домашняя страница пользователя.
- При обнаружении всплывающего окна — с помощью данного переключателя можно определить, будут ли всплывающие окна также отображаться на отдельных вкладках. Или же всплывающие окна будут отображаться в отдельном окне (или не будут отображаться вообще).
- При открытии ссылок из других программ использовать — этот переключатель определяет, как будут отображаться ссылки, на которых вы щелкнете кнопкой мыши. Либо они будут отображаться в отдельном окне, либо как новая вкладка, либо на той же вкладке, что и родительская вебстраница.

- Безопасность — эта вкладка совершенно не изменилась. С ее помощью попрежнему можно настроить уровень безопасности для различных зон Интернета.
- Конфиденциальность — также не изменилась. Благодаря ей можно настроить механизм блокирования всплывающих окон, а также параметры работы с файлами cookies. По умолчанию всплывающие окна запрещены, и при появлении такого окна его отображение блокируется браузером, после чего в верхней части окна появляется панель с уведомлением о том, что было заблокировано всплывающее окно. С помощью контекстного меню данного уведомления можно разрешить отображение возникшего всплывающего окна.
- Содержание — а вот эта вкладка немного преобразилась. Теперь с ее помощью можно не только настроить механизм ограничения доступа к содержимому

различных веб-сайтов (поле Ограничение доступа), просмотреть список доступных сертификатов (поле Сертификаты) или настроить параметры автоматической подстановки ваших данных и паролей в поля и формы (поле Автозаполнение), но и настроить механизм работы с RSS-лентами, а также отобразить мастер Родительский контроль.

Чтобы отобразить настройки работы с RSS-лентами, нужно нажать кнопку Параметры поля Веб-каналы. После этого отобразится окно — в нем можно определить интервал проверки нового содержимого RSS-лент, на которые вы подписались, а также определить, будет ли воспроизводиться звуковой сигнал при обнаружении браузером новых RSS-каналов на загружаемом сайте.

- Подключения — данная вкладка также совершенно не изменилась. По-прежнему с ее помощью можно настроить подключение к Интернету, а также параметры прокси-сервера, если он используется.
- Программы — с помощью этой вкладки можно указать программу просмотра исходного кода HTML-страницы, а также другие программы, ассоциированные с чтением новостей, почты и т. д.
- Дополнительно — как и раньше, вкладка содержит набор дополнительных параметров настройки браузера Internet Explorer.

Программа msfeedssync.exe

Расположение: `%systemroot%\system32\msfeedssync.exe`.

С помощью данной программы командной строки можно выполнить некоторые операции по синхронизации RSS-лент браузера Internet Explorer. Программа поддерживает следующие параметры.

- `Rebuild` — заново назначает параметры синхронизации RSS-лент.
- `Forcesync` — начинает синхронизацию RSS-лент.
- `Disable` — присваивает параметру `REG_DWORD`-типа `SyncStatus`, расположенному в ветви реестра `HKEY_CURENT_USER\Software\Microsoft\Feeds`, значение `0`.
- `Enable` — присваивает значение `1` параметру `REG_DWORD`-типа `SyncStatus`, расположенному в ветви реестра `HKEY_CURENT_USER\Software\Microsoft\Feeds`.
- `Schedule` — выполняет назначение синхронизации RSS-лент.
- `Sync` — проверяет, возможно ли выполнить синхронизацию RSS-лент. Если возможно, то выполняет синхронизацию.

Настройка с помощью групповых политик

Особенностью новой версии браузера Internet Explorer является то, что практически все параметры его работы можно настроить с помощью групповых политик. Конечно, на страницах данной книги все параметры групповых политик описать будет сложно, так как их очень много, но некоторые мы все же рассмотрим.

Основным подразделом, в котором расположены групповые политики браузера Internet Explorer, является Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer разделов Конфигурация компьютера и Конфигурация пользователя.

Все описанные ниже групповые политики изменяют значения параметров типа REG_DWORD.

- Включение полноэкранного режима — установка данной политики приведет к тому, что браузер Internet Explorer будет всегда запускаться в полноэкранном режиме.

  Политика влияет на значение параметра ITBar7Position, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Toolbar\WebBrowser.

- Не разрешать пользователям включать и отключать надстройки — установка этой политики запрещает пользователям добавлять и удалять надстройки браузера Internet Explorer.

  Политика влияет на значение параметра NoExtensionManagement, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions.

- Отключить периодическую проверку обновлений компонентов Internet Explorer — определяет, будет ли браузеру разрешено автоматически выполнять поиск новых обновлений.

  Политика влияет на значение параметра NoUpdateCheck, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main.

- Включить панель меню по умолчанию — указывает, будет ли в браузере по умолчанию отображаться стандартная строка меню.

- Политика влияет на значение параметра AlwaysShowMenus, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main.

Групповые политики, управляющие настройкой браузера, также хранятся во вложенном подразделе Панель управления обозревателем описанного выше раздела Internet Explorer. Эти политики изменяют значения параметров REG_DWORD-типа ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel.

- Отключить вкладку 'Дополнительно' — с помощью данной политики можно запретить отображение вкладки Дополнительно окна Свойства: Интернет.

  Политика влияет на значение параметра AdvancedTab.

- Отключить вкладку 'Подключения' — благодаря этой политике можно запретить отображение вкладки Подключения окна Свойства: Интернет.

  Политика влияет на значение параметра ConnectionsTab.

- Отключить вкладку 'Содержание' — с помощью данной политики можно запретить отображение вкладки Содержание окна Свойства: Интернет.

  Она влияет на значение параметра `ContentTab`.

- Отключить вкладку 'Общие' — благодаря этой политике можно запретить отображение вкладки Общие окна Свойства: Интернет.

  Политика влияет на значение параметра `GeneralTab`.

- Отключить вкладку 'Конфиденциальность' — с помощью данной политики можно запретить отображение вкладки Конфиденциальность окна Свойства: Интернет.

  Политика влияет на значение параметра `PrivacyTab`.

- Отключить вкладку 'Программы' — благодаря этой политике можно запретить отображение вкладки Программы окна Свойства: Интернет.

  Она влияет на значение параметра `ProgramsTab`.

- Отключить вкладку 'Безопасность' — с помощью данной политики можно запретить отображение вкладки Безопасность окна Свойства: Интернет.

  Политика влияет на значение параметра `SecurityTab`.

Команды rundll32.exe, позволяющие работать с браузером Internet Explorer

На страницах данной книги уже встречались врезки, описывающие ту или иную команду `rundll32.exe`, с помощью которой можно выполнить какое-то действие. Такие же команды существуют и для работы с браузером Internet Explorer. Правда, этих команд настолько много, что описывать их во врезках было бы нецелесообразно.

Команды, отображающие различные окна

По результатам выполнения команды `rundll32.exe` можно разбить на отображающие мастера и окна операционной системы Windows Vista и изменяющие параметры реестра или содержимое файлов операционной системы. Наиболее наглядны команды, отображающие окна и мастера Windows, поэтому их мы рассмотрим первыми.

- `rundll32.exe IEAKENG.dll, ModifyRatings` — вызывает окно Content Advisor. Команда корректно выполняется даже в том случае, если установлены следующие групповые политики (то есть она позволяет их обойти):
  - Отключить вкладку 'Содержание' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем — устанавливает значение параметра `REG_DWORD`-типа `ContentTab`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel`, равным 1;
  - Отключить изменение параметров оценок раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer — устанавливает значение параметра `REG_DWORD`-типа `Ratings`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel`, равным 1.

- `rundll32.exe IEAKENG.dll, ModifyZones` — выводит на экран окно Свойства: Интернет, содержащее всего две вкладки: Безопасность и Конфиденциальность. Команда позволяет обойти ограничения групповых политик, запрещающих отображение вкладок окна Свойства: Интернет. Она корректно выполняется даже в том случае, если установлена групповая политика Отключить вкладку 'Безопасность' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем. Эта политика устанавливает значение параметра `REG_DWORD`-типа `SecurityTab`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel`, равным 1.
- `rundll32.exe IEAKENG.dll, ShowInetcpl` — вызывает окно Свойства: Интернет. Команда перед вызовом окна запрещает доступ ко всем его вкладкам с помощью групповых политик. После выполнения команды доступ опять разрешается. Например, с помощью данной команды можно быстро запретить доступ к окну Свойства: Интернет. Для этого достаточно выполнить ее. Затем, после отображения окна, сообщающего о том, что доступ к окну Свойства: Интернет запрещен, не нажимая кнопки OK этого окна, завершить процесс `rundll32.exe` с помощью вкладки Процессы окна Диспетчер задач Windows. После этого доступ к окну Свойства: Интернет будет запрещен.
- `rundll32.exe inetcpl.cpl, LaunchSecurityDialogEx` — выводит на экран окно, в котором можно выбрать уровень безопасности зон Интернета, местной сети, а также надежные и ограниченные узлы.
- `rundll32.exe inetcpl.cpl, LaunchPrivacyDialog` — вызывает окно Свойства: Интернет, открытое на вкладке Конфиденциальность.
- `rundll32.exe inetcpl.cpl, ShowLanguageDialog` — выводит окно Language Preference. Команда корректно выполняется даже в том случае, если установлены следующие групповые политики (то есть она позволяет их обойти):
  - Отключить вкладку 'Общие' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем — устанавливает значение параметра `REG_DWORD`-типа `GeneralTab`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel`, равным 1;
  - Отключить изменение параметров языка раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer.
- `rundll32.exe inetcpl.cpl, LaunchInternetControlPanel` — вызывает окно Свойства: Интернет.
- `rundll32.exe inetcpl.cpl, ShowFeedOptionsDialog` — выводит на экран окно Свойства веб-канала. Команда корректно выполняется даже в том случае, если установлена групповая политика Отключить вкладку 'Содержание' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем. Политика устанавливает значение параметра `REG_DWORD`-типа `ContentTab`, расположенного в ветви системного реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel`, равным 1.

- `rundll32.exe inetcpl.cpl, ShowDeleteBrowsingHistoryDialog` — вызывает окно Удаление истории обзора, с помощью которого можно удалить временные файлы Интернета, cookies, файлы Журнала или сохраненные пароли и данные форм. Команда корректно выполняется даже в том случае, если установлены следующие групповые политики (то есть она позволяет их обойти):
  - Отключить вкладку 'Общие' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем — устанавливает значение параметра `REG_DWORD`-типа `GeneralTab`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel`, равным `1`;
  - Отключить возможность 'Удаление записей в журнале обозревателя' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer — устанавливает значение параметра `DisableDeleteBrowsingHistory` типа `REG_DWORD`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel`, равным `1`.
- `rundll32.exe inetcpl.cpl, OpenLanguageDialog` — вызывает окно настройки языка Выбор языка. Команда корректно выполняется даже в том случае, если установлена групповая политика Отключить вкладку 'Общие' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем. Эта политика устанавливает значение параметра `REG_DWORD`-типа `GeneralTab`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel`, равным `1`.
- `rundll32.exe inetcpl.cpl, DisplayPopupWindowManagementDialog` — выводит на экран окно Параметры блокирования всплывающих окон. Команда корректно выполняется даже в том случае, если установлены следующие групповые политики (то есть она позволяет их обойти):
  - Отключить вкладку 'Конфиденциальность' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем — устанавливает значение параметра `REG_DWORD`-типа `PrivacyTab`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel`, равным `1`;
  - Отключить управление уровнем фильтрации всплывающих окон раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer — устанавливает значение параметра `REG_DWORD`-типа `DisablePopupFilterLevel`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions`, равным `1`;
  - Отключить управление всплывающими окнами раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer — устанавливает значение параметра `REG_DWORD`-типа `NoPopupManagement`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions`, равным `1`;

  - Отключить управление списком разрешенных всплывающих окон раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer — устанавливает значение параметра REG_DWORD-типа RestrictPopupExceptionList, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions, равным 1.

- rundll32.exe inetcpl.cpl, LaunchConnectionDialog — вызывает окно Свойства: Интернет, открытое на вкладке Подключения.
- rundll32.exe inetcpl.cpl, LaunchPerSitePrivacyActionDialog — выводит на экран окно Конфиденциальность для отдельных веб-узлов.
- rundll32.exe inetcpl.cpl, LaunchPopupWindowManagementDialog — вызывает окно Параметры блокирования всплывающих окон.
- rundll32.exe MSRATING.dll, RatingSetupUI — отображает окно ограничения доступа Ограничение доступа. Команда корректно выполняется даже в том случае, если установлены следующие групповые политики (то есть она позволяет их обойти):
  - Отключить вкладку 'Содержание' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем — устанавливает значение параметра REG_DWORD-типа ContentTab, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel, равным 1;
  - Отключить изменение параметров оценок раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer — устанавливает значение параметра REG_DWORD-типа Ratings, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel, равным 1.
- rundll32.exe MSRATING.dll, ClickedOnRAT — вызывает окно Ограничение доступа, используемое для ограничения доступа к Интернету, и окно Системы оценок. Команда корректно выполняется даже в том случае, если установлены следующие групповые политики:
  - Отключить вкладку 'Содержание' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем — устанавливает значение параметра REG_DWORD-типа ContentTab, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel, равным 1;
  - Отключить изменение параметров оценок раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer — устанавливает значение параметра REG_DWORD-типа Ratings, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel, равным 1.
- rundll32.exe shdocvw.dll, DoOrganizeFavDlg — вызывает окно Упорядочить избранное.
- rundll32.exe CRYPTUI.dll, CryptUIStartCertMgr — выводит на экран диалоговое окно Сертификаты, которое открыто на вкладке Личные. Команда

корректно выполняется даже в том случае, если установлены следующие групповые политики:

- Отключить вкладку 'Содержание' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем — устанавливает значение параметра REG_DWORD-типа ContentTab, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel, равным 1;
- Отключить изменение параметров сертификатов раздела Административные шаблоны ▸ Компоненты WindowsInternet Explorer — устанавливает значение параметра REG_DWORD-типа Certificates, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel, равным 1.

- `rundll32.exe wintrust.dll, OpenPersonalTrustDBDialog` — вызывает окно Сертификаты, открытое на вкладке Доверенные издатели. Команда корректно выполняется даже в том случае, если установлены следующие групповые политики:
  - Отключить вкладку 'Содержание' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем — устанавливает значение параметра REG_DWORD-типа ContentTab, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel, равным 1;
  - Отключить изменение параметров сертификатов раздела Административные шаблоны ▸ Компоненты WindowsInternet Explorer — устанавливает значение параметра REG_DWORD-типа Certificates, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel, равным 1.
- `rundll32.exe IEAKENG.dll, ModifyAuthCode` — вызывает окно Сертификаты, содержащее только вкладку Доверенные издатели. Команда корректно выполняется даже в том случае, если установлены следующие групповые политики:
  - Отключить вкладку 'Содержание' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем — устанавливает значение параметра REG_DWORD-типа ContentTab, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel, равным 1;
  - Отключить изменение параметров сертификатов раздела Административные шаблоны ▸ Компоненты WindowsInternet Explorer — устанавливает значение параметра REG_DWORD-типа Certificates, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel, равным 1.

Команды, выполняющие различные действия

Теперь рассмотрим оставшиеся команды `rundll32.exe`, которые не отображают никаких окон или мастеров, но выполняют другие действия в операционной системе Windows Vista.

- `rundll32.exe IEAKENG.dll, ImportProgramsA` — создает в профиле пользователя папку MZ•, содержащую файл `programs.inf` с параметрами из ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Clients` и некоторых других ветвей реестра. Эти ветви хранят сведения, определяемые на вкладке Программы окна Свойства: Интернет.
- `rundll32.exe IEAKENG.dll, ImportRatingsA "путь к inf-файлу"` — создает INF-файл с настройками ограничений доступа к Интернету (Ratings).
- `rundll32.exe iedkcs32.dll, BrandCleanInstallStubs` — устанавливает по умолчанию настройки оболочки браузера Internet Explorer.
- `rundll32.exe iedkcs32.dll, BrandIE4 SIGNUP` — восстанавливает содержимое Избранного, используемое по умолчанию, а также выполняет другие действия, описанные в файле `brndlog.txt` каталога `%userprofile%\AppData\Local\Microsoft\Internet Explorer`.
- `rundll32.exe iedkcs32.dll, Clear` — устанавливает по умолчанию настройки браузера.
- `rundll32.exe inetcpl.cpl, DllInstall` — восстанавливает настройки отображений списков вкладок Дополнительно (окно Свойства: Интернет) и Параметры безопасности (отображается после нажатия кнопки Другой, расположенной на вкладке Безопасность окна Свойства: Интернет).
- `rundll32.exe inetcpl.cpl, ResetIEtoDefaults` — устанавливает настройки браузера по умолчанию. Команда корректно выполняется даже в том случае, если установлены следующие групповые политики (то есть она позволяет их обойти):
  - Отключить вкладку 'Дополнительно' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем — устанавливает значение параметра `REG_DWORD`-типа `AdvancedTab`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel`, равным 1;
  - Запретить сброс параметров Internet Explorer раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем ▸ Вкладка 'Дополнительно' — политика устанавливает значение параметра `REG_DWORD`-типа `DisableRIED`, расположенного в ветви реестра `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Control Panel`, равным 1.
- `rundll32.exe MSRATING.dll, RatingEnable` — включает механизм ограничения доступа к содержимому Интернета. Команда корректно выполняется даже в том случае, если установлены следующие групповые политики:
  - Отключить вкладку 'Содержание' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем — устанавливает значение параметра `REG_DWORD`-типа `ContentTab`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel`, равным 1;
  - Отключить изменение параметров оценок раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer — устанавливает значение

параметра REG_DWORD-типа Ratings, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel, равным 1.

- rundll32.exe MSRATING.dll, ClickedOnPRF "путь к файлу" — загружает настройки из указанного файла правил PICS. Команда корректно выполняется даже в том случае, если установлены следующие групповые политики:
  - Отключить вкладку 'Содержание' раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer ▸ Панель управления обозревателем — устанавливает значение параметра REG_DWORD-типа ContentTab, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel, равным 1;
  - Отключить изменение параметров оценок раздела Административные шаблоны ▸ Компоненты Windows ▸ Internet Explorer — устанавливает значение параметра REG_DWORD-типа Ratings, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel, равным 1.
- rundll32.exe shdocvw.dll, DoFileDownload "путь к файлу" — выполнить загрузку файла.
- rundll32.exe shdocvw.dll, OpenURL "путь к файлу" — открывает URL-файл ярлыка.
- rundll32.exe shdocvw.dll, SetShellOfflineState — установить запуск браузера в автономном режиме.
- rundll32.exe url.dll, OpenURL "путь к файлу" — открывает URL-файл ярлыка.
- rundll32.exe WININET.dll, DeleteIE3Cache — очищает кэш Интернета (папки из ветви %userprofile%\Local Settings\Temporary Internet Files).

4.5. Почта Windows

Расположение: %programfiles%\Windows Mail\WinMail.exe.

Пусть вас не смущает новое название почтового клиента. В операционной системе Windows Vista было решено переименовать стандартный почтовый клиент Outlook в Почта Windows. Несмотря на это и на новый интерфейс почтового клиента, работа с ним напоминает работу с его предыдущими версиями.

Как и раньше, почтовый клиент может работать по протоколам SMTP, IMAP, POP3. Но если Outlook Express также поддерживал работу по протоколу HTTP, то Почта Windows эту возможность больше не поддерживает. Поэтому теперь вы не сможете использовать по протоколу HTTP учетные записи таких почтовых систем, как Hotmail или MSN Mail.

Как и при описании браузера Internet Explorer, начнем описание нового почтового клиента с основного списка нововведений.

- В первую очередь, это преследующая нас повсюду поисковая строка, с помощью которой можно выполнить поиск по заголовкам и содержимому сообщений. Обратите также внимание, что поиск сообщений может вестись и из строки поиска меню Пуск.
- Изменилось само понятие адресной книги (WAB). Теперь нет централизованной базы контактов, хранящейся в реестре, а все контакты представляют собой отдельные файлы в XML-формате, расположенные в специальной папке Контакты.
- Теперь отсутствует возможность создания нескольких учетных записей почтового клиента (удостоверения) на основе одной учетной записи пользователя (на основе SID пользователя). Иными словами, теперь один пользователь может иметь только одну учетную запись почтового клиента. Это и неудивительно, ведь те, кто читал мои предыдущие книги, знают, что если у вас есть учетная запись почтового клиента, то можно за несколько минут получить доступ к учетной записи любого другого пользователя почтового клиента, не зная его пароль.
- В новом почтовом клиенте появился встроенный антиспамовый фильтр, позволяющий удалять нежелательные сообщения из почтового ящика POP3.

Интерфейс почтового клиента

После первого запуска почтового клиента перед вами отобразится его обновленный логотип (рис. 4.15), после чего будет предложено создать новую учетную запись пользователя. Введенные вами учетные данные всегда можно изменить.

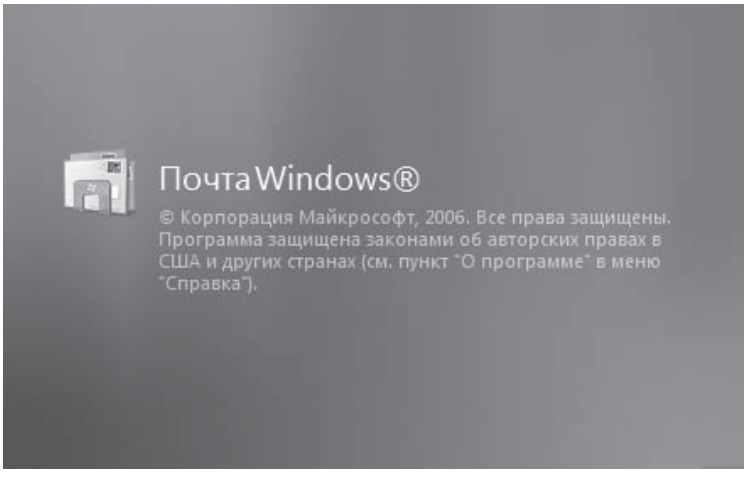


Рис. 4.15. Логотип почтового клиента Почта Windows

Нужно признать, что интерфейс нового почтового клиента изменился не очень сильно (рис. 4.16). Единственное нововведение — это строка поиска. Программисты Microsoft не заменили даже стандартную строку меню, как они это сделали с большинством программ операционной системы.

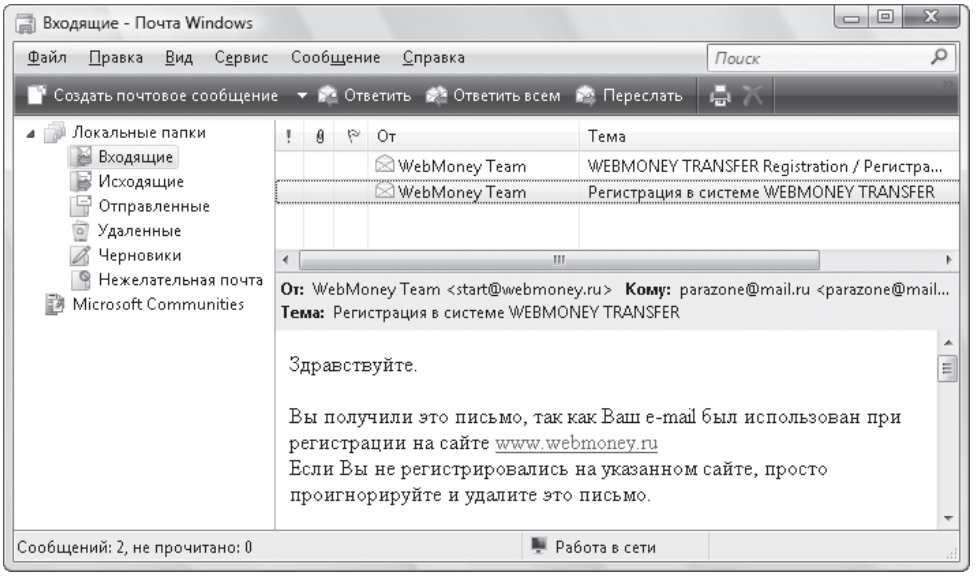


Рис. 4.16. Окно почтового клиента Почта Windows

Окно программы

Как обычно, окно программы делится на три части.

- Первая часть, расположенная в левой части окна программы, содержит список папок и новостных групп, на которые вы подписаны.

  В поле папок, кроме папок для входящей, исходящей, отправленной, удаленной почты и черновиков, присутствует новая папка — Нежелательная почта. Она хранит все письма, которые встроенный антиспамовый фильтр признал неблагонадежными.

  Обратите внимание на новостную группу, на которую вы подписаны по умолчанию (Microsoft Communities). Новости предоставляет сервер msnews.microsoft.com. После того как вы обратитесь к нему в первый раз, будет загружен список всех доступных тематических групп, на которые вы можете подписаться. Все эти группы посвящены тонкостям работы в операционных системах семейства Windows.

- Вторая часть расположена в верхней части окна программы и содержит список сообщений, хранящихся в открытой в данный момент папке.

- Третья часть расположена снизу и включает в себя текст открытого в данный момент сообщения.

Меню программы

В контексте данной главы мы также поверхностно рассмотрим содержимое меню программы Почта Windows, после чего в следующей главе будут более подробно описаны некоторые аспекты работы с почтовым клиентом. Большинство команд раскрывающихся списков меню не изменились.

- Файл — с помощью этого меню можно создать почтовое или новостное сообщение, а также добавить контакт к адресной книге почтового клиента или новую папку в список папок. Благодаря ему можно также сохранить вложенные в полученное письмо файлы в файловой системе компьютера.

  Еще одной стандартной возможностью меню Файл является импорт и экспорт адресной книги, контактов или почтовых сообщений. Например, чтобы импортировать адресную книгу в WAB-формате (используемом предыдущими версиями почтового клиента Outlook Express), нужно воспользоваться командой Файл ▸ Импорт ▸ Контакты Windows. Для импорта почтовых сообщений нужно выбрать команду Файл ▸ Импорт ▸ Сообщения.

  Не исчезла из меню Файл и команда Удостоверения. Однако теперь с ее помощью можно лишь импортировать или экспортировать учетные данные пользователя, но не создавать нового пользователя.

- Правка — с помощью команд данного меню выполняется работа с почтовыми сообщениями: удаление, копирование, перемещение между папками, поиск и т. д.

- Вид — позволяет настроить интерфейс почтового клиента, а также просмотреть сообщения в формате HTML.

- Сервис — содержит основные команды для настройки почтового клиента. К ним относятся команды для настройки:

  - правил почтовых и новостных сообщений (подменю Правила для сообщений);
  - новостных групп, на которые вы подписаны (команда Группы новостей);
  - учетных записей почтовых серверов и новостных групп (команда Учетные записи);
  - антиспамового фильтра (команда Параметры нежелательной почты) и почтового клиента (команда Параметры).

  Меню также включает в себя команды, с помощью которых можно подключиться к почтовому серверу и проверить новые письма (команда Синхронизировать все), отправить все письма, расположенные в папке Исходящие (команда Доставить почту ▸ Доставить все), или получить все письма, расположенные в почтовом ящике.

- Сообщение — с помощью этого меню выполняются все операции над сообщениями: создание нового, ответ на полученное, перенаправление полученного, а также занесение адреса полученного сообщения в черный или белый список антиспамового фильтра (подменю Нежелательная почта).

Работа с почтовым клиентом

Следующим этапом работы с почтовым клиентом является настройка его параметров.

Работа с учетными записями почтовых и новостных серверов

При первом запуске почтового клиента Почта Windows перед вами отобразится мастер настройки учетной записи почтового клиента. Заполнение полей этого мастера обязательно, но не стоит относиться к этому слишком серьезно, так как все введенные вами настройки впоследствии можно будет изменить.

Первым шагом работы мастера является просьба ввести ваши имя и фамилию. Именно эти данные буду использоваться по умолчанию при занесении вашего адреса в адресную книгу.

Дальше нужно указать ваш полный почтовый адрес. После этого нужно ввести входящий и исходящий адреса вашего почтового сервера. Как правило, если вы не знаете эти адреса, на сайте почтового сервера нужно зайти в раздел настроек, где они должны быть указаны. Например, для почтового сервера www.mail.ru входящим адресом является pop.mail.ru, а исходящим — smtp.mail.ru.

Следующим шагом является указание вашего имени (имя — это часть почтового адреса, расположенная справа от символа @) и пароля. После этого настройка учетных записей почтового сервера будет закончена.

Если же вы хотите изменить некоторые введенные вами настройки учетных записей почтового сервера или указать дополнительные настройки, то нужно вызвать окно Учетные записи в Интернете (рис. 4.17). Для этого в меню Сервис нужно выбрать команду Учетные записи.

Это окно содержит список всех созданных вами учетных записей подключения к почтовым или новостным серверам. Обратите внимание, что также в этом окне находится встроенная учетная запись новостного сервера Microsoft Communities.

Чтобы изменить параметры учетной записи, нужно выделить ее и нажать кнопку Свойства. Можно также создать новую учетную запись, удалить старую или установить новую в качестве используемого почтового сервера по умолчанию.

Окно Свойства учетной записи содержит пять вкладок.

- С помощью вкладки Общие можно изменить почтовый адрес учетной записи (рис. 4.18).
- Благодаря вкладке Серверы настраиваются входящий и исходящий адреса почтового сервера, а также ваше имя и пароль как для первого, так и для второго сервера (некоторые почтовые серверы, например www.mail.ru, требуют, чтобы пароль и имя пользователя вводились и для входящего, и для исходящего адреса, несмотря на то что пароль и имя пользователя для обоих серверов совпадают).
- С помощью вкладки Подключение можно выбрать способ подключения к Интернету, если у вас создано несколько подключений (например, одно через обычный модем, а другое через выделенную линию).

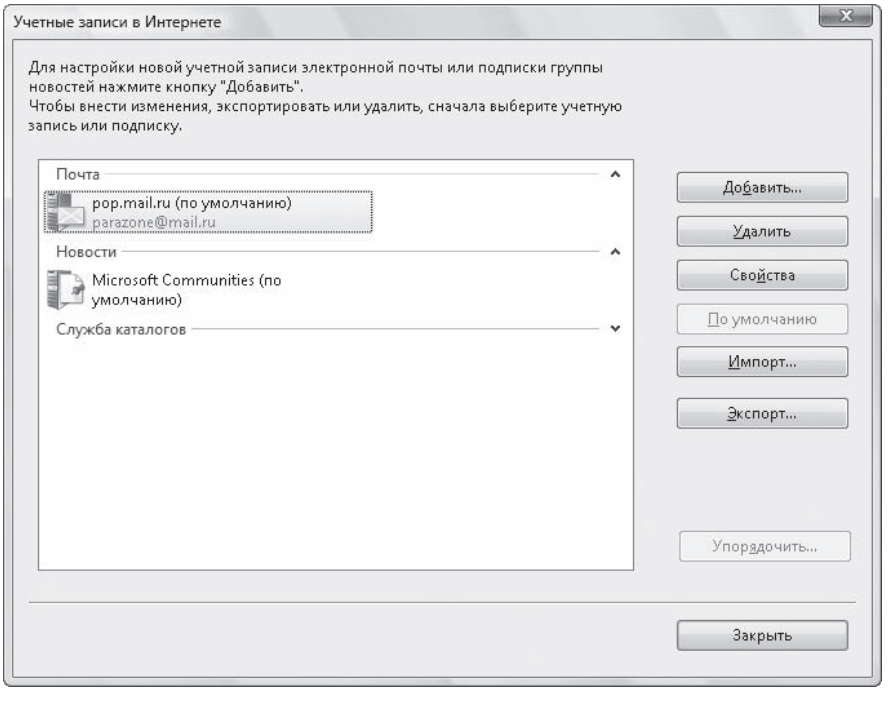


Рис. 4.17. Окно учетных записей почтовых серверов

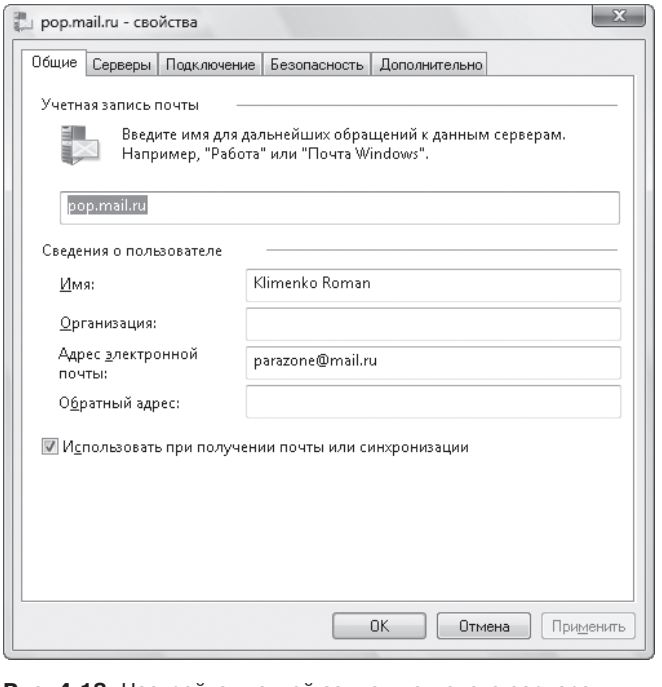


Рис. 4.18. Настройка учетной записи почтового сервера

Остальные вкладки позволяют настроить параметры безопасности и другие параметры работы почтового сервера. Их нужно настраивать с осторожностью или не настраивать вообще — с некоторыми параметрами ваш почтовый сервер может не уметь работать.

Настройка антиспамового фильтра

Антиспамовый фильтр является нововведением почтового клиента Почта Windows. Для его настройки служит окно Параметры нежелательной почты (рис. 4.19), вызвать которое можно с помощью одноименной команды меню Сервис.

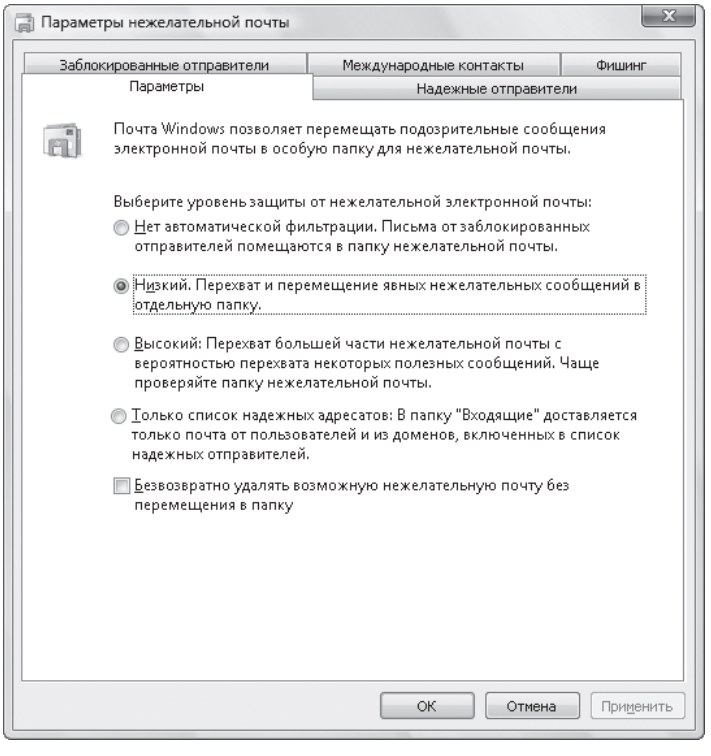


Рис. 4.19. Окно настройки антиспамового фильтра

В окне расположены следующие вкладки.

- Параметры — позволяет настроить поведение антиспамового фильтра. Установив флажок, можно заставить антиспамовый фильтр удалять все подозрительные письма вместо того, чтобы помещать их в специальную папку Нежелательная почта. Остальные же элементы вкладки определяют уровень работы аниспамового фильтра. Возможны следующие уровни:
  - отключить фильтр;
  - низкий уровень фильтрации: помещать в папку Нежелательная почта только письма, определенные явно как спам;

- высокий уровень: помещать все письма, совершенно не имеющие признаков спама, в обычные папки, а остальные письма — в папку Нежелательная почта;
- помещать в папку Нежелательная почта все письма, адрес которых не значится в белом списке антиспамовского фильтра.

- Надежные отправители — позволяет просмотреть адреса, помещенные в белый список антиспамовского фильтра, а также добавить новые адреса или удалить уже существующие. Письма с адресов из белого списка никогда не могут считаться спамом.
- Заблокированные отправители — с помощью этой вкладки можно настроить черный список. Письма с адресов из черного списка всегда считаются спамом.
- Международные контакты — на этой вкладке можно указать определенные домены первого уровня и кодировки текста писем. Если их будут содержать входящие сообщения, то они также будут считаться спамом. Очень интересная возможность. Например, если вы никого не знаете из Албании и никогда там не были, вряд ли вам придет письмо из этой страны, не являющееся спамом.

  Список доменов верхнего уровня, письма от которых будут считаться спамом, можно настроить с помощью окна, вызываемого нажатием кнопки Список блокируемых доменов первого уровня. Список блокируемых кодировок можно настроить с помощью окна, вызываемого нажатием кнопки Список блокируемых кодировок.
- Фишинг — с помощью данной вкладки можно определить, будет ли антиспамовый фильтр также проверять все ссылки, которые содержат полученные письма, на признаки фишинга.

Настройка клиента Почта Windows

Теперь немного поговорим о, наверное, уже знакомом вам окне Параметры (рис. 4.20), которое можно отобразить с помощью одноименной команды меню Сервис. По сравнению с предыдущими версиями почтового клиента содержимое данного окна почти не изменилось. Поэтому просто повторим его основные возможности.

Окно Параметры содержит десять вкладок.

- Общие — определяет программы по умолчанию для чтения электронных сообщений и новостей, а также действия почтового клиента при получении и отправке электронных писем или новостных сообщений: будет ли воспроизводиться звуковой сигнал, будут ли автоматически отображаться папки с непрочитанными письмами, будет ли при запуске почтового клиента автоматически проверяться содержимое почтового сервера и т. д.
- Чтение — в основном определяет параметры отображения прочитанных сообщений: каким цветом они будут отображаться, когда можно считать сообщение прочитанным, можно ли отображать полученные сообщения в HTML-формате или только в текстовом и т. д. Позволяет также изменить шрифт и кодировку, которым будет отображаться текст сообщения.

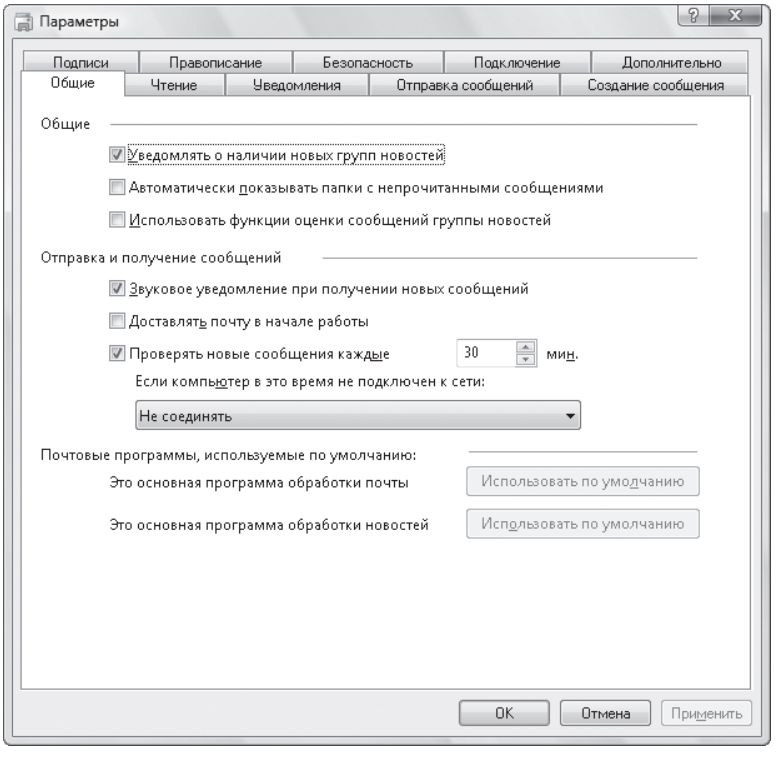


Рис. 4.20. Окно Параметры почтового клиента Почта Windows

- Уведомления — позволяет настроить функцию уведомления о прочтении: будут ли отсылаться уведомления о том, что вы прочли письмо, и нужно ли просить пользователя, которому вы послали письмо, тоже отправлять уведомления, а также будет ли возможно отсылать безопасные уведомления.
- Отправка сообщений — определяет параметры отправки ваших электронных писем и новостных сообщений. Например, в каком формате будут отправляться сообщения (текстовом или HTML), а также будут ли копии отправленных вами сообщений помещаться в папку Отправленные, будут ли сообщения отправляться сразу или сначала они будут помещаться в папку Исходящие и т. д.
- Создание сообщения — определяет параметры создания сообщения. Например, шрифт, который будет использоваться при написании сообщения. Можно также указать «визитную карточку» (информация о вас, которая будет добавляться к каждому написанному сообщению) и шаблон сообщения.
- Подписи — позволяет определить произвольный текст, который будет добавляться к концу каждого написанного вами сообщения. Таким способом могут указываться ваши реквизиты или просто какая-либо фраза, которая характеризует вас с определенной стороны.
- Правописание — определяет настройки правописания: будет ли проверяться правописание в написанных вами письмах, будет ли предлагаться замена для

неправильно написанных вами слов и т. д. Можно определить язык, слова которого будут проверяться.

- Безопасность — определяет настройки безопасности при работе почтового клиента. Например, зону Интернета, к которой будут относиться все полученные вами файлы, будут ли шифроваться и подписываться ваши сообщения. С помощью данной вкладки можно также получить сертификат для возможности подписывания сообщений.
- Подключения — позволяет настроить параметры подключения к Интернету, а также указать, будет ли автоматически разрываться связь после отправки и получения писем.
- Дополнительно — это единственная вкладка, интерфейс которой изменился. Но, несмотря на это, с ее помощью можно выполнить те же действия, что и с помощью одноименной вкладки предыдущей версии почтового клиента. Для этого нужно нажать кнопку Обслуживание данной вкладки.

  Но, кроме того, с помощью данной вкладки можно указать, будет ли:

  - выполняться автоматическое конвертирование вложений сообщений в формат vCard или они останутся в формате по умолчанию;
  - использоваться папка Удаленные для удаленных сообщений при подключении к почтовому серверу с помощью протокола IMAP;
  - в ответное письмо вставляться содержимое исходного письма (письма, на которое вы отвечаете);
  - в ответное письмо вставляться подпись исходного письма.

Настройка с помощью групповых политик

Групповые политики операционной системы Windows Vista позволяют выполнить некоторые операции настройки работы почтового клиента Почта Windows и открытия вложений, получаемых с помощью почтовых клиентов.

Политики настройки Почта Windows описаны в файле `WindowsMail.admx` и расположены в разделе Конфигурация пользователя ▸ Административные шаблоны ▸ Компоненты Windows ▸ Почта Windows. Они изменяют следующие параметры `REG_DWORD`-типа, расположенные в ветви `HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows Mail`:

- `DisableCommunities` — если значение данного параметра равно `1`, то возможность проверки почтовым клиентом сервера групп новостей на наличие сообществ будет запрещена.
- `ManualLaunchAllowed` — при установке значения данного параметра равным `0` запуск почтового клиента запрещен.

Политики настройки работы с вложениями электронной почты описаны в файле `AttachmentManager.admx` и расположены в ветви реестра Конфигурация пользователя ▸ Административные шаблоны ▸ Компоненты Windows ▸ Диспетчер вложений. Они изменяют следующие параметры `REG_DWORD`-типа, расположенные в ветви

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments.

- ScanWithAntiVirus — если значение данного параметра равно 3, то операционная система при открытии вложений будет извещать антивирусные программы и запускать проверку содержимого вложений на наличие вирусов.
- UseTrustedHandlers — данный параметр позволяет указать логику проверки почтовых вложений. Если значение параметра равно 1, то операционная система будет доверять расширению файла. Если значение равно 2, то операционная система будет доверять обработчику приложений (программе, ассоциированной с полученным файлом). Если же значение равно 3, то доверие предоставляться не будет.
- SaveZoneInformation — если значение параметра равно 1, то информация о зоне Интернета, из которой было получено почтовое вложение, будет удаляться из файла.
- HideZoneInfoOnProperties — если значение этого параметра равно 1, то информацию о зоне Интернета, из которой было получено почтовое вложение, будет запрещено удалять (с помощью окна Свойства файла).

Некоторые настройки работы с вложениями также хранятся в параметрах строкового типа ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Associations.

- DefaultFileTypeRisk — имеет тип REG_DWORD. Параметр определяет уровень риска, используемый по умолчанию для файловых вложений. Если его значение равно 1808, то будет использоваться низкий уровень риска (не выдавать предупреждений при открытии файлов). Если значение равно 1807, то будет использоваться средний уровень риска (отображать предупреждение при открытии файла из ограниченной зоны или из зоны Интернета). Если же значение параметра равно 1806, то будет использоваться высокий уровень риска (блокировать открытие файлов из ограниченной зоны и отображать предупреждение при открытии файла из зоны Интернета). По умолчанию используется средний уровень риска.
- HighRiskFileTypes — содержит список расширений для почтовых вложений, которые подпадают под высокий уровень риска.
- LowRiskFileTypes — хранит список расширений для почтовых вложений, которые подпадают под низкий уровень риска.
- ModRiskFileTypes — включает в себя список расширений для почтовых вложений, которые подпадают под средний уровень риска.

Дополнительная настройка почтового клиента с помощью реестра

Несмотря на то что название почтового клиента Windows Vista изменилось, это все тот же почтовый клиент, поддерживающий большинство параметров, которые

поддерживал и почтовый клиент Outlook Express. Однако теперь они расположены в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows Mail.

- Database Corrupt — если присвоить данному параметру REG_DWORD-типа значение 1, то при следующем запуске почтового клиента он восстановит свою базу данных из архивной копии.
- No Modify Accts — этот параметр REG_DWORD-типа может находиться только в ветви реестра корневого раздела HKEY_LOCAL_MACHINE. Если его значение равно 1, то из меню Сервис исчезнет команда Учетные записи, с помощью которой можно было создать или изменить параметры учетных записей пользователей.
- NoSplash — если присвоить данному параметру REG_DWORD-типа значение 1, то при запуске почтового клиента Почта Windows больше не будет отображаться его логотип.
- RequestMDNLocked — если значение данного параметра REG_DWORD-типа равно 1, то будет запрещено изменять состояние флажка Запрашивать уведомления о прочтении для всех отправляемых сообщений, расположенного на вкладке Уведомления окна Параметры.
- SendReceiptsToListLocked — при установке значения этого параметра REG_DWORD-типа равным 1 будет запрещено изменять состояние флажка За исключением случаев, когда сообщение было отправлено в список рассылки и мой адрес отсутствует в поле «Кому:» или «Копия», расположенного на вкладке Уведомления окна Параметры.
- Store Root — этот параметр строкового типа определяет путь к каталогу, содержащему основные данные почтового клиента (файлы учетных записей, папки Входящие, Исходящие и т. д.).
- SendMDNLocked — если значение этого параметра REG_DWORD-типа равно 1, то будет запрещено изменять состояние переключателей области Обработка запросов уведомления о прочтении, расположенной на вкладке Уведомления окна Параметры.
- Security Zone Locked — при установке значения этого параметра REG_DWORD-типа равным 1 будет запрещено изменять состояние переключателей области Выберите зону безопасности для обозревателя Internet Explorer, расположенной на вкладке Безопасность окна Параметры.
- WindowTitle — этот параметр строкового типа позволяет добавить к заголовку почтового клиента свой текст.
- BodyBarPath — имеет строковый тип и определяет путь к рисунку, который будет отображаться в дополнительной панели тела письма. При этом, чтобы отобразить рисунок, также нужно будет присвоить параметру REG_DWORD-типа ShowBodyBar значение 1, чтобы дополнительная панель отобразилась (в самом низу почтового клиента).

Некоторые дополнительные параметры также расположены в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows Mail\Mail.

- Safe Attachments Locked — если значение данного параметра REG_DWORD-типа равно 1, то будет запрещено изменять состояние флажка Не разрешать сохранение или открытие вложений, которые могут содержать вирусы, расположенного на вкладке Безопасность окна Параметры.
- SplitDir — если присвоить данному параметру REG_DWORD-типа значение 1, то в почтовом клиенте поле списка сообщений и поле тела сообщения будут располагаться не горизонтально друг над другом, а вертикально.
- Warn on Mapi Send Locked — если значение этого параметра REG_DWORD-типа равно 1, то будет запрещено изменять состояние флажка Предупреждать, если приложения пытаются отправить почту от моего имени, расположенного на вкладке Безопасность окна Параметры.
- Welcome Message — если присвоить данному параметру REG_DWORD-типа значение 1, то при следующем запуске почтового клиента вам снова придет приветственное сообщение от разработчиков клиента Почта Windows.

Другие программы почтового клиента

В каталоге %programfiles%\Windows Mail, кроме winmail.exe, присутствуют еще две программы, которые могут быть полезны при работе с почтовым клиентом. В этом подразделе мы рассмотрим их назначение, а также способы применения.

Первой программой является wabmig.exe. После ее запуска перед вами отобразится окно Импорт контактов Windows, с помощью которого можно импортировать контакты почтового клиента в файлы других почтовых клиентов.

Программа представляет собой аналог окна, с помощью которого импортирование контактов выполняется в программе Почта Windows. Однако, если вам нужно только импортировать контакты почтового клиента, нет смысла запускать его. Намного быстрее воспользоваться данной программой.

Второй программой является wab.exe. С ее помощью можно отобразить каталог контактов почтового клиента. Однако это еще не все возможности данной программы. Она поддерживает следующие параметры:

- /Find — отображает окно Поиск людей, с помощью которого можно найти определенный контакт в списке контактов;
- /VCard <путь к файлу> — выводит содержимое файла VCard;
- /Group <путь к файлу> — отображает содержимое файла группы;
- /CreateGroup — создает новую группу;
- /Contact <путь к контакту> — отображает существующий контакт;
- /CreateContact — создает новый контакт;

- `/Print <путь к контакту>` — распечатывает контакт;
- `/Import <путь к контакту>` — помещает контакты адресной WAB-книги в адресную книгу почтового клиента;
- `/Upgrade` — обновляет адресную книгу почтового клиента.

4.6. Защитник Windows

Расположение: `%programfiles%\Windows Defender\MSASCui.exe`.

Защитник Windows — это единственная программа, реализующая механизмы безопасности операционной системы Windows Vista, которую мы рассмотрим в этой главе. Мы также рассмотрим несколько мастеров, работа которых основана на программе Защитник Windows.

По умолчанию автоматически при каждом запуске операционной системы также запускается и программа Защитник Windows. Это происходит из-за того, что запуск этой программы прописан в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`.

Программа Защитник Windows предназначена для поиска вредоносного программного обеспечения. После ее запуска перед вами отобразится окно, приведенное на рис. 4.21.

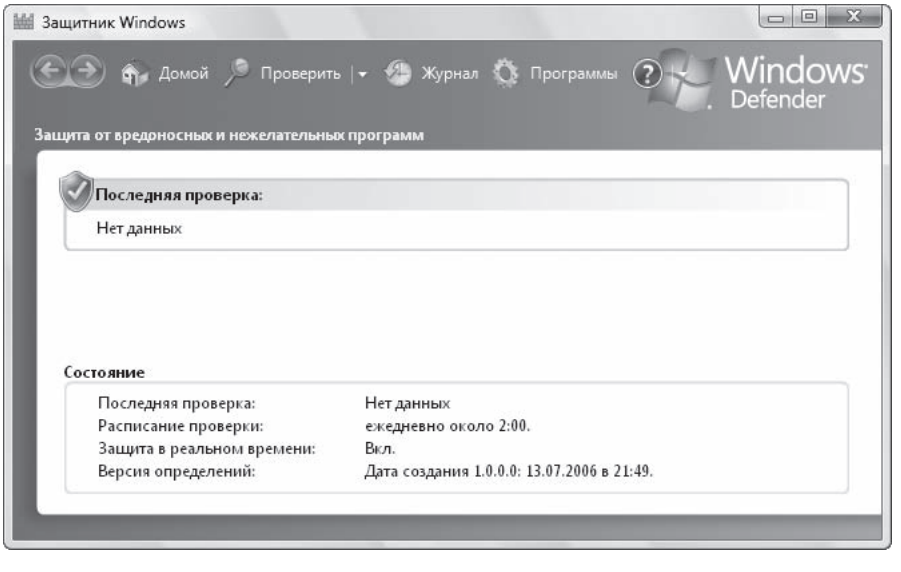


Рис. 4.21. Окно программы Защитник Windows

При запуске программы отображается окно Домой, в котором можно определить, когда в последний раз выполнялся поиск вредоносного программного обеспечения.

Проверка компьютера. Если вы хотите немедленно перейти к сканированию компьютера, то необходимо нажать кнопку Проверить. После этого начнется полное сканирование компьютера. Можно также щелкнуть кнопкой мыши на треугольнике справа данной кнопки, чтобы выбрать быстрое сканирование, полное или сканирование определенных разделов диска.

Программы-исключения. Если же вы хотите просмотреть список разрешенных программ, действия которых никогда не будут считаться подозрительными, то следует воспользоваться кнопкой Журнал.

После этого в появившемся окне нужно щелкнуть кнопкой мыши на ссылке Разрешенные объекты. Если же вы щелкнете кнопкой мыши на ссылке Объекты в карантине, то сможете просмотреть список найденных вирусов, которые были помещены в карантин.

Кроме того, можно просмотреть сведения журнала программы. В него заносятся сведения обо всех подозрительных программах.

И наконец-то, с помощью кнопки Программы можно перейти на окно настройки и дополнительных возможностей программы Защитник Windows (рис. 4.22).

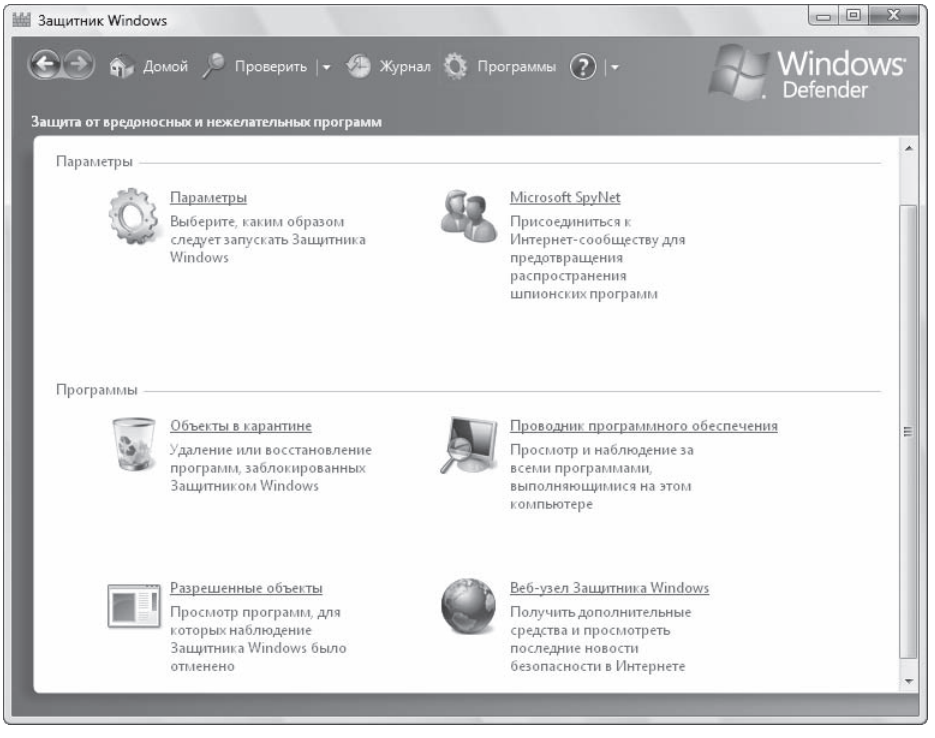


Рис. 4.22. Окно настройки программы Защитник Windows

Его можно назвать самым интересным окном описываемой программы. Рассмотрим возможности этого окна.

Параметры

Выбор данной ссылки предоставляет доступ к настройкам программы Защитник Windows. Например, можно изменить или указать следующие настройки.

- Время автоматического сканирования файловой системы компьютера на вирусы. Для этого предназначено поле Автоматическая проверка. С помощью этого поля можно также определить, будут ли проверяться обновления для базы вирусов перед началом сканирования, а также будет ли применяться действие по умолчанию при обнаружении подозрительной программы (или будет задаваться вопрос пользователю о том, что нужно делать).
- С помощью следующего поля (Действия по умолчанию) можно определить действие по умолчанию, которое будет выполняться при обнаружении подозрительных программ. При этом можно указать различные действия для различных программ в зависимости от степени их опасности.
- Поле Параметры защиты в режиме реального времени позволяет настроить следующие параметры модуля постоянной фоновой защиты компьютера от вирусов: будет ли он включен, будет ли запускаться при входе пользователя в систему, за чем именно он будет следить (например, за запущенными службами или надстройками для Internet Explorer).
- С помощью поля Дополнительные параметры можно настроить такие параметры, как каталоги, содержимое которых сканироваться не будет, указать, будут ли сканироваться заархивированные файлы, будет ли применяться эвристический метод поиска подозрительных программ и подозрительной деятельности.
- С помощью поля Административные параметры можно настроить глобальные параметры работы программы Защитник Windows. Например, указать, будет ли он использоваться вообще, разрешено ли пользователям без прав администратора проводить сканирование системы.

Microsoft SpyNet

Щелкнув кнопкой мыши на этой ссылке, вы можете зайти на специальный форум корпорации Microsoft, посвященный защите компьютеров от вирусов.

Объекты в карантине

С помощью данной ссылки можно просмотреть список программ, которые были занесены в карантин. Если какая-то программа попала в карантин случайно, то можно разрешить ее использование. После этого она добавится в список Разрешенные объекты.

Проводник программного обеспечения

Ссылка предоставляет доступ к четырем дополнительным возможностям программы Защитник Windows.

- Автоматически загружаемые программы — отображает список программ, автоматически запускаемых вместе с операционной системой. При этом отображается

не только имя программы, но и ее описание, издатель, путь к программе, кем был выдан ее сертификат (если такой имеется), с помощью какой именно ветви реестра или каталога она запускается при входе в систему и т. д.

- Текущие выполняемые программы — выводит список процессов, запущенных в данный момент. Для каждого процесса также отображается путь к его исполняемому файлу, от чьей учетной записи процесс запущен, какой PID имеет, какой размер занимает, когда был установлен и т. д. Если же процесс содержит несколько запущенных служб (например, `svchost.exe`), то также отображается список служб, которые работают под этим процессом.
- Программы с подключением к сети — отображает список процессов, которые пытаются получить доступ к сети. Как и в предыдущих возможностях, отображается путь к исполняемому файлу процесса, его размер, версия файла, кем был подписан, от чьего имени был запущен, какой PID имеет и т. д. Но, кроме того, отображаются IP-адреса компьютеров, к которым процесс пытается получить доступ.
- Поставщики службы Winsock — выводит службы и драйверы (провайдеры), взаимодействующие с библиотекой Winsock (библиотека, реализующая доступ к сети). Как и раньше, о провайдере отображается полная информация — от имени библиотеки, реализующей его, до GUID-идентификатора провайдера.

Разрешенные объекты

С помощью данной ссылки можно просмотреть список разрешенных программ, действия которых не считаются подозрительными.

Веб-узел Защитника Windows

Позволяет зайти на сайт программы Защитник Windows. На этом сайте вы можете как скачать новую базу вирусов, так и просто почитать об этой программе.

Настройка с помощью групповых политик

Настроить программу Защитник Windows можно и с помощью групповых политик. Для этого применяются политики, описанные в файле `WindowsDefender.admx` и расположенные в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Защитник Windows.

Политики изменяют значения следующих параметров `REG_DWORD`-типа, расположенных в подразделах ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender`.

- `CheckForSignaturesBeforeRunningScan` — расположен в подразделе `Scan` указанной ветви. Если значение данного параметра равно `1`, то перед началом сканирования всегда будет выполняться поиск и загрузка новых сигнатур нежелательного программного обеспечения.

- SpyNetReporting — параметр находится в подразделе SpyNet. Он позволяет определить режим отправки сведений о найденных вирусах на форум сообщества SpyNet. Например, если значение параметра равно 0, то взаимодействие с сообществом будет запрещено (по умолчанию). Если же значение равно 1, то будет применяться базовый режим взаимодействия — на сайт сообщества будет передаваться только общая информация об обнаруженных новых подозрительных программах. А если значение параметра равно 2, то будет применяться дополнительный режим взаимодействия — на сайт сообщества будет передаваться подробнейшая информация о найденных подозрительных программах (при этом существует вероятность передачи личных данных пользователя).
- ForceFullUpdate — расположен в подразделе Signature Updates. Если значение этого параметра равно 1, то из Интернета всегда будет выполняться загрузка всей базы сигнатур подозрительных программ, а не только той части, которая отсутствует на компьютере.
- DisableLoggingForKnownGood — параметр находится в подразделе Reporting. Если значение параметра равно 1, то в файл журнала Защитника Windows не будет заноситься информация о подозрительных программах, которые пользователь пометил как точно не выполняющие вредоносных действий.
- DisableLoggingForUnknown — расположен в подразделе Reporting. Если значение данного параметра равно 1, то в файл журнала Защитника Windows не будет заноситься информация о подозрительных программах.
- EnableUnknownPrompts — параметр находится в подразделе Real-Time Protection. Если значение равно 1, то при обнаружении подозрительной программы будет выводиться окно, позволяющее запретить ее работу или пометить ее в качестве программы-исключения (которая точно не выполняет вредоносных действий).
- DisableAntiSpyware — если значение этого параметра равно 1, то запуск программы Защитник Windows будет запрещен.
- CheckAlternateDownloadLocation — расположен в подразделе Signature Updates. Если значение этого параметра равно 1, то Защитник Windows будет выполнять обновление сигнатур подозрительных программ с помощью Windows Update, если сервер WSUS в данный момент недоступен. Такое поведение программы установлено по умолчанию.

Параметры реестра, влияющие на работу программы Защитник Windows

Все настройки программы Защитник Windows хранятся в ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender и ее подразделах. В контексте данной книги мы не будем рассматривать параметры, которые можно настроить из самой программы Защитник Windows, а ограничимся только теми, доступ к которым программным способом получить нельзя.

Единственным параметром данной ветви реестра является параметр REG_DWORD-типа ProductUpdateAvailable. Если его значение равно 1, то при следующем запуске программы будет выведено сообщение о необходимости обновления версии программы и появится кнопка, с помощью которой программу можно обновить.

В данной ветви реестра также присутствуют следующие подразделы.

- Signature Updates — содержит сведения о настройках обновления базы вирусов программы Защитник Windows. Кроме стандартных настроек, он включает в себя параметр REG_DWORD-типа UpdateOnStartUp. Если его значение равно 1, то при каждом запуске будет выполняться поиск новых обновлений базы данных вирусов программы Защитник Windows.
- SpyNet — определяет параметры доступа к форуму SpyNet. Среди них присутствует параметр строкового типа SpyNetReportingLocation, который определяет адрес данного форума.
- UX Configuration — среди стандартных параметров данный подраздел хранит параметр REG_DWORD-типа ConsoleFunctionalityAvailable. Он определяет, будет ли разрешен запуск сканирования системы из командной строки.

Мастер Средство удаления вредоносных программ Microsoft Windows

Расположение: %systemroot%\system32\mrt.exe.

Данный мастер не имеет никакого отношения к программе Защитник Windows. Тем не менее, он выполняет схожие с ней действия — ищет различные программы, которые выполняют вредоносные действия (различные шпионские программы).

Чтобы запустить мастер, достаточно воспользоваться командой mrt.exe. При первом запуске мастера необходимо принять его лицензионное соглашение, после чего он предложит выбрать тип сканирования. Можно выполнить быстрое сканирование (переключатель Быстрая проверка), полное сканирование файловой системы компьютера (переключатель Полная проверка) либо выбрать папку, содержимое которой будет просканировано (переключатель Выборочная проверка).

Также существует возможность запуска данного мастера, не содержащего страницу выбора типа сканирования. Если вы воспользуетесь командой mrt.exe /F, то мастер всегда будет выполнять полное сканирование системы.

4.7. Фотоальбом Windows

Расположение: %programfiles%\Windows Photo Gallery\ WindowsPhotoGallery.exe.

Новая программа Фотоальбом Windows пришла на смену используемой в предыдущих версиях операционной системы Windows Программе просмотра изображений и факсов. При этом ее возможности и интерфейс существенно изменились. С ее помощью

теперь можно просмотреть изображения и видеофайлы, хранящиеся в папках Изображения и Видео, а также применить к ним некоторые эффекты.

ПРИМЕЧАНИЕ

С помощью команды rundll32.exe shimgvw.dll, ImageView_Fullscreen "путь к файлу изображения" можно открыть определенный файл в программе просмотра изображений, основанной на возможностях программы Фотоальбом Windows.

В каталоге `%programfiles%\Windows Photo Gallery`, кроме самой программы Фотоальбом Windows, можно найти программу `ImagingDevices.exe`. С ее помощью можно установить сканер или цифровую камеру, а также протестировать их работу.

Интерфейс программы

К интерфейсу программы Фотоальбом Windows вам не придется привыкать долго. Все дело в том, что ее интерфейс напоминает интерфейс музыкального Проигрывателя Windows Media (рис. 4.23).



Рис. 4.23. Окно программы Фотоальбом Windows

Это впечатление особенно усиливает строка управления, располагаемая внизу программы.

Панель управления

Строка управления по форме напоминает строку управления Проигрывателя Windows Media. Она выполняет следующие функции (описаны слева направо).

- Увеличивает эскизы страниц, отображаемых в основном окне программы.
- Устанавливает используемый по умолчанию размер эскизов страниц.
- Позволяет перейти к изображению, расположенному перед выделенным изображением.
- Дает возможность перейти в режим слайд-шоу и отобразить первым выделенное изображение. Чтобы выйти из режима слайд-шоу, нужно выбрать соответствующую команду контекстного меню. Также контекстное меню окна слайд-шоу содержит команды для увеличения или уменьшения скорости отображения рисунков, команду отображения рисунков в случайном порядке.
- Позволяет перейти к изображению, расположенному после выделенного.
- Поворачивает изображение на 90° влево.
- Поворачивает изображение на 90° вправо.
- Удаляет изображение.

Строка меню

Окно программы также содержит строку меню, с помощью которой выполняются основные действия по работе с изображениями, хранящимися в галерее. Строка меню состоит из следующих элементов.

- Файл — с помощью команд данного меню выполняются основные действия по управлению галереей. Например, с его помощью можно добавить в галерею содержимое определенного каталога или памяти цифровой камеры (соответственно, команды Добавить папку в фотоальбом и Импортировать с камеры или сканера). Список всех каталогов, содержимое которых отображается в программе, хранится в параметре `REG_MULTI_SZ`-типа `GalleryScopedFolders`, расположенном в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows Photo Gallery`.

  Можно также определить параметры общего доступа к папкам Изображения и Видео (команда Предоставить общий доступ к устройствам). Удалить, переименовать, копировать или делать дубликат изображения также можно с помощью данного меню. И, конечно, с помощью меню Файл можно получить доступ к настройкам программы Фотоальбом Windows (рис. 4.24).

ПРИМЕЧАНИЕ

Импорт видео можно запретить с помощью параметра REG_DWORD-типа VidCap, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\CaptureWizard. Для этого достаточно данному параметру присвоить значение 1.

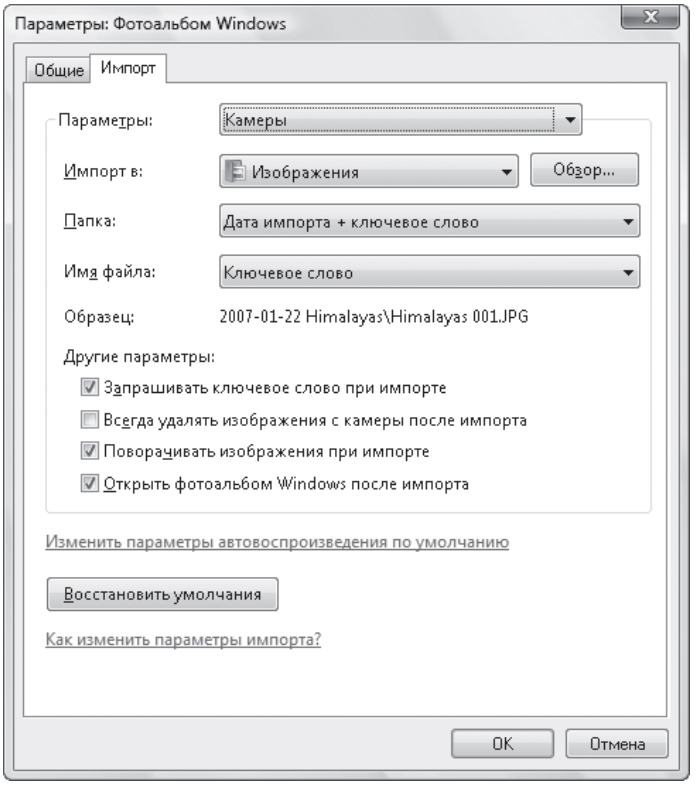


Рис. 4.24. Окно настройки программы Фотоальбом Windows

- Правка — с помощью данного меню можно вызвать панель редактирования изображения (рис. 4.25), которая позволяет выполнить следующие действия: автоматически или вручную изменить контраст и цветовую гамму изображения, применить фильтр, убирающий эффект красных глаз, или обрезать изображение.
- Сведения — при выборе данного меню отображается панель, с помощью которой изображению можно присвоить заголовок и тег. Заголовок отображается при использовании соответствующего вида (он выбирается в контекстном меню основного окна программы Фотоальбом Windows). Тег же используется для сортировки изображений галереи.
- Печать — позволяет распечатать изображение.
- Создать — с помощью данного меню можно записать диск или слайд-шоу на основе выбранных изображений.
- Эл. почта — позволяет отправить изображение по электронной почте.
- Открыть — дает возможность открыть видеофайлы в Проигрывателе Windows Media, а графические изображения — в стандартном графическом редакторе `MsPaint.exe`.



Рис. 4.25. Окно с возможностями редактирования изображения

Панель переходов

Еще одной частью окна программы Фотоальбом Windows является панель, расположенная слева от основного окна. Она предназначена для сортировки изображений, хранящихся в галерее.

Панель позволяет отсортировать изображения по таким критериям, как дата создания, теги, рейтинг, папка, в которой находятся изображения.

Настройка с помощью реестра

С помощью окна Параметры: Фотоальбом Windows можно изменить немногие параметры работы программы, поэтому рассмотрим, как можно изменить дополнительные параметры работы программы Фотоальбом Windows, используя реестр.

Основные параметры программы расположены в ветви системного реестра Windows `HKEY_CURRENT_USER\Software\Microsoft\Windows Photo Gallery\Library`. Рассмотрим наиболее интересные из них.

- `Animations` — этот параметр `REG_DWORD`-типа определяет, будут ли использоваться особые эффекты (эффект перехода одного изображения в другое и т. д.) при переходе между изображениями. Если значение параметра равно `0`, то ани-

мация будет отключена, что существенно повысит скорость работы программы на слабых компьютерах.

- DBPath — имеет строковый тип и позволяет изменить путь к файлу эскизов программы Фотоальбом Windows. По умолчанию значение этого параметра равно %userprofile%\AppData\Local\Microsoft\Windows Photo Gallery\Pictures.pd4.
- MaxThumbSize — этот параметр REG_DWORD-типа позволяет указать максимальный размер в пикселах, до которого можно увеличивать эскизы страниц с помощью ползунка увеличения изображения в окне программы. Максимальное значение данного параметра определяется используемым разрешением вашего монитора (например, 0x400 при разрешении 1024 × 768 пикселов).
- MetadataReadDelay — данный параметр REG_DWORD-типа определяет задержку при чтении метаданных о файле изображения.
- HoverThumbnailThreshold — если значение данного параметра REG_DWORD-типа будет равно 1, то вместо увеличенного эскиза изображения при удержании указателя мыши над ним будет появляться просто описание атрибутов изображения. Если же значение параметра равно 0, то также будет отображаться увеличенный эскиз изображения.

  Определить, будет ли отображаться увеличенный эскиз изображения при наведении на него указателя мыши, можно и с помощью параметра REG_DWORD-типа ShowThumbnailInHoverTooltips.
- UseSounds — этот параметр REG_DWORD-типа определяет, будут ли использоваться звуковые эффекты при работе с программой Фотоальбом Windows.

Можно также настроить дополнительные параметры работы режима слайд-шоу программы Фотоальбом Windows. Для этого нужно воспользоваться параметрами ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows Photo Gallery\SlideShow. Все они имеют тип REG_DWORD.

- EnabledThemeSet — по умолчанию, если операционная система не относит ваш компьютер к мощным и производительным, вы можете просматривать слайд-шоу только с помощью стандартной темы (просмотр изображения таким, какое оно есть).

  Если же вы присвоите этому параметру REG_DWORD-типа значение 1, то при просмотре слайд-шоу в нижней части экрана отобразится дополнительная панель, с помощью которой можно управлять просмотром, а также выбирать темы (отображение изображения в черно-белом варианте и т. д.). Использование этой панели позволяет не только выбирать тему просмотра, но и делает более удобным управление самим процессом просмотра изображений в режиме слайд-шоу.

  Список всех зарегистрированных в операционной системе тем содержится в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Photo Gallery\Slideshow\Themes.

  Все параметры реестра, описанные ниже, используются только при установке значения данного параметра равным 1.

- `AntialiasingQuality` — определяет качество применяемого к изображениям антиалиазинга. Чем больше качество, тем четче будут изображения, но тем сильнее будет нагрузка на процессор компьютера.
- `EnableVideo` — если значение этого параметра `REG_DWORD`-типа равно `1`, то в режиме слайд-шоу можно будет просматривать не только изображения, но и видео.
- `MaxRenderSizeWidth` — этот параметр `REG_DWORD`-типа определяет максимальную ширину в пикселах, при которой можно просматривать видео.
- `MaxRenderSizeHeight` — имеет тип `REG_DWORD` и определяет максимальную высоту в пикселах, при которой можно просматривать видео.
- `PlaybackFramesPerSecond` — данный параметр `REG_DWORD`-типа определяет количество кадров в секунду при воспроизведении.
- `PhodeosPerChunk` — если при попытке воспроизведения слайд-шоу возникает ошибка, то попробуйте присвоить этому параметру `REG_DWORD`-типа значение `1`.
- `UseVSync` — установка значения данного параметра в `1` повышает качество изображения.
- `RunInDXEMode` — его значение определяет, будет ли использоваться режим DXE. При его использовании изображение не растягивается на весь экран.
- `DXExclusiveSize` — если значение данного параметра равно `0`, то изображение будет растягиваться на весь экран даже в режиме DXE. Если же значение параметра равно `1`, то в режиме DXE разрешение экрана будет уменьшаться до минимального, а изображение растягиваться не будет.
- `UseScreenResCache` — определяет, будет ли использоваться кэш для изображений.

4.8. Другие программы

В предыдущем разделе мы рассмотрели наиболее значимые графические приложения, изменившиеся в операционной системе Windows Vista. Сейчас же рассмотрим дополнительные приложения, предоставляющие определенные возможности пользователям операционной системы.

Ножницы — создание снимка экрана

Расположение: `%systemroot%\system32\snippingtool.exe`.

Маленькое, но в некоторых случаях очень полезное приложение. С его помощью можно сделать снимок определенной части экрана, после чего создать на основе снимка файл с расширением GIF, JPG, PNG или HTML (создается страница, содержащая изображение). Конечно, сделать снимок всего Рабочего стола или отдельного окна программы можно было и раньше — с помощью клавиши Print Screen или сочетания клавиш Alt+Print Screen. Но с помощью данной программы можно сделать снимок произвольной области экрана.

ПРИМЕЧАНИЕ

Запуск данной программы можно запретить с помощью параметра REG_DWORD-типа DisableSnippingTool, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\TabletPC. Для этого достаточно присвоить ему значение 1.

Основное окно программы представлено на рис. 4.26. Оно содержит всего три кнопки. С помощью кнопки Создать можно выбрать тип области экрана, которая будет создаваться (снимок всего экрана, определенного окна, снимок прямоугольной области экрана, снимок произвольной области экрана). С помощью кнопки Отмена можно отменить уже созданное вами выделение окна экрана. А с помощью кнопки Параметры можно отобразить окно настроек программы, представленное на рис. 4.27. Обратите внимание на поле Цвет чернил для изменения цвета линии выделения созданного вами снимка экрана. По умолчанию эта линия будет отображаться на полученном снимке. Если же в ней нет необходимости, то лучше снять флажок Показывать линию выделения вручную после записи фрагментов. В противном случае можно изменить цвет линии (по умолчанию снимок очерчивается красной линией).

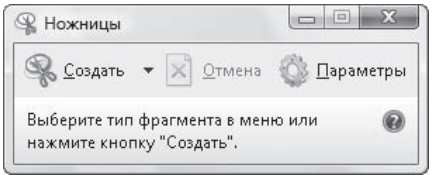


Рис. 4.26. Окно программы Ножницы

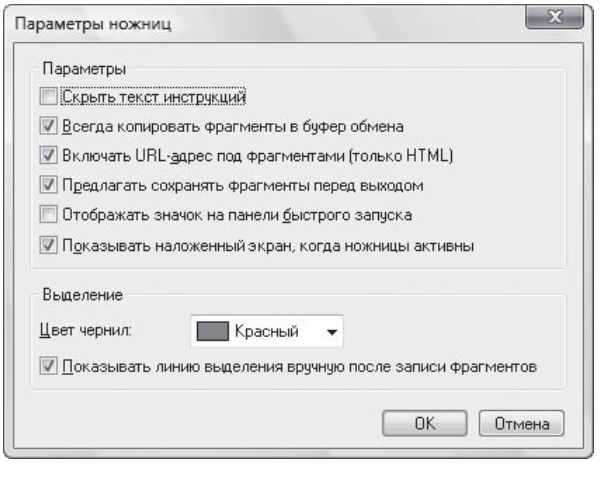


Рис. 4.27. Окно Параметры ножниц

После того как вы выберете необходимый тип создаваемого снимка экрана с помощью кнопки Создать, достаточно определить область, которая войдет в снимок. Для этого ее нужно очертить указателем мыши, нажав ее левую кнопку.

Как только вы создадите область снимка экрана и отпустите левую кнопку мыши, окно программы Ножницы преобразуется в небольшой редактор изображения, содержащий выделенную вами часть экрана (рис. 4.28).

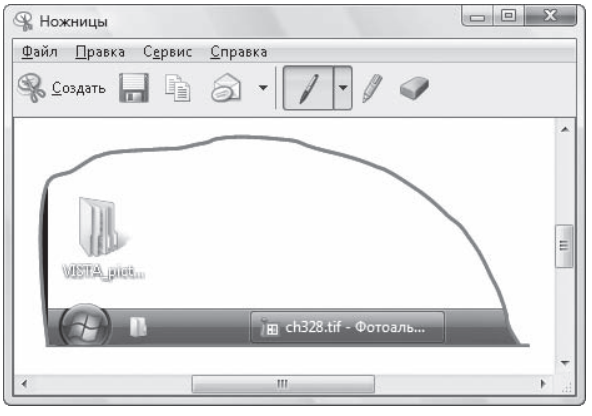


Рис. 4.28. Окно редактирования выделенного снимка экрана

С его помощью созданную вами область экрана можно сохранить, копировать, отправить по почте, а также отредактировать. Редактировать изображение можно всего с помощью двух инструментов. С помощью инструмента Перо можно дорисовать что-либо к снимку, а с помощью инструмента Маркер можно добавить цветовой гамме определенной области изображения желтый цвет. Если же созданные изменения вам не понравятся, то их всегда можно отменить с помощью инструмента Резинка.

Календарь Windows — стандартный органайзер

Расположение: `%programfiles%\Windows Calendar\WinCal.exe`.

Календарь Windows также является новым приложением, входящим в состав операционной системы Windows Vista. Он представляет собой простой органайзер, в который можно заносить информацию о запланированных в будущем мероприятиях (рис. 4.29). Причем особенностью данной программы является то, что доступ к вашим записям могут получить другие пользователи, входящие в состав рабочей группы.

ПРИМЕЧАНИЕ

Запуск данной программы можно запретить с помощью параметра REG_DWORD-типа TurnOffWinCal, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Windows. Для этого достаточно данному параметру присвоить значение 1.

Это можно сделать и с помощью групповой политики Выключить календарь Windows, расположенной в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Календарь Windows. Данная политика описана в файле WinCal.admx.

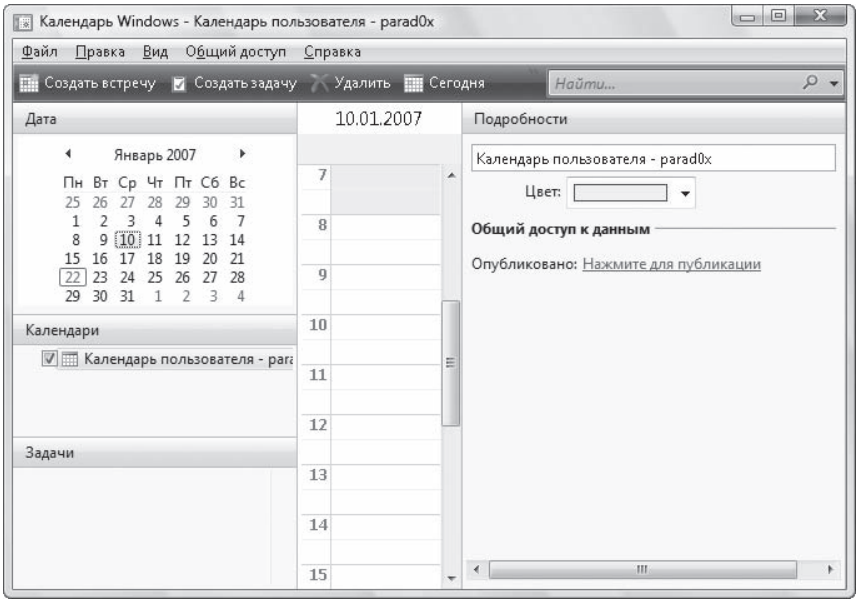


Рис. 4.29. Окно программы Календарь Windows

Чтобы создать запись в органайзере, достаточно нажать кнопку Создать задачу или кнопку Создать встречу. После этого нужно указать в календаре день недели, на который запланировано мероприятие, а затем ввести пояснение к записи, а также время, при наступлении которого операционная система оповестит вас о мероприятии (поле Напоминание).

ПРИМЕЧАНИЕ

Операционная система Windows Vista содержит стандартное назначенное задание Reminders, расположенное в разделе Библиотека планировщика заданий ▸ Microsoft ▸ Windows ▸ WindowsCalender. С помощью данного задания выполняется напоминание о наступлении времени, указанного в записи органайзера. Задание запускается при входе пользователя в систему и выполняет команду F:\Program Files\Windows Calendar\WinCal.exe /reminder.

Чтобы предоставить общий доступ к вашему органайзеру, нужно воспользоваться командой Опубликовать меню Общий доступ.

Игры

Расположение: `%programfiles%\Microsoft Games\`.

Изменился и набор стандартных игр, входящих в поставку операционной системы Windows. Теперь в нем отсутствуют многопользовательские игры, предназначенные для использования через Интернет. Остальные же игры, например Сапер или Паук, стали намного красивее (естественно, благодаря новому интерфейсу Aero).

- Chess Titans — представляет собой обычные шахматы, которые реализованы на основе возможностей нового интерфейса Windows Aero.
- Косынка — стандартная карточная игра операционных систем семейства Windows.
- Червы — также является стандартной карточной игрой операционных систем семейства Windows. Кроме того, что данная игра стала намного красивее, больше в ней ничего не изменилось.
- Инкбол — еще одна новая игра операционной системы Windows Vista. Несмотря на то что она предназначена для пользователей планшетных компьютеров, обычные пользователи также смогут в нее поиграть. Целью игры является перемещение с помощью штрихов мышью нескольких цветных шаров в лузы.

ПРИМЕЧАНИЕ

Запуск данной программы можно запретить с помощью параметра REG_DWORD-типа DisableInkball, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\TabletPC. Для этого достаточно данному параметру присвоить значение 1.

Это можно сделать и с помощью групповой политики Запретить запуск игры 'Инкбол', расположенной в разделе Конфигурация пользователя ▸ Административные шаблоны ▸ Компоненты Windows ▸ Планшетный ПК ▸ Стандартные программы. Данная политика описана в файле TabletShell.admx.

- Mahjong Titans — представляет собой компьютерную версию древней восточной игры.
- Сапер — известная всем стандартная игра операционных систем семейства Windows.
- Purble Place — набор развивающих игр для детей, являющийся нововведением операционной системы Windows Vista.
- Солитер — стандартная карточная игра операционных систем семейства Windows.
- Паук — стандартная карточная игра операционных систем семейства Windows.

Параметры работы с играми в операционной системе Windows Vista можно настроить с помощью нескольких политик, описанных в файле `GameExplorer.admx` и расположенных в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows.

Эти политики изменяют значения следующих параметров `REG_DWORD`-типа, расположенных в ветви `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\GameUX`:

- `ListRecentlyPlayed` — если значение данного параметра равно `0`, то время последней игры не будет отображаться в папке Игры;

- DownloadGameInfo — если значение данного параметра равно 0, то такие данные об игре, как рисунки и рейтинги, не будут загружаться на компьютер с помощью службы метаданных Windows.

Очистка диска от ненужных файлов

Расположение: %systemroot%\system32\cleanmgr.exe.

Программа Очистка дисков не является чем-то новым, но мало найдется пользователей, которые используют ее. С ее помощью можно выполнить очистку дисков компьютера от таких временных файлов, как файлы из каталогов Downloaded Program Files, Temporary Internet Files, Offline Webpages, Корзина, а также временные файлы, файлы thumbnail.db, файлы, создаваемые компонентом Отчеты о проблемах и их решениях при возникновении ошибки и т. д. (вкладка Очистка диска). Кроме того, данная программа позволяет удалить все точки восстановления, созданные службой Восстановление системы (вкладка Дополнительно).

При запуске Очистки дисков перед вами сначала отобразится окно выбора диска, который будет очищаться, а после этого откроется основное окно программы. Скажу сразу, что больше всего типов файлов можно удалить на загрузочном диске запущенной в данный момент операционной системы, так как в списках файлов, которые может очищать данная программа, указаны пути к каталогам на основе переменных окружения.

Кроме того, при запуске данной программы вы можете воспользоваться следующими параметрами.

- /VERYLOWDISK — автоматически очищает каталоги Downloaded Program Files, Temporary Internet Files и Корзина на всех дисках. После этого программа выводит окно, отображающее количество свободного места на диске C:\.
- /SAGESET — позволяет определить файлы, которые будут удаляться при запуске команды cleanmgr.exe /SAGERUN. По умолчанию можно выбрать следующие файлы: из каталога Корзина, временные файлы установки и файлы журналов установки программ, файлы дампа памяти, создаваемые при возникновении аварийного останова системы, CHK-файлы, временные файлы операционной системы и программ, файлы, создаваемые компонентом Отчеты о проблемах и их решениях.

  Можно также создать несколько предопределенных профилей удаления файлов. Для этого нужно использовать параметры /SAGESET:<номер профиля> и /SAGERUN:<номер профиля>. Например, вы можете создать профиль только для удаления содержимого Корзины (например, пусть профиль будет называться 1) и профиль для удаления всех файлов (допустим, 2). После этого, чтобы удалить файлы Корзины на всех дисках, вам будет достаточно воспользоваться командой cleanmgr.exe /SAGERUN:1, а чтобы удалить все ненужные файлы — командой cleanmgr.exe /SAGERUN:2.
- /SAGERUN — удаляет все файлы (на всех дисках), выбранные с помощью окна, отображаемого после запуска команды cleanmgr.exe /SAGESET.

Но это еще не все прелести данной программы. Основной ее плюс заключается в том, что список файлов, которые она может удалять, хранится в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\VolumeCaches`. И вы самостоятельно можете изменять параметры удаляемых файлов или добавлять свои собственные файлы, которые требуется удалить.

Данная ветвь реестра включает в себя набор подразделов, название которых, по сути, неважно. Каждый из них определяет один тип файлов, которые можно удалять с помощью программы Очистка дисков. Эти подразделы содержат следующие параметры.

- `(По умолчанию)` — хранит CLSID-номер, от которого зависит, в каком из окон (выводимом с помощью команды `cleanmgr.exe /SAGESET` или выводимом в главном окне программы `cleanmgr.exe`) будет отображаться возможность удаления файлов данного типа. Например, можно использовать CLSID-номер `{C0E13E61-0CC6-11d1-BBB6-0060978B2AE6}`. Тогда файлы данного типа будут отображаться в окне, вызываемом командой `cleanmgr.exe /SAGESET`.
- `Description` — этот параметр строкового типа содержит описание, отображаемое в окне при выборе данного типа файлов.
- `Temporary Setup Files` — значение данного параметра строкового типа отображается в качестве названия данного типа файлов.
- `FileList` — этот параметр строкового типа хранит шаблоны файлов, которые будут удаляться при выборе в окне удаления файлов данного типа. Можно указывать как один шаблон файлов, так и несколько, разделенных между собой символом `|`. Например, для удаления файлов журналов, создаваемых при установке программ, используется следующее значение данного параметра: `setup*.log|setup*.old|setuplog.txt|winnt32.log`.
- `Flags` — этот параметр `REG_BINARY`-типа определяет флаги удаления.
- `Folder` — имеет строковый тип и определяет папки, в которых будет выполняться поиск файлов, удовлетворяющих критерию, заданному в параметре `FileList`, при удалении файлов данного типа. Можно указывать как одну, так и несколько папок, разделенных между собой символом `|`. Например, так определяются папки, в которых будет выполняться поиск CHK-файлов: `?:\FOUND.000|?:\FOUND.001|?:\FOUND.002` и т. д.
- `StateFlags` — этот параметр `REG_DWORD`-типа определяет состояние флажка напротив данного типа файлов в окне, вызываемом командой `cleanmgr.exe /SAGESET` (флажок установлен или снят).

В качестве примера создадим свой собственный тип файлов, которые можно удалить с помощью команд `cleanmgr.exe /SAGESET` и `cleanmgr.exe /SAGERUN`. Например, довольно часто при ошибке в программе Microsoft Word (при аварийном закрытии открытого в данный момент DOC-файла) в каталоге с открытым в данный момент документом остается множество временных файлов, которые потом приходится удалять вручную. Они имеют следующий формат имен файлов: `~WRL*.tmp` и `~$*.doc`. Попробуем создать фильтр для удаления этих файлов.

Для начала нужно создать подраздел в ветви HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches. Например, назовем его test. После этого в созданном подразделе нужно создать следующие параметры:

- (По умолчанию) — будет равен {C0E13E61-0CC6-11d1-BBB6-0060978B2AE6};
- Display — допустим, будет содержать значение WORD Errors files;
- FileList — будет содержать значение ~WRL*.tmp|~$*.doc;
- Folder — можно указать список каталогов, в которых вы храните нужные DOC-файлы;
- Flags — обязательно должен быть равен 7c000000.

Результат работы можно видеть на рис. 4.30.

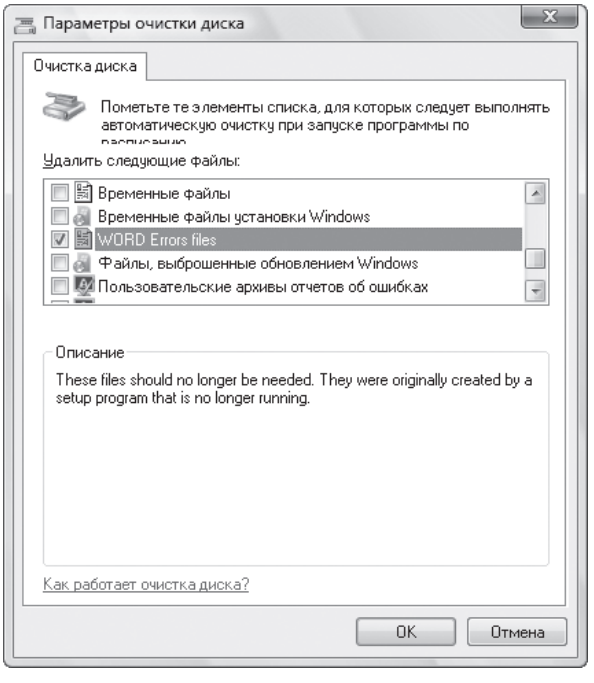


Рис. 4.30. Создание своего типа файлов, которые можно автоматически удалять с помощью программы Очистка диска

Записки — рисуем и записываем

Расположение: %systemroot%\system32\StikyNot.exe.

Вы, наверное, уже привыкли к мини-приложению боковой панели операционной системы Windows Vista, с помощью которого можно быстро делать короткие текстовые записи? Тогда предлагаю вам еще один способ создания быстрых заметок — их зарисовка с помощью мыши или запись звуковых заметок с помощью микрофона.

ПРИМЕЧАНИЕ

Запуск данной программы можно запретить с помощью параметра REG_DWORD-типа DisableStickyNotes, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\TabletPC. Для этого достаточно данному параметру присвоить значение 1.

Все это вам поможет сделать программа `StikyNot.exe` (рис. 4.31).

Пользоваться ей очень просто. Если вам нужно что-нибудь зарисовать, то достаточно навести указатель мыши на основное окно программы, нажать левую кнопку мыши и, удерживая ее, начать зарисовывать. Если же нужно записать звуковую заметку, то нужно нажать кнопку записи внизу слева от полоски длительности записи. После этого начнется запись, которую потом можно в этой же программе и прослушать.

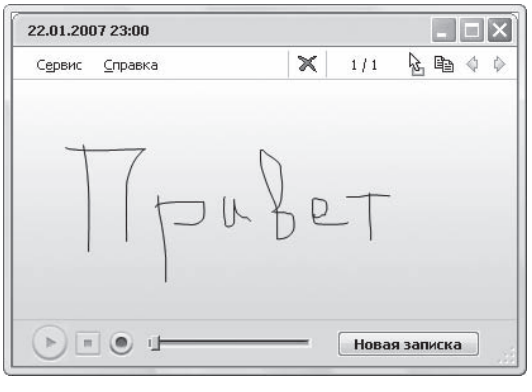


Рис. 4.31. Окно программы Записки

Чтобы создать новую заметку, достаточно нажать кнопку Новая записка. Чтобы перейти к предыдущей или следующей заметке, нужно воспользоваться навигационными стрелками, расположенными в правом верхнем углу экрана. Вы также можете удалить запись (кнопка, изображающая крестик), поместить ее в буфер обмена или копировать.

Параметров программы также не много. С их помощью можно определить, будет ли программа запускаться при входе пользователя в систему, будет ли она всегда располагаться поверх всех окон, будет ли отображаться окно подтверждения при удалении записи. Все эти параметры расположены в списке Сервис ▸ Параметры.

Журнал Windows — блокнот для пера

Расположение: `%programfiles%\Windows Journal\Journal.exe`

Еще одной программой, имеющей схожие с программой Записки возможности, является Журнал Windows. Ее можно описать как программу `notepad.exe`, в которой записи делаются не с помощью клавиатуры, а с помощью мыши или пера.

ПРИМЕЧАНИЕ

Запуск данной программы можно запретить с помощью параметра REG_DWORD-типа DisableJournal, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\TabletPC. Для этого достаточно данному параметру присвоить значение 1.

Основными возможностями данной программы является выполнение записей с помощью ручки или фломастера различных цветов, а также использование ластика для стирания записей, флажков для пометки определенных мест записи и инструмента выделения.

Факсы и сканирование Windows — работа с факсом и сканером

Расположение: `%systemroot%\system32\wfs.exe`.

Эта программа представляет собой своеобразный центр управления работой факсов и сканеров, подключенных к вашему компьютеру. Основное окно программы представлено на рис. 4.32.

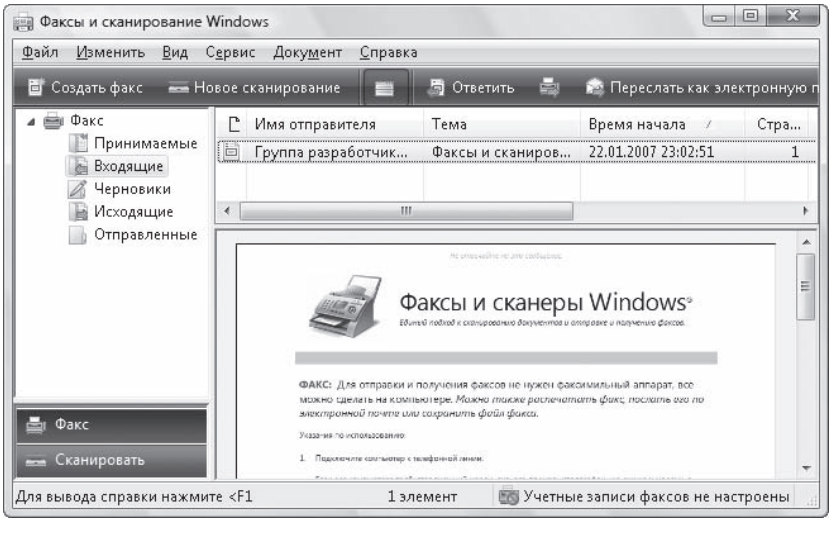


Рис. 4.32. Основное окно программы Факсы и сканирование Windows

С ее помощью вы можете выполнить такие операции, как сканирование изображения, отправка факса, а также одновременное сканирование изображения и его отправка на факс.

По умолчанию отображается страница работы с факсом. Она содержит стандартные папки Принимаемые, Входящие, Черновики и т. д., используемые при передаче документа по факсу. Чтобы отослать документ по факсу, нужно нажать кнопку Создать факс панели инструментов.

Если вы еще ни разу не пользовались возможностью передачи факса, то перед вами отобразится мастер Установка факса. С его помощью нужно указать факс, который будет использоваться при передаче (можно выбрать либо факс-модем, подключенный к компьютеру, либо собственно подключенный к компьютеру факс). После этого мастер предложит вам ввести имя факса и указать, будет ли он использоваться по умолчанию.

После настройки факса перед вами отобразится окно Создать факс, которое в чем-то похоже на окно создания электронного сообщения. В нем вы должны указать адрес получателя, тему сообщения, а также ввести само сообщение, которое будет отправлено по факсу. Также с помощью кнопок панели инструментов можно вставить в факс рисунок, расположенный на жестком диске компьютера, или отсканировать изображение, а также добавить к сообщению вложение. После того как вы создадите сообщение, необходимо будет лишь нажать кнопку Отправка, чтобы оно передалось на факс.

Если же вам нужно отсканировать документ, то следует перейти на страницу работы со сканером. Для этого достаточно нажать кнопку Сканировать, расположенную в нижнем левом углу программы.

Чтобы отсканировать изображение, достаточно нажать кнопку Новое сканирование панели инструментов страницы работы со сканером. После этого программа отобразит список всех доступных вам сканеров и предложит выбрать нужный (окно Выбор устройства). Как только вы его выберете, перед вами отобразится окно Новое сканирование. Для сканирования изображения достаточно нажать кнопку Сканировать этого окна. Кроме того, с помощью данного окна можно указать профиль сканирования, цветовой формат отсканированного изображения (цветное, черно-белое или состоящее только из черного и белого цветов), разрешение, а также яркость и контраст.

Если же вам необходимо просто отсканировать изображение, то для этого не нужно запускать программу Факсы и сканирование Windows. Достаточно воспользоваться программой `wiaacmgr.exe` (**Расположение:** `%systemroot%\system32\wiaacmgr.exe`), которая после своего вызова отобразит точно такое же окно, открывающееся при нажатии кнопки Новое сканирование программы Факсы и сканирование Windows. При этом после того как вы отсканируете изображение, откроется окно Импорт изображений и видео, которое позволяет указать тег созданного изображения.

Windows CardSpace — создание электронных пластиковых карт

При описании содержимого папки Панель управления мы упоминали о новой возможности операционной системы Windows Vista — создании электронных пластиковых карт, которыми впоследствии можно будет расплачиваться в электронных магазинах, поддерживающих эту функцию. Для этого предназначен значок Windows CardSpace папки Панель управления, после выбора которого отобразится одноименное окно.

Создание электронной карты

Чтобы создать новую электронную пластиковую карту, достаточно в окне программы выбрать значок Добавить карточку и нажать кнопку Добавить. После этого вы перейдете к мастеру Добавить карточку, в котором нужно выбрать одну из ссылок.

- Создание новой личной карточки — создать свою собственную электронную пластиковую карту. Эта карта не будет ничем отличаться от электронных пластиковых карт, выдаваемых посредниками (например, банком), кроме одного: она будет недействительна, ведь посредник не сможет подтвердить действительность карты.

  После того как вы выберете этот элемент, перед вами отобразится форма для заполнения данных о карте: название карты, рисунок, используемый на ней, ФИО и данные о вас (пол, возраст), ваш адрес и адрес вашего сайта, ваши телефоны (обычный, мобильный). Обязательным для заполнения является только поле названия карты.

  После того как вы заполните сведения об электронной карте и нажмете кнопку Сохранить, ее значок появится в основном окне программы (рядом со значком Добавить карточку).

- Установка внешней карточки — создать электронную пластиковую карту на основе сведений, предоставленных посредником. Созданная таким образом электронная пластиковая карта ничем не будет отличаться от обычной пластиковой карты, и вы сможете использовать ее при осуществлении покупок в интернет-магазине (если он вообще поддерживает возможность использования электронных пластиковых карт).

  После того как вы выберете этот элемент, нужно будет ввести путь к файлу с расширением CRD. Именно в файле с таким расширением хранится информация о посреднике и вашей новой электронной пластиковой карте.

Работа с электронной картой

После того как вы создадите свою электронную пластиковую карту, обратите внимание на поле Задачи окна программы. С его помощью можно выполнить основные задачи по работе с вашей пластиковой картой.

- Дублировать карточку — создать дубликат выделенной вами электронной пластиковой карты.
- Удалить карточку — удалить выделенную вами электронную пластиковую карту.
- Добавить карточку — создать новую электронную пластиковую карту.
- Архивные карточки — позволяет заархивировать все или некоторые из доступных вам электронных пластиковых карт. После выбора данной команды перед вами отобразится окно, в котором можно выделить те электронные пластиковые карты, сведения о которых нужно заархивировать. После того как вы выделите нужные карты и нажмете кнопку Продолжить, перед вами отобразится следующий шаг мастера, в котором нужно указать путь к файлу, в котором будут заархивированы сведения о пластиковых картах (файл с расширением CRDS).

Последним шагом мастера будет указание пароля, который нужно будет ввести для того, чтобы сведения о пластиковых картах, заархивированных в данном файле, были восстановлены.

- Восстановить карточки — позволяет восстановить сведения о пластиковых картах, заархивированные в файле. После выбора данной команды нужно будет выбрать файл с расширением CRDS и ввести пароль к нему. Если пароль верен, то отобразится список всех электронных карт, сведения о которых заархивированы в файле, а вам будет достаточно выделить те карты, которые нужно восстановить, и нажать кнопку Восстановить.
- Настройка — после выбора данной команды перед вами отобразится окно настроек программы Windows CardSpace. Оно содержит флажок Включение приложений специальных возможностей для Windows CardSpace, с помощью которого можно определить, разрешено ли сторонним программам получать сведения о ваших электронных пластиковых картах.
- Удалить все карточки — позволяет удалить все ваши электронные пластиковые карты.

Помощник по цифровой корзине — программа для покупки продуктов Microsoft

Расположение: `%systemroot%\DigitalLocker\digitalx.exe`.

В операционной системе Windows Vista программисты позаботились о тех пользователях, которые хотели бы всегда быть в курсе новинок программного обеспечения корпорации Microsoft. Специально для них был создан мастер Помощник по цифровой корзине, с помощью которого можно получить доступ к сайту http://digitallocker.windowsmarketplace.com, торгующему программным обеспечением корпорации Microsoft.

Основное окно мастера состоит всего из трех ссылок:

- Подробности в Интернете — загружает страницу сайта, рассказывающую о том, как можно купить программное обеспечение с помощью данного мастера;
- Покупка ПО на веб-узле Windows Marketplace — загружает основную страницу сайта, на которой и выполняются покупки;
- Выполнить вход с существующей учетной записью цифровой корзины — отображает окно регистрации на сайте.

ПРИМЕЧАНИЕ

Запуск программы Помощник по цифровой корзине можно запретить, если присвоить параметру REG_DWORD-типа DoNotRunDigitalLocker, расположенному в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Digital Locker, значение 1.

Настройка системы

Расположение: `%systemroot%\system32\msconfig.exe`.

Эта программа не является нововведением операционной системы Windows Vista, однако в ней произошли некоторые изменения. Как и раньше, она содержит следующие вкладки.

- Общие — позволяет определить, будут ли при загрузке запускаться неосновные системные службы и содержимое папки Автозагрузка.
- Boot — позволяет настроить новое загрузочное меню Windows Vista. Мы уже пользовались этой вкладкой, когда настраивали загрузочное меню.
- Службы — содержит список служб, зарегистрированных в операционной системе, и позволяет отключать запуск этих служб. Сведения об отключенных службах заносятся в ветвь реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\services`.
- Автозагрузка — содержит список программ, запускаемых при входе пользователей в систему, и позволяет отключать запуск этих программ. Сведения об отключенных программах заносятся в подразделы `startupfolder` и `startupreg` ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig`.

ПРИМЕЧАНИЕ

Список всех программ, автоматический запуск которых был отключен при обновлении операционной системы, заносится в ветвь реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\DisabledRunKeys. Формат данной ветви реестра полностью аналогичен формату ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

При этом, если ветвь реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\DisabledRunKeys не пуста, то на вкладке Автозагрузка программы msconfig.exe отобразится кнопка Восстановить автозагрузку программ. С ее помощью можно выборочно восстановить автоматический запуск программ, отключенных при обновлении операционной системы.

Но, кроме них, в программе `msconfig.exe` операционной системы Windows Vista появилась еще одна вкладка: Сервис. Она содержит список элементов, позволяющих запустить те или иные программы операционной системы. Например, с ее помощью можно запустить такие программы, как `winver.exe` (отображает версию операционной системы), `msinfo32.exe` (отображает конфигурацию компонентов компьютера и программ операционной системы), `msra.exe` (окно Удаленный помощник Windows) и т. д. Но не это главное, ведь опытный пользователь все эти программы может запустить самостоятельно из строки окна Запуск программы. С помощью элементов данной вкладки можно также отключить или включить компонент операционной системы Windows Vista UAP.

Работа с возможностями речевого управления компьютером

В операционной системе Windows Vista появился модуль Speech Recognition, с помощью которого можно легко управлять компьютером. С его помощью вы можете как вводить текст в каком-нибудь текстовом редакторе, так и работать с возможностями операционной системы: выключать компьютер, открывать программы, каталоги и файлы, открывать различные окна и выполнять навигацию по ним.

Перед тем как начать пользоваться речевым управлением компьютером, необходимо убедиться, что у вас есть микрофон. После этого придется некоторое время потратить на настройку модуля Speech Recognition и знакомство с командами и возможностями данного модуля.

Для этого зайдите в Панель управления и выберите значок Speech Recognition Options. После этого отобразится список возможностей модуля Speech Recognition, среди которых можно найти следующие.

- Start Speech Recognition — запускает модуль Speech Recognition. После его запуска вверху экрана отобразится представленное на рис. 4.33 окно. Оно состоит из кнопки (элементы окна перечислены слева направо), с помощью которой можно включить или отключить режим прослушивания команд, уровня чувствительности микрофона, основного поля окна, отображающего подсказки и состояние выполнения голосовых команд, а также из кнопок сворачивания и закрытия модуля.



Рис. 4.33. Модуль Speech Recognition

  Перед тем как начать пользоваться голосовыми командами, необходимо включить режим прослушивания. Для этого нужно нажать крайнюю слева кнопку (назовем ее кнопкой микрофона) или произнести фразу Start listening. После этого кнопка микрофона окрасится в синий цвет, а в поле подсказок окна вместо слова Sleeping отобразится слово Listening. Теперь все сказанные вами фразы будут расцениваться как команды (как узнать о возможных командах, будет описано ниже). Если модуль Speech Recognition не сможет распознать сказанную вами фразу, то в поле подсказки отобразится фраза What was that?.

  Если вы хотите отключить режим прослушивания, однако не хотите окончательно закрывать окно модуля Speech Recognition, то просто произнесите фразу Stop listening. Аналогичного эффекта можно добиться, нажав кнопку микрофона. После этого она примет прежний цвет, а в поле подсказки опять отобразится слово Sleeping.

- Set-up microphone — запускает мастер Microsoft Setup Wizard, который позволяет установить и проверить работу микрофона. Первым шагом мастера является

выбор типа микрофона (микрофон от наушников, настольный и т. д.), после чего вам будет предложено произнести в микрофон фразу, а мастер отобразит уровень громкости, зафиксированный микрофоном.

- Take Speech Tutorial — запускает мастер обучения работе с модулем Speech Recognition. Нужно признать, что данный мастер довольно удобен и перед тем как начать пользоваться модулем Speech Recognition, желательно пройти все шаги данного мастера.

  Работа с мастером разбита на несколько шагов, в течение которых вам предлагается произнести в микрофон основные команды и понаблюдать за результатами их выполнения. При этом перечень шагов отображен в нижней части экрана, а под ним приведен список разделов мастера. По умолчанию работа с мастером ограничена только разделом Basics, поэтому вам самостоятельно придется переходить на другие разделы, если, конечно, вы захотите это сделать. Мастер состоит из следующих разделов:

  - Welcome — начальное окно мастера;
  - Basics — базовый курс голосового управления окном модуля Speech Recognition;
  - Dictation — курс голосового ввода текста в текстовый редактор `wordpad.exe`;
  - Commanding — основной курс, состоящий из нескольких примеров использования команд голосового управления операционной системой Windows Vista;
  - Working With Windows — содержит дополнительные уроки по работе с окнами: прокрутка, минимизация, закрытие и т. д.;
  - Conclusion — содержит дополнительные занятия по голосовому управлению операционной системой.

- Train your computer to better understand you — запускает мастер Voice Training. Он предлагает вам произнести несколько фраз, чтобы модуль Speech Recognition смог подстроиться под ваше произношение и тембр голоса.
- Print your Speech Reference Card — отображает справочную информацию по специальным командам, которые вы можете использовать при работе с модулем Speech Recognition. Все эти команды можно было встретить в уроках мастера, вызываемого при выборе значка Take Speech Tutorial.
- Advanced speech options — отображает окно Text to Speech Properties, открытое на вкладке Speech Recognition. С ее помощью можно выбрать язык, на котором будут произноситься основные команды голосового управления операционной системой, выбрать профиль или создать новый профиль (например, если компьютером управляют несколько человек, то каждый из них может иметь настроенный под свое произношение профиль). На этой вкладке вы также можете указать, будет ли модуль Speech Recognition запускаться при входе пользователя в систему и т. д.
- Text to Speech — отображает окно Text to Speech Properties, открытое на вкладке Text To Speech. С ее помощью можно настроить скорость произношения голосовых команд.

Некоторые из компонентов окна Speech Recognition можно вызвать с помощью команд `rundll32.exe`:

- `rundll32.exe "%windir%\system32\speech\speechux\SpeechUX.dll", RunWizard` — отображает мастер настройки модуля по распознаванию голосовых команд операционной системы Windows Vista;
- `rundll32.exe "%windir%\system32\speech\speechux\SpeechUX.dll", RunWizard Tutorial` — открывает мастер обучения (Speech Recognition Tutorial) модуля по распознаванию голосовых команд операционной системы Windows Vista;
- `rundll32.exe "%windir%\system32\speech\speechux\SpeechUX.dll", RunWizard UserTraining` — отображает мастер Voise Training;
- `rundll32.exe "%windir%\system32\speech\speechux\SpeechUX.dll", RunWizard MicTraining` — открывает мастер Microphone Setup Wizards;
- `rundll32.exe "%windir%\system32\speech\speechux\SpeechUX.dll", RunWizard UserEnrollment` — отображает мастер Set Up Speech Recognition.

Программа Звукозапись

Расположение: `%systemroot%\system32\SoundRecorder.exe`.

Как и предыдущие версии, Windows Vista содержит стандартную программу записи звука в файл WMA-формата. Она называется Звукозапись и имеет минимум возможностей. Точнее, с ее помощью можно только начать и закончить запись в файл — ни о каких настройках работы программы нет и речи.

ПРИМЕЧАНИЕ

Запуск данной программы можно запретить с помощью параметра REG_DWORD-типа Soundrec, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SoundRecorder. Для этого достаточно данному параметру присвоить значение 1.

Это можно сделать и с помощью групповой политики Запретить выполнение программы 'Звукозапись', расположенной в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Звукозапись. Политика описана в файле SoundRec.admx.

Если же вы хотите настроить параметры записи, то необходимо воспользоваться параметрами настройки микрофона, которые описаны в окне Звук (открывается с помощью одноименного значка папки Панель управления). Для этого нужно перейти на вкладку Запись, выбрать нужный микрофон и нажать кнопку Свойства. После этого откроется окно Свойства: Микрофон. Обратите внимание на две его вкладки:

- Уровни — позволяет увеличить уровень восприимчивости микрофона;
- Дополнительно — определяет частоту и глубину, используемую при записи данных.

Остальные программы

В этом разделе мы рассмотрим совсем маленькие программы, которые, как правило, вызывают различные окна, отображаемые с помощью папки Панель управления. Все эти программы расположены в каталоге `%systemroot%\system32`.

- `Colorcpl.exe` — отображает окно Управление цветом.
- `ComputerDefaults.exe` — открывает окно Настройка доступа программ и умолчаний.
- `Credwiz.exe` — отображает мастер Сохранение имен пользователей и паролей, с помощью которого можно сохранить пароли учетных записей пользователей в отдельном файле или восстановить их из этого файла.
- `DpiScaling.exe` — открывает окно Масштабирование.
- `FirewallControlPanel.exe` — отображает окно Брандмауэр Windows.
- `Hdwwiz.exe` — открывает мастер Установить оборудование.
- `Iscsicpl.exe` — отображает окно Свойства: Инициатор iSCSI.
- `Mblctr.exe` — открывает окно Центр мобильности Windows.

ПРИМЕЧАНИЕ

Отображение данного окна можно запретить с помощью параметра REG_DWORD-типа NoMobilityCenter, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\MobilityCenter. Для этого достаточно данному параметру присвоить значение 1.

- `Narrator.exe` — запускает программу Экранный диктор, с помощью которой можно прослушать описание тех или иных возможностей использования компонентов операционной системы. После запуска программы вам достаточно подвести указатель мыши к значку или компоненту операционной системы, чтобы прослушать его описание. Основное же окно программы Microsoft Narrator позволяет выбрать голос, которым будут произноситься команды, скорость произношения, а также громкость голоса.
- `Netplwiz.exe` — отображает окно Учетные записи пользователей.
- `NetProj.exe` — открывает мастер Подключение к сетевому проигрывателю.

ПРИМЕЧАНИЕ

Отображение данного мастера можно запретить с помощью параметра REG_DWORD-типа DisableNetworkProjector, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\NetworkProjector. Для этого достаточно данному параметру присвоить значение 1.

- `OptionalFeatures.exe` — отображает окно Компоненты Windows.
- `p2phost.exe` — открывает окно Соседние пользователи.

- `PresentationSettings.exe` — отображает окно Параметры режима презентации. Оно доступно только для пользователей ноутбуков. Кроме того, вы можете воспользоваться следующими параметрами данной программы:
  - `/stop` — завершает работу модуля презентации;
  - `/start` — запускает модуль презентации.

ПРИМЕЧАНИЕ

Отображение данного окна можно запретить с помощью параметра REG_DWORD-типа NoPresentationSettings, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\PresentationSettings. Для этого достаточно данному параметру присвоить значение 1.

- `SystemPropertiesAdvanced.exe` — отображает окно Свойства системы, открытое на вкладке Дополнительно.
- `SystemPropertiesComputerName.exe` — открывает окно Свойства системы на вкладке Имя компьютера.
- `SystemPropertiesHardware.exe` — отображает окно Свойства системы, открытое на вкладке Оборудование.
- `SystemPropertiesPerformance.exe` — открывает вкладку Визуальные эффекты окна Параметры быстродействия.
- `SystemPropertiesProtection.exe` — отображает окно Параметры быстродействия.
- `SystemPropertiesRemote.exe` — открывает окно Свойства системы на вкладке Удаленное использование.
- `Tabcal.exe` — отображает окно калибровки компонента Tablet PC операционной системы Windows Vista (Средство калибровки дигитайзера).
- `Utilman.exe` — открывает окно Центр специальных возможностей.
- `Wuapp.exe` — отображает окно Центр обновления Windows.

На этом закончим рассмотрение стандартных программ операционной системы Windows Vista.

Глава 5

Консоль управления Microsoft

- **Работа с консолью управления Microsoft**
- **Стандартные оснастки**

Консоль управления Microsoft представляет собой программный интерфейс (набор функций Win32 API), а также оболочку, в контексте которой выполняются специально созданные программы (оснастки), позволяющие настраивать тот или иной компонент операционной системы и управлять им.

Кроме оснасток, в работе с консолью управления Microsoft часто используется такое понятие, как консоль. Она представляет собой отдельное окно консоли управления Microsoft, в которое уже при запуске загружается одна или несколько оснасток операционной системы Windows. Консоли представляют собой XML-файлы специального формата, имеющие расширение MSC. Каждая консоль, кроме загружаемых оснасток, характеризуется своей версией. Например, в операционной системе Windows XP используются консоли второй версии.

В Windows Vista используется консоль управления Microsoft версии 6.0 (в Windows XP — версия 5.1), которая имеет некоторые изменения по сравнению со своей предшественницей. Основное изменение заключается в том, что новая консоль управления Microsoft создает консоли третьей версии, тогда как предыдущими операционными системами используется вторая версия (то есть консоли Windows Vista не будут работать в Windows XP). Хотя пока это только косметическое изменение. Как уже было сказано раньше, консоль представляет собой обычный XML-файл (текстовый), и если вы откроете консоль Windows Vista в Блокноте и измените ее версию (в теге `ConsoleVersion=`), то скорее всего данная консоль будет работать и в предыдущих версиях консоли управления Microsoft.

После запуска консоли управления Microsoft перед вами отобразится окно, представленное на рис. 5.1.

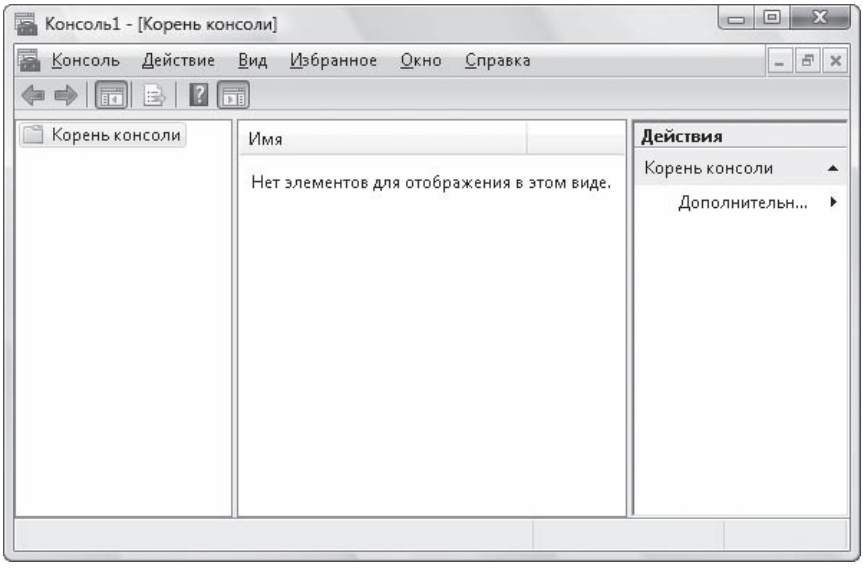


Рис. 5.1. Окно консоли управления Microsoft

Основное поверхностное отличие данной версии консоли управления Microsoft от предыдущих версий заключается в новом поле Действия, которое можно видеть на рис. 5.1. Данное поле дублирует собой назначение содержимого меню Действия.

Если же появление нового поля Действия вам много радости не доставило, то его отображение можно запретить. Однако это можно сделать только для каждой оснастки по отдельности. Например, чтобы запретить отображение поля Действия для оснастки Папка (она является единственной, которая загружается вместе со всеми консолями, а также вместе с консолью управления Microsoft), нужно присвоить параметру REG_DWORD-типа SuppressActionsPane, расположенному в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{C96401CC-0E17-11D3-885B-00C04F72C717}, значение 1. После этого консоль управления Microsoft больше не будет содержать поля Действия, но как только вы загрузите в нее новую оснастку, для которой не запрещено отображение этого поля, и перейдете в нее, поле Действия опять появится.

Если же необходимо запретить отображение поля Действия для всех оснасток консоли управления Microsoft, то достаточно снять флажок Панель действия в окне Настройка вида. Это окно отображается после выбора команды Настроить из меню Вид.

С помощью подраздела системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns можно также запретить отображение расширенного окна оснастки (отображение слева от содержимого оснасток описания выделенного в данный момент элемента). Если вы не обладаете большим монитором и не используете огромные разрешения экрана, то используемый по умолчанию расширенный вид оснасток может только мешать, занимая ненужным описанием лишнее место. В этом случае достаточно удалить подраздел {B708457E-DB61-4C55-A92F-0D4B5E9B1224} из указанной ветви реестра, чтобы консоль управления Microsoft приобрела стандартный вид, используемый в Windows 2000.

5.1. Работа с консолью управления Microsoft

Чтобы добавить оснастку к консоли управления Microsoft, нужно в меню Файл выбрать команду Добавить/Удалить оснастку (или нажать комбинацию клавиш Ctrl+M). После этого отобразится окно Добавление и удаление оснастки. По сравнению с предыдущими версиями консоли управления Microsoft, это окно очень изменилось (рис. 5.2).

Чтобы добавить оснастку к консоли управления Microsoft, нужно дважды щелкнуть кнопкой мыши на нужной оснастке, расположенной в поле Доступные оснастки. После этого может отобразиться окно настройки новой оснастки, и она появится в поле Выбранные оснастки.

Кроме добавления оснасток, с помощью данного окна можно определить расширения, содержащиеся в оснастке, которые будет разрешено использовать. Для этого

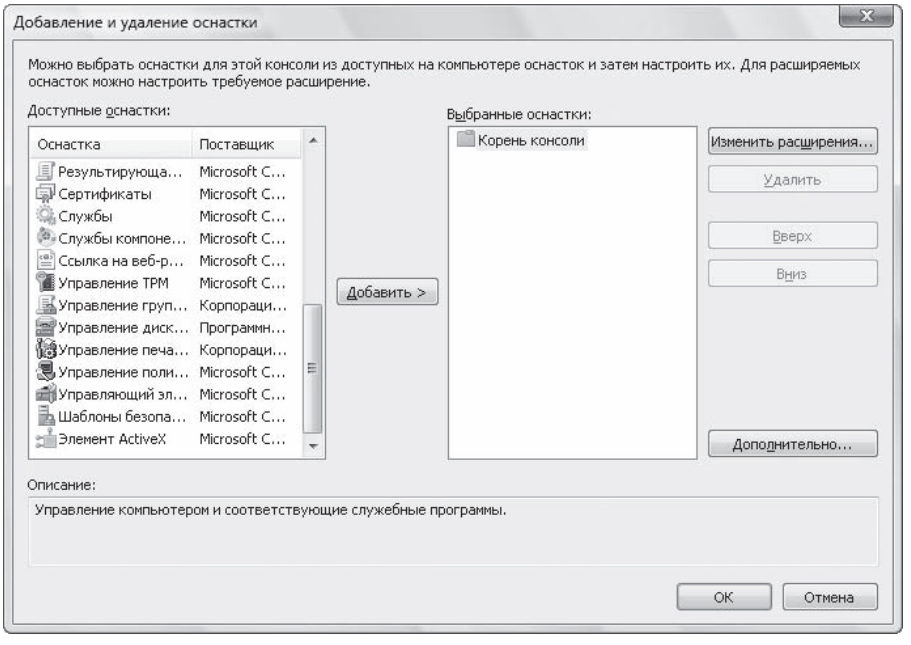


Рис. 5.2. Окно Добавление и удаление оснастки

служит кнопка Изменить расширения. В окне Добавление и удаление оснастки можно также настроить дополнительные параметры добавления оснастки, например добавление оснастки не в корень оснасток, а в выбранную в данный момент папку. Для этого применяется кнопка Дополнительно.

После того как вы выберете нужные оснастки и настроите их, нужно нажать кнопку OK, и выбранные оснастки отобразятся в консоли управления Microsoft. Когда вы закончите работу с нужными оснастками и попытаетесь закрыть консоль управления Microsoft, она спросит у вас, хотите ли вы создать новую консоль на основе загруженных в данный момент оснасток. Все пользовательские консоли сохраняются в каталоге `%userprofile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools`.

Однако не всегда можно загрузить выбранную вами оснастку. С помощью групповых политик можно запретить запуск определенных из них. Для этого применяется подраздел групповых политик Конфигурация пользователя ▸ Административные шаблоны ▸ Компоненты Windows ▸ Консоль управления (MMC) ▸ Запрещенные и разрешенные оснастки. Групповые политики данного подраздела для запрета запуска определенной оснастки создают параметр `REG_DWORD`-типа `Restrict_Run` в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\MMC\{CLSID-номер оснастки}` и присваивают ему значение `1`.

В подразделе Конфигурация пользователя ▸ Административные шаблоны ▸ Компоненты Windows ▸ Консоль управления (MMC) можно также встретить следующие группо-

вые политики, которые изменяют параметры REG_DWORD-типа ветви реестра HKEY_CURRENT_USER\Software\Policies\Microsoft\MMC:

- Запретить пользователям использовать авторский режим — установка данной политики изменяет значение параметра реестра RestrictAuthorMode, что запрещает запуск консолей в авторском режиме, а также запуск программы mmc.exe;
- Ограничить пользователей списком явно разрешенных оснасток — установка этой политики изменяет значение параметра реестра RestrictToPermittedSnapins, что запрещает запуск любых оснасток операционной системы.

Вы уже узнали, как добавить оснастку в консоль управления Microsoft. Но как же хранятся сведения об оснастках в реестре? Каждая оснастка представляет собой ActiveX-объект, настройки которого хранятся в соответствующем подразделе корневого раздела HKEY_CLASSES_ROOT. Но присутствие подраздела оснастки в данном корневом разделе еще не говорит о том, что оснастка отобразится в окне Добавление и удаление оснастки. Список всех оснасток, доступных консоли управления Microsoft, хранится в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns. Он содержит набор дочерних подразделов, названных в честь CLSID-номера оснастки. Каждый из них может хранить следующие параметры.

- About — этот параметр строкового типа указывает CLSID-номер ActiveX-объекта, который определяет окно, отображаемое после выбора команды О программе из меню Справка консоли.
- DisableWatson — имеет тип REG_DWORD и определяет, будут ли ошибки в работе данной оснастки найдены стандартной отладочной программой Windows Vista.
- NameStringIndirect — этот параметр строкового типа содержит название оснастки, отображаемое в окне Добавление и удаление оснастки. Если же данный параметр отсутствует в ветви реестра, то название оснастки определяется параметром строкового типа NameString.
- Provider — имеет строковый тип и определяет создателя этой оснастки.
- SuppressActionsPane — этот параметр REG_DWORD-типа определяет, будет ли для данной оснастки отображаться поле Действия.
- Version — параметр имеет строковый тип и определяет версию этой оснастки.

Кроме того, в разделе оснастки могут находиться два дочерних подраздела. Первый называется StandAlone. Если он присутствует в разделе оснастки, то она будет отображаться в окне Добавление и удаление оснастки. Второй же называется NodeTypes. Он определяет CLSID-номер ActiveX-объектов расширений (эти объекты описаны в соответствующих подразделах ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\NodeTypes), которые входят в состав данной оснастки. Именно список этих расширений можно отредактировать с помощью кнопки Изменить расширения окна Добавление и удаление оснастки.

5.2. Стандартные оснастки

Большинство оснасток операционной системы Windows Vista перешли из предыдущих версий данной операционной системы. Поэтому, несмотря на то что некоторые из них существенно изменились, пользователь, уже имевший дело с оснастками предыдущих версий, легко разберется в оснастках Windows Vista.

Интерфейс некоторых стандартных оснасток операционной системы изменился, однако их функциональные возможности остались на том же уровне, поэтому нельзя сказать о чем-то кардинально новом в оснастках Windows Vista. Однако пользоваться ими так же удобно и легко, как и раньше.

На страницах данной книги мы подробно рассмотрим не только новые оснастки, но и те, которые уже были в предыдущих версиях Windows и, как показала практика, работа с которыми затруднительна для рядового пользователя. Остальные же оснастки будут рассмотрены лишь поверхностно.

Работа с файлами и файловой системой

Сертификаты

CLSID-номер оснастки: `{53D6AB1D-2488-11D1-A28C-00C04FB94F17}`.

Библиотека: `certmgr.dll`.

Используется в стандартных консолях: `certmgr.msc`.

С помощью оснастки Сертификаты можно управлять следующими сертификатами: пользовательскими, удаленной или локальной службы, а также локального или удаленного компьютера.

Выбрать, какие именно сертификаты нужно загрузить, можно при добавлении оснастки Сертификаты в консоль управления Microsoft. При этом отобразится окно настройки оснастки, содержащее переключатель Эта оснастка всегда будет управлять сертификатами для, который можно установить в любое из следующих положений: моей учетной записи пользователя, учетной записи службы, учетной записи компьютера. Если вы выберете управление сертификатом службы или сертификатом компьютера, то следующим шагом мастера будет выбор компьютера, к которому нужно подключиться. Если вы выберете управление сертификатом службы, то на выборе компьютера работа мастера не закончится — после этого также нужно будет выбрать из списка конкретную службу.

Независимо от того, чьи сертификаты вы загружаете, окно оснастки Сертификаты будет содержать следующие подразделы.

- Личные — содержит персональные сертификаты. По умолчанию они есть только у пользователей и у компьютера. Персональный сертификат компьютера удостоверяет его сетевое имя. У пользователей же существует два персональных сертификата. Первый из них принадлежит шифрованной файловой систе-

ме EFS. Второй же определяет доверительные отношения в одноранговых сетях.

- Доверенные корневые центры сертификации — включает в себя сертификаты доверенных корневых центров, среди которых есть сертификаты не только известных центров сертификации Интернета, но и сертификат локального компьютера. Список таких сертификатов по умолчанию одинаков как для пользователей или служб, так и для компьютера.
- Доверительные отношения в предприятии — хранит сертификаты, определяющие доверительные отношения в предприятии. По умолчанию данный раздел пуст.
- Промежуточные центры сертификации — содержит сертификаты основных промежуточных центров сертификации. Этот раздел включает в себя два подраздела: Список отзыва сертификатов и Сертификаты. Первый из них определяет список отзыва сертификатов, а второй — сертификаты промежуточных центров. Данные списки по умолчанию одинаковы как для пользователей или служб, так и для компьютера.
- Объект пользователя Active Directory — хранит сертификаты объектов пользователя Active Directory. Если ваш компьютер не входит в домен Active Directory, то данный список будет пуст.
- Доверенные издатели — определяет список доверенных издателей, сертификаты которых будут считаться истинными.
- Сертификаты, к которым нет доверия — определяет список сертификатов, которым доверять нельзя. По умолчанию данный раздел содержит несколько сертификатов Microsoft с истекшим временем жизни.
- Сторонние корневые центры сертификации — указывает сертификаты сторонних корневых центров сертификации.
- Доверенные лица — определяет сертификаты пользователей, которым можно доверять. По умолчанию доверенным пользователем является ваша учетная запись.
- Доверенные корневые сертификаты смарт-карты — указывает доверенные сертификаты смарт-карт.

Вы также можете выполнить поиск определенного сертификата, вместо того чтобы искать его в одном из подразделов. Для этого в контекстном меню раздела оснастки Сертификаты (или ее определенного подраздела) нужно выбрать команду Поиск сертификатов. После этого отобразится окно, с помощью которого можно выполнить поиск на основе введенной строки текста. При этом поиск может вестись в имени того, кому выдан сертификат (элемент Кому выдан раскрывающегося списка Искать в поле) или кем выдан сертификат (Кем выдан), в серийном номере сертификата (Серийный номер), а также в хэше MD5 (Хэш MD5) или SHA1 (Хэш SHA1).

Если вы нашли нужный вам сертификат, то с помощью его контекстного меню можно выполнить такие задачи, как просмотр сведений о нем (кому и кем выдан, серийный номер, когда выдан и на какой срок, хэши сертификата, является

ли на данный момент действующим и т. д.), просмотр параметров работы сертификата, а также экспортирование сертификата.

Чтобы просмотреть сведения о сертификате, нужно выбрать команду Открыть.

Чтобы просмотреть параметры сертификата, нужно выбрать команду Свойства. После этого отобразится окно, представленное на рис. 5.3. С помощью вкладки Общие можно изменить название сертификата и его описание, а также выбрать те из доступных назначений сертификата, которые будут действовать на вашем компьютере. С помощью вкладки Перекрестные сертификаты можно указать дополнительные адреса, из которых будет выполняться загрузка перекрестных сертификатов.

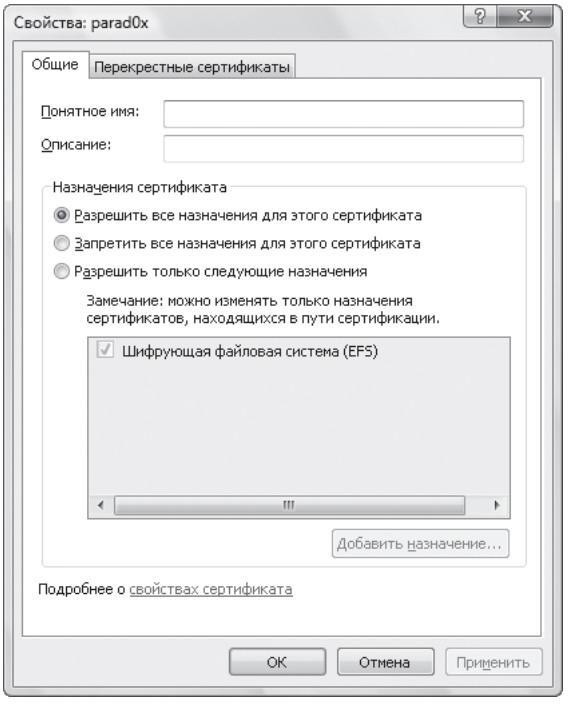


Рис. 5.3. Настройка параметров работы сертификата

Чтобы экспортировать сертификат, нужно выбрать команду Все задачи ▸ Экспорт.

Сертификат можно и импортировать. Для этого нужно в контекстном меню дочернего подраздела оснастки Сертификаты выбрать команду Все задачи ▸ Импорт.

Программа certreq.exe

Расположение: `%systemroot%\system32\certreq.exe`.

Для работы с центром сертификатов можно использовать новую программу командной строки `certreq.exe`. Описание ее возможностей можно просмотреть,

используя команду `certreq /?`. Основные же способы применения данной программы описаны ниже.

- `CertReq` — отправляет запрос к центру сертификации. После ввода данной команды отобразится окно выбора файла запроса.
- `CertReq -Submit <файл запроса>` — отправляет запрос к центру сертификации. Для просмотра дополнительных параметров данной команды введите `CertReq -Submit -?`.
- `CertReq -Retrieve <идентификатор запроса>` — возвращает ответ на предыдущий запрос к центру сертификации. Для просмотра дополнительных параметров данной команды введите `CertReq -Retrieve -?`.
- `CertReq -New` — создает новый запрос на основе INF-файла настроек запроса. Можно как указывать путь к INF-файлу в данной команде, так и не указывать. Если INF-файл указан не будет, то после ввода команды отобразится окно выбора INF-файла. Для просмотра дополнительных параметров данной команды введите `CertReq -New -?`.
- `CertReq -Accept <-machine или -user>` — устанавливает полученный сертификат PKCS #7 или X.509 в контексте данного компьютера или текущего пользователя. В данной команде можно как указывать путь к сертификату, так и не указывать. Если сертификат не указан, то после ввода команды отобразится окно выбора сертификата. Для просмотра дополнительных параметров данной команды введите `CertReq -Accept -?`.
- `CertReq -Policy` — создает взаимное свидетельство или квалифицированный запрос для существующего файла запроса. В данной команде можно как указывать путь к запросу, так и не указывать. Если путь к запросу не указан, то после ввода команды отобразится окно выбора файла запроса. Для просмотра дополнительных параметров данной команды введите `CertReq -Policy -?`.
- `CertReq -Sign` — подписывает файл запроса. В данной команде можно как указывать путь к файлу запроса, так и не указывать. Если путь к запросу не указан, то после ввода данной команды отобразится окно выбора файла запроса. Для просмотра дополнительных параметров данной команды введите `CertReq -Sign -?`.

Программа certutil.exe

Расположение: `%systemroot%\system32\certutil.exe`.

Если предыдущая программа командной строки была предназначена только для работы с центром сертификации, то эта предназначена для работы с сертификатами и службой сертификатов домена Active Directory. Она поддерживает очень большое количество возможностей и предназначена для работы в домене, поэтому на страницах данной книги параметры этой программы описаны не будут. Описание всех возможностей программы можно просмотреть, введя команду `certutil /?`.

При работе с программой может понадобиться просмотр ее файла журнала. Он расположен в каталоге %systemroot% и имеет название `certutil.log`.

Управление дисками

CLSID-номер оснастки: `{dbfca500-8c31-11d0-aa2c-00a0c92749a3}`.

Библиотека: `dmdskmgr.dll`.

Используется в стандартных консолях: `compmgmt.msc`, `diskmgmt.msc`.

С помощью данной оснастки можно добавить, удалить или отредактировать параметры разделов жесткого диска, установленного на компьютере. С ее помощью вы можете увеличивать размер тома (для динамических дисков), форматировать разделы, изменять файловую систему, изменять букву диска, изменять активный раздел (раздел, который содержит загрузочные файлы, его также называют системным).

Работа с данной оснасткой, как и ее интерфейс, совершенно не изменились. При добавлении оснастки вы можете выбрать компьютер, информацию которого она должна отображать. После этого оснастка будет добавлена.

Оснастка Управление дисками имеет одно расширение, которое можно отключить. Это расширение VSSUI.

Общие папки

CLSID-номер оснастки: `{58221C65-EA27-11CF-ADCF-00AA00A80033}`.

Библиотека: `filemgmt.dll`.

Используется в стандартных консолях: `compmgmt.msc`, `fsmgmt.msc`.

С помощью данной оснастки можно просмотреть список общих папок данного компьютера, а также список открытых по сети в данный момент файлов и список созданных сетевых сессий. Используя оснастку Общие папки, можно создавать, удалять или редактировать параметры общих папок.

Перед загрузкой оснастки ее нужно настроить. Для этого предназначен мастер. Он предложит вам указать компьютер, данные которого будут загружены в оснастку, а также те из частей оснастки, которые будут отображаться (либо только папки общего доступа, сессии или открытые файлы, либо все вместе).

Работа с оснасткой Общие папки операционной системы Windows Vista полностью аналогична работе с оснасткой предыдущих версий Windows, поэтому на страницах данной книги мы не будем рассматривать ее работу.

В операционной системе Windows Vista присутствует стандартная программа командной строки предыдущих версий Windows `openfiles.exe` (**Расположение:** `%systemroot%\system32\openfiles.exe`). С ее помощью также можно просмотреть список открытых в данный момент файлов общих каталогов. Для этого применяется команда `openfiles.exe /query`. А с помощью команды `openfiles.exe /disconnect <параметры>` можно завершить работу определенного пользова-

теля с открытым в данный момент ресурсом общего доступа. Описание ее параметров можно отобразить с помощью команды `openfiles.exe /disconnect /?`.

Кроме того, в Windows Vista данная программа стала поддерживать новый параметр — `/Local`. Если воспользоваться командой `openfiles.exe /Local on`, то программа `openfiles.exe` будет отображать не только список открытых файлов из каталогов общего доступа, но и список локальных открытых файлов. Выполнение приведенной выше команды присваивает значение `4000` параметру `REG_DWORD`-типа `GlobalFlag` ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager`.

Работа с сетью

Монитор IP-безопасности

CLSID-номер оснастки: `{57C596D0-9370-40C0-BA0D-AB491B63255D}`.

Библиотека: `ipsmsnap.dll`.

Используется в стандартных консолях: нет.

Оснастка Монитор IP-безопасности также практически не изменилась. Основным ее назначением является слежение за работой локальной политики IP-безопасности, назначаемой оснасткой Локальные параметры безопасности. Однако с помощью команды Добавить компьютер контекстного меню раздела оснастки можно выбрать удаленный компьютер, работу политик которого нужно проконтролировать.

ПРИМЕЧАНИЕ

Сведения о работе драйвера IPSec можно просмотреть с помощью счетчиков производительности объекта IPSec Driver. Благодаря ему можно узнать те же сведения, что и с помощью статистики данной оснастки.

Можно также воспользоваться счетчиками объектов Generic IKE and AuthIP, IPSec AuthIPv4, IPSec AuthIPv6, IPSec IKEv4 и IPSec IKEv6.

Оснастка не имеет расширений и каких-нибудь параметров, настраиваемых при ее загрузке в консоль управления Microsoft, поэтому после загрузки оснастки перед вами отобразится ее основное окно (рис. 5.4). Мы не будем подробно рассматривать работу данной оснастки, но кратко описать ее возможности все же стоит.

Оснастка Монитор IP-безопасности состоит из следующих разделов.

- Активная политика — это новый раздел, которого не было в оснастке для операционных систем Windows XP. Он отображает такие сведения о применяемой в данный момент политике, как ее название, описание, дата последнего изменения, хранилище политики, а также остальные сведения, используемые при работе вашего компьютера в составе домена Active Directory.

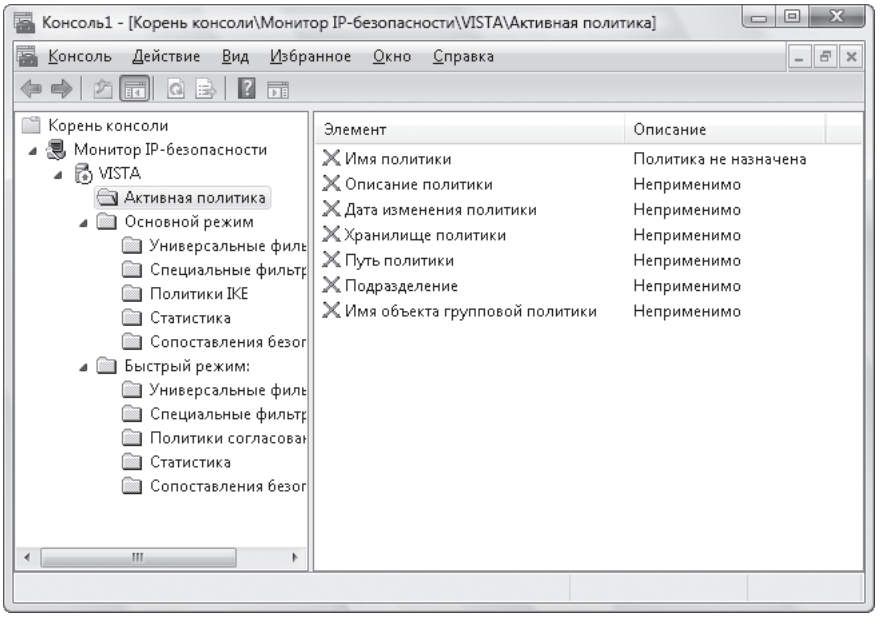


Рис. 5.4. Окно оснастки Монитор IP-безопасности

- Основной режим — определяет параметры работы протокола IPSec в основном режиме. Раздел включает в себя следующие подразделы.
  - Универсальные фильтры — отображает сведения о применяемом фильтре (о его настройках).
  - Специальные фильтры — содержит список специальных фильтров, отдельно для входящих и исходящих пакетов.

    С помощью контекстного меню данного подраздела можно выполнить поиск совпадающих фильтров. Для этого нужно воспользоваться командой Найти совпадающие фильтры.

    В отображенном после выбора команды окне можно ввести IP-адрес, порт узла источника и узла назначения, используемый протокол, а также указать, среди фильтров для каких пакетов будет выполняться поиск (входящих или исходящих) (рис. 5.5).
  - Политики IKE — содержит применяемое в данный момент действие политики IKE.
  - Статистика — определяет общую статистику, например статистику по основному и быстрому режиму, а также общее количество принятых пакетов и количество поврежденных пакетов.
  - Сопоставление безопасности — содержит список сопоставлений безопасности.
- Быстрый режим — определяет параметры работы протокола IPSec в быстром режиме. Раздел включает в себя те же подразделы, что и раздел Основной режим.

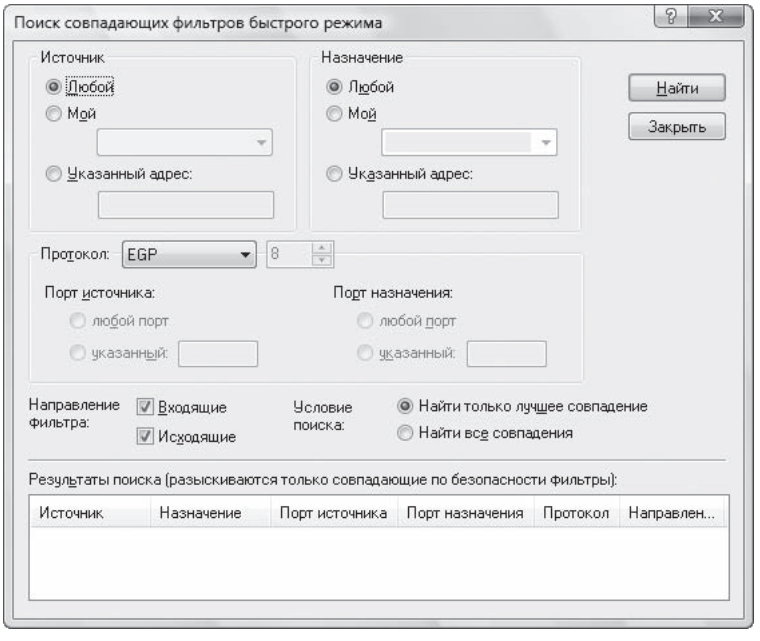


Рис. 5.5. Окно поиска совпадающих фильтров

Единственным его отличием является то, что его подраздел Статистика определяет сведения о других статистических параметрах. Например, к ним относятся следующие сведения, определяющие количество:

- активных сопоставлений безопасности (SA);
- разгруженных сопоставлений безопасности;
- незаконченных операций с ключами;
- удаленных ключей;
- повторно сгенерированных ключей;
- активных туннелей;
- поврежденных пакетов SPI;
- незашифрованных или непроверенных пакетов;
- и т. д.

Локальные параметры безопасности

CLSID-номер оснастки: `{DEA8AFA0-CC85-11d0-9CE2-0080C7221EBD}`.

Библиотека: `ipsecsnp.dll`.

Используется в стандартных консолях: `secpol.msc`.

С помощью предыдущей оснастки мы выполняли мониторинг работы политик IPSec, однако если вы не создали ни одной политики IPSec, то мониторинг ни

к чему не приведет. Как раз для создания политик IPSec и служит оснастка Локальные параметры безопасности.

При ее загрузке можно указать компьютер, политики которого будут настраиваться, после чего формирование настроек оснастки будет закончено. Оснастка не имеет расширений.

Создание политики IPSec

Если вы в первый раз запускаете данную оснастку, то ее основное окно будет пустым и вам сначала придется создать новую политику. Для этого нужно воспользоваться командой Создать политику безопасности IP контекстного меню раздела оснастки. После этого отобразится Мастер политики IP-безопасности, который предложит вам ввести название новой политики, ее описание, указать, будет ли при установлении соединения использоваться правило по умолчанию, а также способ аутентификации соединения. Возможна аутентификация с помощью протокола Kerberos (может применяться при подключении вашего компьютера к домену Active Directory), с помощью сертификата (может применяться, если в вашей сети имеется центр сертификации) или с помощью пароля. После того как вы укажете способ аутентификации, работа мастера создания политики будет завершена. Заметьте, что в последнем окне мастера установлен флажок Изменить свойства. Если вы его не снимете, то после завершения работы мастера отобразится окно свойств созданной вами политики. Конечно, его можно будет отобразить и потом, выбрав команду Свойства из контекстного меню созданной политики.

Окно свойств имеет две вкладки: Правила и Общие.

- Правила — с помощью данной вкладки можно создать правила политики или изменить параметры уже созданного правила. По умолчанию уже будет создано правило, которое разрешает соединяться со всеми компьютерами без использования туннелирования, но на основе выбранного ранее метода аутентификации. Чтобы изменить это правило, нужно нажать кнопку Изменить, после чего отобразится окно Свойства: Изменить правило, состоящее из вкладок Методы безопасности и Методы проверки подлинности. С помощью вкладки Методы безопасности можно выбрать, будет использоваться только создание контрольной суммы каждого переданного пакета или также будет выполняться шифрование каждого пакета. С помощью вкладки Методы проверки подлинности можно изменить способ аутентификации компьютера источника и компьютера назначения.

  Можно также воспользоваться кнопкой Добавить, чтобы создать новое правило. После этого запустится мастер, который предложит вам указать IPv4 и IPv6-адрес компьютера, если вы хотите организовать туннель, выбрать сеть, для которой будет применяться правило (любое сетевое соединение, соединение в пределах локальной сети или удаленное соединение), создать новые фильтры или выбрать уже созданный фильтр, создать способ взаимодействия с фильтром и выбрать способ аутентификации.

- Общие — позволяет изменить название и описание политики, а также определить интервал обновления политики и настроить такие параметры ключей PFS, как количество сессий или минут, после которого будет генерироваться новый

ключ PFS, а также алгоритм шифрования, который будет использоваться для ключа PFS.

Все политики IPSec, создаваемые с помощью данной оснастки, хранятся как подразделы с именами вида `ipsecPolicy{CLSID-номер}` ветви системного реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local`.

Создание фильтров политики

Но, кроме политики, нужно также создать один или несколько фильтров и действия при их применении. Это можно сделать как в процессе создания нового правила, как было сказано раньше, так и с помощью команды Управление списками IP-фильтра и действиями фильтра контекстного меню раздела оснастки Локальные параметры безопасности. После ее выбора отобразится одноименное окно, которое имеет две вкладки: Управление списками фильтров IP и Управление действиями фильтра.

- Управление списками фильтров IP — позволяет создать новый фильтр в списке фильтров (кнопка Добавить) или изменить параметры уже существующего (кнопка Изменить). При создании нового фильтра вам предложат указать адреса возможных компьютеров-источников и компьютеров-назначений, пакеты которых не будут отбрасываться, а также тип используемого протокола.
- Управление действиями фильтра — дает возможность создать новое действие (кнопка Добавить) или изменить параметры уже существующего (кнопка Изменить). При создании нового действия нужно указать, будут пакеты, подходящие под критерии фильтра, пропускаться, отбрасываться или для них будет отключена политика безопасности, будет ли разрешено создание небезопасного подключения, если безопасное подключение не поддерживается, будет использоваться только проверка целостности пакетов или также будет выполняться их шифрование.

Все фильтры, создаваемые с помощью данной оснастки, хранятся как подразделы с именами вида `ipsecFilter{CLSID-номер}` ветви системного реестра Windows `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local`.

Установка политики по умолчанию

После того как вы создадите политику, ее нужно установить для использования по умолчанию. Для этого в контекстном меню политики нужно выбрать команду Назначить. После этого все соответствующие политике соединения будут устанавливаться с помощью протокола IPSec, а оснастка Монитор IP-безопасности будет отображать параметры работы созданной вами политики. Если же нужно отключить политику, чтобы больше не использовались безопасные подключения, достаточно в контекстном меню политики выбрать команду Снять.

Название политики, используемой по умолчанию, хранится в параметре строкового типа `ActivePolicy` ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local`.

Конфигурация клиента NAP

CLSID-номер оснастки: {a1bc4eca-66b2-44e8-9915-be02e84438ba}.

Библиотека: napsnap.dll.

Используется в стандартных консолях: NAPCLCFG.MSC.

Данная оснастка является нововведением операционной системы Windows Vista. С ее помощью можно настроить параметры работы компонента NAP операционной системы, позволяющего блокировать сетевой доступ к вашему компьютеру другим компьютерам, не удовлетворяющим определенным вами требованиям. Учтите, что для работы механизма NAP необходимо, чтобы работала служба Агент защиты сетевого доступа.

При загрузке оснастки вам будет предложено подключиться к используемой базе данных механизма NAP локального компьютера или создать новую базу данных (или выбрать уже существующую, но не используемую по умолчанию).

Основное окно оснастки представлено на рис. 5.6.

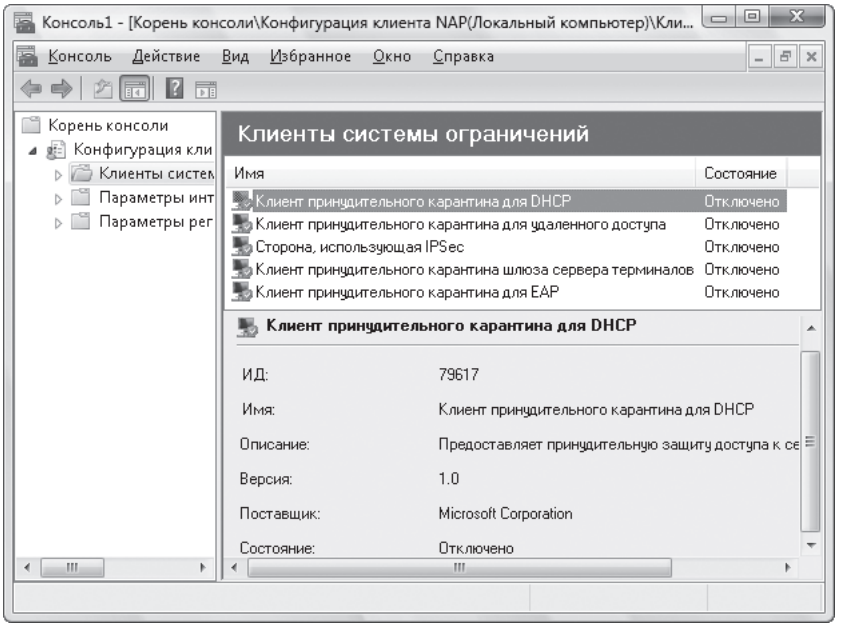


Рис. 5.6. Окно оснастки Конфигурация клиента NAP

Оснастка состоит из следующих подразделов: Клиенты системы ограничений, Параметры интерфейса пользователя, Параметры регистрации работоспособности. Далее мы рассмотрим их подробнее. Но сначала обратите внимание на команду Свойства контекстного меню раздела оснастки. С ее помощью отображается окно, в котором можно включить журналы трассировки для механизма NAP, а также указать режим трассировки: базовый, дополнительный или режим отладки.

ПРИМЕЧАНИЕ

Сведения о работе механизма NAP заносятся в журнал Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Network Access Protection.

Подраздел Клиенты системы ограничений

Данный подраздел содержит в себе набор различных клиентов, доступ к которым можно ограничить на основе указанных в подразделе Параметры регистрации работоспособности правил. По умолчанию присутствуют следующие клиенты:

- Клиент принудительного карантина для DHCP — имеет идентификатор 79617 и определяет клиентов DHCP;
- Клиент принудительного карантина для удаленного доступа — его идентификатор равен 79618, определяет клиентов удаленного доступа;
- Сторона, использующая IPSec — имеет идентификатор 79619 и определяет клиентов, работающих через протокол IPSec;
- Клиент принудительного карантина шлюза сервера терминалов — его идентификатор равен 79621, определяет клиентов шлюза терминальной службы;
- Клиент принудительного карантина для EAP — имеет идентификатор 79623 и определяет клиентов EAP.

По умолчанию на указанные выше клиенты не распространяются правила механизма NAP. Чтобы указать применения правил для одного из клиентов, нужно в его контекстном меню выбрать команду Включить.

Сведения о клиентах, которые доступны в оснастке, находятся в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\napagent\Qecs`. Каждый клиент имеет в данной ветви реестра свой подраздел, название которого соответствует идентификатору клиента. В этих подразделах находятся общие сведения о клиентах. А вот информация о том, включен клиент или нет, содержится в других подразделах — в параметре `REG_DWORD`-типа `Enabled` подразделов, названных в честь идентификатора клиента, ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\napagent\LocalConfig\Qecs`.

Подраздел Параметры интерфейса пользователя

С помощью данного подраздела можно указать изображение и имя, которое будет отображаться напротив одного из подключенных в данный момент клиентов, для которых действуют правила NAP. Для этого применяется команда Свойства контекстного меню элемента Параметры интерфейса пользователя.

Сведения, устанавливаемые с помощью данного подраздела, содержатся в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\napagent\LocalConfig\UI\1049`.

Подраздел Параметры регистрации работоспособности

Данный подраздел позволяет настроить правила, которые будут применяться для включенных с помощью подраздела Клиенты системы ограничений клиентов, а также

группу, которая сможет обходить созданные правила. Он содержит следующие дочерние подразделы: Политика запроса и Группы доверенных серверов.

Подраздел Политика запроса включает в себя следующие правила.

- Алгоритм хэширования — дает возможность указать алгоритм, который должен использоваться при создании хэша. По умолчанию используется алгоритм sha1RSA, но можно выбрать один из алгоритмов MD5, MD4, MD2 и т. д.
- Поставщик службы криптографии — позволяет указать службу криптографии, которую клиент должен использовать при подключении. По умолчанию используется служба Microsoft RSA Schannel Cryptographic Provider.

С помощью подраздела Группы доверенных серверов можно указать группу компьютеров, которые могут подключаться к включенным клиентам подраздела Клиенты системы ограничений, даже если их настройки не соответствуют указанным в правилах параметрам. Для этого в контекстном меню подраздела нужно выбрать команду Создать, после чего в отобразившемся мастере следует указать название группы, а также добавить в нее IP- или URL-адреса компьютеров.

Параметры создаваемых с помощью данного подраздела групп содержатся в подразделах ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\napagent\LocalConfig\Enroll\HcsGroups\<название группы>`.

Окно Защита сетевого доступа

Расположение: `%systemroot%\system32\NAPSTAT.exe`.

Кроме оснастки Конфигурация клиента NAP, для работы с компонентом NAP операционной системы можно также использовать программу `napstat.exe`. С ее помощью можно просмотреть текущее состояние работы данного компонента, а также список сетевых подключений, которые разрешены или запрещены NAP.

После запуска программы в области уведомлений появится сообщение о том, запущен ли в данный момент компонент NAP. Если служба Агент защиты сетевого доступа в данный момент не запущена, то не будет работать и компонент NAP. Контекстное меню данного напоминания содержит две команды: Защита сетевого доступа и Папка сетевых подключений. С помощью первой можно отобразить одноименное окно, которое определяет, имеете ли вы доступ к сетевой среде. С помощью же второй команды отображается окно Сетевые подключения, содержащее список сетевых подключений и адаптеров, которые установлены на вашем компьютере.

Работа с компонентом NAP с помощью классов WMI

Если вы знакомы с инструментарием управления Windows, то получить доступ к NAP сможете и в создаваемых вами сценариях или с помощью таких стандартных программ операционной системы, как `wbemtest.exe` и `WMIC`. Для этого в операционной системе Windows Vista появилось новое пространство имен `\\root\NAP`. Оно включает в себя три класса: `NAP_Client`, `NAP_SystemHealthAgent` и `NAP_EnforcementClient`.

- NAP_Client — управляет работой службы операционной системы Агент защиты сетевого доступа. По умолчанию в репозитарии CIM существует один экземпляр данного класса, имеющий название @. Он поддерживает следующие свойства, доступные только для чтения.
  - Description — содержит описание службы Агент защиты сетевого доступа. Тип: string.
  - fixupURL — определяет URL-адрес, если клиенту запрещен доступ к компьютеру. Тип: string.
  - Name — содержит название службы Агент защиты сетевого доступа. Тип: string.
  - napEnabled — определяет, запущена ли служба Агент защиты сетевого доступа в данный момент. Тип: boolean.
  - napProtocolVersion — указывает версию протокола, используемого службой Агент защиты сетевого доступа. Тип: string.
  - probationTime — определяет время истечения испытательного срока, если клиент NAP находится на нем. Тип: string.
  - systemIsolationState — указывает состояние клиента NAP на локальном компьютере. Если данное свойство возвращает значение 1, то доступ к сети локальному компьютеру разрешен. Если свойство возвращает 2, то клиент находится на испытательном сроке. Если же свойство возвращает значение 3, то доступ к сети для данного компьютера запрещен. Тип: uint32.
- NAP_SystemHealthAgent — содержит информацию о зарегистрированных клиентах SHA. Данный класс включает в себя следующие свойства, доступные только для чтения.
  - Description — содержит описание данного клиента SHA (Security Health Agent). Тип: string.
  - fixupState — отображает состояние адресной записи клиента SHA. Возможны следующие возвращаемые состояния: «успех», «в прогрессе», «не обновлено». Тип: uint32.
  - friendlyName — определяет название клиента SHA. Тип: string.
  - id — является ключевым. Оно определяет идентификатор клиента, по которому можно получить доступ к свойствам данного экземпляра класса. Тип: uint32.
  - infoClsid — содержит CLSID-номер, который определяет интерфейс INapComponentInfo COM-сервера. Тип: string.
  - isBound — определяет, ограничен ли клиент SHA агентом NAP. Тип: boolean.
  - percentage — указывает процент выполнения приготовлений. Если значение свойства равно 101, то данное свойство не поддерживается. Тип: uint8.

- `registrationDate` — определяет дату регистрации данного клиента SHA. Тип: `string`.
- `vendorName` — указывает производителя данного клиента SHA. Тип: `string`.
- `Version` — определяет версию данного клиента SHA. Тип: `string`.

- `NAP_EnforcementClient` — содержит информацию о зарегистрированных клиентах, доступ к которым можно ограничить (EC). Именно экземпляры этого класса отображаются в подразделе Клиенты системы ограничений оснастки Конфигурация клинета NAP. Данный класс включает в себя следующие свойства, доступные только для чтения.
  - `Description` — содержит описание данного клиента EC. Тип: `string`.
  - `friendlyName` — определяет название клиента EC. Тип: `string`.
  - `id` — является ключевым. Оно определяет идентификатор клиента EC, по которому можно получить доступ к свойствам данного экземпляра класса. Тип: `uint32`.
  - `infoClsid` — содержит CLSID-номер, который определяет интерфейс INapComponentInfo COM-сервера. Тип: `string`.
  - `isBound` — определяет, ограничен ли клиент EC агентом NAP. Тип: `boolean`.
  - `registrationDate` — указывает дату регистрации данного клиента EC. Тип: `string`.
  - `vendorName` — определяет производителя данного клиента EC. Тип: `string`.
  - `Version` — указывает версию данного клиента EC. Тип: `string`.

Безопасность

Диспетчер авторизации

CLSID-номер оснастки: `{1F5EEC01-1214-4D94-80C5-4BDCD2014DDD}`.

Библиотека: `azroleui.dll`.

Используется в стандартных консолях: `azman.msc`.

Данная оснастка представляет собой нововведение операционной системы Windows Vista. С ее помощью можно управлять хранилищем авторизации, которое включает в себя данные менеджера авторизации, необходимые для работы некоторых программ.

Оснастка Диспетчер авторизации может работать только на локальном компьютере, и после ее первого запуска вам предложат создать хранилище авторизации. Если вы этого не сделаете, то при следующем запуске оснастки она сообщит вам о том, что хранилище авторизации не обнаружено. В этом случае нужно в меню Действие консоли выбрать команду Параметры. После этого перед вами отобразится окно, в котором можно выбрать режим работы с хранилищем авторизации. По умолчанию используется режим администратора, в котором можно только управлять го-

товым хранилищем авторизации. Если же нужно создать новое хранилище авторизации, то требуется перейти в режим разработчика (установить переключатель окна в положение Режим разработчика). После этого в меню Действие появится новая команда — Новое хранилище авторизации, с помощью которой можно создать новое хранилище авторизации.

Окно, вызываемое командой Новое хранилище авторизации (рис. 5.7), позволяет выбрать путь к хранилищу авторизации, его описание, а также формат файла, в котором хранилище будет содержаться. Возможны следующие форматы файла.

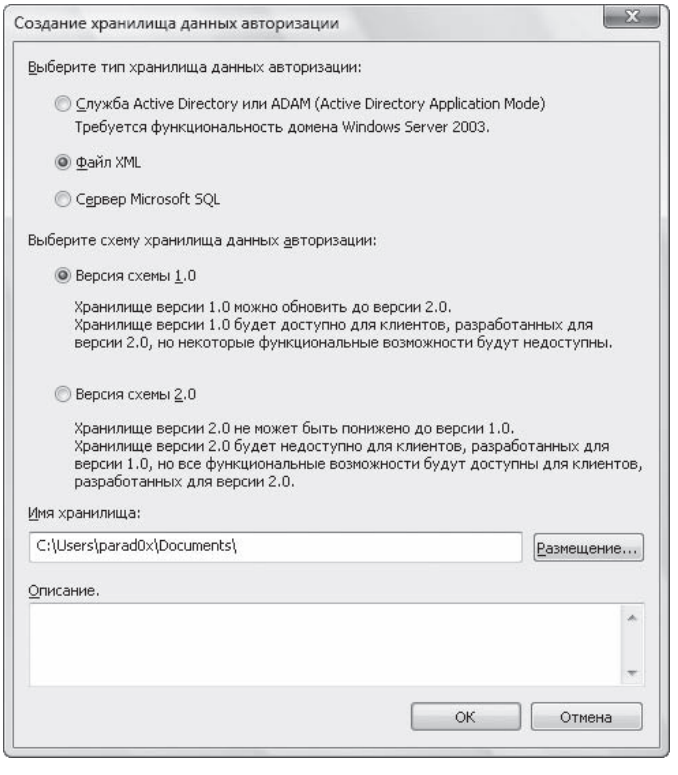


Рис. 5.7. Окно создания хранилища авторизации

- Служба Active Directory или ADAM (Active Directory Application Mode) — позволяет содержать хранилище авторизации на контроллере домена Active Directory. В этом случае указывать путь к хранилищу авторизации не нужно.
- Файл XML — позволяет содержать хранилище авторизации в XML-файле. Это наиболее медленный и небезопасный способ хранения, но для его использования не требуется ни разворачивания домена Active Directory, ни установки базы данных Microsoft SQL. По умолчанию хранилище авторизации будет содержаться в папке Документы профиля пользователя.
- Сервер Microsoft SQL — позволяет содержать хранилище авторизации в базе данных SQL. В этом случае нужно указать путь к серверу SQL.

Можно также выбрать версию схемы для создаваемого хранилища авторизации. Вторая версия более функциональна, чем первая, но к ней не смогут получить доступ клиенты, использующие первую версию схемы.

После того как вы создадите хранилище авторизации, оно автоматически будет загружено в оснастку Диспетчер авторизации. Созданное вами хранилище пока что является пустым, и для его использования нужно создать набор групп пользователей, к которым будут применяться настройки этого хранилища. Но сначала рассмотрим параметры настройки самого хранилища авторизации. Для их отображения нужно выбрать команду Свойства из контекстного меню созданного вами хранилища авторизации (то есть из контекстного меню раздела Корень консоли ▸ Диспетчер авторизации ▸ «название вашего хранилища авторизации» консоли управления Microsoft). После этого перед вами отобразится окно, представленное на рис. 5.8.

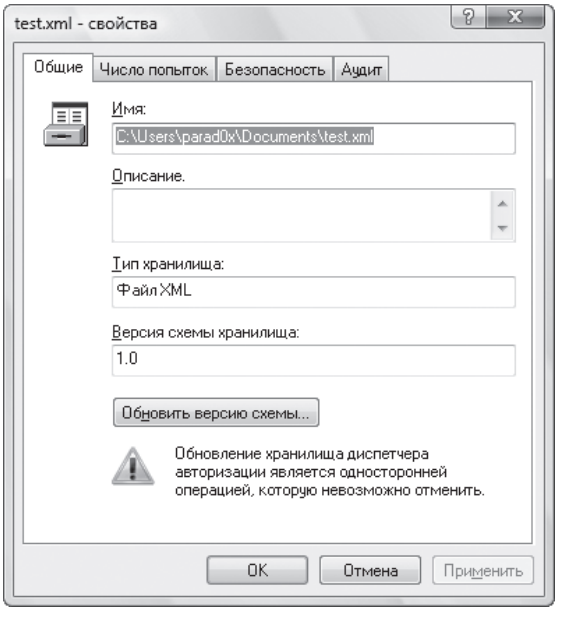


Рис. 5.8. Свойства хранилища авторизации

Оно содержит следующие вкладки.

- Общие — позволяет изменить путь к хранилищу авторизации, его название и описание.
- Число попыток — дает возможность настроить таймаут ожидания ответа от запросов LDAP, применения правил хранилища авторизации, а также максимальное количество кэшируемых правил хранилища авторизации.
- Безопасность — позволяет определить права доступа к хранилищу авторизации определенных учетных записей пользователей. Пользователи могут обладать либо правами администратора, либо только правами на чтение.

- Аудит — дает возможность определить, будет ли производиться аудит изменений в хранилище авторизации, а также аудит работы приложений.

Создание групп пользователей

После этого в контекстном меню раздела Группы хранилища авторизации нужно выбрать команду Новая группа приложения. Это приведет к отображению окна Создание группы пользователей приложения (рис. 5.9). С его помощью можно указать имя группы, ее описание, а также тип. В зависимости от типа группы изменяется способ добавления учетных записей пользователей к ней. Существуют следующие типы групп.

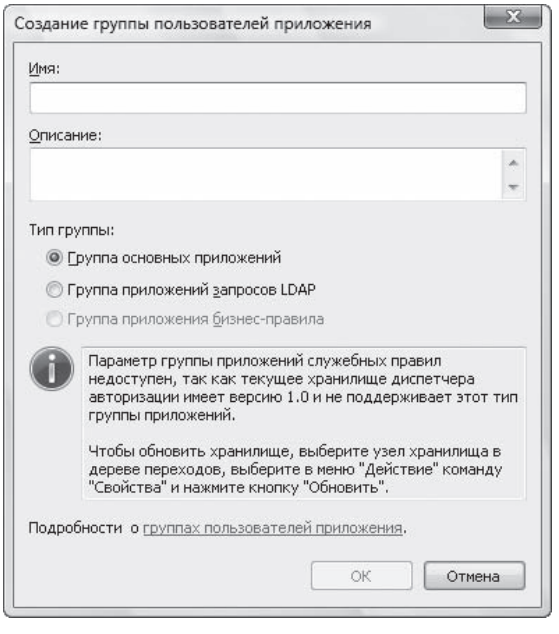


Рис. 5.9. Окно создания группы

- Группа приложений бизнес-правила — пользователи добавляются в группу на основе сценария, создаваемого непосредственно в окне свойств группы, или сценария, хранящегося в одной из папок файловой системы компьютера. Сценарий можно создавать как на языке Jscript, так и на VBScript.
- Группа приложений запросов LDAP — пользователи добавляются в группу на основе создаваемого на вкладке Запрос окна свойств группы, запроса к каталогу Active Directory.
- Группа основных приложений — стандартная группа, пользователи которой могут добавляться как с помощью других групп хранилища авторизации, так и с помощью стандартного выбора учетной записи пользователя, имеющейся на этом компьютере или компьютере контроллера домена. Окно свойств данной группы содержит вкладки Члены группы и Исключения. С помощью первой вкладки можно указать пользователей, входящих в группу, а с помощью второй вкладки — пользователей, не входящих в группу. Обе вкладки содержат

раскрывающийся список Выбрать дополнительных участников из, с помощью которого можно выбрать либо добавление пользователей на основе уже существующих в хранилище авторизации групп (Диспетчер авторизации), либо добавление учетной записи локального пользователя операционной системы (Windows и Active Directory).

После того как будет создана группа нужного вам типа, в нее нужно добавить пользователей. Независимо от типа группы это делается с помощью команды Свойства контекстного меню созданной группы.

Создание авторизированных приложений

Для создания нового авторизированного приложения нужно войти в хранилище авторизации в режиме разработчика (не забывайте, что по умолчанию выполняется вход в режиме администратора). После этого в контекстном меню хранилища авторизации появится команда Новое приложение, выбор которой приведет к отображению одноименного окна, с помощью которого можно указать название нового приложения.

После создания нового приложения в разделе хранилища авторизации будет создан подраздел, названный в честь указанного вами имени приложения. В этом подразделе будут присутствовать три дочерних подраздела: Группы, Определения и Назначения ролей (рис. 5.10). Работа с подразделом Группы ничем не отличается от работы с одноименным подразделом хранилища авторизаций.

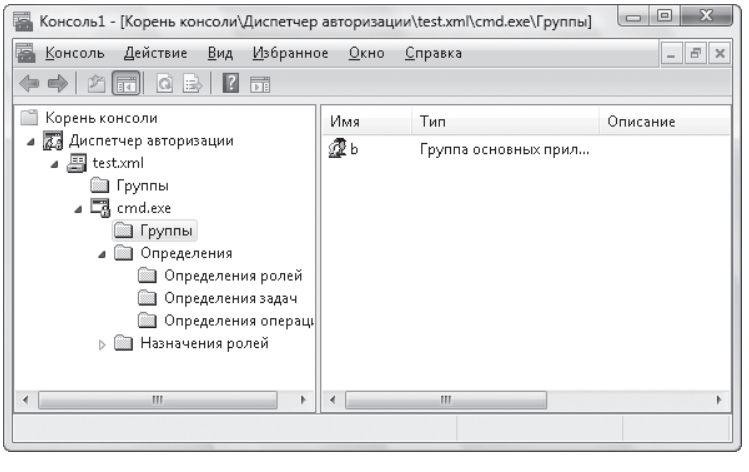


Рис. 5.10. Окно консоли azman.msc с загруженным хранилищем

Просмотр событий

CLSID-номер оснастки: `{b05566ad-fe9c-4363-be05-7a4cbb7cb510}`.

Библиотека: `EventViewer.dll`.

Используется в стандартных консолях: `comexp.msc` (расположена в каталоге `%systemroot%\system32\com`), `compmgmt.msc`, `eventvwr.msc`. Эту оснастку

можно запустить и с помощью программы `eventvwr.exe`. Особенностью такого запуска является возможность использования параметров данной программы, с помощью которых можно указать удаленный компьютер, фильтр и т. д. Более подробно о параметрах этой программы можно узнать, если вызвать команду `eventvwr.exe /?`.

При запуске данной оснастки нужно указать компьютер, информация которого будет загружена в оснастку. Оснастка Просмотр событий не является нововведением операционной системы Windows Vista. Как и раньше, она позволяет получить доступ к системным журналам, содержащим сведения о работе компонентов операционной системы и сторонних программ. Однако интерфейс оснастки Просмотр событий существенно изменился.

После загрузки оснастки перед вами отобразится окно, представленное на рис. 5.11.

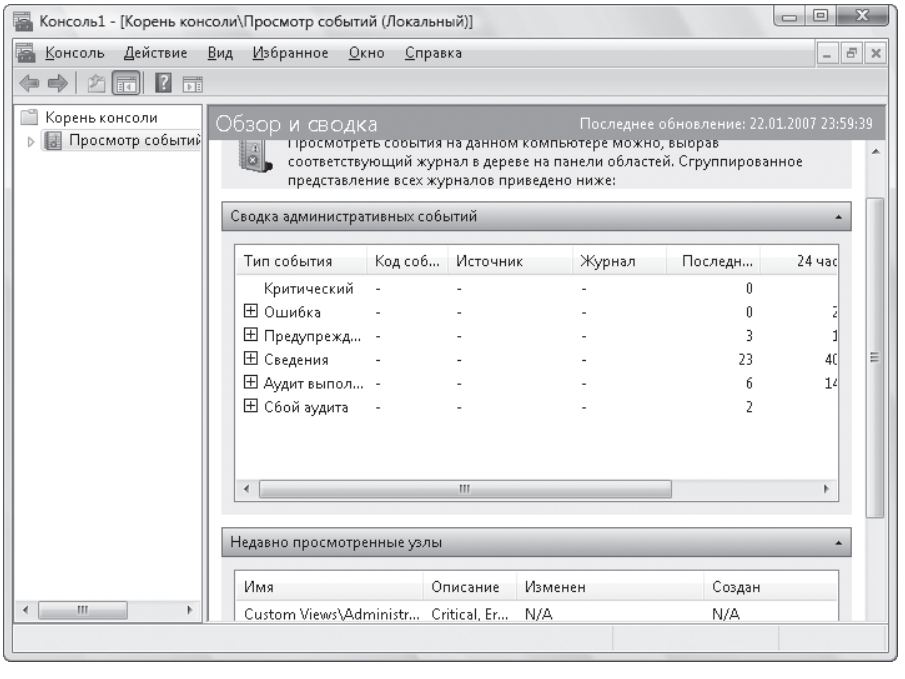


Рис. 5.11. Окно оснастки Просмотр событий

Оснастка Просмотр событий состоит из четырех разделов: Настраиваемые представления, Журналы Windows, Журналы приложений и служб и Подписки. Но перед тем как описывать эти разделы, стоит сказать несколько слов и об основном окне оснастки.

Основное окно оснастки

Основное окно отображается при выделении раздела Просмотр событий оснастки. Часть этого окна представлена на рис. 5.11. Оно содержит набор полей, отображающих статистику возникновения ошибок, а также позволяющих быстро получить доступ к последним возникшим ошибкам.

Основное окно оснастки состоит из следующих полей.

- Сводка административных событий — хранит статистику возникновения записей определенного типа: Критический, Ошибка, Предупреждение, Сведения и Аудит выполнен успешно. При этом определяется как общее количество записей определенного типа, содержащихся в журнале, так и количество ошибок, произошедших за последний час, день и неделю. Кроме того, если вы раскроете список определенного типа записей, то сможете просмотреть названия служб и программ, которые сгенерировали записи (а также название журнала, в котором находится запись, и идентификатор события). С помощью данного списка вы также сможете просмотреть количество таких записей (отображается и количество записей от конкретной службы, полученных за последний час, день, неделю, и общее количество записей, созданных данной службой или программой).

  Если вы дважды щелкнете кнопкой мыши на названии службы или программы, сгенерировавшей определенные записи, то перейдете в раздел оснастки Настраиваемые представления, в котором автоматически будет создан подраздел, содержащий информацию обо всех записях, сгенерированных данной службой. Соответственно, вы сможете просмотреть как общие сведения о записях, созданных службой, так и описание этих записей.

  Можно также получить список всех записей определенного типа. Для этого нужно в контекстном меню типа записи поля Сводка административных событий выбрать команду Просмотр всех экземпляров этого события. После этого вы также перейдете в раздел оснастки Настраиваемые представления. В нем будет автоматически создан подраздел, содержащий список всех записей выбранного вами типа.

- Недавно просмотренные узлы — содержит список журналов, а также подразделов раздела оснастки Настраиваемые представления, которые в последнее время были изменены или созданы. Соответственно, для каждого элемента списка данного поля присутствует дата изменения и создания.

  Кроме того, с помощью команды Просмотр событий в настраиваемом представлении или журнале контекстного меню элемента списка данного поля можно быстро перейти в соответствующий журнал или подраздел раздела Настраиваемые представления оснастки.

- Сводка журнала — хранит сведения обо всех журналах, отображаемых в оснастке Просмотр событий. Среди предоставляемых данным полем сведений имеется путь к журналу, его текущий размер, дата последнего изменения, разрешено ли заносить записи в журнал, а также тип очистки журнала (будет ли он перезаписываться при преодолении определенного размера, будет ли выполняться архивная копия).

  С помощью команды Просмотр событий в журнале контекстного меню определенного журнала, отображаемого в поле Сводка журнала, можно также быстро перейти в раздел соответствующего журнала.

Раздел Настраиваемые представления

Раздел Настраиваемые представления предназначен для хранения фильтров, на основе которых генерируется список определенных записей. Фильтры хранятся в виде подразделов данного раздела, и с помощью поля Сводка административных событий основного окна оснастки мы уже создавали такие фильтры.

Однако определенный фильтр можно создать и вручную. Для этого в контекстном меню раздела Настраиваемые представления нужно выбрать команду Создать настраиваемое представление. После этого отобразится окно, представленное на рис. 5.12.

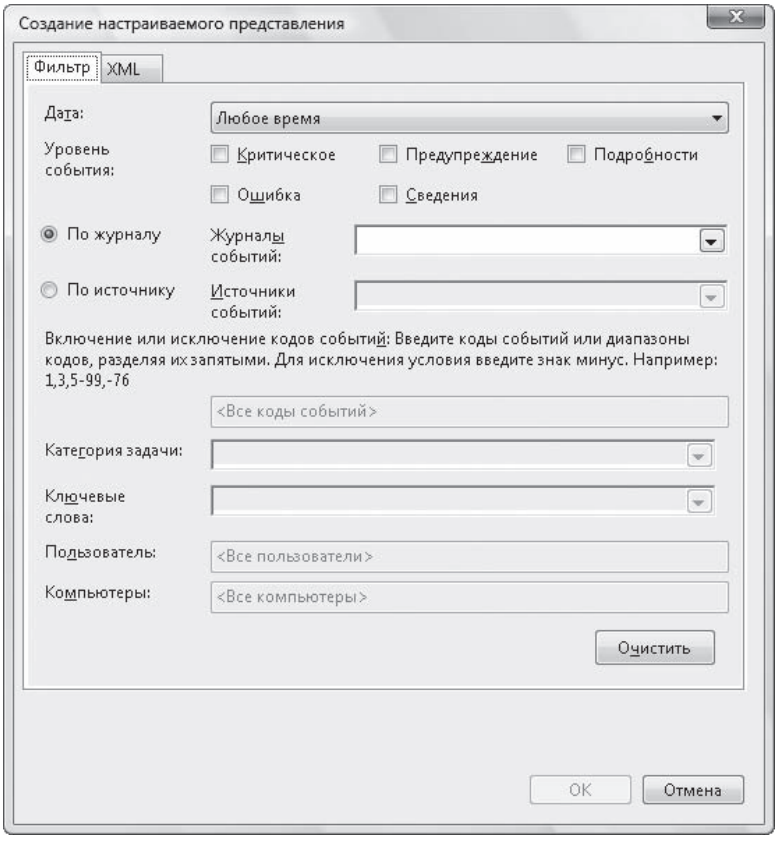


Рис. 5.12. Окно создания пользовательского фильтра

Основная работа по настройке фильтра выполняется на вкладке Фильтр данного окна. Она содержит следующие элементы.

- Дата — этот раскрывающийся список позволяет указать определенные дни. Записи, созданные в эти дни, должны быть отображены в результате применения создаваемого фильтра. Список позволяет как указать отображение записей, созданных за последний час, день и т. д., так и более точно настроить дни

с помощью элемента списка Настраиваемый диапазон, после выбора которого отобразится окно, где можно указать начальный и конечный день и час.

- Уровень события — содержит набор флажков, определяющих типы записей, которые должны быть отображены после применения фильтра.
- Журналы событий — этот раскрывающийся список позволяет определить журналы, в которых будет выполнен поиск записей. После раскрытия списка перед вами отобразится дерево журналов оснастки Просмотр событий. Напротив каждого журнала этого дерева расположен снятый флажок. Чтобы включить поиск в нужных журналах, необходимо установить флажки напротив них.
- Источники событий — позволяет определить службу, программу или компонент операционной системы, чьи записи должны быть отображены после применения фильтра.
- Включение или исключение кодов событий — это текстовое поле позволяет указать идентификаторы событий, записи которых должны быть отображены после применения фильтра, или, наоборот, не должны быть отображены. Идентификаторы событий пишутся через запятую. Если нужно указать идентификатор события, записи которого не будут отображаться, перед ним надо поставить знак минус (-).
- Категория задачи — в этом текстовом поле можно указать категорию задач, которые должны отображаться после применения фильтра.
- Ключевые слова — позволяет указать ключевые слова, которые должны встречаться в записи, чтобы она осталась после применения фильтра.
- Пользователь — в этом текстовом поле можно указать пользователя, при работе которого были созданы нужные записи.
- Компьютеры — позволяет указать компьютер, на котором были созданы нужные записи.

После того как вы настроите фильтр с помощью вкладки Фильтр, можно перейти на вкладку XML, чтобы подкорректировать его. Она содержит поле, в котором отображается созданный вами запрос к системным журналам. Если вы установите флажок Изменить запрос вручную, то сможете самостоятельно изменить созданный запрос.

После того как фильтр будет окончательно создан, достаточно нажать кнопку OK, что приведет к открытию окна с просьбой ввести название нового фильтра, его описание, а также указать подраздел раздела Настраиваемые представления, в котором будет создан фильтр. После этого в разделе Настраиваемые представления появится новый подраздел с указанным вами именем, и вы автоматически перейдете в него.

Если вы уже создали свой фильтр, но хотели бы подправить некоторые его параметры, не нужно создавать новый фильтр. Достаточно в контекстном меню созданного фильтра выбрать команду Фильтр. После этого отобразится уже знакомое вам окно (представлено на рис. 5.12), в котором можно изменить параметры фильтра.

Кроме того, с помощью контекстного меню созданного фильтра можно выполнить такие действия, как поиск в результатах применения фильтра (команда Найти),

экспортирование фильтра в файл (Экспортировать настраиваемое представление), импортирование фильтра из файла (Импортировать настраиваемое представление), а также удаление фильтра (Удалить).

Раздел Журналы Windows

Этот раздел содержит список основных стандартных журналов операционной системы. Помимо стандартных для предыдущих версий операционных систем Windows журналов Приложение, Безопасность и Система, данный раздел содержит два новых журнала: Настройка и Пересланные события (они не относятся к стандартным журналам операционной системы, так как значок, отображаемый напротив них, отличается от значков стандартных журналов, отображаемых напротив журналов Приложение, Безопасность и Система). Первый из них определяет записи, созданные операционной системой Windows Vista, ее компонентами или сторонними программами в процессе их установки. Второй же определяет записи о произошедших событиях, на которые вы самостоятельно подписались.

ПРИМЕЧАНИЕ

Как и раньше, просмотреть содержимое записей в стандартных журналах операционной системы можно и с помощью репозитария CIM. Для этого достаточно воспользоваться классом Win32_NTLogEvent, принадлежащим пространству имен \\root\cimv2. Например, данный класс поддерживает следующие свойства: CategoryString (определяет категорию записи), ComputerName (определяет название компьютера, на котором была сгенерирована запись), Type (определяет тип записи, например ошибка, предупреждение, информация, аудит-успех, аудит-отказ), Logfile (ключевое свойство, определяющее стандартный журнал, в котором хранится данная запись), Message (определяет содержимое записи), RecordNumber (ключевое свойство, определяющее номер записи в журнале), SourceName (определяет создателя записи), TimeGenerated (определяет время создания записи).

Если какой-то журнал содержит слишком много записей, то к его содержимому также можно применить фильтр. Для этого в контекстном меню раздела журнала нужно выбрать команду Фильтр. После этого отобразится уже знакомое вам окно настройки фильтра, однако отличием создаваемого фильтра является то, что он применяется непосредственно к записям выбранного журнала, а не создает подраздел в разделе Настраиваемые представления. Поэтому после работы с результатами фильтра нужно будет установить фильтр по умолчанию, чтобы отображались все записи журнала.

Можно также выполнить поиск записи по части слова. Для этого применяется команда Найти контекстного меню раздела журнала. А с помощью команды Очистить журнал контекстного меню можно очистить журнал от хранящихся в нем записей.

Если же вам необходимо изменить настройки ведения определенного системного журнала, то в его контекстном меню нужно выбрать команду Свойства, после чего отобразится окно Свойства журнала. С его помощью можно изменить путь к журналу, его максимальный размер, а также действия при достижении максимального размера (очищать журнал, архивировать его или ничего не делать). Используя

окно Свойства журнала, можно также просмотреть дату создания журнала и его текущий размер.

ПРИМЕЧАНИЕ

Настройки стандартных журналов операционной системы можно просмотреть с помощью класса Win32_NTEventlogFile, принадлежащего пространству имен \\root\cimv2. Например, данный класс поддерживает следующие свойства: FileName (определяет имя журнала), FileSize (определяет размер журнала), LastModified (определяет дату последнего изменения журнала), MaxFileSize (определяет максимальный размер журнала), Name (ключевое свойство, определяющее путь к файлу журнала и его имя), NumberOfRecords (определяет количество записей в журнале), OverwriteOutDated (определяет интервал хранения записей в журнале), Sources (содержит список источников, которые могут создавать записи в данном журнале). Этот класс также поддерживает следующие методы: BackupEventlog (выполнить архивирование записей, хранящихся в журнале), ClearEventlog (очистить содержимое журнала).

Эти настройки можно изменить и с помощью групповых политик, описанных в файле EventLog.admx и расположенных в подразделах Приложение, Безопасность, Настройка и Система раздела Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Служба журнала событий. Данные политики влияют на параметры подразделов ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog.

В операционной системе Windows Vista запись сведений в стандартные журналы (а также в журналы раздела Журналы приложений и служб) основана на каналах. Каждый журнал имеет свой собственный канал, название которого отображается в поле Канал окна Свойства журнала. Например, для журнала Пересланные события канал также называется Пересланные события. Сведения о настройках каналов хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels`. Каждый канал имеет свой собственный подраздел в данной ветви реестра, название которого соответствует названию канала. Все каналы операционной системы имеют одни и те же параметры реестра, влияющие на их работу. Вот некоторые из них.

- `Enabled` — этот параметр `REG_DWORD`-типа определяет, разрешено ли заносить записи в журнал, который использует данный канал. Значение данного параметра может изменяться с помощью флажка Включить ведение журнала окна Свойства журнала. Однако с помощью данного окна это можно сделать не для всех журналов. Например, для журнала Пересланные события данный флажок изменять нельзя, хотя можно отключить канал Пересланные события непосредственно с помощью параметра `Enabled`.
- `BufferSize` — параметр имеет `REG_DWORD`-тип и определяет размер буфера, используемого каналом.
- `File` — этот параметр строкового типа определяет путь к файлу, который используется журналом, основанным на данном канале. Значение данного параметра отображается в поле Путь журнала окна Свойства журнала.
- `MinBuffers` — параметр имеет `REG_DWORD`-тип и определяет минимальное количество буферов, используемых каналом.

- MaxBuffers — этот параметр REG_DWORD-типа определяет максимальное количество буферов, используемых каналом.
- MaxSize — имеет REG_DWORD-тип и определяет максимальный размер журнала (в байтах), использующего данный канал. Значение этого параметра также можно изменить с помощью поля Макс. размер журнала (КБ) окна Свойства журнала.
- AutoBackupLogFiles — этот параметр REG_DWORD-типа определяет, будет ли автоматически архивироваться журнал, созданный на основе данного канала, перед удалением или перезаписью (когда журнал достиг максимального размера). Значение данного параметра равно 1, если переключатель При достижении максимального размера окна Свойства журнала установлен в положение Архивировать заполненный журнал, не переписывая события.
- ChannelAccess — имеет строковый тип и определяет права доступа к каналу и, соответственно, к журналу, использующему этот канал.
- Retention — этот параметр REG_DWORD-типа определяет интервал времени (в часах), по истечении которого операционная система будет очищать содержимое журнала, основанного на данном канале. Значение данного параметра равно 0, если переключатель При достижении максимального размера окна Свойства журнала установлен в положение Переписывать события при необходимости. В остальных случаях значение данного параметра равно 0xffffffff.
- Type — параметр имеет REG_DWORD-тип и определяет, будет ли отображаться журнал в оснастке eventvwr.msc. Если значение данного параметра равно 1, то журнал отображается. Если же значение данного параметра равно 2 или 3, то журнал в оснастке eventvwr.msc отображаться не будет, так как он используется для других целей. Например, таким способом скрыты журналы ADSI/Debug, Alt-Tab/Diagnostic и т. д.

Однако в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels содержатся сведения не обо всех каналах. Сведения о стандартных каналах (и стандартных журналах, которые их используют) хранятся в ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog. В операционной системе Windows Vista к стандартным каналам относятся следующие: Приложение, События оборудования, Internet Explorer, Media Center, Безопасность и Система. Каждый из этих каналов имеет одноименный подраздел в ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog. Эти подразделы могут хранить те же параметры, что и подразделы ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels. Однако подразделы Application, Security и System также могут содержать следующие дополнительные параметры.

- DisplayNameFile — этот параметр строкового типа определяет путь к библиотеке, в которой хранится название журнала. Однако вместо библиотеки в нем можно указать само название журнала.
- DisplayNameID — параметр имеет REG_DWORD-тип и определяет смещение в библиотеке, по которому хранится название журнала. Если в параметре

`DisplayNameFile` указано непосредственно название журнала, то этот параметр использовать необязательно.

- `PrimaryModule` — этот параметр строкового типа определяет название основного модуля операционной системы, который управляет работой данного стандартного журнала.
- `RestrictGuestAccess` — если значение данного параметра `REG_DWORD`-типа равно `1`, то пользователь **Гость** не сможет получить доступ к содержимому данного журнала.

Подразделы `Application`, `Security` и `System` включают в себя вложенные подразделы, определяющие службы и программы, которые могут заносить записи в соответствующий журнал. Например, вы можете удалить некоторые из вложенных подразделов, чтобы записи от программ, которые описываются подразделами, не заносились в журнал.

Для примера попробуем создать свой собственный журнал, который будет отображаться в подразделе **Журналы приложений и служб** оснастки `eventvwr.msc`. Он будет называться **Disk** и содержать сведения о проверке жесткого диска, а также о квотах. В листинге 5.1 представлен пример REG-файла, который создает соответствующий журнал. После импортирования приведенного в листинге REG-файла сведения о проверке жесткого диска и изменении квот будут заноситься сразу в два журнала — **Disk** и **Приложение**. Если же нужно, чтобы сведения не заносились в журнал **Приложение**, то подразделы `Chkdsk` и `DiskQuota` нужно удалить из ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application`.

Листинг 5.1. Создаем свой журнал

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Disk]
"DisplayNameFile"=hex(2):44,69,73,6b,00
"File"=hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,73,79,73,74,65,6d,33,32,5c,77,69,6e,65,
76,74,5c,4c,6f,67,73,5c,44,69,73,6b,2e,65,6c,66,00
"MaxSize"=dword:01400000
"PrimaryModule"="Disk"
"Retention"=dword:00000000
"RestrictGuestAccess"=dword:00000001
"AutoBackupLogFiles"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Disk\Chkdsk]
"TypesSupported"=dword:00000007
"EventMessageFile"=hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,53,79,73,74,65,6d,33,
32,5c,75,6c,69,62,2e,64,6c,6c,00

[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Disk\DiskQuota]
"EventMessageFile"=hex(2):25,53,79,73,74,65,6d,52,6f,6f,74,25,5c,53,79,73,74,65,6d,33,32,
5c,64,73,6b,71,75,6f,74,61,2e,64,6c,6c,00
"TypesSupported"="0x00000007"
```

Еще одним изменением оснастки Просмотр событий является отображение сведений о записи непосредственно в ее окне. Однако те же сведения можно отобразить в отдельном окне, дважды щелкнув кнопкой мыши на нужной записи (рис. 5.13). Отображаемое после этого окно содержит две вкладки: Общие и Подробности. Первая отображает информацию о записи и создавшей ее программе или службе, а также общее описание записи. Вторая же вкладка включает в себя расширенные сведения о записи. При этом она содержит переключатель, который можно установить в одно из следующих положений: Понятное представление и Режим XML. Установив его в первое положение, можно отобразить только сведения о записи, тогда как установка во второе положение отображает также саму структуру XML-файла, который генерирует эти сведения.

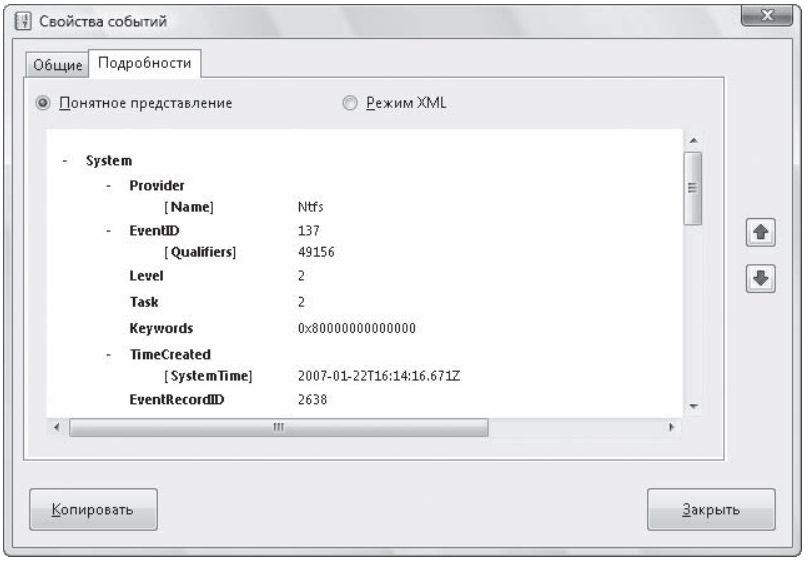


Рис. 5.13. Окно сведений о записи

Раздел Журналы приложений и служб

Данный раздел содержит записи из других журналов, которые не являются системными, но создаются стандартными программами и службами операционной системы Windows Vista. Иначе говоря, если раньше вам приходилось каждый день просматривать множество файлов журналов, расположенных в каталоге %systemroot% и его подкаталогах, то теперь содержимое всех этих файлов журналов отображается в оснастке Просмотр событий, что позволяет упростить процесс администрирования операционной системы.

Раздел Журналы приложений и служб включает в себя следующие подразделы.

- Репликация DFS — определяет события, которые произошли при работе службы Репликация DFS.
- События оборудования — указывает события, которые возникли при работе компонентов компьютера.

- Internet Explorer — определяет записи, которые получены от браузера Internet Explorer.
- Media Center — указывает записи, которые получены от оболочки Windows Media Center.
- Microsoft — по умолчанию содержит вложенный раздел Windows, в котором хранятся дочерние подразделы, названные в честь служб и компонентов операционной системы Windows Vista. Эти подразделы хранят журналы работы соответствующих служб и компонентов операционной системы. Например, обратите внимание на подраздел CodeIntegrity, журнал которого содержит сведения о неподписанных драйверах, запускаемых пользователем.

ПРИМЕЧАНИЕ

В каталоге %userprofile%\AppData\Local\Microsoft\Event Viewer находится файл Settings.xml. Он содержит настройки оснастки Просмотр событий, описанные в XML-формате. Одной из таких настроек является тег <DirectChannelsVisible>. Если между скобками установить значение 1, то в разделе Журналы приложений и служб оснастки также будут отображаться журналы, содержащие сведения об отладке и трассировке компонентов операционной системы (напротив этих журналов отображаются значки зеленого и синего цвета). По умолчанию данные журналы не отображаются.

Работа со всеми этими журналами аналогична работе со стандартными журналами операционной системы.

Раздел Подписки

С помощью данного раздела можно подписаться на события (под событием понимается создание записи от определенной службы или компонента операционной системы в системном журнале удаленного компьютера), возникающие на удаленных компьютерах. Когда событие, на которое вы подписались, произойдет, будет создана соответствующая запись в журнале Пересланные события (по умолчанию, но его можно изменить).

Чтобы подписаться на событие, нужно в контекстном меню раздела Подписки выбрать команду Создать подписку. После этого отобразится окно, представленное на рис. 5.14.

В окне расположены следующие элементы.

- Название подписки — определяет название подписки. Можете указать любое.
- Описание — указывает описание подписки.
- Журнал на конечном компьютере — этот раскрывающийся список позволяет указать журнал, в который будут помещаться записи о возникающих событиях, указанных в данной подписке. По умолчанию используется стандартный журнал Пересланные события. Однако вы можете выбрать любой другой несистемный журнал.
- Исходные компьютеры — поле содержит список компьютеров, на которых будет отслеживаться возникновение определенных событий. С помощью кнопки До-

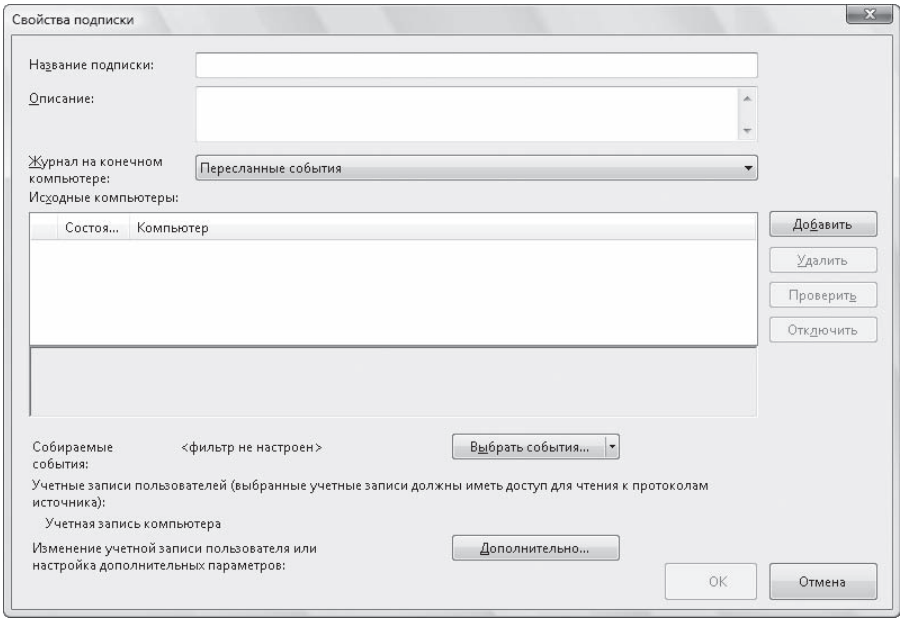


Рис. 5.14. Окно создания подписки на события

бавить можно добавить в список новый компьютер. С помощью кнопки Удалить можно удалить определенный компьютер из списка. С помощью кнопки Проверить можно послать запрос WinRM, чтобы проверить корректность работы необходимых служб.

- Выбрать события — этот раскрывающийся список позволяет создать новый фильтр либо воспользоваться уже существующим. Если вы выберете элемент Изменить данного списка, то откроется уже знакомое вам окно создания фильтра. Именно на основе данного фильтра будут определяться записи журналов удаленного компьютера, которые будут отображаться в журнале Пересланные события локального компьютера.
- Дополнительно — после нажатия данной кнопки перед вами отобразится окно Дополнительные параметры подписки. С его помощью можно изменить учетную запись, от имени которой будет выполняться подписка на события, а также порт, по которому будет установлено соединение с удаленным компьютером, и один из режимов оптимизации использования пропускной способности сети.

Существует несколько режимов оптимизации: Настраиваемая, Уменьшенная пропускная способность, Уменьшенная задержка и Обычная. Друг от друга они отличаются значениями четырех параметров реестра, которые расположены соответственно в подразделах `Custom`, `MinBandwidth`, `MinLatency` и `Normal` ветви `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\EventCollector\ConfigurationModes`. Вот эти параметры реестра.

- `DeliveryMode` — имеет строковый тип и может принимать значения `push` (используется режимами оптимизации Уменьшенная пропускная способность

и Уменьшенная задержка) или pull (используется режимами оптимизации Настраиваемая и Обычная). Он определяет способ доставки событий (кто именно инициирует процесс доставки сведений о событии).

- HeartBeatInterval — параметр имеет тип REG_DWORD и определяет интервал проверки возникновения событий. Значение данного параметра равно 3600000, 21600000, 3600000 и 900000, соответственно, для режимов оптимизации Настраиваемая, Уменьшенная пропускная способность, Уменьшенная задержка и Обычная.
- MaxItems — параметр REG_DWORD-типа. Он определяет максимальное количество событий в коллекции. Для режима оптимизации Обычная значение данного параметра равно 5, а для остальных режимов — 20.
- MaxLatencyTime — имеет тип REG_DWORD и определяет максимальное время ожидания возникновения событий. Значение данного параметра равно 900000, 21600000, 30000 и 900000, соответственно, для режимов оптимизации Настраиваемая, Уменьшенная пропускная способность, Уменьшенная задержка и Обычная.

Сведения о созданных подписках хранятся в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\EventCollector\Subscriptions. Каждая созданная подписка имеет в этой ветви свой собственный подраздел, название которого соответствует названию подписки. Каждый из этих подразделов хранит одни и те же параметры, большинство из которых изменяются с помощью окна Свойства подписки. Знание этих параметров может пригодиться при автоматическом создании подписок. Кроме того, чтобы создать подписку с помощью окна Свойства подписки, необходимо получить доступ к компьютеру-назначению по сети (если доступ к нему в данный момент отсутствует, то вы не сможете создать подписку). А при создании подписки с помощью реестра не имеет значения, доступен ли удаленный компьютер в данный момент.

- Enabled — этот параметр REG_DWORD-типа определяет, выполняется ли сбор событий на основе подписки в данный момент.
- ConfigurationMode — имеет строковый тип и определяет используемый подпиской режим оптимизации. Он может принимать следующие значения: Normal, Custom, MinBandwidth, MinLatency.
- Query — этот параметр строкового типа указывает запрос. На основе этого запроса определяются события, на которые выполнена данная подписка.
- TransportName — имеет строковый тип и определяет протокол, используемый для транспортировки событий. По умолчанию используется протокол HTTP, однако можно присвоить данному параметру значение HTTPS, чтобы использовался защищенный протокол.
- TransportPort — этот параметр строкового типа определяет порт, используемый для транспортировки событий.
- DeliveryMode, MaxItems, MaxLatencyTime, HeartBeatInterval — смотрите одноименные параметры подразделов ветви HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\EventCollector\ConfigurationModes, описанные выше.

- CommonUserName — этот параметр строкового типа определяет имя пользователя, от имени которого выполняется подключение к удаленному компьютеру.
- CredentialType — имеет строковый тип и определяет тип аутентификации пользователя на удаленном компьютере. По умолчанию используется значение Default.

Кроме того, существует несколько параметров реестра, влияющих на работу всех подписок. Они содержатся в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\EventCollector\Globals и имеют тип REG_DWORD:

- RetryInterval — определяет интервал, с которым операционная система будет пытаться получить сведения о возникшем событии, на которое есть подписка;
- RetryCount — указывает максимальное количество повторов на получение сведений о событии.

Работа со стандартными журналами Windows с помощью команды wevtutil.exe

Работать со стандартными журналами Windows можно и с помощью новой программы командой строки операционной системы Windows Vista. Чтобы просмотреть полный перечень возможностей данной команды и их описание, нужно воспользоваться командой wevtutil /?. Мы же на страницах данной книги рассмотрим только основные команды данной программы.

- Wevtutil el — отображает список стандартных журналов операционной системы локального компьютера.
- Wevtutil el /r:<компьютер> /u:<пользователь> /p:<пароль> — выводит список стандартных журналов операционной системы удаленного компьютера, используя для подключения к нему указанное имя пользователя и пароль. Можно также использовать параметр /a: для определения способа аутентификации пользователя на удаленном компьютере. Можно указать следующие значения данного параметра: Default, Negotiate, Kerberos или NTLM.
- Wevtutil gl <имя стандартного журнала> — отображает настройки стандартного журнала локального или удаленного компьютера. Эта команда выводит следующие настройки журналов: имя, включен или отключен в данный момент, тип, имя создателя, права доступа, путь к файлу, максимальный размер файла, выполняется ли его автоматическая архивация и т. д.
- Wevtutil sl <имя стандартного журнала> <изменяемый параметр журнала> — позволяет изменить параметры работы определенного журнала. Они изменяются с помощью следующих установок.
  - /e:<true или false> — позволяет включить или отключить запись в данный журнал.
  - /i:<определяет способ изоляции> — позволяет изменить способ изоляции, определяющий сессию, с которой данный журнал разделяет

работу. Например, значение данного параметра может быть равно `system` или `application`.

- `/lfn:<новое имя журнала>` — изменяет имя выбранного журнала.
- `/rt:<true или false>` — если значение данного параметра равно `false`, то новые события будут переписывать собой старые события журнала. В противном случае старый файл журнала будет сохраняться.
- `/ab:<true или false>` — позволяет включить или отключить автоматическую архивацию файла журнала. Если автоматическая архивация должна быть включена, то также должно быть включено значение параметра `/rt:`.
- `/ms:<максимальный размер>` — определяет максимальный размер файла журнала в байтах. Минимальное значение данного параметра может быть равно `1048576`.
- `/l:<уровень>` — указывает уровень фильтрации содержимого создаваемого файла журнала.
- `/k:<ключевые слова>` — определяет ключевые слова для фильтрации содержимого журнала.
- `/ca:<права доступа>` — указывает права доступа на регистрацию событий в журнале (в формате SDDL).
- `/c:<путь к файлу XML>` — определяет путь к файлу, содержащему новые настройки журнала. Синтаксис данного файла приведен в описании программы, и его можно отобразить, введя команду `wevtutil /sl /?`.

- `Wevtutil ep` — отображает список провайдеров, которые могут заносить сведения о своей работе в стандартные журналы операционной системы.
- `Wevtutil gp <имя провайдера>` — выводит основные сведения о данном провайдере. К списку основных сведений относятся: имя и CLSID-номер провайдера, путь к библиотеке провайдера, ссылка на ресурс сайта Microsoft, описывающий назначение данного провайдера, название журнала, в который провайдер записывает свои сведения, идентификатор записей и т. д.
- `Wevtutil epl <имя стандартного журнала> <путь к файлу с расширением ELF>` — экспортирует содержимое стандартного журнала локального или удаленного компьютера в ELF-файл.
- `Wevtutil cl <имя стандартного журнала>` — очищает содержимое указанного стандартного журнала.

Программа eventcreate.exe

Расположение: `%systemroot%\system32\eventcreate.exe`.

Никуда не исчезла и стандартная программа командной строки `eventcreate.exe`, с помощью которой можно создавать в стандартных журналах операционной системы свои записи. Поскольку эта программа не является чем-то новым, мы просто о ней упомянем.

Основной синтаксис этой программы следующий: `eventcreate /t <тип события> /id <идентификатор события> /l <название журнала> /d <описание>`. Здесь:

- тип события может принимать следующие стандартные значения: `ERROR`, `WARNING`, `INFORMATION` и `SUCCESS`;
- идентификатор должен быть числом от 1 до 1000;
- название журнала может принимать только следующие значения: `Application`, `System` или название любого другого журнала из раздела `Applications and Services Logs` оснастки Просмотр событий.

Управление групповой политикой

CLSID-номер оснастки: `{E12BBB5D-D59D-4E61-947A-301D25AE8C23}`.

Библиотека: `GPOAdmin.dll`.

Используется в стандартных консолях: `gpmc.msc`.

Оснастка может использоваться только на компьютерах, подключенных к домену Active Directory. В этом случае она представляет собой более функциональную оснастку, чем стандартная оснастка Редактор объектов групповой политики.

Оснастка Управление групповой политикой состоит из следующих оснасток и утилит Active Directory: Active Directory Users and Computers, Active Directory Sites and Services и Resultant Set of Policy. С ее помощью удобно управлять групповыми политиками в каждом лесе корпоративной среды. Для каждого леса отображаются следующие подразделы данной оснастки:

- Domains — содержит информацию обо всех доменах, из которых состоит данный лес;
- Sites — хранит информацию обо всех узлах, из которых состоит данный лес;
- Group Policy Modeling — позволяет выполнить моделирование групповой политики для определенного компьютера или пользователя на основе только что измененных групповых политик (которые еще не вступили в силу);
- Group Policy Results — дает возможность выполнить моделирование групповой политики для определенного компьютера или пользователя на основе уже применяющихся политик.

В контексте этой книги мы не будем подробно рассматривать данную оснастку.

Редактор объектов групповой политики

CLSID-номер оснастки: `{8FC0B734-A0E1-11D1-A7D3-0000F87571E3}`.

Библиотека: `GPEdit.dll`.

Используется в стандартных консолях: `gpedit.msc`.

Эта оснастка представляет собой основной способ редактирования групповых политик, дающих возможность дополнительной настройки операционной системы и ее компонентов с помощью специальных параметров реестра, изменять которые могут только администраторы. Соответственно, запустить данную оснастку можно только с правами администратора.

При загрузке оснастки перед вами отобразится мастер. С его помощью можно определить компьютер, параметры групповой политики которого вы будете изменять. Но это еще не все возможности изменения — если вы нажмете кнопку Обзор, то сможете изменить не только компьютер, но и пользователя, на которого будут распространяться изменяемые вами групповые политики (рис. 5.15). При этом заметьте, что можно выбирать не только конкретного пользователя, но и пользователей группы Администраторы, а также пользователей всех групп, не являющихся административными. Однако учтите, что если вы выберете пользователя, то будут загружены групповые политики, распространяемые на него, но не будут загружены групповые политики, распространяемые на весь компьютер.

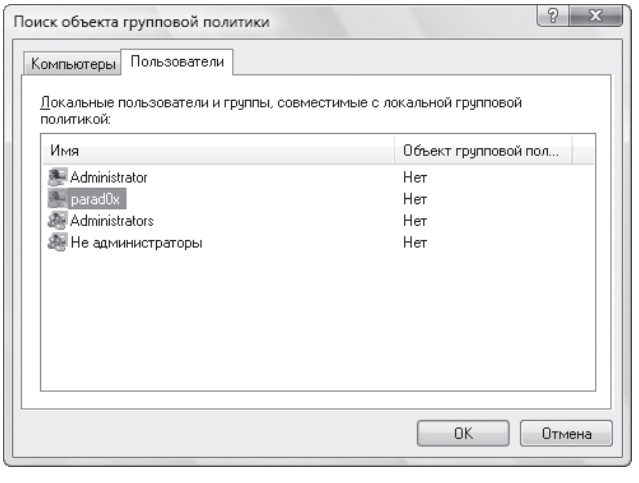


Рис. 5.15. Выбор пользователя, групповые политики которого будут загружены

Оснастка Редактор объектов групповой политики состоит из множества расширений, которые вы можете по своему желанию оставить или отключить. К ним относятся следующие расширения.

- Административные шаблоны (Компьютеры) — определяет, будет ли отображаться раздел оснастки Политика "Локальный компьютер" ▸ Конфигурация компьютера ▸ Административные шаблоны.
- Административные шаблоны (Пользователи) — указывает, будет ли отображаться раздел оснастки Политика "Локальный компьютер" ▸ Конфигурация пользователя ▸ Административные шаблоны.
- Расширенный вид — в начале этой главы рассказывалось, как с помощью реестра запрещать отображение расширенного вида консоли управления. Однако это-

го же эффекта можно достичь и с помощью редактирования расширений конкретной оснастки. Для этого достаточно запретить загрузку данного расширения.

- Редактор перенаправления папок (пользователей) — определяет, будет ли отображаться раздел оснастки Политика "Локальный компьютер" ▸ Конфигурация пользователя ▸ Конфигурация программ ▸ Перенаправление папок. Этот раздел отображается в оснастке только в том случае, если компьютер входит в домен Active Directory.
- Настройка Internet Explorer — указывает, будет ли отображаться раздел оснастки Политика "Локальный компьютер" ▸ Конфигурация пользователя ▸ Конфигурация Windows ▸ Настройка Internet Explorer.
- QoS на основе политики — оснастка Редактор объектов групповой политики загружает два таких расширения — одно для пользователя, а другое для всего компьютера. Соответственно, они определяют, будет ли отображаться подраздел Policy-based QoS в разделе Конфигурация компьютера ▸ Конфигурация Windows и в разделе Конфигурация пользователя ▸ Конфигурация Windows.
- Расширение помещенных подключений принтеров (компьютеров) — определяет, будет ли отображаться раздел оснастки Политика "Локальный компьютер" ▸ Конфигурация компьютера ▸ Конфигурация Windows ▸ Развернутые принтеры.
- Расширение помещенных подключений принтеров (пользователей) — указывает, будет ли отображаться раздел оснастки Политика "Локальный компьютер" ▸ Конфигурация пользователя ▸ Конфигурация Windows ▸ Развернутые принтеры.
- Сценарии (вход/выход из системы) — определяет, будет ли отображаться раздел оснастки Политика "Локальный компьютер" ▸ Конфигурация пользователя ▸ Конфигурация Windows ▸ Сценарии (вход/выход из системы).
- Сценарии (запуск/завершение) — указывает, будет ли отображаться раздел оснастки Политика "Локальный компьютер" ▸ Конфигурация компьютера ▸ Конфигурация Windows ▸ Сценарии (запуск/завершение).
- Параметры безопасности — запрет на загрузку данного расширения удаляет подраздел Параметры безопасности как из раздела Политика "Локальный компьютер" ▸ Конфигурация компьютера, так и из раздела Политика "Локальный компьютер" ▸ Конфигурация пользователя.
- Установка программ (компьютеры) — определяет, будет ли отображаться раздел оснастки Политика "Локальный компьютер" ▸ Конфигурация компьютера ▸ Конфигурация программ ▸ Установка программ. Он отображается в оснастке только в том случае, если компьютер входит в домен Active Directory.
- Установка программ (пользователи) — указывает, будет ли отображаться раздел оснастки Политика "Локальный компьютер" ▸ Конфигурация пользователя ▸ Конфигурация программ ▸ Установка программ. Он отображается в оснастке только в том случае, если компьютер входит в домен Active Directory.

Мы не будем рассматривать такие разделы данной оснастки, как Конфигурация программ (так как он имеет функциональное назначение только при работе в домене)

и Развернутые принтеры (так как он представляет собой отдельную оснастку Управление печатью).

Итак, оснастка Редактор объектов групповой политики состоит из следующих подразделов (рис. 5.16).

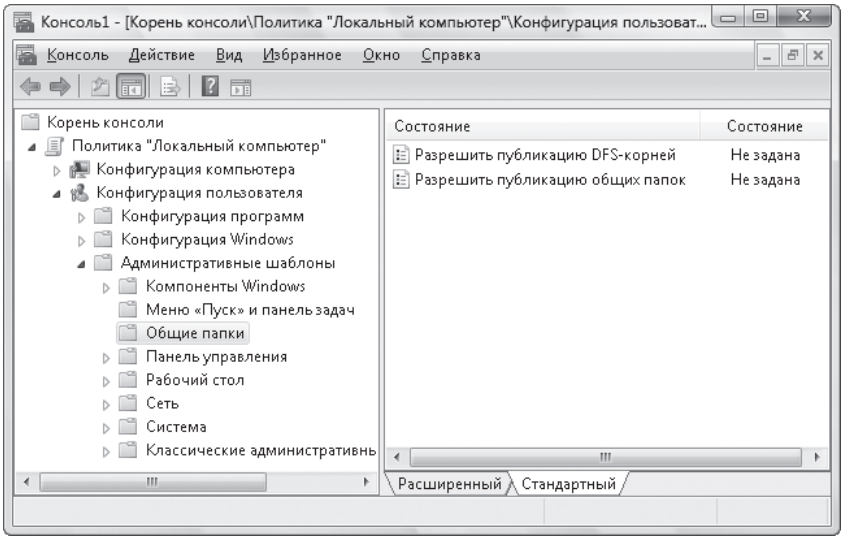


Рис. 5.16. Оснастка Редактор объектов групповой политики

- Конфигурация программ — если компьютер подключен к домену, то с помощью этого раздела можно опубликовать или назначить пользователю определенные программы, а также перенаправить содержимое стандартных папок компьютера в другие папки.
- Конфигурация Windows — определяет дополнительные настройки групповых политик, с помощью которых можно повысить безопасность работы компьютера (подраздел Параметры безопасности), определить сценарии, которые будут запускаться при входе (загрузке) или выходе (выключении) пользователя из операционной системы (подраздел Сценарии), а также изменить настройки интерфейса браузера Internet Explorer (подраздел Настройка Internet Explorer).
- Административные шаблоны — указывает административные шаблоны, являющиеся основной частью групповых политик и позволяющие ограничить возможности работы определенных пользователей или всех пользователей компьютера.

Далее мы подробнее рассмотрим эти подразделы.

Подраздел Конфигурация программ

По сравнению с предыдущими версиями операционной системы Windows, подраздел Конфигурация программ оснастки Редактор объектов групповой политики совершенно не изменился, поэтому мы рассмотрим его лишь поверхностно.

Как и раньше, он содержит разделы Политики учетных записей и Локальные политики, которые, в свою очередь, включают в себя следующие дочерние подразделы.

- Политика паролей — как и раньше, с помощью данного раздела можно настроить такие параметры создания и хранения паролей, как максимальное и минимальное количество дней хранения паролей от учетных записей пользователей, минимальная длина пароля. Можно указать, должен ли пароль обязательно, кроме символов, содержать цифры и несимвольные знаки (восклицательный, подчеркивая и т. д.), должен ли пароль храниться в базе данных SAM с использованием обратного шифрования (понижает безопасность, но может быть необходимо при взаимодействии с некоторыми устаревшими программами и операционными системами) и т. д.
- Политика блокировки учетной записи — с помощью данного раздела можно настроить такие параметры входа в систему, как количество неправильных попыток ввода пароля, после которых учетная запись будет заблокирована, указать, на какое время будет заблокирована учетная запись, а также через какое время счетчик неправильных попыток входа в систему будет сброшен.
- Политика аудита — как и раньше, данный раздел позволяет определить параметры аудита доступа к системе (сведения аудита заносятся в системный журнал Безопасность оснастки Просмотр событий). Можно выбрать следующие значения аудита: Успех (определенное событие прошло успешно) и Отказ (пользователь не имеет права совершать это событие). При этом, как и раньше, можно выполнять аудит следующих событий: вход в систему пользователя или служебных учетных записей, изменение параметров учетных записей пользователей, получение доступа к объектам (папкам, файлам и т. д.), использование административных привилегий и т. д.
- Назначение прав пользователя — позволяет указать учетные записи пользователей, которым будут даны дополнительные привилегии при работе в системе или, наоборот, некоторые стандартные привилегии которых будут запрещены. Этот раздел не является чем-то новым — он присутствовал и в предыдущих версиях операционной системы Windows.
- Параметры безопасности — раздел также не является чем-то новым. Он определяет некоторые настройки безопасности компьютера, которые должен знать и уметь изменять каждый администратор. Поэтому, если вы упустили этот момент администрирования компьютера, обязательно загляните в данный раздел, чтобы просмотреть его возможности. А на страницах книги мы рассмотрим только то содержимое данного раздела, которого не было в операционной системе Windows XP.
    - Управление учетными записями пользователей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором — эта политика позволяет определить, будет ли для администраторов компьютера отображаться окно оповещения о необходимости запуска программы с административными правами, и если будет, то что оно будет содержать: либо просто предупреждение, либо поле для ввода пароля администратора. По умолчанию требуется подтверждение.

Политика влияет на значение параметра REG_DWORD-типа ConsentPromptBehaviorAdmin ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Если его значение равно 0, то окно UAC отображаться не будет. Если его значение равно 1, то будет отображаться окно с просьбой ввода пароля. Если же его значение равно 2, то будет отображаться окно UAC с предупреждением.

- Управление учетными записями пользователей: поведение запроса на повышение прав для обычных пользователей — позволяет определить, будет ли для пользователей, не имеющих прав администратора, отображаться окно оповещения о необходимости запуска программы с административными правами, и если будет, то что оно будет содержать: либо просто предупреждение, либо поле для ввода пароля администратора. По умолчанию требуется ввод пароля.

  Политика влияет на значение параметра REG_DWORD-типа ConsentPromptBehaviorUser ветви системного реестра Windows HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Если его значение равно 0, то окно UAC отображаться не будет. Если значение равно 1, то будет отображаться окно с просьбой ввода пароля. Если же его значение равно 2, то будет отображаться окно UAC с предупреждением.

- Управление учетными записями пользователей: обнаружение установки приложений и запрос на повышение прав — указывает, будет ли UAC отображать свое окно при обнаружении попытки установки программного обеспечения, при которой необходимы административные права. По умолчанию будет отображать.

  Политика влияет на значение параметра REG_DWORD-типа EnableInstallerDetection ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

- Управление учетными записями пользователей: все администраторы работают в режиме одобрения администратором — определяет, будут ли все администраторы локального компьютера работать в режиме LUA. По умолчанию администраторы не работают в этом режиме.

ПРИМЕЧАНИЕ

Сведения о работе механизма UAC заносятся в журнал Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ UAC.

Политика влияет на значение параметра REG_DWORD-типа EnableLUA ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

- Управление учетными записями пользователей: при сбоях записи в файл или реестр виртуализация в размещение пользователя — указывает, будет ли приме-

няться механизм виртуализации каталогов и ветвей реестра, в которые пытается записать значения определенная программа, но при этом у пользователя нет доступа к этим каталогам и ветвям. По умолчанию применяется.

ПРИМЕЧАНИЕ

Сведения о работе с виртуальными папками заносятся в журнал Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ UAC-FileVirtualization.

Политика влияет на значение параметра REG_DWORD-типа EnableVirtualization ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

- Управление учетными записями пользователей: режим одобрения администратором для встроенной учетной записи администратора — определяет, будет ли работать пользователь Администратор в режиме LUA.

  Политика влияет на значение параметра REG_DWORD-типа FilterAdministratorToken ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

- Управление учетными записями пользователей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав — указывает, будет ли запрещен доступ ко всем открытым окнам и Рабочему столу при отображении окна UAC. По умолчанию доступ запрещен.

  Политика влияет на значение параметра REG_DWORD-типа PromptOnSecureDesktop ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

- Управление учетными записями пользователей: повышение прав только для подписанных и проверенных исполняемых файлов — определяет, будет ли разрешено запускать с административными правами программы, не имеющие достоверной подписи. По умолчанию разрешено.

  Политика влияет на значение параметра REG_DWORD-типа ValidateAdminCodeSignatures ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

- Системная криптография: обязательное применение сильной защиты ключей пользователей, хранящихся на компьютере — позволяет определить, будет ли применяться усиленная защита хранилища пользовательских ключей.

  Политика влияет на значение параметра REG_DWORD-типа ForceKeyProtection ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Cryptography. Если значение данного параметра равно 0, то добавление нового пользовательского ключа в хранилище не требует подтверждения. Если значение равно 1, то добавление нового пользовательского ключа в хранилище требует подтверждения. Если же значение равно 2, то добавление нового пользовательского ключа в хранилище требует ввода пароля.

- Параметры системы: использовать правила сертификатов для исполняемых файлов Windows для политик ограниченного использования программ — позволяет указать, будет ли разрешено изменять параметры запуска файлов на данном компьютере на основе сертификатов файлов (по умолчанию запускаются все файлы, но можно разрешить запуск только сертифицированных файлов или файлов из определенного каталога).

  Политика влияет на значение параметра `REG_DWORD`-типа `AuthenticodeEnabled` ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers`.

- Параметры системы: необязательные подсистемы — с помощью этой политики можно изменить значение параметра `optional`. Он содержит список подсистем операционной системы Windows Vista, которые автоматически будут загружаться в память компьютера процессом `winlogon.exe` при входе пользователей в систему. Естественно, что все ненужные подсистемы лучше удалить, чтобы их поддержка не понижала скорость работы операционной системы.

  Политика влияет на значение параметра `REG_MULTI_SZ`-типа `optional` ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems`. По умолчанию значение параметра равно `POSIX`.

- Сетевой доступ: запретить анонимный доступ к именованным каналам и общим ресурсам — позволяет запретить анонимный доступ к нулевым каналам и ресурсам общего доступа. Это повышает безопасность компьютера, но при этом некоторые службы предыдущих версий операционной системы Windows не смогут получить сетевой доступ к операционной системе. По умолчанию доступ запрещен.

  Политика влияет на значение параметра `REG_DWORD`-типа `RestrictNullSessAccess` ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters`.

Кроме того, раздел Параметры безопасности содержит и такие стандартные подразделы, как Политики открытого ключа и Политики ограниченного использования программ.

С помощью подраздела Политики открытого ключа можно опубликовать сертификаты определенного типа, не используя рассмотренную нами ранее оснастку Сертификаты. Типы сертификатов, которые можно опубликовать, аналогичны типам сертификатов, отображаемых в оснастке Сертификаты, и были рассмотрены ранее. Кроме того, обратите внимание на вложенный подраздел Файловая система EFS. Именно с помощью команды Добавить агент восстановления данных контекстного меню данного подраздела можно добавить агент восстановления (на основе сертификата пользователя).

С помощью подраздела Политики ограниченного использования программ, как и раньше, определяются правила, на основе которых система будет решать, можно пользователю запустить определенный файл или нет. Если вы решили создать такие

правила, то сначала в контекстном меню данного подраздела выберите команду Создать политику ограниченного использования программ, после чего в подразделе Политики ограниченного использования программ будут созданы два дочерних подраздела: Уровни безопасности и Дополнительные правила.

Как и раньше, ограничивать доступ к файлам и каталогам можно на основе четырех правил.

- Создать правило для сертификата — позволяет ограничить доступ к сценарию или пакету установщика Windows (расширение MSI) на основе сертификатов, которые были им выданы. Если сценарий или пакет установщика Windows не имеют указанного в правиле сертификата, то их использование будет запрещено. Это правило является наиболее защищенным, хотя и доступно только для сценариев и MSI-файлов.
- Создать правило для хэша — дает возможность ограничить доступ к файлам на основе хэша, которым они подписаны. Правило создается для определенного файла, при этом также создается хэш файла. Если кто-то попытается модифицировать файл, для которого определен хэш с помощью правила, то такой файл больше не будет разрешено запускать, так как его хэш не будет совпадать с тем, который определен правилом.

  Если же создается правило на основе хэша, которое будет запрещать запуск определенного файла, то пользователь сможет его довольно легко обойти — достаточно будет изменить содержимое файла, чтобы изменился и его хэш.
- Создать правило для зоны сети — позволяет ограничить доступ к файлам установщика Windows на основе зоны Интернета, из которой был получен данный файл.
- Создать правило для пути — дает возможность ограничить доступ к файлам на основе каталога, в котором они расположены.

Чтобы создать одно из описанных выше правил, нужно воспользоваться контекстным меню подраздела Дополнительные правила.

Но перед этим необходимо изменить общий уровень доступа к файлам, используемый в системе. Возможные уровни определены в подразделе Уровни безопасности, и, чтобы изменить уровень, достаточно в контекстном меню нужного уровня выбрать команду По умолчанию. Если раньше подраздел Уровни безопасности содержал всего два возможных уровня, то в операционной системе Windows Vista их три.

- Запрещено — если вы установите данный уровень доступа, то по умолчанию доступ к любым файлам компьютера для всех пользователей будет запрещен. Не забудьте только после этого создать несколько дополнительных правил, которые разрешали бы пользователям доступ к определенным каталогам.
- Обычный пользователь — если вы установите данный уровень доступа, то по умолчанию доступ к любым файлам компьютера будет разрешен только с правами пользователя. Доступ с правами администратора или опытного пользователя будет запрещен.

- Неограниченный — используется по умолчанию. При этом пользователям разрешен доступ ко всем файлам компьютера без ограничений (естественно, если только доступ к файлам не запрещен с помощью ACL).

Подраздел Сценарии

Подраздел Сценарии также совершенно не изменился по сравнению с предыдущими версиями операционной системы Windows. С его помощью можно указать путь к VBS или JS-сценарию, BAT-файлу или любой программе, которая должна автоматически запускаться либо при входе пользователя в систему или выходе из нее (подраздел Сценарии раздела Конфигурация пользователя), либо при запуске процесса `winlogon.exe` или выключении компьютера (подраздел Сценарии раздела Конфигурация компьютера).

Работа со сценариями. Как и раньше, если вы назначаете на выполнение сценарий, расположенный на локальном компьютере, то он должен находиться в одном из следующих каталогов (на самом деле он может находиться где угодно, но ведь не зря же разработчики ввели специальные каталоги файловой системы для хранения сценариев).

- `%systemroot%\System32\GroupPolicy\User\Scripts\Logon` — сценарий должен исполняться при входе текущего пользователя в систему. Запускается с правами пользователя.
- `%systemroot%\System32\GroupPolicy\User\Scripts\Logoff` — сценарий должен исполняться при выходе текущего пользователя из системы. Запускается с правами пользователя.
- `%systemroot%\System32\GroupPolicy\Machine\Scripts\Shutdown` — сценарий должен исполняться при выключении компьютера любым пользователем. Запускается с правами системы.
- `%systemroot%\System32\GroupPolicy\Machine\Scripts\Startup` — сценарий должен исполняться при загрузке процесса `winlogon.exe` любым пользователем. Запускается с правами системы.

Как и раньше, сведения об указанных вами сценариях, запускаемых автоматически, записываются как в реестр, так и в специальный файл файловой системы.

Сведения о сценариях, автоматически запускаемых для пользователя, хранятся в файле `scripts.ini` каталога `%systemroot%\System32\GroupPolicy\User\Scripts`. Сведения о сценариях, автоматически запускаемых для всех пользователей, хранятся в файле `scripts.ini` каталога `%systemroot%\System32\GroupPolicy\Machine\Scripts`. Оба этих файла очень просты в понимании и позволяют редактировать свое содержимое вручную, без использования оснастки Редактор объектов групповой политики.

Сведения о запускаемых сценариях хранятся в подразделах ветвей системного реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts` и `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\Scripts`.

Групповые политики настройки выполнения сценариев. Операционная система Windows Vista содержит специальные групповые политики для настройки выполнения сценариев. Все они расположены в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Сценарии и описаны в файле `Scripts.admx`. Например, в данном подразделе можно встретить следующие групповые политики (все они влияют на параметры типа `REG_DWORD`, расположенные в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`).

- `Allow-LogonScript-NetbiosDisabled` — если значение данного параметра равно `1`, то пользовательские сценарии входа будут выполняться даже в том случае, если во время входа в перекрестный лес NetBIOS и WINS отключены и DNS-серверы не настроены.
- `MaxGPOScriptWait` — значение данного параметра определяет максимальное время (в секундах), которое могут выполняться сценарии входа и выхода, и может принимать значения от 1 до 32 000 секунд. По умолчанию сценарии могут выполняться не более десяти минут.
- `RunLogonScriptSync` — если значение данного параметра равно `1`, то все пользовательские сценарии входа в систему будут выполняться синхронно с самим процессом входа. Иными словами, пока сценарии не будут выполнены, оболочка пользователя отображена не будет. По умолчанию сценарии выполняются асинхронно. Этот параметр находится и в ветви реестра корневого раздела `HKEY_CURRENT_USER`.
- `HideShutdownScripts` — при установке значения этого параметра равным `0` сценарии, которые выполняются при завершении работы операционной системы, будут отображаться на экране. По умолчанию сведения об их выполнении не отображаются. Этот параметр находится и в ветви реестра корневого раздела `HKEY_CURRENT_USER`.
- `RunStartupScriptSync` — если значение данного параметра равно `0`, то все сценарии входа в систему будут выполняться асинхронно по отношению друг к другу. Иначе говоря, пока не будет выполнен один сценарий, второй выполняться не будет. По умолчанию сценарии выполняются асинхронно.
- `HideStartupScripts` — при установке значения этого параметра равным `0` сценарии, которые выполняются при входе в систему синхронно, будут отображаться в окне командной строки. По умолчанию сведения об их выполнении не отображаются. Этот параметр находится и в ветви реестра корневого раздела `HKEY_CURRENT_USER`.

Подраздел Настройка Internet Explorer

Совершенно не изменился и подраздел Настройка Internet Explorer раздела Политика "Локальный компьютер" ▸ Конфигурация пользователя ▸ Конфигурация Windows. Как и раньше, он содержит следующие подразделы.

- Пользовательский интерфейс обозревателя — позволяет настроить такие элементы окна браузера Internet Explorer, как заголовок окна (подраздел Заголовок

обозревателя), файлы изображений для фона панели инструментов браузера, а также позволяет добавить собственные кнопки к панели инструментов (подраздел Настройка панели инструментов). Кроме того, с помощью данного подраздела можно изменить файлы изображений для статического и динамического логотипов браузера Internet Explorer (подраздел Эмблема и анимированные рисунки). Следует только понимать, что при использовании нового интерфейса операционной системы вообще не существует такого понятия, как логотип или изображение панели инструментов, поэтому, для того чтобы увидеть изменения, нужно работать в операционной системе Windows Vista с интерфейсом ранних версий операционной системы.

Все параметры, изменяемые с помощью данного подраздела, записываются в текстовый файл `install.ins` (по умолчанию изменять данный файл могут только администраторы и система), расположенный в каталоге `%systemroot%\system32\GroupPolicy\User\MICROSOFT\IEAK`. Сами же измененные параметры записываются в реестр с помощью процесса `svchost.exe`, запущенного с правами системы.

- Подключение — дает возможность настроить следующие параметры браузера Internet Explorer:
  - строку, добавляемую к строке User-Agent, идентифицирующей обозреватель (подраздел Строка обозревателя);
  - используемые для подключения к Интернету адреса и порты прокси-сервера (подраздел Параметры прокси-сервера);
  - адрес компьютера, который содержит сценарии (INS-файл для настройки параметров обозревателя и JS-сценарий для настройки прокси) для автоматической настройки обозревателя через определенный промежуток времени (подраздел Автоматическая настройка обозревателя).

  С помощью данного подраздела можно также экспортировать настройки, изменяемые с помощью вкладки Подключения окна Свойства: Интернет, в файлы, расположенные в каталоге `%systemroot%\system32\GroupPolicy\User\MICROSOFT\IEAK\BRANDING\cs`, чтобы впоследствии содержимое этих файлов автоматически импортировалось в браузер Internet Explorer.
- URL-адреса — позволяет настроить содержимое папок Избранное и Ссылки (подраздел Избранное и ссылки), а также изменить такие стандартные адреса браузера Internet Explorer, как адрес домашней страницы, панели поиска и страницы поддержки (подраздел Важные URL-адреса).
- Безопасность — дает возможность экспортировать настройки зон Интернета и настройки ограничений браузера (Ratings) в INF-файлы, чтобы впоследствии содержимое этих файлов автоматически импортировалось в браузер Internet Explorer (подраздел Зоны безопасности и оценка содержимого). Зоны безопасности экспортируются в файлы `seczones.inf` и `seczrsop.inf`, расположенные в каталоге `%systemroot%\system32\GroupPolicy\User\MICROSOFT\IEAK\BRANDING\ZONES`, а параметры ограничений браузера экспортируются в INF-файлы `ratings.inf` и `ratrsop.inf` каталога `%systemroot%\`

system32\GroupPolicy\User\MICROSOFT\IEAK\BRANDING\RATINGS. С помощью этого подраздела можно также экспортировать параметры настройки сертификатов доверенных издателей и доверенных агентств выдачи сертификатов (подраздел Параметры Authenticode).

- Программы — позволяет выполнить экспортирование параметров из вкладки Программы окна Свойства: Интернет в файл programs.inf, расположенный в каталоге %systemroot%\system32\GroupPolicy\User\MICROSOFT\IEAK\BRANDING\PROGRAMS, чтобы впоследствии содержимое этого файла автоматически импортировалось в браузер Internet Explorer.

Раздел Административные шаблоны

Административные шаблоны — это единственное, что существенно изменилось в операционной системе Windows Vista. Точнее, изменились не сами административные шаблоны, а способы их создания. Если раньше все групповые политики хранились в пяти файлах с расширением ADM, то теперь для их хранения используется множество файлов с расширениями ADMX и ADML, которые представляют собой XML-файлы (то есть также изменился и синтаксис создания данных файлов).

Файлы, имеющие расширение ADMX, расположены в каталоге %systemroot%\PolicyDefinitions. Они содержат описания ветвей реестра и параметров, изменяющихся групповыми политиками, а также ссылки на одноименные файлы с расширением ADML, хранящие описания групповых политик, изменяющих эти ветви реестра. Файлы с расширением ADML расположены в каталоге %systemroot%\PolicyDefinitions\en-US (для английской локализации административных шаблонов). На протяжении предыдущих глав мы рассматривали групповые политики, которые позволяли настраивать те или иные компоненты операционной системы, а также подразделы оснастки gpedit.msc и файлы, в которых эти групповые политики хранятся. Поэтому сейчас мы не будет рассматривать ни структуру подразделов групповых политик, ни назначение стандартных ADMX и ADML-файлов.

ПРИМЕЧАНИЕ

Сведения о применении групповых политик заносятся в журнал Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ GroupPolicy.

Согласитесь, что было бы глупо изменять формат файлов, содержащих групповые политики, и полностью отказываться от всех написанных ранее административных файлов с расширением ADM. Именно поэтому групповые политики Windows Vista поддерживают как новый формат файлов административных шаблонов, так и старый. Теперь все файлы с расширением ADM заносятся в подраздел групповых политик Административные шаблоны ▸ Классические административные шаблоны (ADM). При этом операционная система Windows Vista по умолчанию содержит один ADM-файл, который расположен в каталоге %systemroot%\inf и управляет

настройкой ограничений на передачу отчетов об ошибках в работе операционной системы и программ корпорации Microsoft.

Хранение групповых политик. Все групповые политики, которые вы применили с помощью оснастки Редактор объектов групповой политики, заносятся не только в реестр, но и в два специальных файла с именем `registry.pol`. Они расположены в каталогах `%systemroot%\system32\GroupPolicy\Machine` и `%systemroot%\system32\GroupPolicy\User`. Параметры из этих файлов через определенные промежутки времени заносятся в реестр (как и в предыдущих операционных системах, можно воспользоваться командой `gpupdate.exe`, чтобы вручную внести в реестр содержимое файлов `registry.pol`).

Именно из-за этих файлов удаление параметров групповых политик непосредственно с помощью реестра не приведет ни к каким результатам — они будут заново созданы при следующем помещении содержимого файлов `registry.pol` в реестр. Поэтому если вы установили какие-либо ограничения с помощью групповых политик, то и удалить их вы сможете только с помощью групповых политик.

Если компьютер находится в домене, то для него применяются не только локальные групповые политики, но и групповые политики на уровне домена и организационной единицы. Как и раньше, политики на уровне домена будут замещать собой политики локального компьютера, а групповые политики на уровне организационной единицы будут замещать собой политики на уровне домена.

Работа с групповыми политиками с помощью дополнительных программ

Теперь рассмотрим несколько программ командной строки, которые предназначены для работы с групповыми политиками. Первая из них является нововведением операционной системы Windoiws Vista. Вторая же присутствовала и в предыдущих версиях Windows.

- Migration Table. **Расположение:** `%systemroot%\system32\mtedit.exe`.

  Эту программу можно использовать при копировании групповых политик из одного домена в другой, для определения и изменения специфических для домена данных. При копировании групповых политик из одного домена в другой политики старого домена не всегда смогут работать на новом домене. Например, если политики основаны на SID учетных записей пользователей, которые никак не могут совпадать у двух доменов, данные политики работать не будут. В этом случае вам может понадобиться программа Migration Table, которая позволяет указать данные старого домена, например SID учетных записей и данные, на которые они будут автоматически заменены при копировании в новый домен.

  С помощью программы Migration Table можно указать изменение следующих данных: SID групп и учетных записей пользователей, имена компьютеров, а также пути UNC. Эти данные могут встречаться как непосредственно в груп-

повых политиках, так и в ACL для групповых политик или дополнительных файлов.

После работы Migration Table создается текстовый файл в формате XML с расширением MIGTABLE. Конечно, вы можете редактировать или даже самостоятельно создавать данный файл, не используя программы Migration Table, однако с ее помощью создание файла миграции существенно облегчается.

Для запуска программы Migration Table лучше всего воспользоваться оснасткой Управление групповой политикой. Для этого достаточно в контекстном меню домена или объекта групповой политики выбрать команду Открыть редактор таблиц миграции, после чего отобразится окно программы.

Чтобы просмотреть дополнительную информацию о данной программе, достаточно воспользоваться меню Справка для вывода справки по работе с ней.

- Group Policy Update Utility v6.0. **Расположение:** `%systemroot%\system32\Gpupdate.exe`.

  Эта программа командной строки также присутствовала в предыдущих версиях операционной системы Windows, поэтому мы не будем рассматривать ее подробно. С ее помощью можно выполнить немедленное обновление групповых политик компьютера на основе локальных и групповых политик домена. Для этого достаточно воспользоваться данной программой без параметров. При обновлении можно также указать следующие основные параметры.

  - `/target:` — может принимать значения `computer` и `user`. Определяет тип политик, которые будут обновлены (по умолчанию обновляются оба типа политик).
  - `/Logoff` — при завершении обновления политики выйти из системы.
  - `/boot` — при завершении обновления политики перезагрузить компьютер.
  - `/sync` — новый параметр данной программы, который может использоваться вместе с предыдущими параметрами. Его использование приводит к синхронному применению групповых политик.

Настройка групповых политик

Как ни странно звучит название этого подраздела книги, но операционная система Windows Vista содержит специальные групповые политики для настройки работы механизма групповых политик и RSoP (о RSoP будет рассказано при описании оснастки Результирующая политика). Все они расположены в подразделе Административные шаблоны ▸ Система ▸ Групповая политика разделов Конфигурация компьютера и Конфигурация пользователя. Они описаны в файле `GroupPolicy.admx`.

Локальные пользователи и группы

CLSID-номер оснастки: `{5D6179C8-17EC-11D1-9AA9-00C04FD8FE93}`.

Библиотека: `localsec.dll`.

Используется в стандартных консолях: `compmgmt.msc`, `lusrmgr.msc`.

Работа с данной оснасткой, как и ее интерфейс, также совершенно не изменились. При добавлении оснастки вы можете выбрать компьютер, информацию которого она должна отображать. После этого оснастка будет добавлена.

С помощью оснастки Локальные пользователи и группы вы можете добавлять, удалять или редактировать содержимое групп пользователей или параметры определенных учетных записей пользователей. Например, можно изменить группу, к которой принадлежит определенная учетная запись пользователя, описание, пароль к учетной записи, путь к профилю учетной записи пользователя, указать, может ли пользователь самостоятельно изменять пароль. А можно вообще отключить определенную учетную запись пользователя.

ПРИМЕЧАНИЕ

Параметры учетных записей компьютера можно просмотреть с помощью экземпляров класса Win32_UserAccount, принадлежащего пространству имен \\root\cimv2. Например, данный класс поддерживает следующие свойства: AccountType (определяет свойства учетной записи), Disabled (указывает, отключена ли данная учетная запись), Domain (ключевое свойство, определяющее домен, в котором зарегистрирована учетная запись), LocalAccount (указывает, является ли данная учетная запись локальной), Lockout (определяет, заблокирована ли данная учетная запись), Name (ключевое свойство, определяющее название учетной записи), PasswordChangeable (указывает, можно ли изменить пароль для данной учетной записи), PasswordExpires (определяет, имеет ли пароль для данной учетной записи срок действия), PasswordRequired (указывает, установлен ли пароль для данной учетной записи), SID (определяет SID учетной записи).

Группы пользователей

По умолчанию в Windows Vista созданы следующие группы пользователей.

- IIS_IUSRS — пользователи данной группы могут работать с веб-сервером IIS локального компьютера. По умолчанию в данную группу входит пользователь NT AUTHORITY\IUSR.
- Администраторы — пользователям данной группы предоставлены максимальные привилегии на локальном компьютере. По умолчанию в данную группу входит пользователь Администратор, а также первый пользователь, которого вы создавали при инсталляции операционной системы.
- Гости — пользователи данной группы обладают минимальными правами в операционной системе. По умолчанию в данную группу входит пользователь Гость.
- Криптографические операторы — пользователи этой группы могут выполнять шифрование и расшифровку данных. В остальном их права соответствуют правам участников группы Пользователи.
- Операторы архива — пользователи данной группы могут выполнять архивирование и восстановление системы с помощью стандартного мастера Windows. В остальном их права соответствуют правам пользователей группы Пользователи.

- Операторы настройки сети — пользователям этой группы разрешено выполнять настройку сетевых интерфейсов локального компьютера. В остальном их права соответствуют правам пользователей группы Пользователи.
- Опытные пользователи — им разрешено создавать других пользователей и другие группы (но не обладающих никакими административными правами), разрешен доступ к каталогу %programfiles% и многим дополнительным ветвям реестра, а также разрешено запускать или останавливать службы. В остальном их права соответствуют правам участников группы Пользователи.
- Пользователи — обладают основными правами по работе в системе, но не обладают никакими административными правами. По умолчанию в данную группу входят пользователи NT AUTHORITY\Authenticated Users и NT AUTHORITY\INTERACTIVE.
- Пользователи DCOM — пользователи данной группы могут выполнять любые операции с DCOM-объектами, зарегистрированными на локальном компьютере. В остальном их права соответствуют правам участников группы Пользователи.
- Пользователи журналов производительности — пользователям данной группы разрешено пользоваться журналами производительности локального компьютера. В остальном их права соответствуют правам участников группы Пользователи.
- Пользователи системного монитора — пользователям этой группы разрешено удаленно просматривать журналы производительности локального компьютера. В остальном их права соответствуют правам участников группы Пользователи.
- Пользователи удаленного рабочего стола — пользователям данной группы разрешен доступ к удаленному Рабочему столу операционной системы.
- Репликатор — пользователь данной группы может зарегистрироваться в службе репликации контроллера домена.
- Читатели журнала событий — пользователи этой группы обладают правом чтения стандартных журналов операционной системы.

Хранение сведений в реестре

Сведения о пользователях и группах, зарегистрированных в операционной системе Windows Vista, содержатся в базе данных SAM. Она проецируется на две ветви реестра: HKEY_LOCAL_MACHINE\SAM и HKEY_LOCAL_MACHINE\SECURITY. По умолчанию администратор не может получить доступ к ветви HKEY_LOCAL_MACHINE\SECURITY, однако если вы отредактируете права доступа к данной ветви, то сможете просмотреть ее содержимое. Хотя это даст не многое: как ветвь реестра HKEY_LOCAL_MACHINE\SECURITY, так и HKEY_LOCAL_MACHINE\SAM хранит данные в зашифрованном виде.

Список всех стандартных групп пользователей содержится в ветви системного реестра HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Builtin\Aliases\Names (в виде подразделов данной ветви). В данной ветви хранятся только названия групп, остальные же сведения о них хранятся в параметре REG_BINARY-типа C ветви

HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Builtin\Aliases\<номер группы>. Например, в данном параметре находится описание группы.

Если же вы создаете свою группу, то сведения о ней заносятся в параметр типа REG_BINARY C ветви системного реестра HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Aliases\<номер группы>, а ее название заносится как дочерний подраздел в ветвь реестра HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Aliases\Names.

Названия всех учетных записей пользователей хранятся как дочерние подразделы ветви реестра HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names. Остальная же информация об учетных записях пользователей находится в параметрах REG_BINARY-типа ветви реестра HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\<номер пользователя>. Например, параметр V хранит сведения о полном имени учетной записи и ее описании. Параметр UserPasswordHint содержит подсказку пользователя (при вводе пароля во время создания учетной записи пользователя можно было ввести подсказку, которая будет отображаться, если вы ввели пароль неправильно). А в параметре UserTile хранится путь к изображению, которое ассоциируется с учетной записью пользователя и отображается в меню Пуск.

Список пользователей, профили которых созданы в операционной системе (как обычных пользователей, так и таких стандартных учетных записей как, например, LOCAL SYSTEM, LOCAL SERVICE и NETWORK SERVICE), также находится в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList. Она включает в себя вложенные подразделы, названные в честь SID учетной записи и содержащие сведения о профиле для данного SID. Например, в параметре строкового типа ProfileImagePath этих ветвей реестра хранится путь к каталогу профиля.

ПРИМЕЧАНИЕ

С помощью команды rundll32.exe sysdm.cpl, EditUserProfiles можно отобразить окно Профили пользователей, которое позволяет изменить тип профиля пользователя (локальный или перемещаемый), удалить профиль пользователя или переместить его в другой каталог.

Особенностью ветви HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList является то, что в ней также определяются сведения о стандартных профилях операционной системы. Эта ветвь включает в себя следующие параметры строкового типа.

- Default — хранит путь к профилю, который будет использоваться как основа при создании нового профиля пользователя (при первом входе в операционную систему пользователя, учетная запись которого была недавно создана).
- ProfilesDirectory — содержит путь к каталогу, хранящему профили пользователей операционной системы.

- `ProgramData` — хранит путь к каталогу, используемому установленными в операционной системе программами для хранения своих данных.
- `Public` — содержит путь к каталогу профиля Общие.

Результирующая политика

CLSID-номер оснастки: `{6DC3804B-7212-458D-ADB0-9A07E2AE1FA2}`.

Библиотека: `GPEdit.dll`.

Используется в стандартных консолях: `rsop.msc`.

Впервые оснастка Результирующая политика появилась в операционной системе Windows XP. Она предоставляет простой способ просмотра групповых политик, которые действуют на того или иного пользователя.

Если в оснастке Редактор объектов групповой политики отображаются все групповые политики, доступные для данной операционной системы, то в оснастке Результирующая политика отображаются только те групповые политики, которые были установлены. Кроме того, особенностью данной оснастки является то, что она отображает групповые политики, учитывая их состояние, определенное как групповыми политиками локального компьютера, так и групповыми политиками, установленными на уровне домена и организационной единицы. При этом оснастка позволяет определить групповые политики, состояние которых конфликтует на уровне локального компьютера, домена или организационной единицы.

После открытия оснастки Результирующая политика ее основное окно будет пустым. Чтобы отобразить итоги работы результирующей политики, сначала нужно определить компьютер и пользователя, для которого будет генерироваться результирующая политика. Для этого в контекстном меню подраздела оснастки нужно выбрать команду Создать данные RSoP. После этого отобразится соответствующий мастер, позволяющий выбрать компьютер и пользователя данного компьютера.

После генерации результирующей политики в подразделе оснастки будет создано два дочерних подраздела, уже знакомых вам по оснастке Редактор объектов групповой политики: Конфигурация компьютера и Конфигурация пользователя. Как и раньше, они будут содержать дочерние подразделы Конфигурация программ, Конфигурация Windows и Административные шаблоны (если была определена хотя бы одна политика данного подраздела).

Подраздел Административные шаблоны будет содержать только те политики, которые были установлены для выбранного пользователя. При этом в свойствах установленной политики, помимо стандартных вкладок Параметр (обратите внимание, что с помощью данной вкладки можно просмотреть состояние групповой политики, но нельзя его изменить) и Объяснение, появится еще одна вкладка — Приоритет. С помощью этой вкладки можно определить, на каком уровне была назначена соответствующая политика: на уровне локального компьютера, домена или организационной единицы.

Подраздел Конфигурация Windows всегда будет включать в себя как минимум один подраздел — Параметры безопасности. Его содержимое отображается независимо от того, изменяли вы его или нет. При этом содержимое данного подраздела немного изменится. В нем будут отображаться как стандартные подразделы Политики учетных записей, Локальные политики, Политики открытого ключа, Политики ограниченного использования программ и Политики IP-безопасности, так и несколько дополнительных подразделов, параметры которых редактируются с помощью оснастки Шаблоны безопасности.

- Журнал событий — отображает параметры ведения стандартных журналов оснастки Просмотр событий.
- Группы с ограниченным доступом — выводит список пользователей, права которых были временно повышены до определенной группы.
- Системные службы — отображает состояние службы компьютера, которое было назначено ей с помощью групповой политики.
- Реестр — выводит ветви реестра, разрешения доступа к которым были изменены.
- Файловая система — отображает каталоги файловой системы, разрешения доступа к которым были изменены.
- Политики проводной сети (IEEE 802.3) — выводит параметры настройки сетей IEEE 802.3.
- Политики беспроводной сети (IEEE 802.11) — отображает параметры настройки беспроводных сетей IEEE 802.11.

Как и в предыдущих версиях операционной системы, в Windows Vista присутствует программа командной строки `gpresult.exe` **(Расположение:** `%systemroot%\system32\gpresult.exe`**)**, с помощью которой также можно получить сведения о результирующих политиках. После запуска данной программы без параметров перед вами отобразятся следующие сведения: тип и версия операционной системы, домен, список доступных на компьютере групп, а также логин текущего пользователя, дата последнего применения групповых политик. Также будет указано, было ли выполнено подключение к компьютеру с использованием медленной линии (а также порог скорости, при котором линия считается медленной). Конечно, отобразятся и сами примененные групповые политики.

Если же вы хотите отобразить результирующие политики конкретного пользователя, то нужно воспользоваться параметром `/user`. А с помощью параметра `/scope`, значениями которого могут быть слова `user` или `computer`, можно указать тип групповых политик, которые нужно отобразить.

Если же нужно подключиться к удаленному компьютеру, то достаточно воспользоваться параметрами `/s <компьютер>`, `/u <пользователь>` и `/p <пароль>`.

Анализ и настройка безопасности

CLSID-номер оснастки: `{011BE22D-E453-11D1-945A-00C04FB984F9}`.

Библиотека: `wsecedit.dll`.

Используется в стандартных консолях: нет.

Оснастка не является нововведением операционной системы Windows Vista. Однако мы рассмотрим ее (хоть и не подробно), так как работа с ней немного запутана, хотя и не представляет особой сложности.

Работа с оснасткой

Оснастка Анализ и настройка безопасности предназначена для просмотра текущей конфигурации параметров компьютера, назначаемых с помощью шаблонов другой оснастки — Шаблоны безопасности, которую мы рассмотрим немного позже. При этом вы не только можете проанализировать состояние параметров компьютера, но и указать те из параметров, значения которых будут изменены согласно параметрам выбранного шаблона.

После запуска оснастки перед вами отобразится пустое окно. Чтобы начать работать с оснасткой, нужно в ее контекстном меню выбрать команду Открыть базу данных. После этого отобразится окно открытия базы данных SDB. Если вы впервые запускаете оснастку Анализ и настройка безопасности, то просто введите в окне название новой базы, которая будет создана после того, как вы нажмете кнопку OK. После создания базы данных перед вами отобразится список шаблонов безопасности (по умолчанию располагаются они в каталоге `%systemroot%\security\templates`), из которого нужно выбрать нужный шаблон. Шаблоны безопасности и их создание будут описаны в оснастке Шаблоны безопасности.

После того как вы загрузите нужный шаблон в оснастку Анализ и настройка безопасности, в ее контекстном меню станет активна команда Анализ компьютера. Как только вы ее выберете, начнется анализ конфигурации параметров компьютера, которые изменяются с помощью выбранного шаблона. Результаты анализа будут отображены в виде подразделов оснастки Анализ и настройка безопасности. Эти подразделы аналогичны подразделам выбранного вами шаблона безопасности.

Итак, теперь вы можете просмотреть, соответствуют ли текущие параметры настройки компьютера параметрам выбранного шаблона. Но что же делать, если значение какого-то параметра не соответствует значению, указанному в шаблоне (заметьте, что в этом случае напротив соответствующего параметра отображается перечеркнутый крестик)? В этом случае в контекстном меню соответствующего параметра нужно выбрать команду Свойства. После этого откроется окно, которое отображает текущее значение параметра и имеет флажок Определить следующую политику в базе данных. Если вы установите данный флажок, то в поле под ним отобразится значение данного параметра, указанное в шаблоне безопасности (рис. 5.17). С помощью этого же поля вы можете ввести свое значение данного параметра, отличное от того, которое указано в шаблоне безопасности. После того как вы нажмете кнопку OK, значение шаблона безопасности заменит собой текущее значение компьютера. Но только в окне оснастки! Чтобы значения измененных вами параметров действительно были записаны в реестр компьютера, нужно в контекстном меню данной оснастки выбрать команду Настроить компьютер. После этого измененные вами значения параметров будут помещены в реестр компьютера.

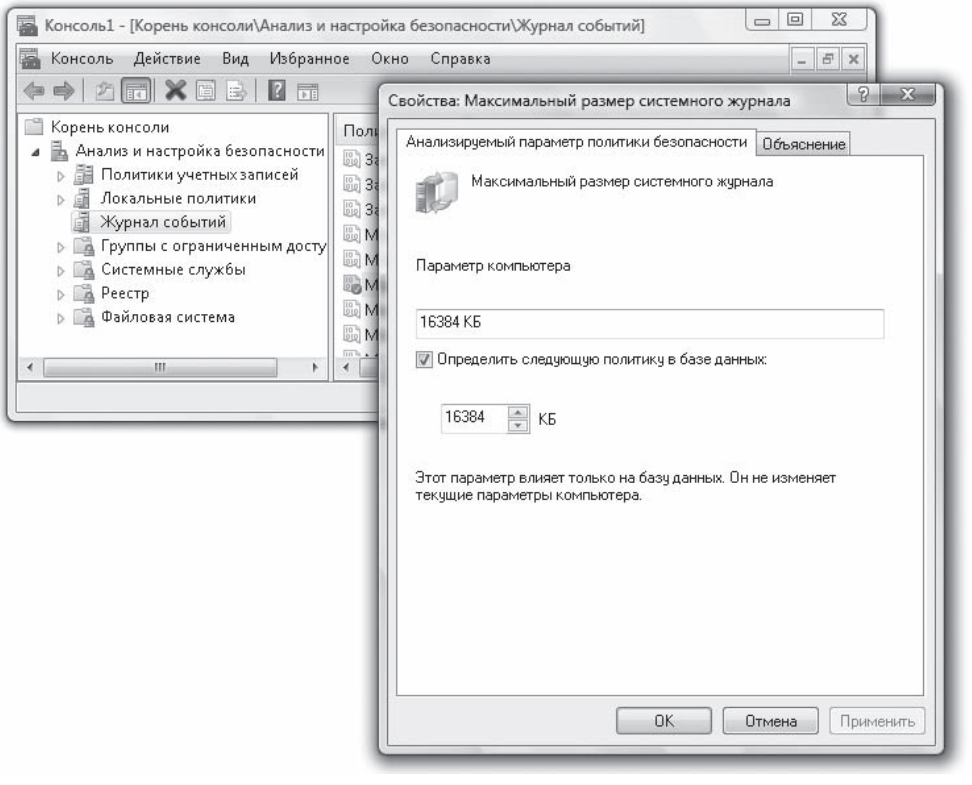


Рис. 5.17. Установка значения параметров шаблона безопасности

Использование программы secedit.exe

Для анализа параметров безопасности компьютера можно использовать программу командной строки `secedit.exe`. Возможности данной программы полностью совпадают с возможностями оснастки Анализ и настройка безопасности. Она поддерживает следующие параметры: `/configure`, `/analyze`, `/import`, `/export`, `/validate` и `/generaterollback`. Для просмотра описания использования определенной команды достаточно ввести команду `secedit.exe <команда>`.

Шаблоны безопасности

CLSID-номер оснастки: `{5ADF5BF6-E452-11D1-945A-00C04FB984F9}`.

Библиотека: `wsecedit.dll`.

Используется в стандартных консолях: нет.

Эта оснастка, как и предыдущая, не является нововведением операционной системы Windows Vista. С ее помощью можно создать новые или отредактировать поставляемые с операционной системой стандартные шаблоны безопасности. Если у вас нет стандартных шаблонов безопасности, то можно создать свой собственный

шаблон или скопировать стандартные шаблоны безопасности операционной системы Windows XP в каталог `%systemroot%\security\templates`. Вы также можете взять несколько шаблонов безопасности из каталога `%systemroot%\inf` операционной системы Windows Vista и перенести их в каталог `%userprofile%\Documents\security\Templates`. В нем находятся следующие шаблоны безопасности: `defltbase.inf`, `defltwk.inf`, `sceregvl.inf`, `secrecs.inf`.

Для примера создадим свой собственный шаблон безопасности. Для этого в контекстном меню оснастки достаточно выбрать команду Создать шаблон. После этого достаточно указать имя шаблона и его описание, после чего он будет создан. Если у вас уже есть шаблоны, то вы можете редактировать их или создать новый шаблон на основе значений параметров существующего. Для этого в контекстном меню шаблона нужно выбрать команду Сохранить как.

Каждый шаблон состоит из следующих подразделов.

- Политики учетных записей — этот подраздел знаком вам по оснастке Групповая политика. Однако, кроме вложенных подразделов Политика паролей и Политика блокировки учетных записей, доступных в оснастке Групповая политика, он содержит еще один дочерний подраздел: Политика Kerberos. Он определяет параметры работы протокола Kerberos, используемого в домене Active Directory.
- Локальные политики — также знаком вам по оснастке Групповая политика. Как и там, этот подраздел включает в себя такие вложенные подразделы, как Политика аудита, Назначение прав пользователя, Параметры безопасности.
- Журнал событий — содержит такие параметры настройки ведения стандартных журналов Windows, как максимальные размеры журналов, указания, будет ли разрешено просматривать журналы пользователям группы Гости, какой интервал очистки журналов будет использоваться и т. д.
- Группы с ограниченным доступом — позволяет добавить в определенную группу временного пользователя (для повышения его прав на некоторое время). Для добавления ограниченного пользователя в группу нужно создать саму группу, в которую будет добавляться пользователь. Для этого нужно в контекстном меню подраздела Группы с ограниченным доступом выбрать команду Добавить группу. После этого система предложит вам указать нужную группу, а затем предложит добавить в нее новых пользователей.
- Системные службы — содержит список всех служб, доступных в системе, и позволяет определить способы их запуска.
- Реестр — позволяет указать права доступа к различным ветвям реестра. Для этого сначала нужно добавить в данный подраздел необходимую ветвь реестра, что легко сделать с помощью команды Добавить раздел контекстного меню. После этого оснастка предложит вам указать права для доступа к данной ветви реестра.
- Файловая система — позволяет указать права доступа к различным каталогам файловой системы Windows XP. Для этого сначала нужно добавить в данный подраздел путь к каталогу. Это делается с помощью команды Добавить файл контекстного меню. После этого оснастка предложит вам выбрать права для

доступа к данному каталогу или файлу, а также указать, будут ли определенные вами права распространяться на все вложенные в каталог папки и файлы.

После того как вы отредактируете шаблон безопасности, необходимо сохранить все сделанные изменения. Для этого в контекстном меню шаблона безопасности нужно выбрать команду Сохранить. После этого можно применить настройки созданного вами шаблона безопасности с помощью оснастки Анализ и настройка безопасности.

Управление TPM

CLSID-номер оснастки: `{7d3830aa-e69e-4e17-8bd1-1b87b97099da}`.

Библиотека: `tpmcompc.dll`.

Используется в стандартных консолях: `tpm.msc`.

Данная оснастка является нововведением операционной системы Windows Vista. С ее помощью можно управлять работой микросхемы TPM, которая устанавливается на современные материнские платы и позволяет хранить конфиденциальные данные пользователя, а также параметры конфигурации компьютера и операционной системы. Благодаря данной микросхеме можно повысить безопасность компьютера в отношении таких угроз, как самовольное добавление оборудования в компьютер, самовольная установка программ и т. д.

Групповые политики для настройки TPM

Работу с TPM можно ограничить с помощью групповых политик. Для этого применяются политики, описанные в файле `TPM.admx` и расположенные в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Служба доверенного платформенного модуля. Политики данного подраздела изменяют следующие параметры `REG_DWORD`-типа, расположенные в ветви `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\TPM`.

- `ActiveDirectoryBackup` — если значение данного параметра равно `1`, то будет разрешено копировать основную информацию о данных владельца TPM (криптографический хэш главного пароля TPM) на контроллер домена Active Directory.
- `RequireActiveDirectoryBackup` — если значение параметра равно `1`, то копирование основной информации владельца TPM на контроллер домена Active Directory будет обязательным. При этом пароль владельца TPM не будет назначен, если архивирование нового пароля на контроллере домена не прошло успешно.

Некоторые возможности работы TPM можно настроить и с помощью следующих параметров `REG_DWORD`-типа ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\TPM\BlockedCommands`.

- `Enabled` — если значение данного параметра равно `1`, то операционная система будет использовать параметры строкового типа, расположенные в дочернем подразделе `List` ветви реестра, чтобы запретить определенные команды TPM.

- `IgnoreDefaultList` — при установке значения этого параметра равным `1` список команд TPM, выполнять которые по умолчанию запрещено, будет игнорироваться. Однако список дочернего подраздела `List` данной ветви реестра и локальный список команд TPM по-прежнему будут работать.
- `IgnoreLocalList` — если значение данного параметра равно `1`, то локальный список команд TPM, выполнять которые запрещено, будет игнорироваться. Однако список дочернего подраздела `List` данной ветви реестра по-прежнему будет работать. Также будет работать список, определенный по умолчанию.

Возможности репозитария CIM

Репозитарий CIM операционной системы Windows Vista также позволяет работать с чипом TPM. Для этого предназначено пространство имен `\\root\CIMV2\Security\MicrosoftTpm`. Оно включает в себя лишь один класс: `Win32_Tpm`, который определяет настройки работы чипа TPM и даже позволяет управлять его работой. Класс содержит следующие свойства, доступные только для чтения:

- `ManufacturerId`, тип: `uint32` — определяет идентификатор производителя чипа TPM;
- `ManufacturerVersion`, тип: `string` — указывает версию чипа TPM;
- `ManufacturerVersionInfo`, тип: `string` — определяет версию чипа TPM;
- `PhysicalPresenceVersionInfo`, тип: `string` — указывает версию чипа TPM;
- `SpecVersion`, тип: `string` — определяет версию чипа TPM.

Класс также поддерживает следующие методы.

- `AddBlockedCommand` — добавляет команду к списку блокируемых команд.

  Входящий параметр: строковый параметр, определяющий команду.

  Возвращаемые параметры: нет.
- `ChangeOwnerAuth` — изменяет параметры аутентификации.

  Входящие строковые параметры:

  - содержащий старую строку аутентификации;
  - хранящий новую строку аутентификации.

  Возвращаемые параметры: нет.
- `Clear` — удаляет настройки чипа TPM.

  Входящий параметр: строковый параметр, содержащий строку аутентификации.

  Возвращаемые параметры: нет.
- `ConvertToOwnerAuth` — преобразует пароль в строку аутентификации.

  Входящий параметр: строковый параметр, содержащий пароль для аутентификации.

  Возвращаемый параметр: строковый параметр, содержащий строку аутентификации.

- `CreateEndorsementKeyPair` — создает пару ключей подтверждения.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

- `Disable` — отключает чип TPM.

  Входящий параметр: строковый параметр, содержащий строку аутентификации.

  Возвращаемые параметры: нет.

- `Enable` — включает чип TPM.

  Входящий параметр: строковый параметр, содержащий строку аутентификации.

  Возвращаемые параметры: нет.

- `GetPhysicalPresenceRequest` — возвращает физическое присутствие запроса.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет запрос, имеет тип `uint32`.

- `GetPhysicalPresenceResponse` — возвращает физическое присутствие ответа.

  Входящие параметры: нет.

  Возвращаемые параметры:

  - определяет запрос, имеет тип `uint32`;
  - определяет ответ, имеет тип `uint32`.

- `GetPhysicalPresenceTransition` — возвращает физическое присутствие перемещения.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет перемещение, имеет тип `uint32`.

- `IsActivated` — определяет, активирован ли TPM.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет, активирован ли TPM. Имеет тип `boolean`.

- `IsCommandBlocked` — определяет, заблокирована ли команда.

  Входящий параметр: определяет порядок команды, имеет тип `uint32`.

  Возвращаемый параметр: определяет, заблокирована ли команда, имеет тип `uint32`.

- `IsCommandPresent` — определяет команду, выполняемую в текущий момент.

  Входящий параметр: определяет порядок команды, имеет тип `uint32`.

  Возвращаемый параметр: определяет команду, выполняемую в текущий момент, имеет тип `uint32`.

- `IsEnabled` — определяет, включен ли TPM.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет, включен ли TPM, имеет тип `boolean`.

- `IsEndorsementKeyPairPresent` — определяет, подтверждена ли текущая пара ключей.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет, подтверждена ли текущая пара ключей, имеет тип `boolean`.

- `IsOwned` — определяет, является ли TPM-модуль основным.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет, является ли TPM-модуль основным, имеет тип `boolean`.

- `IsOwnerClearDisabled` — определяет, запрещена ли очистка.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет, запрещена ли очистка, имеет тип `boolean`.

- `IsOwnershipAllowed` — определяет, разрешено ли владение.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет, разрешено ли владение, имеет тип `boolean`.

- `IsPhysicalClearDisabled` — определяет, запрещена ли физическая очистка.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет, запрещена ли физическая очистка, имеет тип `boolean`.

- `IsPhysicalPresenceHardwareEnabled` — определяет, разрешены ли текущие компоненты компьютера.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет, разрешены ли текущие компоненты компьютера, имеет тип `boolean`.

- `IsSrkAuthCompatible` — определяет, поддерживается ли аутентификация.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет, поддерживается ли аутентификация, имеет тип `boolean`.

- `RemoveBlockedCommand` — удаляет блокирующую команду.

  Входящий параметр: определяет порядок команды, имеет тип `uint32`.

  Возвращаемые параметры: нет.

- `ResetAuthLockOut` — сбрасывает блокировку аутентификации.

  Входящий параметр: определяет аутентификацию, имеет тип `uint32`.

  Возвращаемые параметры: нет.

- `ResetSrkAuth` — сбрасывает аутентификацию.

  Входящий параметр: строковый параметр, содержащий строку аутентификации.

  Возвращаемые параметры: нет.

- `SelfTest` — выполняет самотестирование TPM.

  Входящие параметры: нет.

  Возвращаемый параметр: массив параметров типа `uint8`, содержащих результаты самотестирования TPM.

- `SetPhysicalPresenceRequest` — устанавливает текущий физический запрос.

  Входящий параметр: определяет запрос, имеет тип `uint32`.

  Возвращаемые параметры: нет.

- `TakeOwnership` — позволяет изменить владельца.

  Входящий параметр: строковый параметр, содержащий строку аутентификации.

  Возвращаемые параметры: нет.

Брандмауэр Windows в режиме повышенной безопасности

CLSID-номер оснастки: `{b05566ac-fe9c-4368-be02-7a4cbb7cbe11}`.

Библиотека: `AuthFWSnapin.dll`.

Используется в стандартных консолях: `secpol.msc`, `WF.msc`.

В операционной системе Windows Vista, помимо стандартного окна Брандмауэр Windows, который совершенно не изменился, присутствует новая оснастка Брандмауэр Windows в режиме повышенной безопасности. Возможности этой оснастки существенно превышают возможности окна Брандмауэр Windows.

Сведения о работе стандартного брандмауэра операционной системы Windows Vista можно просмотреть с помощью счетчиков производительности объектов WFPv4 и WFPv6. Например, с их помощью можно узнать следующие сведения:

- количество отброшенных за последнюю секунду входящих и исходящих пакетов (счетчики Отброшено входящих пакетов/сек и Отброшено исходящих пакетов/сек), а также общее количество отброшенных пакетов (счетчик Отброшено пакетов/сек);
- количество заблокированных за последнюю секунду входящих и исходящих соединений (счетчики Заблокировано входящих подключений/сек и Заблокировано исходящих подключений/сек), а также количество разрешенных соединений (счетчики Разрешено входящих подключений/сек, Разрешено исходящих подключений/сек);
- общее количество входящих и исходящих соединений (счетчики Входящие подключения и Исходящие подключения), а также количество активных из них (счетчики Активные входящие подключения и Активные исходящие подключения).

При загрузке оснастки Брандмауэр Windows в режиме повышенной безопасности нужно указать компьютер, параметры брандмауэра которого будут загружены в оснастку. Основное окно оснастки представлено на рис. 5.18.

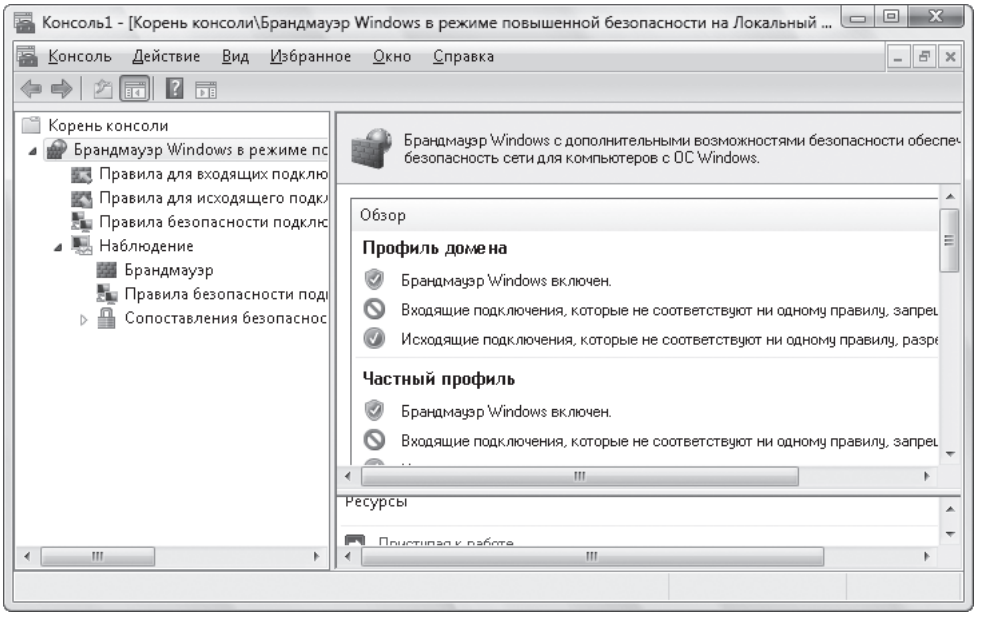


Рис. 5.18. Оснастка Брандмауэр Windows в режиме повышенной безопасности

Основное окно оснастки состоит из следующих элементов.

- Обзор — отображает основные сведения о настройках брандмауэра: включен ли брандмауэр для доменного профиля (используется, если компьютер является частью домена Active Directory), частной сети и публичной сети (при создании сетевого подключения можно определить, является это подключение частным, то есть локальным, или публичным, то есть через Интернет), настроены ли фильтры входящего и исходящего соединения. Кроме того, данное поле содержит в себе ссылку Свойства брандмауэра Windows, с помощью которой отображается основное окно настройки брандмауэра.
- Приступая к работе — содержит четыре ссылки на подразделы оснастки Брандмауэр Windows в режиме повышенной безопасности: Правила безопасности подключений, Правила для входящих подключений, Правила для исходящих подключений и Наблюдение.
- Ресурсы — включает в себя ссылки на различные разделы справки операционной системы, описывающей те или иные аспекты работы с оснасткой Брандмауэр Windows в режиме повышенной безопасности.

Окно Свойства

Окно настройки основных параметров работы брандмауэра можно отобразить как с помощью ссылки Свойства брандмауэра Windows основного окна оснастки, так

и с помощью команды Свойства контекстного меню подраздела оснастки. Окно имеет четыре вкладки (рис. 5.19).

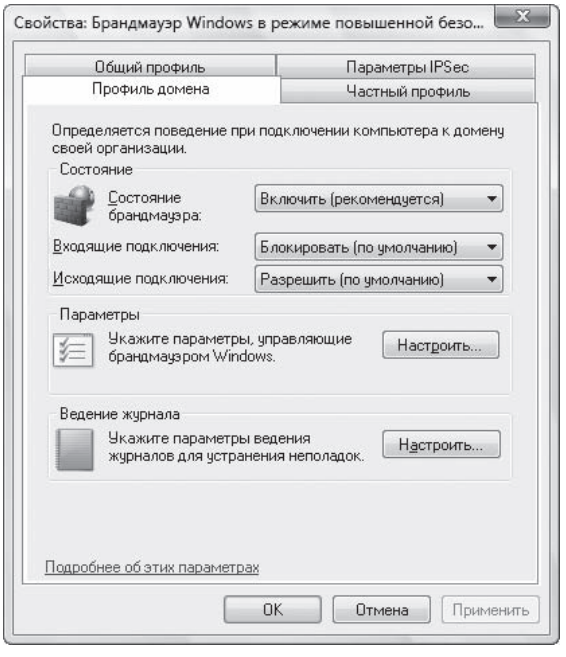


Рис. 5.19. Окно Свойства: Брандмауэр Windows в режиме повышенной безопасности

Вкладки Профиль домена, Частный профиль и Общий профиль имеют одни и те же возможности настройки, но настраивают, соответственно, работу доменного, частного и публичного профиля работы брандмауэра. Данные вкладки имеют следующие поля.

- Состояние — с помощью данного поля можно включить или отключить работу брандмауэра для данного типа сетевых подключений (раскрывающийся список Состояние брандмауэра), а также можно настроить действие по умолчанию для входящих и исходящих подключений (разрешены или не разрешены данные подключения).
- Параметры — если вы нажмете кнопку Настроить, то сможете настроить дополнительные параметры работы брандмауэра, указанные в следующих раскрывающихся списках:
  - Вывести уведомление — определяет, будет ли отображаться сообщение о том, что входящее подключение было заблокировано;
  - Разрешить одноадресный ответ — указывает, разрешено ли отвечать направленными сообщениями на групповые и широковещательные сообщения;
  - Правила локального брандмауэра — определяет, разрешено ли применять правила стандартного брандмауэра данного компьютера;

- Правила безопасности локальных подкл. — указывает, разрешено ли применять правила сетевых подключений данного компьютера.

- Ведение журнала — если вы нажмете кнопку Настроить, то сможете настроить такие параметры ведения файла журнала, как путь к нему, максимальный размер файла, а также указать, будут ли в нем регистрироваться успешно установленные сетевые соединения и потерянные пакеты.

Это окно также содержит вкладку Параметры IPSec, на которой расположена кнопка Настроить и раскрывающийся список Исключить ICMP из IPSec. С помощью списка можно определить, будут ли пакеты протокола ICMP исключаться из трафика IPSec.

Если вы нажмете кнопку Настроить, то отобразится окно Выбор параметров IPSec, позволяющее настроить следующие параметры работы протокола IPSec.

- Обмен ключами (основной режим) — дает возможность изменить алгоритм шифрования, используемый при обмене ключами, алгоритм шифрования и проверки целостности передаваемых пакетов, а также время жизни ключа (как на основе количества прошедшего времени, так и на основе количества созданных сессий).

  По умолчанию используется проверка целостности пакетов на основе алгоритма SHA1, но можно также использовать алгоритм MD5.

  Используется шифрование пакетов с помощью алгоритма AES-128, но можно также использовать такие алгоритмы, как AES-256, AES-192, 3DES, DES (AES-256 обеспечивает самое надежное шифрование, а DES — самое ненадежное, но быстрое).

  По умолчанию используется шифрование ключей с помощью алгоритма Диффи-Хелмана второй группы. Можно также использовать такие разновидности алгоритма Диффи-Хелмана, как алгоритм первой группы, четырнадцатой, а также алгоритм эллиптической кривой P-256 или P-384. Алгоритм первой группы обеспечивает наименьшую защиту ключа. Алгоритмы на основе эллиптической кривой обеспечивают самое надежное шифрование, однако они поддерживаются только операционной системой Windows Vista.

- Защита данных (быстрый режим) — также позволяет изменить алгоритмы, используемые для шифрования и проверки целостности пакетов. Кроме того, с помощью данного поля можно определить, какой протокол и в какой последовательности будет использоваться при подключении по протоколу IPSec (ESP (использует как проверку целостности пакетов, так и шифрование) или AH (использует только проверку целостности пакетов)).

- Метод проверки подлинности — дает возможность изменить способ аутентификации пользователей при создании соединения на основе протокола IPSec. При этом можно указать следующие методы аутентификации:

  - аутентификация компьютера и пользователя на основе протокола Kerberos;

- аутентификация компьютера на основе протокола Kerberos;
- аутентификация пользователя на основе протокола Kerberos;
- использование сертификата пользователя для аутентификации;
- использование пароля.

Обратите также внимание на команду Восстановить значения по умолчанию контекстного меню оснастки. С ее помощью можно изменить все настройки брандмауэра на стандартные, если созданные настройки не удовлетворяют вашим требованиям. Стандартные настройки брандмауэра хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Defaults\FirewallPolicy`. Текущие же параметры настройки брандмауэра хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy`. Эти ветви реестра содержат одинаковые подразделы.

- `DomainProfile`, `PublicProfile` и `StandardProfile` — хранят настройки данного профиля брандмауэра. Например, в них содержатся такие параметры типа `REG_DWORD`, как `EnableFirewall` и `DisableNotification`. Кроме того, эти подразделы могут содержать дочерний подраздел `Logging`, хранящий настройки ведения файла журнала.
- `FirewallRules` — содержит параметры строкового типа, каждый из которых определяет одно правило для брандмауэра.
- `RestrictedServices` — хранит сведения о службах, доступ к сети которых запрещен.

Подраздел Правила для входящих подключений

Этот подраздел оснастки содержит список всех правил для входящих подключений операционной системы. Он хранит множество стандартных правил, однако не все из них включены. Если напротив названия правила установлен значок в виде флажка, то данное правило используется. Если же напротив правила изображен значок со стрелкой вниз, то правило не используется. Чтобы включить или выключить использование данного правила, нужно в его контекстном меню выбрать соответственно команду Включить правило или Отключить правило. Можно также изменить параметры созданного правила. Для этого используется команда Свойства контекстного меню правила. После ее выбора отобразится окно, содержащее следующие вкладки.

- Общие — позволяет настроить имя правила и его описание, а также действие, которое будет выполнено при удовлетворении данного правила. В качестве действия могут использоваться следующие возможности:
  - разрешить все подключения, удовлетворяющие данному правилу;
  - разрешить только подключения на основе протокола IPSec (также можно дополнительно определить, должен ли при подключении использоваться протокол ESP);
  - заблокировать все подключения, удовлетворяющие данному правилу.

- Программы и службы — дает возможность указать программы и службы, подключения которых подпадают под данное правило. По умолчанию правило создается для любых программ.
- Пользователи и компьютеры — позволяет определить компьютеры и пользователей, соединения которых будут всегда разрешены.
- Протоколы и порты — дает возможность настроить локальный и удаленный порт, а также протокол, который должен использоваться при соединении, чтобы оно удовлетворяло данному правилу. С помощью кнопки Параметры для некоторых протоколов можно определить конкретные типы пакетов данного протокола, на которые будет распространяться правило.
- Область — позволяет указать локальные и удаленные IP-адреса, для которых будет применяться данное правило.
- Дополнительно — дает возможность настроить дополнительные параметры работы правила. В частности, можно определить профиль сети, для которого будет применяться данное правило, а также интерфейс сетевого подключения, для которого будет применяться правило (локальное подключение, беспроводное подключение или удаленное подключение).

Конечно, по умолчанию присутствует довольно много правил для входящих подключений, но часто необходимо создать свое собственное правило. Для этого применяется команда Создать правило контекстного меню подраздела Правила для входящих подключений. После выбора данной команды отобразится мастер создания нового правила, который состоит из пяти шагов. На первом шаге нужно указать, на основе каких данных будет определяться работа правила (на основе названия программы, на основе службы, на основе определенного порта и протокола или на основе нескольких типов данных). После этого необходимо указать действие при удовлетворении сетевого подключения правилу, профиль сети, для которого будет применяться правило, имя правила и т. д. Все возможности настройки правила, которые предоставляет мастер, были описаны выше, при рассмотрении окна настройки правила.

Когда созданных правил для входящих подключений станет много, вам могут потребоваться такие команды контекстного меню подраздела Правила для входящих подключений как Фильтровать по профилю, Фильтровать по состоянию и Фильтровать по группе, которые позволят отобразить только удовлетворяющие фильтру правила.

Все описанные выше возможности подраздела Правила для входящих подключений присутствуют и в подразделе Правила для исходящего подключения. Как видно из названия, этот подраздел определяет правила для исходящих подключений.

Подраздел Правила безопасности подключения

С помощью данного подраздела можно создать правила для сетевых подключений между двумя компьютерами на основе протокола IPSec. Благодаря этим правилам можно определить параметры работы протокола IPSec для подключений между двумя определенными компьютерами сети. По умолчанию в данном подразделе не существует ни одного правила.

Как и в предыдущих подразделах, чтобы создать новое правило IPSec, нужно воспользоваться командой Новое правило контекстного меню подраздела. После этого отобразится мастер, позволяющий создать следующие правила:

- Изоляция — запрещает соединения на основе таких критериев аутентификации, как членство в домене;
- Освобождение от проверки подлинности — правило, при котором соединение с определенным компьютером не будет требовать аутентификации;
- Сервер-сервер — правило аутентификации между двумя определенными компьютерами;
- Туннельный — правило аутентификации между шлюзами компьютеров;
- Настраиваемый — составное правило.

Как и раньше, для настройки правила все-таки лучше воспользоваться окном Свойства данного правила. Для правил IPSec это окно содержит следующие вкладки.

- Общие — как и раньше, позволяет изменить имя правила и его описание, однако с помощью данной вкладки нельзя изменить действие правила, ведь для правил IPSec такого понятия вообще не существует. Благодаря этой вкладке можно включить или отключить правило.
- Компьютеры — дает возможность указать локальные и удаленные IP-адреса, для которых будет применяться данное правило.
- Проверка подлинности — позволяет указать способ аутентификации, который должен применяться при соединении компьютеров, указанных на вкладке Компьютеры.
- Дополнительно — с помощью этой вкладки можно определить профиль сети, а также интерфейс сетевого подключения, для которых будет применяться правило (локальное подключение, беспроводное подключение или удаленное подключение). Кроме того, с ее помощью можно определить параметры создаваемого между двумя компьютерами туннеля (IP-адреса двух компьютеров).

Подраздел Наблюдение

С помощью данного подраздела можно просмотреть список правил, применяемых в данный момент. Он содержит следующие дочерние подразделы.

- Брандмауэр — отображает список правил для подключений на основе IP-протокола. С помощью окна Свойства определенного правила можно просмотреть такие сведения о работе правила, как протокол, порты, локальные и удаленные адреса, приложения и службы, тип интерфейса, для которого применяется данное правило.
- Правила безопасности подключения — определяет применяемые в данный момент правила для подключений на основе протокола IPSec.
- Сопоставления безопасности — содержит список сетевых подключений на основе протокола IPSec, установленных в данный момент.

Не стоит также забывать и о самом подразделе Наблюдение. После его выбора перед вами отобразятся текущие настройки профилей стандартного брандмауэра Windows: включен ли данный профиль, блокируются ли по умолчанию входящие и исходящие подключения, какие параметры ведения файла журнала используются и т. д. Все эти параметры изменялись с помощью окна Свойства подраздела Брандмауэр Windows в режиме повышенной безопасности и были рассмотрены ранее.

Окно Параметры брандмауэра Windows

Несмотря на то что операционная система Windows Vista обзавелась новой оснасткой для работы со стандартным брандмауэром, окно Брандмауэр Windows, известное вам по предыдущим версиям операционной системы, никуда не исчезло. Однако теперь доступ непосредственно к нему можно получить не с помощью одноименного значка папки Панель управления, а с помощью программы `FirewallSettings.exe`. И теперь он называется Параметры брандмауэра Windows. Что же касается возможностей данного окна, то они совершенно не изменились.

ПРИМЕЧАНИЕ

Окно Параметры брандмауэра Windows можно отобразить и с помощью команды rundll32.exe firewall.cpl, ShowControlPanel.

Окно Параметры брандмауэра Windows представляет собой более простой способ изменения некоторых параметров работы публичного профиля стандартного брандмауэра Windows Vista. Он содержит следующие вкладки.

- Общие — позволяет включить или отключить публичный профиль брандмауэра Windows Vista, а также определить, будет ли разрешено указывать исключения, на которые настройки брандмауэра действовать не будут.
- Исключения — дает возможность определить исключения, на которые настройки брандмауэра действовать не будут (исключения представляют собой правила оснастки Брандмауэр Windows в режиме повышенной безопасности). Если напротив программы из списка данной вкладки установлен флажок, то пакеты соответствующей программы или службы будут пропускаться брандмауэром. С помощью данной вкладки вы можете как указать новую программу и порт, так и изменить параметры уже указанных программ. Используя флажок Уведомлять, когда брандмауэр блокирует новую программу данной вкладки, можно определить, будет ли выдаваться сообщение о блокировании пакетов программ, не входящих в список исключений. Здесь можно добавить указанную программу в список исключений.

  По умолчанию установлены следующие исключения.

  - Общий доступ к файлам и принтерам — предоставляет доступ к ресурсам общего доступа компьютера.
  - Удаленный помощник — позволяет получить удаленный доступ к компьютеру с помощью мастера Удаленный помощник Windows. Работа с удаленным помощником будет описана далее в этой книге.

- Маршрутизация и удаленный доступ — предоставляет доступ одноименной службе.
- Возможности подключения устройств на платформе Windows Mobile — открывает порт 990 протокола TCP для взаимодействия компьютера и таких устройств, как, например, коммуникаторы.

■ Дополнительно — дает возможность настроить параметры ведения файла журнала для публичного профиля, указать пакеты ICMP, которые брандмауэру разрешено пропускать, указать сетевые соединения, для которых брандмауэр включен, а также восстановить настройки брандмауэра по умолчанию.

Окно Брандмауэр Windows

Получить доступ к стандартному брандмауэру операционной системы можно и с помощью окна Брандмауэр Windows, которое отображается после щелчка кнопкой мыши на одноименном значке папки Панель управления.

ПРИМЕЧАНИЕ

Сведения о диагностике работы окна Брандмауэр Windows заносятся в журнал Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Firewall-CPL.

Можно также просмотреть различные сведения о диагностике работы службы Брандмауэр Windows. Для этого применяются журналы разделов MPS-CLNT, MPS-DRV, MPS-SRV подраздела Журналы приложений и служб ▸ Microsoft ▸ Windows.

По сути, окно Брандмауэр Windows является чем-то вроде набора ссылок для запуска окна Параметры брандмауэра Windows, рассмотренного выше. Это окно содержит сведения о том, активен ли в данный момент брандмауэр Windows, отображаются ли уведомления при блокировании подключения, какой сетевой профиль используется для подключения к локальной сети (публичный или частный). Кроме предоставления сведений, окно Брандмауэр Windows хранит несколько ссылок, однако все они отображают окно Параметры брандмауэра Windows, рассмотренное выше.

Настройка брандмауэра с помощью программы netsh.exe

Настроить работу стандартного брандмауэра операционной системы можно также с помощью команд программы командной строки `netsh.exe`. Программа поддерживает две команды, предназначенные для настройки брандмауэра: `firewall` и `advfirewall`. Первая присутствовала и в операционной системе Windows XP, вторая же является нововведением Windows Vista.

Команда firewall. Она позволяет управлять возможностями, предоставляемыми стандартным окном Брандмауэр Windows. Для этого команда поддерживает следующие дочерние команды.

■ `Show` — позволяет просмотреть сведения о текущих настройках брандмауэра. Она, в свою очередь, поддерживает следующие дочерние команды.

- `Allowedprogram.` — отображает список программ-исключений, работа которых в сети блокироваться не будет.

- `Config` — выводит все настройки брандмауэра (все остальные дочерние команды команды `show` показывают лишь определенную часть настроек, которые отображаются командой `config`).
- `Currentprofile` — отображает профиль брандмауэра, используемый в данный момент.
- `Icmpsetting` — выводит параметры блокирования пакетов протокола ICMP (какие типы пакетов брандмауэр будет игнорировать, а какие — блокировать). Подробнее о пакетах ICMP вы можете прочесть далее.
- `Logging` — отображает параметры ведения файла журнала (путь к нему, его максимальный размер, какие сведения будут в него заноситься).

ПРИМЕЧАНИЕ

В файл журнала брандмауэра помещается следующая информация: время поступления пакета, действие брандмауэра (блокировка пакета или его игнорирование), протокол, используемый для передачи пакета, исходный IP-адрес (и порт) и IP-адрес назначения (и порт), размер пакета, контрольные флаги протокола TCP.

- `Opmode` — выводит режимы работы брандмауэра, которые разрешены операционной системой.
- `Portopening` — отображает список портов-исключений, работа с сетью через которые не будет блокироваться брандмауэром.
- `Service` — выводит список служб-исключений, работа с сетью которых не будет блокироваться брандмауэром.
- `State` — отображает сведения о текущем состоянии брандмауэра (объединяет команды `Portopening`, `Opmode`, `multicastbroadcastresponse` и `notifications`).
- `Multicastbroadcastresponse` — определяет, разрешен ли режим однонаправленного ответа на широковещательные запросы.
- `Notifications` — определяет, будут ли отображаться уведомления о том, что брандмауэр заблокировал работу определенной программы.

- `Add` — позволяет добавить программу или порт, работа через который не будет блокироваться брандмауэром. Команда, в свою очередь, поддерживает следующие дочерние команды.
  - `Allowedprogram` — добавить программу-исключение.
  - `Portopening` — добавить порт-исключение.
- `Set` — дает возможность настроить параметры работы стандартного брандмауэра. Команда поддерживает следующие дочерние команды.
  - `Allowedprogram` — позволяет изменить настройки определенной программы-исключения.
  - `Icmpsetting` — дает возможность настроить параметры блокирования пакетов ICMP.

- `Logging` — позволяет настроить параметры ведения файла журнала.
- `Opmode` — дает возможность настроить режим работы брандмауэра (глобальный или для отдельного сетевого интерфейса).
- `Portopening` — позволяет изменить настройки определенного порта-исключения.
- `Service` — дает возможность разрешить или запретить блокирование определенной службы. С помощью данной команды можно управлять только определенными службами (ключевые слова, определяющие службы: `FILEANDPRINT`, `REMOTEADMIN`, `REMOTEDESKTOP`, `UPNP`, `ALL`).
- `Notifications` — позволяет настроить параметры отображения уведомлений при блокировании работы программы с сетью.
- `Multicastbroadcastresponse` — дает возможность определить, разрешен ли режим однонаправленного ответа на широковещательные запросы.

- `Delete` — позволяет удалить программу или порт, работа через которые ранее не блокировалась брандмауэром. Команда поддерживает следующие дочерние команды.
  - `Allowedprogram` — удалить программу-исключение.
  - `Portopening` — удалить порт-исключение.
- `Reset` — установить все настройки стандартного брандмауэра по умолчанию.

С помощью счетчиков производительности вы можете просмотреть информацию о получении и отправке пакетов ICMP разных типов. Для этого применяются счетчики объекта ICMP (или объекта ICMPv6). Например, с помощью данных счетчиков можно узнать следующее.

- Количество отправленных пакетов типа Destination Unreachable (место назначения недостижимо), Time Exceeded (истечение допустимого на передачу времени), Source Quench (принимающий узел не успевает обработать получаемые сообщения), Parameter Problem (параметры принятого сообщения ошибочны), Redirect (перенаправление), Echo Reply (эхо-ответы), Timestamp Reply (запрос на получение штампа времени), Address Mask (запрос на получение маски адреса). Соответственно, для этого применяются счетчики Отправлено сообщений 'Destination Unreachable', Отправлено сообщений 'Time Exceeded', Отправлено сообщений 'Source Quench', Отправлено сообщений 'Parameter Problem', Отправлено сообщений о перенаправлении/сек, Отправлено эхо-ответов/сек, Отправлено ответов штампа времени/сек, Отправлено ответов с маской адреса.
- Количество полученных пакетов типа Destination Unreachable, Time Exceeded, Source Quench, Parameter Problem, Redirect, Echo Reply, Timestamp Reply, Address Mask.
- Общее количество отправленных и полученных сообщений (счетчики Сообщений/сек, Получено сообщений/сек, Отправлено сообщений/сек), а также количество отправленных и полученных сообщений, которые не были обработаны из-за ошибки (счетчики Ошибок при получении сообщений, Ошибок исходящих сообщений).

Команда advfirewall. С помощью данной команды вы можете управлять новым стандартным брандмауэром операционной системы Windows Vista (реализован-

ным в оснастке Брандмауэр Windows в режиме повышенной безопасности). Возможности данной команды будут описаны в гл. 8, посвященной сетевым функциям операционной системы.

Другие компоненты операционной системы

Службы компонентов

CLSID-номер оснастки: {C9BC92DF-5B9A-11D1-8F00-00C04FC2C17B}.

Библиотека: comsnap.dll.

Используется в стандартных консолях: comexp.msc, также можно запустить с помощью файла dcomcnfg.exe.

Оснастка Службы компонентов является стандартной оснасткой операционных систем семейства Windows, но мало пользователей ее используют. С ее помощью можно просмотреть список зарегистрированных в системе COM-компонентов и приложений COM+, а также настроить параметры их взаимодействия с удаленными компьютерами и локальными пользователями. Благодаря данной оснастке можно также настроить работу координатора распределенных транзакций (MSDTC).

Используя оснастку, вы можете получить доступ к ActiveX-объектам как локального, так и удаленного компьютера. По умолчанию выполняется подключение к локальному компьютеру, но вы можете подключиться к удаленному компьютеру с помощью команды Создать ▸ Компьютер контекстного меню раздела Компьютеры загруженной оснастки Службы компонентов.

Оснастка состоит из следующих разделов.

- Приложения COM+ — позволяет управлять приложениями COM+, установленными на данном компьютере (приложение COM+ представляет собой набор компонентов COM, которые взаимодействуют друг с другом и выполняют управление очередями или реализуют возможность настройки параметров безопасности на основе ролей). С помощью контекстного меню данного раздела можно также установить новое приложение COM+ (команда Создать ▸ Приложение). Естественно, это можно сделать и с помощью службы Установщик Windows.

  Раздел содержит набор вложенных подразделов, которые и определяют приложения COM+. Одним из таких стандартных подразделов является подраздел Системное приложение. Он определяет параметры работы системного приложения, которое управляет функциями настройки и развертывания служб компонентов (то есть пользователи, имеющие доступ к данному приложению, могут управлять работой COM-компонентов и устанавливать новые).

  Каждый из подразделов, в свою очередь, может включать в себя дочерние подразделы. Например, следующие.

  - Компоненты — хранит список COM-компонентов данного приложения COM+. С помощью контекстного меню данного подраздела вы можете добавить новый COM-компонент к списку используемых. Для этого нужно

выбрать команду Создать ▸ Компонент, после чего отобразится мастер добавления компонентов, содержащий список всех зарегистрированных на компьютере COM-компонентов.

Каждый компонент может включать в себя два вложенных подраздела: Интерфейсы и Подписки. Первый содержит список всех интерфейсов, доступных компоненту (с помощью команды Свойства контекстного меню конкретного интерфейса можно настроить параметры его работы). Второй же определяет доступные компоненту подписки (с помощью команды Свойства контекстного меню конкретной подписки можно настроить параметры ее работы).

С помощью контекстного меню компонента можно выполнить такие действия над ним, как перемещение (команда Переместить) в другое приложение, которое поддерживает данный компонент, создание псевдонима для компонента (команда Псевдоним), выполняющего те же действия, но имеющего другой CLSID-номер, а также отключение данного компонента (команда Запретить). Однако следует заметить, что не все компоненты поддерживают приведенные выше действия.

- Устаревшие компоненты — хранит список устаревших COM-компонентов приложения COM+, которые больше не применяются, так как есть более новые версии. С помощью контекстного меню данного подраздела вы можете добавить новый COM-компонент к списку используемых. Для этого нужно выбрать команду Создать ▸ Устаревший компонент, после чего отобразится мастер добавления компонентов, содержащий список всех зарегистрированных на компьютере COM-компонентов.

  Работа с компонентами данного подраздела аналогична работе с компонентами подраздела Компоненты.

- Роли — определяет список ролей (категории пользователей, заданные разработчиком), на основе которых построена модель безопасности данного приложения.

  Например, существуют такие роли, как Администратор, Считыватель, Серверное приложение, Любое приложение и Доверенный пользователь QC. Чтобы добавить пользователя к одной из приведенных выше ролей, нужно в контекстном меню подраздела Пользователи данной роли выбрать команду Создать ▸ Роль. Если же нужно удалить пользователя из группы, то воспользуйтесь командой Удалить контекстного меню значка конкретного пользователя.

  Пользователи, входящие в роль Администратор, имеют права доступа к данному приложению COM+ как на чтение, так и на запись. Им разрешено модифицировать любые параметры COM-компонентов, а также устанавливать новые COM-компоненты. По умолчанию данной ролью обладают пользователи, входящие в группу администраторов локального компьютера.

  Пользователи, входящие в роль Любое приложение, имеют права запуска как серверных приложений COM+, так и библиотечных приложений COM+. По умолчанию данной ролью обладают все пользователи данного компьютера.

Пользователи, входящие в роль Доверенный пользователь QC, имеют право передачи сообщения для компонентов в очереди от имени других пользователей (то есть с присвоением идентификаторов других пользователей, например, от имени пользователя, имеющего больше полномочий, чем сам пользователь). По умолчанию данной ролью не может пользоваться ни один пользователь.

Пользователи, входящие в роль Считыватель, имеют права доступа к данному приложению COM+ только на чтение. Иначе говоря, им разрешено лишь просматривать текущие параметры работы COM-компонентов. По умолчанию данной ролью обладают все пользователи данного компьютера.

Пользователи, входящие в роль Серверное приложение, имеют права запуска серверных приложений COM+. По умолчанию данной ролью обладают все пользователи данного компьютера.

- Настройка DCOM — позволяет настраивать параметры запуска приложений COM (приложение COM представляет собой набор компонентов COM, которые взаимодействуют друг с другом, но не имеют модели безопасности, построенной на основе ролей) (рис. 5.20). Для этого в контекстном меню необходимого приложения COM нужно выбрать команду Свойства.

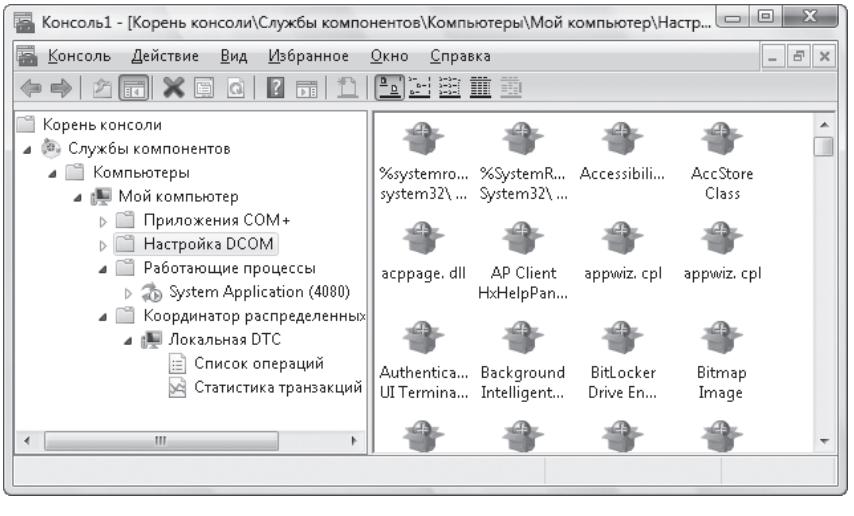


Рис. 5.20. Раздел Настройка DCOM оснастки Службы компонентов

- Работающие процессы — содержит список запущенных в данный момент процессов приложений COM+. С помощью команды Записать дамп контекстного меню необходимого приложения можно создать дамп памяти, в которой выполняется процесс, чтобы впоследствии проанализировать причины возникновения тех или иных ошибок.
- Координатор распределенных транзакций — хранит такие сведения о работе координатора распределенных транзакций, как список транзакций, в которых в данный момент участвует компьютер (раздел Список операций), а также список всех прошедших транзакций (раздел Статистика транзакций).

С помощью команды Свойства контекстного меню локальной службы координатора транзакций (раздел Локальная DTC) можно также настроить следующие параметры работы данной службы:

- путь к файлу журнала и его размер (вкладка Слежение);
- учетную запись пользователя, от имени которого будет запускаться служба DTC;
- другие параметры безопасности (вкладка Безопасность);
- настройки журнала трассировки работы службы (вкладка Ведение журнала).

Журнал трассировки содержит такие данные о транзакции, как ее код, время и сообщение о результате транзакции.

Все параметры трассировки координатора распределенных транзакций хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\MSDTC`.

Параметры безопасности же хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDTC\Security`.

Используя оснастку Службы компонентов, можно получить доступ к общим параметрам работы COM-компонентов. Для этого в контекстном меню раздела, определяющего компьютер, к которому вы подключены, нужно выбрать команду Свойства.

Настройка общих параметров работы COM-компонентов

После выбора команды Свойства в контекстном меню нужного раздела отобразится окно, представленное на рис. 5.21.

Окно содержит следующие вкладки.

- Общие — позволяет указать описание данного компьютера.
- Параметры — дает возможность указать время ожидания следующей транзакции, а также прокси-серверы, используемые для приложений COM (RSN).
- Набор протоколов — определяет протоколы, с которыми будет работать служба DCOM. По умолчанию используется протокол TCP\IP. С помощью кнопки Свойства можно указать список портов, которые при этом будут использоваться.
- Безопасность COM — с помощью данной вкладки можно изменить права доступа определенных пользователей к COM-компонентам, используемые по умолчанию. Вкладка состоит из двух полей: Права доступа и Разрешения на запуск и активацию. С помощью первого поля можно определить права доступа определенных пользователей к приложениям, а с помощью второго — изменить разрешения определенных пользователей на запуск и активацию объектов.

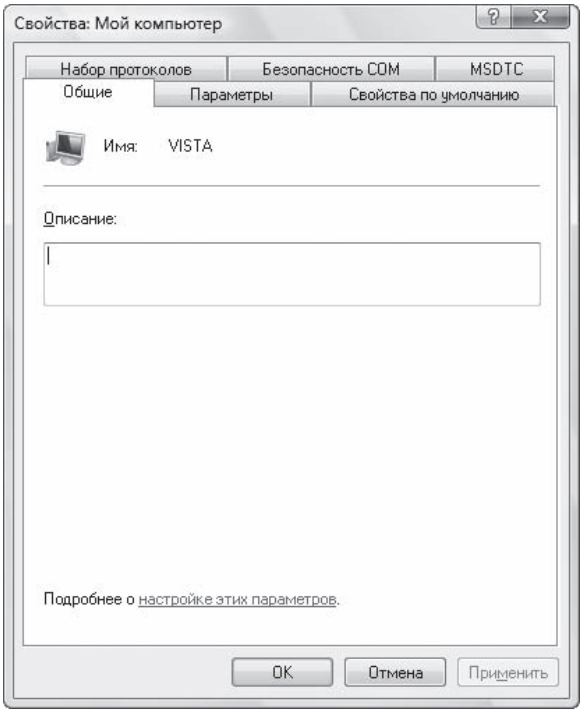


Рис. 5.21. Окно настройки работы COM-компонентов

Пользователи, у которых есть разрешение на активацию, могут работать с приложениями, только если у них есть разрешение на доступ. Поэтому таким пользователям нужно предоставить оба разрешения.

- MSDTC — благодаря этой вкладке можно определить, будет использоваться локальный координатор или удаленный.
- Свойства по умолчанию — с помощью данной вкладки можно отключить работу службы DCOM. После этого локальные приложения COM не смогут работать с приложениями COM удаленного компьютера, однако на взаимодействие локальных приложений COM это не окажет никакого влияния. Вы также можете включить или отключить службы доступа к компьютеру из Интернета с помощью COM.

Рассмотрим последнюю вкладку. Обе указанные возможности изменяют параметры ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole`. Отключение DCOM приводит к тому, что параметру строкового типа `EnableDCOM` присваивается значение `N`. Если же вы отключаете доступ к компьютеру из Интернета с помощью COM, то значение `N` присваивается параметру строкового типа `EnableDCOMHTTP`. При этом также включается использование прокси-сервера RPC (параметру типа `REG_DWORD Enabled` ветви `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\RpcProxy` присваивается значение `1`).

Кроме того, благодаря данной вкладке можно настроить параметры работы службы DCOM, для чего используются параметры поля Свойства связи DCOM по умолчанию. Например, с помощью данной вкладки можно настроить уровень проверки подлинности и уровень заимствования прав.

Уровень проверки прав, используемый по умолчанию, определяется в параметре REG_DWORD-типа LegacyAuthenticationLevel ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole. Возможны следующие уровни проверки подлинности.

- Отсутствует — проверка подлинности не выполняется. При этом значение параметра LegacyAuthenticationLevel равно 1.
- Подключиться — выполняется лишь при установке связи с удаленным приложением. Данный уровень подлинности используется по умолчанию. При этом значение параметра равно 2.
- Связь — проверка выполняется при каждом получении удаленным приложением запроса от клиента. При этом значение параметра равно 3.
- Пакет — выполняется для всех данных, получаемых удаленным приложением от клиента. При этом значение параметра равно 4.
- Целостности пакетов — проверка подлинности выполняется для всех данных, полученных как от клиента, так и от удаленного приложения. При этом значение параметра равно 5.
- Секретности пакетов — проверка выполняется для всех данных, полученных как от клиента, так и от удаленного приложения. Кроме того, все данные шифруются. При этом значение параметра равно 6.

Уровень заимствования прав, используемый по умолчанию, определяется в параметре REG_DWORD-типа LegacyImpersonationLevel ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole. Возможны следующие уровни заимствования прав.

- Аноним — скрывает истинные полномочия клиента, используя минимальные полномочия. При этом значение параметра LegacyImpersonationLevel равно 1.
- Определить — позволяет запросить полномочия клиента в случае необходимости. Уровень используется по умолчанию. При этом и последующих значениях заимствования прав становится активным флажок Повышенная безопасность для отслеживания ссылок. Если он установлен, то значение параметра строкового типа LegacySecureReferences, расположенного в ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole, равно Y. При этом значение параметра LegacyImpersonationLevel равно 2.
- Олицетворение — по умолчанию использует полномочия клиента. Если сервер находится на другом компьютере, то полномочия клиента распространяются

только на ресурсы, расположенные на компьютере сервера. При этом значение параметра `LegacyImpersonationLevel` равно `3`.

- Делегирование — позволяет использовать полномочия клиента не только запущенному приложению COM, но и другим приложениям, которые запустит данное приложение. Иначе говоря, полномочия клиента распространяются не только на ресурсы компьютера сервера, но и на другие компьютеры, на которых запущено приложение COM. При этом значение параметра `LegacyImpersonationLevel` равно `4`.

Настройка параметров работы приложений COM+

Чтобы настроить параметры работы определенного приложения COM+, нужно в его контекстном меню выбрать команду Свойства. После этого отобразится окно, представленное на рис. 5.22.

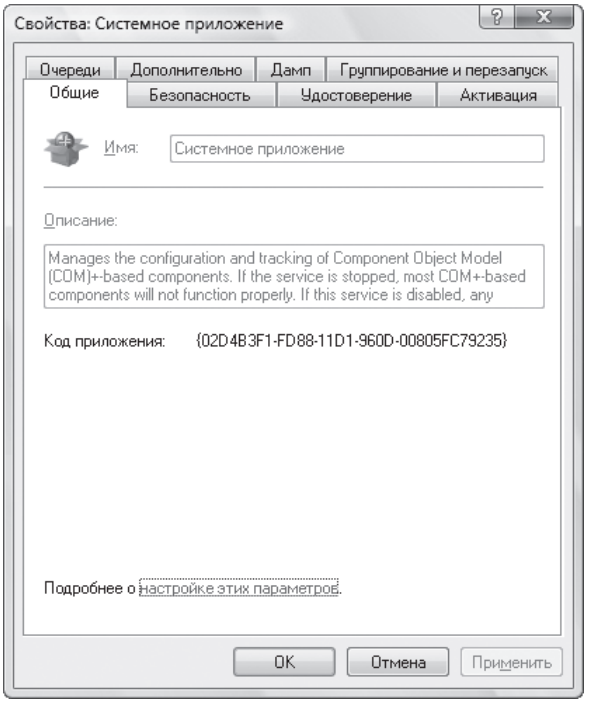


Рис. 5.22. Окно настройки параметров работы приложения COM+

Окно содержит следующие вкладки.

- Общие — содержит описание приложения COM+, а также его CLSID-номер.
- Безопасность — хранит настройки безопасности работы данного приложения COM+, среди которых встречаются уже знакомые вам по предыдущему окну уровень проверки подлинности и уровень заимствования прав.

- Удостоверение — определяет учетную запись пользователя, от имени которого запускается данное приложение COM+.
- Активация — указывает, является данное приложение библиотечным или серверным (к серверному приложению могут подключаться удаленные клиенты), а также использует ли оно протокол SOAP. Если протокол SOAP используется, то к приложению COM можно будет подключаться как к веб-службе XML. Доступ к веб-службам XML производится с помощью веб-сервера по протоколу HTTP или HTTPS.
- Очереди — определяет проверку подлинности сообщений очереди MSMQ, а также указывает, можно ли обратиться к данному приложению COM+ с помощью очередей MSMQ.

  Очереди компонентов позволяют клиенту обратиться к службе из серверного приложения COM+, даже если оно временно недоступно. В этом случае запрос клиента помещается в очередь и обрабатывается, когда серверное приложение станет доступным.
- Дополнительно — определяет дополнительные параметры работы приложения. Например, будет ли оно автоматически завершать свою работу после определенного времени бездействия, будет ли запускаться в отладочном режиме, будут ли запрещены операции удаления и изменения.
- Дамп — указывает путь к файлу дампа приложения COM+, который будет создаваться с помощью команды Записать дамп контекстного меню запущенного приложения COM+, а также максимальное количество хранимых дампов.
- Группирование и перезапуск — определяет размер группы приложения, а также параметры его перезапуска.

По умолчанию размер группы равен 1, что соответствует отключению службы группирования приложений COM+. Использование нескольких приложений в группе запускает службу группирования приложений, благодаря чему повышается надежность системы, так как процессы с одним потоком масштабируются на группу.

В качестве параметров автоматического перезапуска можно указать максимальное время работы службы, максимальное количество используемой памяти, максимальное время ожидания ответа от приложения, максимальное количество вызовов или активизаций. Автоматический перезапуск приложения COM+ позволяет повысить стабильность работы данного приложения. Все дело в том, что, как правило, чем дольше приложение COM+ работает, тем больше оперативной памяти оно использует или тем медленнее работает из-за возникших внутренних ошибок. Перезапуск же приложения позволяет освободить ненужную оперативную память, а также избавиться от возникших ошибок.

Настройка параметров безопасности приложений COM

Чтобы настроить параметры безопасности приложения COM, нужно выбрать команду Свойства контекстного меню нужного приложения. Напомню, что список зарегистрированных приложений COM содержится в разделе Настройка DCOM.

После этого отобразится окно, представленное на рис. 5.23.

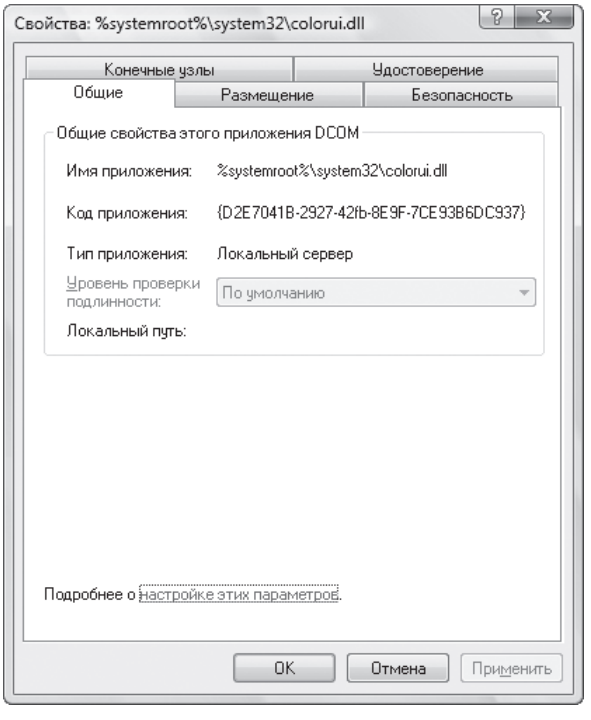


Рис. 5.23. Окно настройки приложения COM

Окно содержит следующие вкладки.

- Общие — отображает CLSID-номер приложения COM, а также его тип и имя. С ее помощью можно изменить уже знакомый вам уровень проверки удаленным сервером подлинности клиента.
- Размещение — с помощью данной вкладки можно определить, на каком компьютере будет запускаться приложение. Приложение COM может запускаться на локальном компьютере, на указанном удаленном компьютере или на компьютере, который содержит данные приложения.
- Безопасность — благодаря этой вкладке можно настроить разрешения определенных пользователей на запуск и активацию приложения, на доступ к нему, а также на настройку приложения. При этом можно отдельно настроить разрешения для приложения, расположенного на локальном компьютере, и для приложения, расположенного на удаленном компьютере.
- Конечные узлы — с помощью данной вкладки можно определить набор протоколов и конечных узлов, доступных для клиентов сервера DCOM.
- Удостоверение — определяет учетные записи пользователя, от имени которого будет запускаться приложение COM.

Расширения оснастки Службы компонентов

Как вы уже знаете, при загрузке оснасток с помощью окна Добавление и удаление оснастки, используя кнопку Изменить расширения, можно определить расширения оснастки, которые будет разрешено использовать (по умолчанию разрешено использовать все расширения). Оснастка Службы компонентов является одной из немногих, состоящих из расширений. Она состоит из двух расширений: Расширение страницы свойств DTC MMC и Оснастка DTC MMC. Если вы отключите первое расширение, то из окна настройки общих параметров работы COM-компонентов исчезнет вкладка MSDTC. Отключение же второго расширения приведет к невозможности работы с оснасткой Службы компонентов.

Диспетчер устройств

CLSID-номер оснастки: `{74246bfc-4c96-11d0-abef-0020af6b0b7a}`.

Библиотека: `devmgr.dll`.

Используется в стандартных консолях: `compmgmt.msc`, `devmgmt.msc`.

Оснастка позволяет просмотреть информацию об установленном на вашем компьютере оборудовании, список драйверов, которые им используются (или откатить недавно переустанавливаемые драйверы), а также список IRQ, которые назначены оборудованию.

ПРИМЕЧАНИЕ

Вызвать оснастку Диспетчер устройств можно и с помощью команды rundll32.exe devmgr.dll, DeviceManager_Execute.

Работа с данной оснасткой, как и ее интерфейс, совершенно не изменились. При добавлении оснастки вы можете выбрать компьютер, информацию которого она должна отображать. После этого оснастка Диспетчер устройств будет добавлена.

Стабильность и производительность

CLSID-номер оснастки: `{7478EF61-8C46-11d1-8D99-00A0C913CAD4}`.

Библиотека: `wdc.dll`.

Используется в стандартных консолях: `compmgmt.msc`, `perfmon.msc`. Оснастку также можно вызвать, если запустить программу `perfmon.exe`.

Оснастка Стабильность и производительность операционной системы Windows Vista, по сравнению с оснастками предыдущих версий операционной системы Windows, существенно преобразилась (рис. 5.24).

Теперь она состоит из подразделов Средства наблюдения, Группы сборщиков данных и Отчеты, не говоря уже об основном окне оснастки.

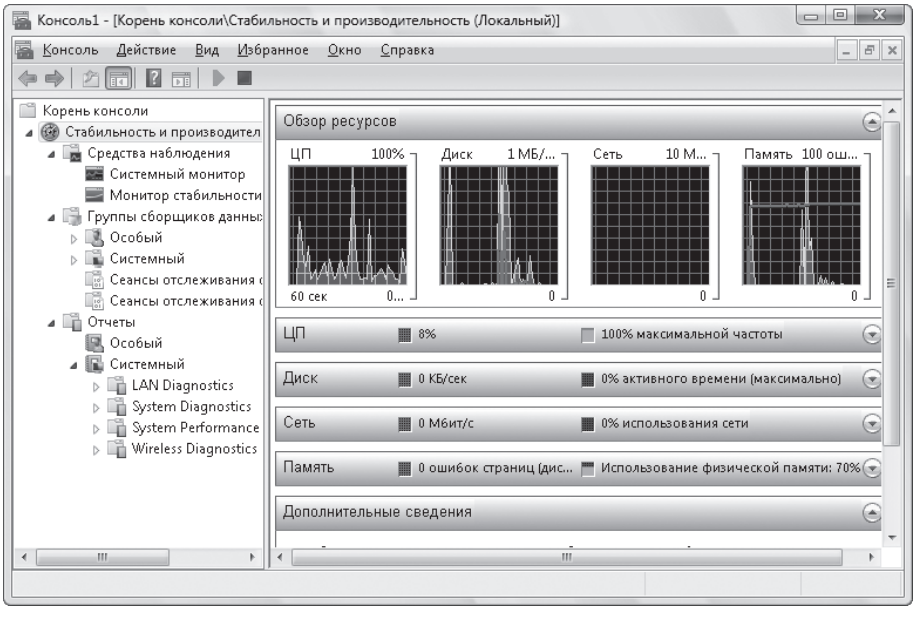


Рис. 5.24. Основное окно оснастки Стабильность и производительность

ПРИМЕЧАНИЕ

Сведения о работе компонента Системный монитор заносятся в журнал Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Reliability-Analysis-Engine.

Основное окно оснастки

Основное окно оснастки отображается при переходе к разделу Стабильность и производительность. Оно содержит следующие элементы.

- Обзор ресурсов — отображает четыре окна мониторинга состояния системы.
  - Первое окно показывает состояние работы процессора. В нем зеленым цветом отображается загруженность процессора, а синим — текущая частота процессора (если процессор способен автоматически понижать частоту своей работы). Если вы щелкнете кнопкой мыши в данном окне, то раскроется список ЦП.
  - Второе окно показывает состояние работы диска. В нем зеленым цветом отображается количество считываемых за секунду килобайт данных (на графике максимальной величиной является 100 Кбайт/с), а синим — процент активного времени. Если вы щелкнете кнопкой мыши в данном окне, то раскроется список Диск.
  - Третье окно показывает состояние работы сетевых компонентов. В нем зеленым цветом отображается активность сетевого интерфейса (на графике максимальной величиной является 10 Мбайт/с), а синим — процент

утилизации сети (чем выше процент утилизации при работе сети, тем более оптимальной считается ее работа). Если вы щелкнете кнопкой мыши в данном окне, то раскроется список Сеть.

- Четвертое окно показывает состояние работы оперативной памяти. В нем зеленым цветом отображается количество ошибок доступа к оперативной памяти в секунду (максимум 100 ошибок в секунду, большое количество ошибок говорит о том, что необходимо увеличить объем оперативной памяти компьютера, так как слишком часто операционная система обращается к файлу подкачки), а синим — процент использования оперативной памяти. Если вы щелкнете кнопкой мыши в данном окне, то раскроется список Память.

- ЦП — после раскрытия этого списка перед вами отобразится перечень процессов, которые загружают процессор в данный момент. Выводится их название, описание, PID процесса, количество созданных ими потоков, текущий процент загрузки процессора, а также среднее значение загрузки процессора данным приложением.
- Диск — раскрыв этот список, вы увидите перечень файлов, которые в данный момент записываются на диск или считываются с него. Отображается путь к файлу, название процесса, который работает с файлом, PID-процесса, работающего с файлом, а также количество байт, считываемых или записываемых в данный момент.
- Сеть — после раскрытия данного списка перед вами отобразится перечень процессов, работающих с сетевыми интерфейсами. Выводится название процесса, его PID, IP-адрес, с которым установлено соединение, количество отправленных и полученных байт/мин, а также общее количество переданных интерфейсом байт/мин.
- Память — раскрыв этот список, вы увидите перечень процессов, которые в данный момент работают с оперативной памятью. Выводится их название, PID, количество ошибок доступа к оперативной памяти в минуту, связанных с невозможностью найти требуемые данные (потому что они были сброшены в файл подкачки), а также количество общей, частной и рабочей оперативной памяти (сумма общей и частной), которую использует процесс.
- Дополнительные сведения — содержит набор ссылок, с помощью которых можно прочитать больше о возможностях оснастки Стабильность и производительность.
  - Справка по предоставлению ресурсов — отображает справку по основному окну оснастки Стабильность и производительность.
  - Справка системного монитора — выводит общую информацию об оснастке.
  - Справка по сбору данных — отображает справку о работе с подразделом Группы сборщиков данных оснастки Стабильность и производительность.
  - Создание группы сборщиков данных и диагностического отчета — выводит информацию о том, как можно создавать объекты, собирающие сведения о работе определенного системного компонента.
  - Наблюдение за работой системы с помощью системного монитора — отображает информацию о мониторинге системной активности с помощью элементов данной оснастки.

- Планирование и управление данными — выводит информацию о работе с объектами, собирающими сведения от определенного системного компонента.

Обратите также внимание на две последние кнопки панели инструментов оснастки. С их помощью можно остановить и заново запустить мониторинг производительности системы в реальном времени. Это может быть необходимо как для повышения производительности работы с оснасткой, так и для более детального ознакомления с запущенными в какой-то момент времени процессами, работающими с системой. После остановки мониторинга список процессов того или иного элемента основного окна оснастки не очищается, поэтому можно спокойно их просмотреть, не боясь, что через секунду процесс исчезнет из списка.

Подраздел Средства наблюдения

Данный подраздел представляет собой средство для мониторинга работы счетчиков производительности компьютера в реальном времени. Он состоит из подразделов Системный монитор и Монитор стабильности. Подраздел Системный монитор не является чем-то новым для операционных систем семейства Windows, поэтому его мы рассмотрим лишь поверхностно. А работу с подразделом Монитор стабильности мы вообще не будем пока рассматривать, так как он является отдельной оснасткой консоли управления Microsoft и добавляется в оснастку Стабильность и производительность как расширение.

Подраздел Стабильность и производительность представляет собой ActiveX-объект, который может в реальном времени отображать работу запущенных счетчиков производительности компьютера (рис. 5.25).

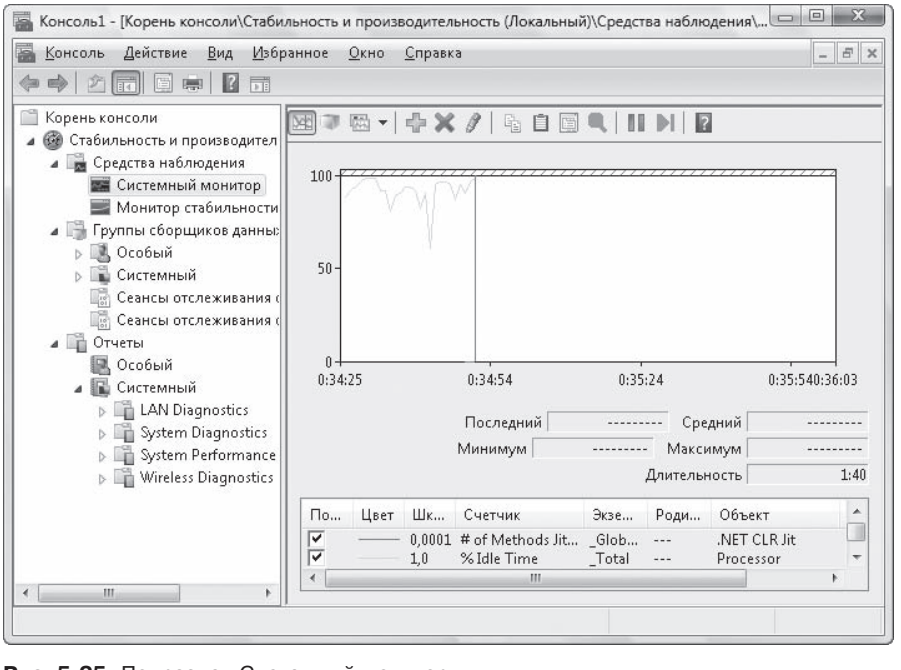


Рис. 5.25. Подраздел Системный монитор

Работа со счетчиками производительности. По умолчанию не запущен ни один счетчик. Чтобы запустить счетчик, нужно в контекстном меню окна выбрать команду Добавить счетчики. После этого отобразится окно добавления счетчиков производительности, представленное на рис. 5.26. Оно содержит следующие элементы.

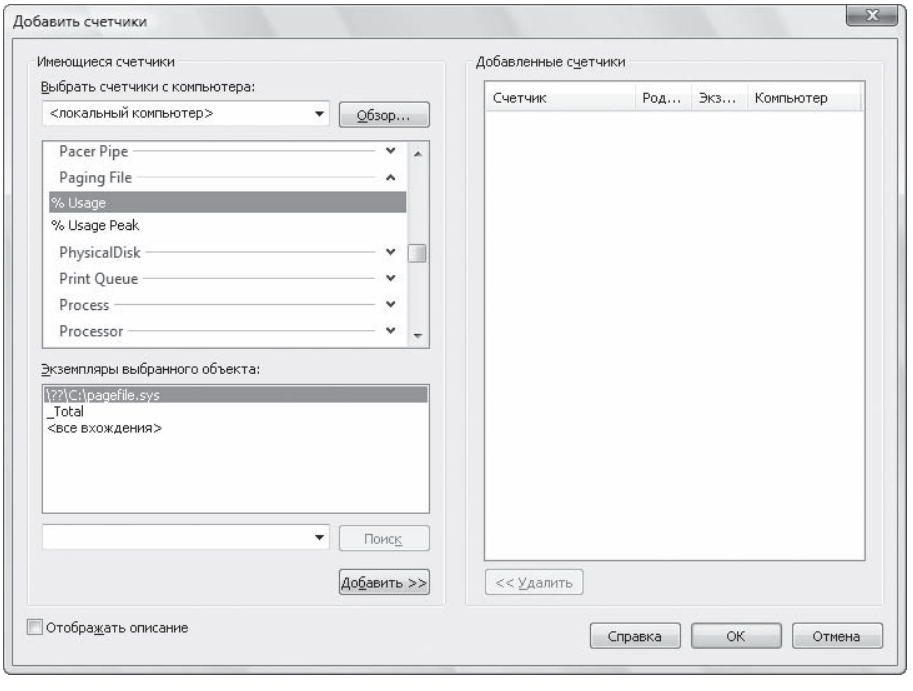


Рис. 5.26. Добавление счетчиков производительности

- Поле выбора компьютера, счетчики производительности которого будут загружены в оснастку.
- Список счетчиков производительности, доступных на данном компьютере. Сначала нужно дважды щелкнуть кнопкой мыши на объекте, чтобы отобразились доступные для него счетчики производительности, после чего выбрать нужный счетчик и нажать кнопку Добавить>>. Кроме того, если вы установите флажок Отображать описание, то будет показано описание счетчика производительности.

  Как и раньше, вам доступны счетчики производительности таких популярных объектов, как процессор, оперативная память, файл подкачки, сетевые интерфейсы, протоколы IP, TCP, UDP и т. д. Кроме того, в операционной системе Windows Vista появились следующие новые объекты (это, конечно, не все).

  - IPv6 — содержит счетчики для регистрации количества переданных, полученных, потерянных и т. д. пакетов протокола IPv6.
  - TCPv6 — включает в себя счетчики для регистрации количества переданных, полученных, потерянных и т. д. пакетов протокола TCPv6, а также для регистрации количества активных, пассивных, завершенных и т. д. сеансов, созданных с помощью данного протокола.

- UDPv6 — содержит счетчики для регистрации количества переданных, полученных, потерянных и т. д. дейтаграмм протокола UDPv6.
- ICMPv6 — включает в себя счетчики для регистрации количества переданных, полученных, потерянных и т. д. сообщений протокола ICMPv6.
- Статистика общесистемной безопасности — содержит счетчики для получения таких сведений, как количество процессов, зарегистрированных с помощью NTLM или Kerberos аутентификации за одну секунду, количество посланных запросов KDC TGS за одну секунду, количество созданных SSL соединений за последнюю секунду и т. д.
- Статистика безопасности по процессу — включает в себя счетчики для получения сведений о количестве потоков или привилегий у определенного работающего в данный момент процесса.
- Windows Workflow Foundation — содержит множество счетчиков для наблюдения за компонентом операционной системы Windows Workflow Foundation.
- WFP, WFPv4 и WFPv6 — включает в себя множество счетчиков для наблюдения за провайдером Windows Filtering Platform.
- iSCSI Initiator Instance — содержит счетчики для получения сведений о работе сессий iSCSI.

- Поле Экземпляры выбранного объекта позволяет указать, для какого экземпляра объекта загружается счетчик производительности (если существует несколько экземпляров объекта, например несколько процессоров). При этом с помощью поля поиска вы можете быстро найти нужный экземпляр, если их много.
- Поле Добавленные счетчики отображает список уже добавленных счетчиков производительности.

После того как вы добавите нужные счетчики производительности и закроете окно Добавить счетчики, они будут добавлены в окно подраздела Системный монитор. С помощью команды Свойства контекстного меню окна подраздела, как и раньше, можно изменить такие параметры отображения счетчиков, как их цвет, толщина линий на графике, масштаб графика и многое другое.

Наблюдать за работой счетчиков производительности в реальном времени довольно удобно, но в некоторых случаях у вас может не быть на это времени. В этом случае существует возможность записи состояния выбранных вами счетчиков производительности в файл. Для этого достаточно загрузить нужные счетчики производительности, как мы сделали это раньше, а потом выбрать команду Создать ▸ Группа сборщиков данных контекстного меню подраздела Системный монитор (для работы данной возможности необходимо, чтобы служба Планировщик заданий была запущена). После этого перед вами отобразится мастер создания объекта, собирающего сведения о работе запущенных счетчиков производительности. Он предложит вам указать имя нового объекта, путь к файлу, в котором будут храниться данные счетчика производительности, а также учетную запись, от имени которой будет запущен объект, и будет ли объект запущен сразу после своего создания.

После этого объект будет создан и вы сможете увидеть его в подразделах User Defined разделов Группы сборщиков данных и Отчеты оснастки Стабильность и производительность. Ну, а как работать с этими подразделами, вы узнаете из следующих разделов этой главы.

Основные счетчики производительности. За то время, как в операционных системах семейства Windows появилось такое понятие, как счетчики производительности, пользователями этой операционной системы были написаны целые статьи о том, как работать со счетчиками производительности и показания каких счетчиков наиболее интересны рядовому пользователю. Ниже будут перечислены несколько счетчиков производительности, показания которых проверяются чаще всего.

Первым набором счетчиков, на которые обращают внимание при диагностике компьютера, являются счетчики, следящие за работой жестких дисков. С их помощью можно узнать не только о том, нужно ли покупать более скоростной жесткий диск, но и о том, достаточно ли оперативной памяти установлено в компьютере.

- \Физический диск(_Total)\Средняя длина очереди записи на диск — определяет количество процессов, находящихся в очереди на запись информации на физический диск. Если значение этого счетчика часто превышает 2, то пора задуматься о покупке более скоростного диска.
- \Физический диск(_Total)\% активности диска — определяет процент времени, в течение которого жесткий диск выполняет операции чтения и записи. Слишком большое значение данного счетчика может говорить как о необходимости приобретения более скоростного диска, так и о необходимости покупки дополнительного объема оперативной памяти.

С помощью счетчиков производительности можно также следить за использованием оперативной памяти. Основным объектом для этого является объект Память.

- \Память\Байт свободной памяти и обнуленных страниц памяти — определяет количество оперативной памяти в байтах, доступное операционной системе. Значение данного счетчика больше 4 Кбайт может говорить о необходимости приобретения дополнительной оперативной памяти.
- \Память\Обмен страниц/сек — указывает количество перемещений между файлом подкачки и оперативной памятью в секунду. Постоянное большое значение данного счетчика говорит о необходимости приобретения дополнительного объема оперативной памяти.
- \Память\ошибок страницы/сек — определяет количество ошибок доступа к оперативной памяти в секунду, при которых оказывается, что необходимые данные находятся не в оперативной памяти, а в файле подкачки. Постоянное большое значение данного счетчика говорит о необходимости приобретения дополнительного объема оперативной памяти.
- \Физический диск(_Total)\Средний размер одного обмена с диском (байт) — указывает средний размер файлов, перемещаемых между жестким диском и оперативной памятью во время операции чтения и записи. Постоянное слишком

большое значение данного счетчика (например, больше 4 Кбайт) говорит о том, что операционная система слишком часто обращается к файлу подкачки. Следовательно, нужно увеличить объем оперативной памяти.

И конечно, не стоит забывать о счетчиках производительности, следящих за использованием процессора.

- \Процессор(_Total)\% загруженности процессора — определяет процентное соотношение времени, которое процессор занят обработкой команд потоков. Постоянное слишком большое значение этого счетчика (больше 80 %) говорит о том, что необходимо приобретать более мощный процессор.
- \Процессор(_Total)\Прерываний/сек — счетчик определяет среднее количество прерываний, которые процессор обрабатывает в секунду. Слишком большое значение этого счетчика может говорить о том, что в операционной системе существуют проблемы функционирования устройств, требующих аппаратные прерывания.
- \Система\Длина очереди процессора — определяет количество потоков, находящихся в очереди доступа к процессору. Если значение данного счетчика больше одного (для однопроцессорных систем), значит, пора приобретать более быстрый процессор.

В некоторых случаях бывает необходимо проследить и за работой сетевой карты компьютера. Для этого предназначен счетчик \Сетевой интерфейс(<имя сетевой карты>)\Всего байт/сек. Он определяет общее количество входящего и исходящего трафика, проходящего через данную сетевую карту. Постоянное слишком большое значение данного счетчика говорит о необходимости приобретения более скоростной сетевой карты либо установки дополнительной сетевой карты.

Программы для работы со счетчиками производительности. Как и в предыдущих версиях, в стандартную поставку Windows Vista входит несколько программ командой строки, предназначенных для работы со счетчиками производительности. Некоторые из этих программ были дополнены новыми параметрами, остальные же остались без изменения.

Первой программой, которую мы рассмотрим, будет программа `lodctr.exe`, предназначенная для обновления или архивирования информации о счетчиках производительности, зарегистрированных в операционной системе. Далее описаны несколько примеров использования данной программы.

- `lodctr.exe <имя INI-файла>` — позволяет переустановить счетчики производительности на основе данных, определенных в соответствующем INI-файле. Любой INI-файл, содержащий информацию о счетчиках производительности, хранит строку `drivername`, определенную в разделе `[info]`. Например, в каталоге `%systemroot%\system32` операционной системы Windows Vista находятся следующие INI-файлы, определяющие счетчики производительности: `OUTLPERF.ini` и `pacerprf.ini`. А в файле `PerfStringBackup.ini` хранится архивная копия всех счетчиков производительности и их описания.

- `/S:<путь к файлу и его имя>` — сохраняет информацию о счетчиках производительности и их описании в файл. Потом с помощью параметра `/R:<путь к файлу и его имя>` данной программы можно восстановить настройки счетчиков из созданного ранее файла. Также можно воспользоваться параметром `/R` без дополнений для восстановления стандартного списка счетчиков производительности.

  С помощью этого параметра создается обычный текстовый файл, поэтому его удобно использовать для ознакомления с описанием счетчиков производительности.

- `/D:<имя службы>` — отключает счетчики производительности, определяемые данной службой. Команда устанавливает значение параметра `REG_DWORD`-типа `Disable Performance Counters`, расположенного в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<служба или драйвер>\Performance`, равным `1`.

  Чтобы включить отключенные ранее счетчики производительности, нужно воспользоваться параметром `/E:<имя службы>`. С помощью параметра `/T:<имя службы>` можно установить счетчики производительности службы. А используя параметр `/Q:<имя службы>`, можно отобразить информацию о настройках счетчиков производительности соответствующей службы.

  Все описанные выше параметры являются новыми параметрами операционной системы Windows Vista. В Windows XP они не поддерживались.

- `/M:<XML-файл>` — устанавливает провайдера счетчиков производительности Windows Vista на основе настроек, определенных в XML-файле.

Еще одной программой, которую мы рассмотрим в данном разделе книги, будет программа командной строки `unlodctr.exe`. С ее помощью можно удалить из реестра сведения о счетчиках производительности, добавляемых конкретным драйвером, файлом манифеста или провайдером. Далее приведены примеры использования данной программы. Каждая команда позволяет удалить из реестра счетчики производительности:

- `unlodctr.exe <драйвер>` — добавляемые указанным драйвером;
- `unlodctr.exe /m:<файл манифеста>` — описанные в указанном файле манифеста;
- `unlodctr.exe /g:<GUID-номер провайдера>` — принадлежащие провайдеру, имеющему соответствующий GUID-номер;
- `unlodctr.exe /p:<имя провайдера>` — принадлежащие конкретному провайдеру.

Параметры реестра. Параметры работы счетчиков производительности хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`. С помощью параметров и подразделов данной ветви реестра можно как просмотреть сам список счетчиков производительности и их

описания, так и запретить использование счетчиков. Данная ветвь реестра и ее подразделы могут включать в себя следующие параметры.

- `Disable Performance Counters` — если значение данного параметра `REG_DWORD`-типа равно `1`, то вы не сможете получить доступ к счетчикам производительности локального компьютера.
- `TotalInstanceName` — этот параметр строкового типа хранит название экземпляра `Total`.
- `Updating` — если значение данного параметра `REG_DWORD`-типа равно `0`, то вы не сможете получить доступ к счетчикам производительности локального компьютера.
- `Counter` — этот параметр типа `REG_MULTI_SZ` содержит список всех счетчиков, доступных в операционной системе. Он хранится в подразделе `009` указанной ветви реестра.
- `Help` — параметр типа `REG_MULTI_SZ` содержит описание всех счетчиков, доступных в операционной системе. Он хранится в подразделе `009` данной ветви реестра.

Сами же параметры работы определенного счетчика производительности содержатся в параметрах ветвей реестра следующего формата: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<служба или драйвер>\Performance`.

- `First Counter` и `Last Counter` — эти параметры `REG_DWORD`-типа определяют номера счетчиков, настройки которых хранятся в данной ветви реестра.
- `First Help` и `Last Help` — параметры `REG_DWORD`-типа, определяют номера описаний счетчиков, настройки которых хранятся в данной ветви реестра.
- `IsMultiInstance` — если значение данного параметра `REG_DWORD`-типа равно `1`, то счетчики производительности, определяемые в ветви реестра, поддерживают отслеживание работы нескольких экземпляров.
- `Library` — этот параметр строкового типа содержит название библиотеки, в которой описаны функции работы с данными счетчиками.
- `Open Timeout` — параметр `REG_DWORD`-типа, определяет максимальное время ожидания загрузки счетчиков, описанных в данной ветви реестра.

Подраздел Группы сборщиков данных

С помощью данного подраздела можно создать набор данных, собирающих сведения о работе определенного системного компонента (для работы этой возможности необходимо, чтобы была запущена служба Планировщик заданий). Рассмотрим подразделы, которые включает в себя подраздел Группы сборщиков данных.

Первый подраздел называется Особый. Как вы знаете, именно в него помещаются наборы данных, созданные с помощью контекстного меню подраздела Системный монитор. Однако с помощью команды Создать ▸ Группа сборщиков данных контекстного меню данного подраздела вы самостоятельно можете создавать пользовательские

наборы данных. После выбора данной команды перед вами отобразится мастер создания набора данных, схожий с мастером подраздела Системный монитор. Как и в предыдущем случае, вы можете указать имя создаваемого набора данных, путь к файлу, в котором будут храниться данные данного набора, а также учетную запись, от имени которой будут запущены объекты создаваемого набора данных, и указать, будет ли набор данных запущен сразу же после своего создания.

Однако также данный мастер предложит вам указать, на основе каких данных будет создан набор. Можно установить переключатель в одно из двух положений.

- Создать из шаблона — позволяет создать набор данных на основе следующих, доступных по умолчанию, шаблонов.
  - Основной — создает объект, собирающий сведения, журнал трассировки, а также объект конфигурации.

    Объект собирает сведения от всех счетчиков производительности объекта Процессор.

    Журнал производительности использует для своей работы провайдера Windows Kernel Trace.

    Объект конфигурации следит за параметрами ветви `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion`.
  - System Diagnostics — применяется при выполнении диагностики работы операционной системы. Этот шаблон создает множество журналов трассировки, объектов конфигурации и следит за состоянием счетчиков производительности объектов Процессы, Процессор, Физический диск, Память, Система, Сервер, а также объектов, определяющих работу сетевых протоколов, и множества других объектов.

    System Performance — используется при проверке производительности компьютера и поиске слабых мест в его конфигурации. Этот шаблон следит за состоянием счетчиков производительности тех же объектов, что и шаблон System Diagnostics.
- Создать вручную — позволяет самостоятельно указать, что будет создаваться. Можно создать объект оповещения, который будет активизироваться при возникновении какого-нибудь события, или объект, собирающий сведения в файл журнала (при этом можно указать, какие объекты будут в него входить: объект, собирающий сведения от счетчиков производительности, журнал трассировки или объект конфигурации).

  Если вы выбрали создание объекта, собирающего сведения в файл журнала, то следующим шагом мастера будет настройка этого объекта.
  - Добавление счетчиков производительности и указание интервала сбора сведений от них, если вы указали, что объект, собирающий сведения в файл журнала, будет, в свою очередь, содержать объект, собирающий сведения от счетчиков производительности. Добавление счетчиков основано на окне Добавить счетчики, которое мы уже рассматривали при описании подраздела Системный монитор данной оснастки.

- Выбор провайдеров и настройка их свойств, если вы указали, что объект, собирающий сведения в файл журнала, будет содержать в себе журнал трассировки. Более подробно журналы трассировки будут описаны при рассказе о подразделе Сеансы отслеживания событий данной оснастки.
- Выбор ветвей реестра, если вы указали, что объект, собирающий сведения в файл журнала, будет, в свою очередь, включать в себя объект конфигурации.

Если же вы выбрали создание объекта оповещения, то мастер предложит вам выбрать счетчики производительности, а также указать порог их значения, при котором будет выполняться оповещение администратора.

Теперь рассмотрим параметры настройки самих наборов данных, создаваемых с помощью данного подраздела оснастки. Независимо от того, каким способом вы создали набор данных, он будет иметь одни и те же параметры настройки. Точнее, будут создаваться копии одного и того же набора данных, так как набор данных представляет собой простой контейнер, который может хранить, например, объекты, собирающие сведения от счетчиков производительности, журналы трассировки, объекты конфигурации и объекты оповещения. Основным способом настройки параметров работы набора данных является команда Свойства контекстного меню объекта. После ее выбора отобразится окно, состоящее из следующих вкладок.

- Общие — позволяет изменить описание и ключевые слова набора данных, а также учетную запись пользователя, от имени которого будет запускаться данный набор данных.
- Папка — дает возможность изменить путь к каталогу, в котором будут храниться файлы, генерируемые объектами, собирающими сведения от счетчиков производительности, а также префикс, который будет добавляться к каждому новому файлу, чтобы отличать его от предыдущих.
- Безопасность — позволяет настроить разрешения доступа к данному набору данных для различных учетных записей.
- Расписание — дает возможность создать задание, которое будет запускать в определенное время и в определенный день недели указаный набор данных.
- Условие остановки — позволяет определить условия, при которых работа запущенного набора данных будет остановлена или он будет перезапущен. Условием может быть истекшее время работы набора данных или достижение определенного размера файла журнала, создаваемого набором данных.
- Задача — дает возможность указать команду (программу или сценарий), которая будет выполняться при остановке набора данных.

Можно также определить настройки очистки каталогов, которые создаются набором данных. Для этого в его контекстном меню нужно выбрать команду Диспетчер данных, после чего отобразится окно, состоящее из следующих вкладок.

- Диспетчер данных — определяет условия, при которых будет происходить очистка каталога, содержащего файлы набора данных. Ее условно можно разделить

на две области. В первой определяются сами условия, а во второй указывается, будет ли создаваться файл журнала, описывающий процесс удаления.

В первом поле расположены следующие элементы.

- Флажок Минимум места на диске и поле под ним позволяют указать оставшийся объем свободного места на диске, при котором каталог набора данных будет очищаться.
- Флажок Максимум папок и поле под ним позволяют указать количество вложенных в каталог набора данных папок, при котором каталог набора данных будет очищаться.
- Раскрывающийся список Политика ресурсов позволяет выбрать, какие файлы будут удаляться в первую очередь: самые объемные или созданные раньше всех.
- Установка флажка Применить политику перед запуском группы сборщиков данных приводит к тому, что при каждом запуске набора данных будет проверяться каталог набора данных с целью определения, нужно удалять его содержимое или нет.
- Флажок Максимальный размер корневого пути и поле под ним позволяют указать максимальный размер каталога набора данных.

- Действия — позволяет создать действия, которые будут происходить при указанных условиях. При создании действия можно определить, когда оно будет возникать: при достижении каталогом определенного размера или при истечении определенного количества дней. Можно также определить само действие, которое будет происходить. Доступны следующие действия:
  - перемещение созданного CAB-файла в другой каталог;
  - создание CAB-файла на основе содержимого каталога набора данных;
  - удаление содержимого каталога набора данных;
  - удаление созданного CAB-файла;
  - удаление рапортов.
- Правила — дает возможность импортировать или экспортировать набор правил для работы с набором данных.

Вы также можете добавить в набор данных дополнительные объекты. Для этого служит команда Создать ▸ Сборщик данных контекстного меню набора данных.

После выбора данной команды отобразится окно мастера, в котором нужно выбрать тип объекта, установив переключатель в нужное положение: объект, собирающий сведения от счетчиков производительности (Счетчик производительности), журнал трассировки (Данные отслеживания событий), объект конфигурации (Сведения о конфигурации системы) или объект оповещения (Оповещение счетчика производительности). После этого нужно будет настроить выбранный объект. Настройка объектов ничем не отличается от той, которая выполнялась при создании набора данных.

После того как выбранный объект будет создан, его можно дополнительно настроить с помощью окна, отображаемого при выборе команды Свойства в контекстном меню созданного объекта. В зависимости от типа объекта с помощью данного окна можно настроить следующие параметры.

- Счетчик производительности — позволяет добавить новые счетчики производительности или удалить уже существующие. Можно также определить интервал опроса счетчиков производительности и количество опросов, после которого они будут прекращены. Кроме того, можно указать тип создаваемого файла, путь к нему и способ перезаписи файлов. Возможны следующие типы файлов.
  - Текстовый файл (разделитель запятая) — записывает данные счетчиков в обычный текстовый файл, разделяя их запятыми. Этот файл можно просматривать с помощью таких программ, как Microsoft Excel или Microsoft Word или любого другого текстового редактора.
  - Текстовый файл (разделитель табуляция) — записывает данные счетчиков в обычный текстовый файл, разделяя их табуляцией. Этот файл можно просматривать с помощью таких программ, как Microsoft Excel или Microsoft Word или любого другого текстового редактора.
  - SQL — позволяет заносить показания счетчиков в общую базу данных SQL. При этом нужно также указать путь к базе данных.
  - Двоичный — используется по умолчанию и обеспечивает наиболее быстрый способ создания и просмотра файлов журналов, если их необходимо просматривать только с помощью данной оснастки.
- Данные отслеживания событий — настройки окна для данного объекта описаны далее при описании подраздела Сеансы отслеживания событий оснастки Стабильность и производительность.
- Сведения о конфигурации системы — состоит из следующих вкладок:
  - Реестр — позволяет добавить или удалить ветви реестра;
  - Пути управления — дает возможность создать или удалить запросы к репозитарию CIM;
  - Захват файла — позволяет добавить или удалить пути к файлам;
  - Сбор данных о состоянии — дает возможность ввести запрос;
  - Файл — с помощью этой вкладки можно указать название файла, который будет создаваться данным объектом, а также способ его перезаписи.
- Оповещение счетчика производительности — состоит из следующих вкладок:
  - Alerts — позволяет добавить или удалить счетчики производительности, указать их порог, а также интервал, с которым будет происходить их опрос;
  - Alert Action — дает возможность определить, будут ли заноситься оповещения в стандартный системный журнал Приложение оснастки Просмотр событий;

- Alert Task — позволяет указать команду, которая будет выполняться при остановке данного объекта.

После того как вы полностью настроите набор данных и его содержимое, его нужно запустить. Для этого служит команда Пуск контекстного меню набора данных. После запуска набора данных начнется запись сведений в файл журнала. Как только вы остановите работу набора данных (с помощью команды Стоп контекстного меню набора данных), файл его работы будет создан, и вы сможете просмотреть работу счетчиков производительности в подразделе Отчеты данной оснастки.

Следующий подраздел называется Системный. Он включает в себя список системных наборов данных. С помощью команды Создать ▸ Группа сборщиков данных контекстного меню данного подраздела можно создать системный набор данных.

Работа с наборами данных этого подраздела ничем не отличается от работы с наборами данных подраздела оснастки Особый. Однако вы не сможете отредактировать параметры работы системных наборов данных, хотя всегда сможете запустить и остановить их.

По умолчанию в данном подразделе хранятся следующие наборы данных.

- LAN Diagnostics (Диагностика локальной сети) — определяет набор счетчиков производительности, следящих за работой сетевых протоколов, а также объекты трассировки, следящие за работой сетевых служб, и объекты конфигурации, следящие за изменением параметров реестра, влияющих на работу сети.
- System Diagnostics (Диагностика системы) — указывает набор объектов, с помощью которых можно наблюдать за работой основных компонентов компьютера и операционной системы.
- System Performance (Производительность системы) — определяет набор счетчиков производительности, следящих за работой основных компонентов компьютера и позволяющих определить слабые места в конфигурации компьютера.
- Wireless Diagnostics (Диагностика беспроводной сети) — указывает набор счетчиков производительности, следящих за работой сетевых протоколов, а также объекты трассировки, следящие за работой служб доступа к беспроводной сети, и объекты конфигурации, следящие за изменением параметров реестра, влияющих на работу беспроводной сети.

Следующим рассмотрим подраздел Сеансы отслеживания событий. Он содержит сведения о запущенных в данный момент журналах трассировки, а также позволяет создать новые журналы.

С помощью данного подраздела вы можете остановить работу данных журналов трассировки (но при следующей перезагрузке они будут запущены снова), для чего достаточно в контекстном меню журнала выбрать команду Стоп. Вы также можете просмотреть или изменить параметры работы журнала трассировки. Для этого в контекстном меню журнала нужно выбрать команду Свойства, после чего отобразится окно свойств журнала (рис. 5.27), содержащее следующие вкладки.

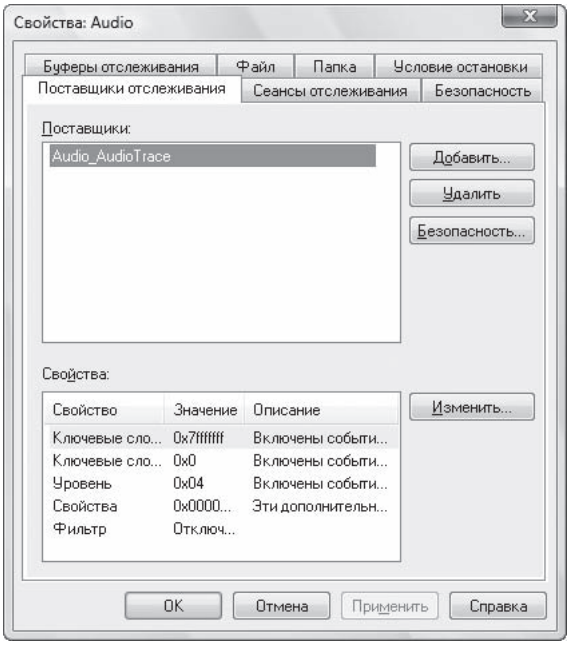


Рис. 5.27. Свойства журнала трассировки

- Поставщики отслеживания — с помощью этой вкладки вы можете удалить либо добавить провайдеров, которые будут управлять работой данного журнала трассировки и собирать сведения о соответствующих компонентах операционной системы (провайдер представляет собой библиотеку, которая содержит функции по слежению за работой определенного компонента системы).

  Используя эту вкладку, вы также можете настроить параметры работы провайдера. Для этого достаточно выбрать провайдера из верхнего поля, соответствующее свойство из нижнего поля, а потом нажать кнопку Изменить.

- Сеансы отслеживания — позволяет изменить параметры сессии данного журнала трассировки. Например, можно указать, куда будут помещаться данные журнала трассировки (в файл, буфер или будут обрабатываться в реальном времени).

- Безопасность — дает возможность настроить разрешения доступа к журналу для учетных записей пользователей.

- Буферы отслеживания — позволяет настроить буфер, в который будут помещаться данные журнала трассировки перед записью в файл. Можно указать минимальный, максимальный и текущий размер буфера, а также интервал записи данных из буфера в файл.

- Файл — дает возможность настроить такие параметры файла журнала трассировки, как его имя, а также тип записи в файл (будут ли данные добавляться в конец файла или будут перезаписывать уже существующие данные).

- Папка — позволяет изменить каталог, в котором будет храниться файл журнала трассировки.

- Условие остановки — дает возможность указать максимальный размер файла трассировки, а также время работы журнала трассировки, после истечения которого он будет автоматически остановлен.

Если же данный журнал трассировки вам не нужен, то вы всегда сможете его удалить с помощью команды Удалить контекстного меню журнала. Только перед этим не забудьте остановить работу журнала трассировки.

Вы также можете создать свой журнал трассировки. Для этого нужно воспользоваться командой Создать ▸ Группа сборщиков данных контекстного меню подраздела Сеансы отслеживания событий, после чего запустится мастер создания журнала трассировки. Работа с данным мастером аналогична работе с рассмотренными ранее мастерами.

Рассмотрим подраздел Сеансы отслеживания событий запуска. Он содержит сведения о журналах трассировки, автоматически запускаемых при входе пользователя в систему.

Работа с ним практически ничем не отличается от работы с рассмотренным выше подразделом Сеансы отслеживания событий. Однако процесс отключения журналов трассировки данного подраздела отличается от процесса отключения журналов трассировки подраздела Сеансы отслеживания событий. Чтобы отключить журнал трассировки, нужно отобразить его окно Свойства, после чего перейти на вкладку Сеансы отслеживания и снять флажок Разрешено. Это приведет к полному отключению журнала трассировки — журнал останется отключенным даже после перезагрузки компьютера.

Обратите также внимание на команду Запустить как сеанс отслеживания событий контекстного меню элемента данного подраздела. С ее помощью можно запустить журнал трассировки. После запуска журнала трассировки он отобразится в подразделе Сеансы отслеживания событий оснастки.

В остальном же работа с журналами трассировки подраздела Сеансы отслеживания событий запуска не отличается от работы с журналами трассировки подраздела Сеансы отслеживания событий.

Сведения о журналах трассировки данного подраздела хранятся в дочерних подразделах ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger`.

Каждый отдельный запущенный процесс трассировки снижает общую производительность компьютера, поэтому «излишнюю» трассировку компонентов лучше отключать, чтобы повысить скорость работы операционной системы.

ПРИМЕЧАНИЕ

Если вы отключите запуск журналов трассировки EventLog-Application, EventLog-Security и EventLog-System, то стандартные журналы Windows Vista работать не будут. Также не сможет запуститься служба Журнал событий Windows.

Раз уж мы заговорили о трассировке, то обратим внимание на еще одну ветвь системного реестра — `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing`. Дочерние подразделы этой ветви также определяют запускаемые процессы трассировки. Возможно, вы уже заметили, что трассировку координатора распределенных транзакций (MSDTC) мы отключали именно с помощью подраздела данной ветви реестра. Чтобы отключить трассировку определенного компонента операционной системы, нужно параметру `REG_DWORD`-типа `Active`, расположенному в дочерних подразделах данной ветви реестра, присваивать значения `0`.

Подраздел Отчеты

С помощью данного подраздела можно просмотреть сведения, созданные объектом, собирающим информацию от счетчиков производительности. Для этого в данном подразделе существуют вложенные подразделы User Defined и Система. Соответственно, для отображения сведений от объектов, созданных пользователем, и от системных объектов.

Как только вы создадите с помощью одного из дочерних подразделов подраздела Группы сборщиков данных объект, собирающий сведения от счетчиков производительности, будет создан соответствующий объекту подраздел и в дочернем подразделе Особый подраздела Отчеты.

Теперь, как только вы запустите соответствующий объект, собирающий сведения о работе компонентов системы, а потом остановите его, собранные сведения будут отображаться в подразделе Отчеты. Вам будет достаточно только выделить его, чтобы просмотреть собранные сведения (рис. 5.28).

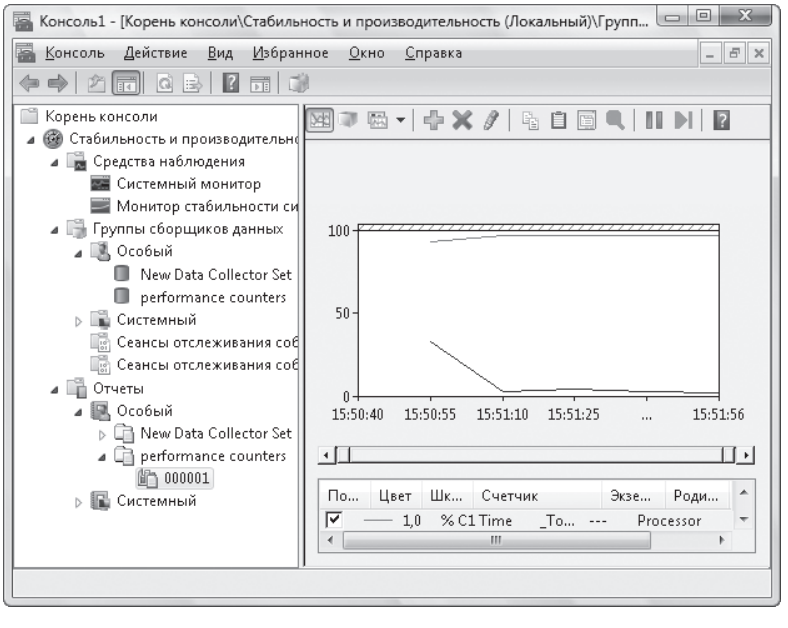


Рис. 5.28. Отображение сведений, собранных счетчиками производительности объекта

Программы для работы со счетчиками производительности и файлами трассировки

Выше мы уже рассмотрели несколько программ для работы со счетчиками производительности. Сейчас же рассмотрим остальные программы.

Редактирование файлов, создаваемых после работы счетчиков производительности. Как вы уже знаете, после того как объект, работающий со счетчиками производительности (Счетчик производительности), был запущен и остановлен, создается файл журнала, содержащий сведения о работе счетчиков производительности. Каталог и название этого файла определяются на вкладке Файл окна Свойства данного объекта. Формат же файла определяется на вкладке Счетчики производительности окна Свойства данного объекта.

Если вы отслеживаете работу множества счетчиков производительности, то работать с ними одновременно будет трудно. Способ работы с получаемым файлом зависит и от его формата. Например, файлы в текстовом формате можно просмотреть в обычном текстовом редакторе, однако файлы в бинарном формате можно легко загрузить в ActiveX-объект Системный монитор.

К счастью, существует программа командной строки, которая легко преобразует файлы одного формата в другой, а также позволяет отфильтровать содержимое файла на основе имени счетчика производительности. Это программа `relog.exe`, способы использования которой описаны далее.

- **Преобразование формата файла.** Чтобы преобразовать файл из одного формата в другой, можно воспользоваться следующей командой: `relog <файл> -o <исходящий файл с другим расширением>`. Например, команда `relog f:\test.csv -o f:\test2.blg` создает новый бинарный файл на основе текстового файла.
- **Фильтрация содержимого файла.** Для создания нового файла, содержащего только информацию об определенных счетчиках производительности, нужно воспользоваться следующей командой: `relog <файл> -c "счетчик производительности" -o <исходящий файл>`. Например: `relog f:\test.csv -c "\Processor(_Total)\% Processor Time" -o f:\test2.csv`. Счетчик производительности указывается в формате `\\компьютер\объект(экземпляр)\счетчик`.

  Вместо параметра `-c <счетчик производительности>` можно использовать параметр `-cf <файл>` для указания файла, содержащего список счетчиков производительности.

Остальные параметры данной программы можно просмотреть, воспользовавшись командой `relog.exe /?`.

Преобразование файлов трассировки в текстовый формат. В операционной системе Windows Vista присутствует программа командной строки, предназначенная для преобразования файлов трассировки (имеют расширение ETL) в текстовые файлы с расширением CSV.

Чтобы преобразовать файлы трассировки, достаточно воспользоваться следующей командой: `tracerpt <список файлов трассировки, которые нужно преобразовать, через пробел> -o <создаваемый программой файл с расширением CSV>`. Дополнительные же параметры данной программы можно просмотреть с помощью команды `tracerpt /?`. В операционной системе Windows Vista, по сравнению с Windows XP, количество параметров данной программы существенно увеличилось.

Запуск счетчиков производительности. Для работы со счетчиками производительности не обязательно использовать оснастку Стабильность и производительность, и тем более специально для этого создавать объект подраздела Группы сборщиков данных. Например, чтобы запустить работу какого-нибудь счетчика производительности, можно воспользоваться программой командной строки `typeperf.exe`.

Например, команда `typeperf.exe <счетчик производительности>` запускает счетчик производительности и каждую секунду отображает на экране информацию о его работе. Вместо счетчика производительности можно указать параметр `-cf <файл>`, чтобы программа запускала все счетчики производительности, описанные в данном файле.

Более сложным примером использования данной программы является запись сведений о работе счетчиков производительности в файл. Для этого применяется команда: `typeperf.exe <счетчик производительности> -f <формат создаваемого файла> -o <создаваемый файл>`. Формат создаваемого файла может принимать значения CSV, TSV, BIN, SQL.

В любом случае, чтобы завершить работу счетчиков производительности, нужно нажать сочетание клавиш Ctrl+C.

Работа с наборами данных. И последней программой командной строки, возможности которой мы рассмотрим, будет программа `logman.exe`, позволяющая создавать, удалять, запускать, останавливать и архивировать наборы данных. Она имеет много параметров, поэтому мы рассмотрим только несколько основных ее возможностей.

- `logman.exe create|update <тип объекта> <имя объекта> <параметры работы объекта>` — позволяет создать набор параметров (или изменить параметры работы уже созданного набора параметров), содержащий объект указанного типа. Возможны следующие значения типа объекта: `counter`, `trace`, `alert`, `cfg`, `api`. Чтобы просмотреть список возможных параметров программы, введите команду `logman.exe create <тип объекта> /?`.

  Например, такая команда, как `logman.exe create counter test2 -c "\Processor(_Total)\% Processor Time"`, создает набор данных `test2`, содержащий объект `test2`, отслеживающий работу счетчика производительности \Процессор(_Total)\% загруженности процессора.

- `logman.exe start|stop <имя набора данных>` — дает возможность запустить или остановить работу указанного набора данных.

- `logman.exe export <имя набора данных> -xml <путь к XML-файлу>` — создает шаблон на основе указанного набора данных. Чтобы восстановить

набор данных из созданного ранее шаблона, достаточно воспользоваться командой `logman.exe import <имя нового набора данных> -xml <путь к XML-файлу>`.

- `logman.exe query <имя набора данных>` — отображает настройки работы данного набора данных.
- `logman.exe delete <имя набора данных>` — удалить набор данных.

Управление печатью

CLSID-номер оснастки: `{D06342BD-9057-4673-B43A-0E9BBBE99F11}`.

Библиотека: `pmcsnap.dll`.

Используется в стандартных консолях: `printmanagement.msc`.

Данная оснастка представляет собой нововведение операционной системы Windows Vista. С ее помощью можно управлять работой серверов печати локального или удаленного компьютера.

ПРИМЕЧАНИЕ

Сведения о работе очереди печати, используемой для хранения заданий печати перед тем как передать их на принтер, содержатся в журнале Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ PrintSpooler.

При конфигурировании оснастки (перед ее загрузкой) вам предложат указать адреса удаленных компьютеров, серверами печати которых нужно управлять (рис. 5.29). Чтобы добавить сервер печати локального компьютера, нужно в мастере нажать кнопку Добавить локальный сервер.

Основное окно оснастки состоит из трех подразделов: Настраиваемые принтеры, Серверы печати и Развернутые принтеры. Далее мы рассмотрим каждый из этих подразделов в отдельности. А пока обратите внимание на контекстное меню подраздела оснастки. Оно содержит две интересные команды. С помощью команды Добавление и удаление серверов вы можете добавить в оснастку службы печати других удаленных компьютеров. А с помощью команды Миграция принтеров можно импортировать или экспортировать драйверы принтера и очереди печати в файл. После выбора данной команды перед вами отобразится мастер. Он попросит вас указать при экспортировании компьютер, драйверы принтеров которого нужно экспортировать, а также файл, в который их нужно экспортировать. При этом учтите, что мастер работает с удаленными принтерами с помощью стандартного ресурса общего доступа `print$`. Если доступ к этому ресурсу будет запрещен, то мастер не сможет корректно экспортировать настройки принтера.

ПРИМЕЧАНИЕ

Команда Миграция принтеров контекстного меню оснастки просто вызывает программу PrintBrmUi.exe, расположенную в каталоге %systemroot%\system32.

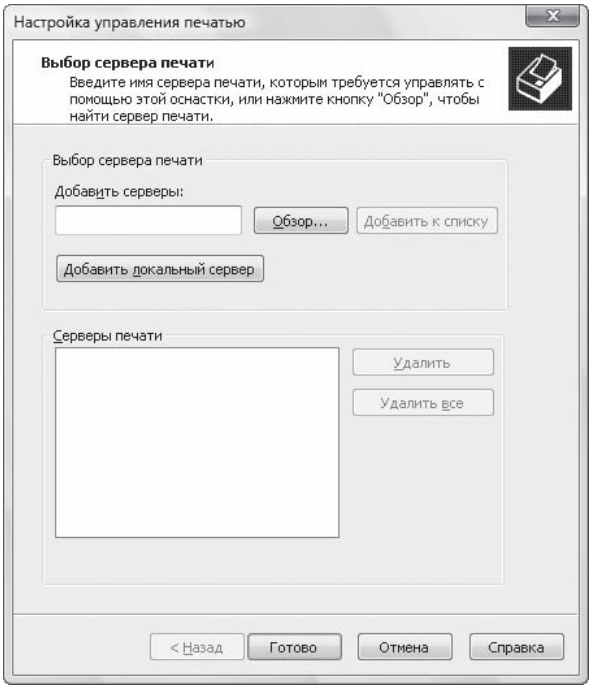


Рис. 5.29. Выбор служб печати

Настраиваемые принтеры

С помощью данного подраздела можно создать фильтр, на основе которого будет отображаться список доступных в данный момент принтеров. Но перед самостоятельным созданием фильтра рассмотрим три стандартных фильтра, которые вложены в этот подраздел.

- Все принтеры — этот фильтр (точнее будет сказать, что это просто подраздел, так как он не имеет фильтра) отображает список всех доступных вам принтеров, а также их состояние, размер очереди печати и компьютер службы принтеров, к которой принадлежит данный принтер.

  Кроме того, если в контекстном меню данного подраздела вы выберете команду Скрыть расширенное представление (она представляет собой расширение оснастки, поэтому может отсутствовать, если соответствующее расширение оснастки отключено), то отобразится дополнительная вкладка оснастки. С ее помощью можно просмотреть такие параметры заданий, находящихся в очереди печати принтера, как имя документа, статус работы (уже напечатан или еще нет), имя пользователя, пославшего документ на печать, количество страниц в документе, его размер и т. д.

- Все драйверы — этот подраздел также не имеет фильтра. Он отображает список всех установленных в операционной системе драйверов принтеров. С помощью контекстного меню элементов данного списка можно удалить соответствующий пакет драйверов или просмотреть его настройки.

- С заданиями печати — этот фильтр отображает список всех принтеров, размер очереди печати которых больше нуля (соответствует фильтру `filter:jobs_in_queue GREATER_THAN '0'`). Точно так же вы можете изменить фильтр данного подраздела с помощью команды Свойства его контекстного меню.
- В состоянии "Не готов" — фильтр отображает список всех принтеров, которые в данный момент не смогут обработать ваш запрос. Он основан на фильтре, который вы сможете увидеть, если в контекстном меню подраздела выберете команду Свойства. После этого отобразится окно, представленное на рис. 5.30.

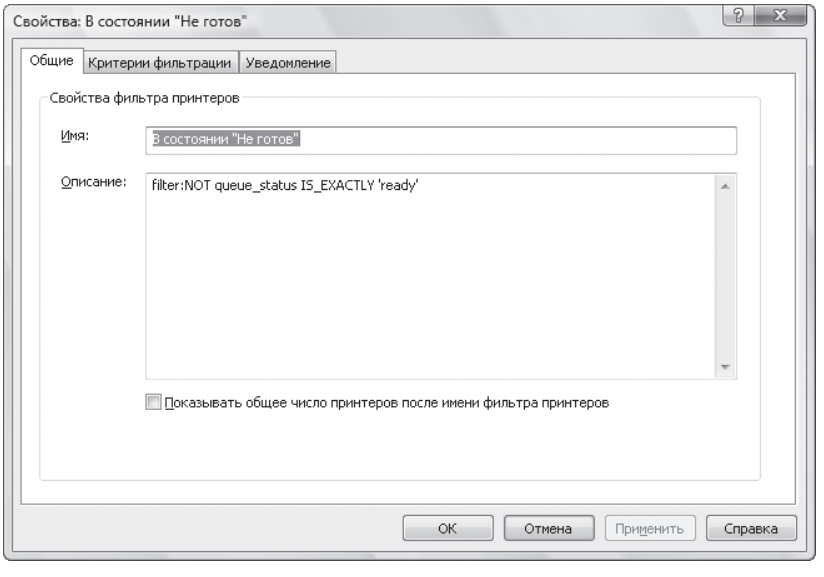


Рис. 5.30. Окно настройки стандартного фильтра

Рассмотрим окно настройки стандартного фильтра. Оно содержит три вкладки.

- Общие — отображает описание фильтра, которое для стандартных фильтров соответствует строке самого фильтра. На этой вкладке также присутствует флажок Показывать общее число принтеров после имени фильтра принтеров. Если вы установите его, то справа от имени подраздела фильтра будет отображаться количество принтеров, удовлетворяющих введенному вами фильтру.
- Критерии фильтрации — представляет своеобразный мастер создания фильтра. На данной вкладке присутствует множество разделенных раскрывающихся списков.
    - Списки области Поле определяют поля, по которым будет выполняться фильтрация. Например, можно выполнять фильтрацию по статусу очереди печати, имени принтера, имени драйвера принтера, размеру очереди печати, комментарию, расположению принтера в сети, имени принтера для общего доступа и т. д.
    - Раскрывающиеся списки области Условие определяют условия фильтрации по указанному полю. В зависимости от выбранного значения раскрывающе-

гося списка области Поле список данного поля может состоять либо из множества условий, либо только из двух: Совпадает с и Не совпадает с (если переводить формально, то они означают соответственно «равно» и «не равно»).

- Списки из раздела Значение определяют значения, которым могут быть равны или не равны поля фильтра. Например, доступны следующие значения данных раскрывающихся списков: Готов (принтер готов к работе), Приостановлен (печать на принтере приостановлена), Ошибка (ошибка печати), Печать (выполняется печать), Тонер или чернила на исходе (осталось мало краски или тонера), Нет тонера или чернил (краска или тонер закончились) и т. д.

- Уведомление — с помощью данной вкладки можно указать программу или создать электронное сообщение, которое будет посылаться при удовлетворении созданного вами фильтра.

Итак, если вам не хватает стандартных фильтров подраздела, то с помощью команды Добавить новый фильтр принтеров контекстного меню подраздела Настраиваемые принтеры можно создать свой собственный подраздел фильтра. После вызова данной команды перед вами отобразится мастер, который предложит вам указать все те параметры, которые мы рассматривали ранее при описании окна Свойства стандартных фильтров оснастки.

Независимо от того, в каком из фильтров подраздела Настраиваемые принтеры отображаются принтеры, их контекстное меню содержит следующие значимые команды.

- Открыть очередь печати — вызывает стандартную программу операционной системы, отображающую очередь печати указанного принтера и позволяющую управлять элементами очереди печати.
- Приостановить печать — приостановить печать с помощью данного принтера.
- Развернуть с помощью групповой политики — с помощью данной команды можно опубликовать выбранный принтер в домене Active Directory.
- Настроить используемые по умолчанию параметры печати — вызывает окно изменения настроек принтера. Содержимое данного окна определяется непосредственно драйвером принтера.
- Управление доступом — отображает окно Свойства данного принтера, открытое на вкладке Доступ.
- Пробная печать — распечатывает тестовую страницу на данном принтере.
- Свойства — отображает окно Свойства данного принтера.
- Удалить — удаляет выбранный вами принтер и его драйверы.

Серверы печати

С помощью данного подраздела можно просмотреть параметры работы принтеров, доступных на указанном сервере печати. Для этого служат следующие его дочерние подразделы.

- Драйверы — содержит список всех драйверов принтеров, установленных на данном компьютере. С помощью контекстного меню драйвера вы можете просмотреть

такие его свойства (команда Свойства), как имя, путь к драйверу, для каких версий операционной системы Windows он предназначен, а также список всех файлов, которые входят в пакет драйвера (были установлены вместе с ним). Используя контекстное меню драйвера, вы сможете удалить его (команда Удалить) или весь пакет драйвера (команда Удалить пакет драйвера).

Кроме того, с помощью контекстного меню подраздела Драйверы можно установить новый драйвер (команда Добавить драйвер), а также отобразить окно Свойства: Сервер печати, открытое на вкладке Драйверы (команда Управление драйверами). Окно Свойства: Сервер печати предоставляет такие же возможности, что и подраздел Серверы печати данной оснастки.

- Формы — включает в себя список всех форм (размеры страниц, с которыми могут выполнять печать принтеры), доступных для установленных принтеров сервера, а также их параметры: ширину и высоту в миллиметрах для текста и изображений.

  Кроме того, с помощью контекстного меню подраздела Формы можно отобразить окно Свойства: Сервер печати, открытое на вкладке Формы (команда Управление формами).

- Порты — содержит список всех локальных, сетевых или WSD-портов, к которым подключены принтеры, а также имя принтера, который подключен к данному порту. С помощью команды Удалить контекстного меню порта вы можете удалить данный порт. А с помощью команды Настроить порт можно настроить параметры работы порта, если он их имеет. Например, для LPT-портов можно настроить интервал ожидания между передачами в секундах.

  Кроме того, с помощью контекстного меню подраздела Порты можно создать новый локальный порт, порт TCP/IP или порт WSD (команда Добавить порт), а также отобразить окно Свойства: Сервер печати, открытое на вкладке Порты (команда Управление портами).

- Принтеры — включает в себя список всех принтеров, установленных на сервере печати, а также позволяет добавить новый принтер (команда Добавить принтер контекстного меню подраздела Принтеры). Кроме того, с помощью данного подраздела можно управлять работой принтеров сервера печати — контекстное меню принтеров содержит те же параметры, что и контекстное меню принтеров рассмотренного ранее подраздела Настраиваемые принтеры.

Развернутые принтеры

Данный подраздел включает в себя список всех принтеров, опубликованных в каталоге Active Directory. В контексте данной книги мы не будем его рассматривать.

Монитор стабильности системы

CLSID-номер оснастки: `{F1FAFB1C-1ABC-49f7-B216-F98213B9B7F5}`.

Библиотека: `RelMon.dll`.

Используется в стандартных консолях: `perfmon.msc`.

С целью повышения информативности операционной системы Windows Vista в вопросах возникновения ошибок в ее состав теперь входит новая оснастка, отображающая сведения о возникших ошибках программ, компонентов компьютера, компонентов операционной системы и др. Данные для этой оснастки предоставляются провайдером Reliability Analysis Component (RAC) один раз в 24 часа.

Основное окно оснастки состоит из шести блоков, представляющих собой один график и пять раскрывающихся списков.

- График возникновения ошибок определенного типа — состоит из графика, который показывает кривую возникновения любых ошибок, а также из поля под ним, с помощью которого определяется тип возникшей ошибки и дата ее возникновения.
- Установка и удаление программ — отображает список всех ошибок, возникших при установке или удалении программ, а также название программ, их версии и дату установки (удаления).
- Ошибки приложений — показывает список всех ошибок, возникших при работе программ, а также названия этих программ, их версии, дату возникновения ошибки и тип ошибки.
- Неполадки оборудования — отображает список всех ошибок, возникших при работе компонентов компьютера, а также тип этих компонентов, имя компонента, дату возникновения ошибки и ее тип.
- Неполадки Windows — показывает список всех ошибок, возникших при работе компонентов операционной системы, а также дату возникновения ошибки, ее тип ошибки и описание.
- Разные неполадки — отображает список всех смешанных ошибок, которые не подходят ни под одно из предыдущих описаний ошибок, а также дату возникновения ошибки, ее тип и описание.

Службы

CLSID-номер оснастки: `{58221C66-EA27-11CF-ADCF-00AA00A80033}`.

Библиотека: `filemgmt.dll`.

Используется в стандартных консолях: `comexp.msc` (расположена в каталоге `%systemroot%\system32\com`), `compmgmt.msc`, `services.msc`.

Возможности данной оснастки в операционной системе Windows Vista по сравнению с оснасткой предыдущих версий операционной системы совершенно не изменились. Как и раньше, с ее помощью можно управлять работой служб локального или удаленного компьютера, а также настраивать такие параметры работы служб, как способ их запуска, учетная запись, с правами которой запускаются службы, и действия при возникновении ошибок при запуске служб.

Описание служб, доступных в операционной системе Windows Vista по умолчанию, будет приведено в гл. 6.

Планировщик заданий

CLSID-номер оснастки: `{c7b8fb06-bfe1-4c2e-9217-7a69a95bbac4}`.

Библиотека: `TaskScheduler.dll`.

Используется в стандартных консолях: `compmgmt.msc`, `taskschd.msc`.

В операционной системе Windows Vista на смену ActiveX-объекту, представляющему собой папку, содержащую список автоматически запускаемых задач, пришла новая оснастка Планировщик заданий. Следует сказать, что конечный пользователь от этого только выигрывает, так как новая оснастка имеет намного больше возможностей.

ПРИМЕЧАНИЕ

Сведения о работе механизма Планировщик заданий заносятся в журнал Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Task Scheduler.

При загрузке оснастки указывается компьютер, к которому нужно подключиться, после чего отобразится основное окно оснастки (рис. 5.31).

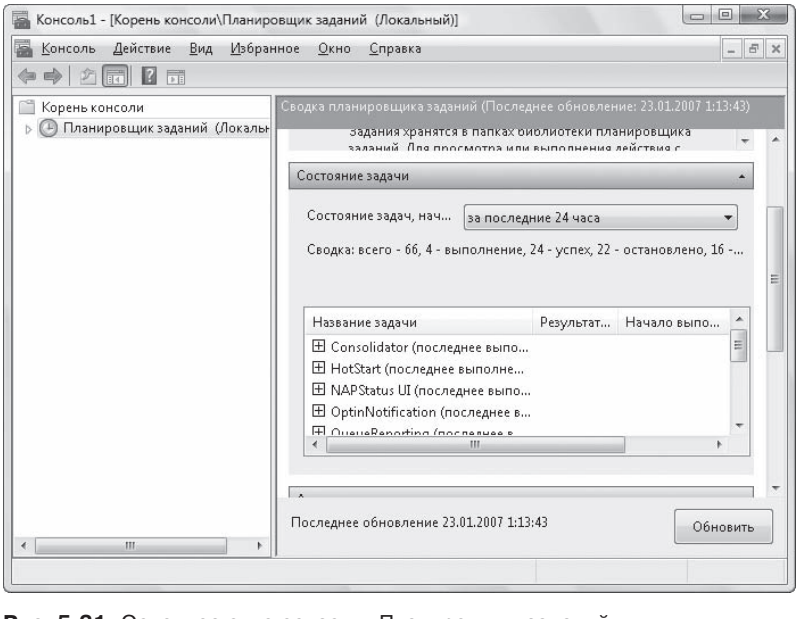


Рис. 5.31. Основное окно оснастки Планировщик заданий

Основное окно оснастки

Главное окно оснастки состоит из следующих элементов.

- Обзор планировщика заданий — содержит описание возможностей оснастки.
- Состояние задачи — отображает список заданий, которые были запущены за последние 24 часа (с помощью раскрывающегося списка Показать можно также

отобразить список задач, запущенных за последний час, неделю или месяц). При этом вы можете раскрыть элемент списка запущенных задач (символ + слева от названия запущенного задания), чтобы просмотреть, удалось ли запустить задание, а также когда оно было запущено и остановлено.

- Активные задачи — выводит список задач, которые запущены в данный момент и работа которых еще не завершена. Из этого списка вы можете узнать имя задания, следующее время его запуска, а также сведения о том, с каким интервалом запускается задание.

Подраздел Библиотека планировщика заданий

Список всех заданий, которые могут запускаться автоматически в определенное время, содержится в одном из дочерних подразделов подраздела Библиотека планировщика заданий. Он включает в себя набор подразделов, которые созданы для удобства сортировки заданий. Вы и сами можете создать свой подраздел в подразделе Библиотека планировщика заданий. Для этого в контекстном меню этого подраздела нужно выбрать команду Создать папку.

Каждый из подразделов может хранить задания, отображаемые в правой верхней панели оснастки. При этом в правой нижней панели оснастки будут отображаться свойства данного задания. Также свойства задания можно отобразить, выбрав в его контекстном меню команду Свойства. Отобразится окно (рис. 5.32), содержащее следующие вкладки.

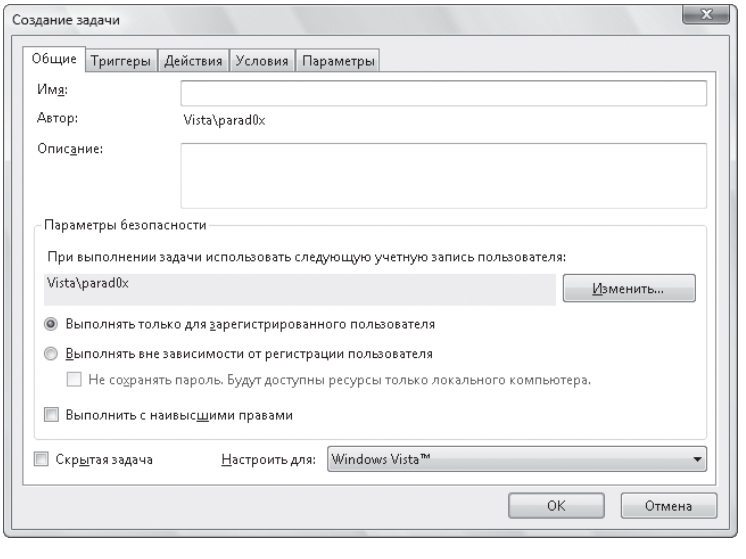


Рис. 5.32. Окно свойств задания

- Общие — определяет описание задания, учетную запись пользователя, от имени которого задание запускается, а также дополнительные параметры запуска: будет ли задание запускаться только в том случае, если пользователь находится в системе, будет ли задание запускаться с повышенными привилегиями, будет ли задание при своей работе отображаться в оснастке Планировщик заданий.

- Триггеры — позволяет настроить время запуска задания. После того как вы нажмете кнопку Создать, перед вами отобразится окно, имеющее следующие элементы.
  - Раскрывающийся список Начать задачу — можно указать, когда будет запускаться задание. По умолчанию задание запускается в указанное время, но с помощью данного списка можно выбрать такие варианты запуска, как запуск при входе пользователя в систему, запуск при наступлении определенного события, запуск при блокировке или разблокировке компьютера, запуск при сетевом подключении пользователя и т. д. В зависимости от выбранного элемента данного списка изменяется содержимое области Параметры.
  - Область Параметры — содержит основные настройки запуска задания, которые зависят собственно от способа запуска задания. Например, при запуске задания по расписанию с помощью данного поля можно указать время запуска и остановки задания, а также дни недели, когда оно будет запускаться. Если задание запускается при возникновении события, то с помощью данного поля нужно определить идентификатор события, программу или службу, которая сгенерировала событие, а также один из журналов Windows (отображаемых в оснастке Просмотр событий), в который помещаются сведения о возникновении данного события.
  - Область Дополнительные параметры — параметры практически никогда не меняются (могут только отсутствовать некоторые его возможности, если они не влияют на выбранный способ запуска задания) и определяют дополнительные возможности настройки запуска задания. К ним относятся следующие указания: через какой промежуток времени запущенное задание будет автоматически останавливаться, через какой промежуток времени запуск задания будет повторяться и т. д.
- Действия — позволяет определить действие, которое будет автоматически выполняться при запуске задания. Чтобы задать новое действие, нужно нажать кнопку Создать, после чего отобразится окно, в котором вы можете указать тип действия и его параметры. Возможны следующие типы действий.
  - Запустить программу — запустить одну или несколько программ или сценариев. В качестве параметров нужно указать путь к программе, а также параметры ее запуска.
  - Отправка электронной почты — отправить электронное сообщение. В качестве параметров нужно указать электронный адрес отправителя и получателя, тему сообщения, текст сообщения. Можно также указать путь к вложению файла, а также сервер SMTP, на который будет отправлено сообщение.
  - Вывод сообщения — отобразить на экране сообщение. При этом нужно указать заголовок и текст сообщения.
- Условия — дает возможность настроить дополнительные условия запуска и остановки задания. К ним можно отнести: запуск задания только после определенного времени работы компьютера, запуск задания только на компьютере, подключенном к сетевой розетке (не питающегося в данный момент от батареи), запуск задания, только если доступно определенное сетевое подключение.

- Параметры — позволяет определить основные настройки работы задания. К ним относятся указания: разрешено ли запускать задание вручную, будет ли перезапущено задание после того как оно по каким-то причинам будет экстренно остановлено (а также настройки перезапуска). С помощью данной вкладки можно также определить действия при запуске нового задания, если при этом предыдущее задание еще работает.
- Журнал — содержит список событий стандартных журналов Windows, которые были созданы данным заданием.

Управление заданиями

С помощью контекстного меню определенного задания вы можете управлять его работой. Для этого предназначены следующие команды его контекстного меню:

- Выполнить — вручную запустить задание;
- Завершить — прекратить работу задания;
- Отключить — отключить автоматический запуск задания;
- Удалить — полностью удалить задание.

Если же вам нужно создать задание, то воспользуйтесь командой Создать простую задачу или Создать задачу контекстного меню одного из подразделов оснастки. Если вы выберете команду Создать простую задачу, то отобразится мастер создания задания, который попросит вас указать только необходимые для работы задания параметры. Если же вы воспользуетесь командой Создать задачу, то отобразится окно параметров задания, которое мы уже рассмотрели ранее (см. рис. 5.32).

Контекстное меню оснастки также содержит две дополнительные команды.

- Отобразить все выполняемые задания — после выбора данной команды перед вами отобразится окно, содержащее список всех запущенных в данный момент заданий. С его помощью вы можете как просмотреть время запуска задания, так и остановить данное задание.
- Настройка учетной записи службы AT — с помощью данной команды можно изменить учетную запись, от имени которой будет запускаться служба автоматического запуска заданий. По умолчанию она запускается с правами системы.

Программа schtasks.exe

Работать с назначенными задачами можно и с помощью стандартной программы командной строки `schtasks.exe`. Рассмотрим возможности этой программы на примерах ее использования.

Просмотр сведений о заданиях. Для отображения списка назначенных заданий определенного компьютера достаточно воспользоваться следующей командой: `schtasks.exe /Query /S <компьютер> /U <пользователь> /P <пароль>`. Если же вы хотите отобразить сведения о заданиях локального компьютера, то параметры `/s`, `/u`, `/p` можно опустить.

Данная команда выводит такие сведения о задании, как подраздел оснастки Планировщик заданий, в котором задание расположено, имя задания, имя удаленного

компьютера, на котором задание создано, дату следующего запуска задания, а также указание, при каких событиях задание запускается.

В этой команде можно указать параметр `/V`, чтобы было отображено больше сведений о задании. В этом случае будут отображены все возможные сведения.

Создание и удаление задания. Команда создания задания имеет много параметров, рассказывать о которых не имеет смысла. Далее будет приведен самый простой способ создания задания, а информацию об остальных параметрах можно просмотреть с помощью команды `schtasks.exe /create /?`.

Самым простым способом создания задания является команда `schtasks.exe /create /SC <интервал запуска задания> /TN <название задания> /TR <команда, которая будет выполняться при старте задания>`. С помощью этой команды создается определенное задание на локальном компьютере, запускаемое с определенным интервалом времени. Естественно, что также в приведенной выше команде можно использовать рассмотренные ранее параметры `/s`, `/u`, `/p` для создания задания на удаленном компьютере.

Параметр `/SC` может принимать следующие значения:

- `MINUTE` — запускать задание каждую минуту;
- `HOURLY` — каждый час;
- `DAILY` — каждый день;
- `WEEKLY` — один раз в неделю;
- `MONTHLY` — один раз в месяц;
- `ONCE` — только сейчас, при этом также нужно указать параметр `/ST <время запуска задания>`;
- `ONSTART` — при входе любого пользователя;
- `ONLOGON` — при входе текущего пользователя;
- `ONIDLE` — при простое системы;
- `ONEVENT` — при возникновении определенного события.

При создании задания можно также указать пользователя, от имени которого оно будет запускаться. Для этого применяются параметры `/RU <пользователь>` и `/RP <пароль>`.

Если же вам необходимо удалить задание, то нужно воспользоваться командой `schtasks.exe /delete /tn <имя задания>`. После этого программа спросит вас, действительно ли вы хотите удалить задание. Если вы нажмете клавишу `Y`, то оно будет удалено. При этом с помощью параметра `/F` можно подавить вывод подтверждения на удаление.

Запуск и остановка задания. Запуск и остановка задания являются довольно простыми задачами. Для их выполнения достаточно воспользоваться командой `schtasks.exe /run|/end /tn <имя задания>`. При этом также можно использовать параметры `/s`, `/u`, `/p` для запуска и остановки задания на удаленном компьютере.

Изменение настроек задания. Чтобы изменить настройки запуска задания, нужно воспользоваться командой вида `schtasks.exe /change /tn <имя задания> <параметры, значения которых нужно изменить>`. Описание параметров, которые можно здесь использовать, можно просмотреть с помощью команды `schtasks.exe /change /?`.

Управляющий элемент WMI

CLSID-номер оснастки: `{5C659257-E236-11D2-8899-00104B2AFB46}`.

Библиотека: `wbemcntl.dll`.

Используется в стандартных консолях: `compmgmt.msc`, `WmiMgmt.msc`.

С помощью данной оснастки можно настроить параметры работы инструментария управления Windows на локальном или удаленном компьютере. Ее возможности совершенно не изменились. Как и раньше, чтобы отобразить параметры работы инструментария управления Windows, нужно воспользоваться командой Свойства контекстного меню оснастки. После этого отобразится окно, состоящее из следующих вкладок.

- Общие — отображает основные сведения о компьютере: его имя, версию операционной системы, номер установленного пакета обновлений, версию инструментария управления Windows, а также путь к каталогу инструментария управления Windows.
- Архивация или восстановление — позволяет выполнить архивацию или восстановление репозитария CIM, а также настроить параметры архивации.
- Безопасность — дает возможность настроить параметры доступа пользователей к определенным пространствам имен репозитария CIM.
- Дополнительно — позволяет указать пространство имен репозитария CIM, которое будет использоваться в сценариях по умолчанию (если создатель сценария не указал конкретное имя пространства имен). Как и раньше, по умолчанию используется пространство имен `root\cimv2`.

Другие оснастки

Элемент ActiveX

CLSID-номер оснастки: `{C96401CF-0E17-11D3-885B-00C04F72C717}`.

Библиотека: `mmcndmgr.dll`.

Используется в стандартных консолях: нет.

Она является стандартной оснасткой всех операционных систем семейства Windows NT. Несмотря на это (в данной книге будут полностью описаны лишь новые оснастки Windows Vista, остальные будут описаны поверхностно), о данной оснастке стоит поговорить подробней, так как очень мало пользователей понимают ее назначение. Все дело в том, что она является не вещью в себе, а своеобразным конструктором, с помощью которого вы можете добавить в создаваемую консоль любой ActiveX-объект, зарегистрированный в операционной системе.

После выбора данной оснастки перед вами отобразится мастер Вставка элемента управления ActiveX (рис. 5.33), с помощью которого можно выбрать нужный ActiveX-объект. Окно мастера состоит из двух элементов. Первым является раскрывающийся список, с помощью которого можно выбрать категорию ActiveX-объектов, а вторым является список всех ActiveX-объектов данной категории.

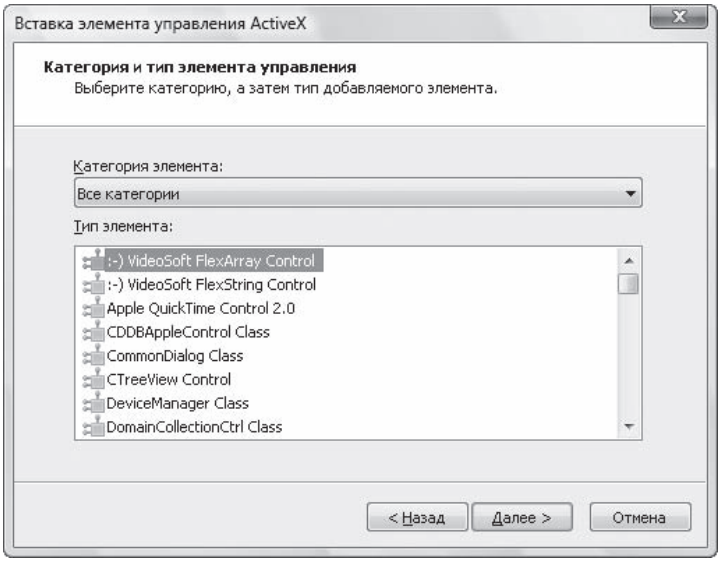


Рис. 5.33. Мастер для выбора добавляемого ActiveX-объекта

Следующим шагом мастера является присвоение имени новому ActiveX-объекту, после чего его работа будет закончена.

Например, можно воспользоваться услугами следующих ActiveX-объектов:

- с помощью ActiveX-объекта Элемент управления Календарь можно добавить в консоль управления Microsoft календарь;
- используя ActiveX-объект Microsoft Office Spreadsheet, можно добавить в консоль управления Microsoft лист Microsoft Excel;
- ActiveX-объект Windows Media Player позволяет добавить в консоль управления Microsoft окно музыкального проигрывателя;
- ActiveX-объект System Monitor Control позволяет добавить в консоль управления Microsoft окно системного монитора, с помощью которого можно наблюдать за состояниями счетчиков производительности.

Управление компьютером

CLSID-номер оснастки: `{58221C67-EA27-11CF-adcf-00AA00A80033}`.

Библиотека: `mycomput.dll`.

Используется в стандартных консолях: `compmgmt.msc`.

Оснастка Управление компьютером представляет собой набор следующих оснасток: Планировщик заданий, Просмотр событий, Локальные пользователи и группы, Стабильность и производительность, Диспетчер устройств, Управление дисками, Службы и Управляющий элемент WMI. Кроме того, сама оснастка Управление компьютером не является нововведением операционной системы Windows Vista, поэтому описывать ее нет смысла.

При выборе оснастки Управление компьютером можно указать компьютер, к которому вы будете подключаться. После этого она будет загружена.

Кроме того, с помощью кнопки Изменить расширения окна Добавление и удаление оснастки можно указать расширения, из которых состоит данная оснастка и которые будут загружены. Фактически, таким способом можно запретить отображение ненужных вам оснасток, которые выводятся после загрузки оснастки Управление компьютером, так как расширения как раз и представляют собой загружаемые оснастки.

Папка

CLSID-номер оснастки: `{C96401CC-0E17-11D3-885B-00C04F72C717}`.

Библиотека: `mmcndmgr.dll`.

Используется в стандартных консолях: используется по умолчанию во всех консолях.

Единственным назначением данной оснастки является создание дочернего подраздела в корне консоли. После того как вы загрузите эту оснастку, будет создан подраздел с именем Папка, но вы можете его переименовать.

Теперь вы можете загружать оснастки не только в корень консоли, но и в созданный подраздел корня. Но перед этим в окне Добавление и удаление оснастки нужно нажать кнопку Дополнительно и в появившемся окне установить флажок Разрешить изменять родительскую оснастку. После этого активизируется раскрывающийся список Родительская оснастка окна Добавление и удаление оснастки, в котором нужно выбрать не раздел Корень консоли, используемый по умолчанию, а созданный вами ранее подраздел. Теперь все загружаемые вами оснастки будут отображаться не в корне консоли, а в созданном вами подразделе.

Ссылка на веб-ресурс

CLSID-номер оснастки: `{C96401D1-0E17-11D3-885B-00C04F72C717}`.

Библиотека: `mmcndmgr.dll`.

Используется в стандартных консолях: нет.

Она представляет собой стандартную оснастку консоли управления Microsoft. С ее помощью можно добавить в консоль раздел, при выборе которого компьютер будет переходить к указанному сайту Интернета и отображать его содержимое.

При загрузке оснастки вас попросят ввести название сайта, а также имя раздела, который будет создан в консоли управления Microsoft.

Глава 6

Стандартные службы Windows Vista

- **Основные сведения о службах**
- **Работа со службами с помощью программ операционной системы**
- **Службы Windows Vista**

В составе операционной системы Windows Vista появилось множество новых служб, которые предоставляют различные возможности и, конечно, влияют на производительность работы компьютера. В этой главе мы рассмотрим назначение всех доступных служб операционной системы Windows Vista, а также попробуем разобраться, как их работа влияет на производительность компьютера, нужны ли они вообще. Мы рассмотрим основные параметры реестра, предназначенные для настройки тех или иных служб, но сначала разберемся, что вообще представляют собой службы и как хранится информация о них в реестре.

6.1. Основные сведения о службах

Служба представляет собой программу, как правило, работающую в фоновом режиме и расширяющую возможности операционной системы. При этом все службы состоят из трех компонентов: собственно файла службы, программы управления службой (SCP) и диспетчера управления службами (SCM).

Файл службы отличается от обычной программы только тем, что в нем реализованы дополнительные функции взаимодействия с SCM.

Программа управления службой (SCP) предназначена для запуска, остановки и настройки службы (для взаимодействия с SCM). Каждая служба может поставляться со своей собственной программой управления, однако чаще всего службы используют стандартный SCP операционной системы Windows. Например, SCP является оснастка операционной системы `services.msc` или программа командной строки `sc.exe`.

Диспетчер управления службами SCM реализован в виде файла `services.exe` и содержит сведения обо всех зарегистрированных в операционной системе службах. Он запускается процессом `Winlogon.exe` еще до запуска графического интерфейса (окно входа в систему).

ПРИМЕЧАНИЕ

Диспетчер SCM взаимодействует с SCP с помощью именованного канала \Pipe\Ntsvcs. SCM при запуске очередной службы также создает канал \Pipe\Net\ NtControlPipeX, после чего ждет подключения запускаемой службы к этому каналу.

Если по истечении определенного интервала (по умолчанию 30 секунд) служба так и не подключилась к каналу, то SCM завершает работу службы. Интервал ожидания подключения службы к каналу определяется параметром REG_DWORD-типа ServicesPipeTimeout, расположенным в ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control.

Если же служба подключилась к каналу, то SCM передает по каналу команду окончательного запуска службы.

Сведения обо всех службах и драйверах, установленных в системе, хранятся в подразделах ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`. Эта ветвь является постоянным представлением базы служб SCM.

Каждая установленная служба или драйвер (независимо от того, работает он в данный момент или нет) имеет свой собственный подраздел в данной ветви реестра. Этот подраздел создается в тот момент, когда служба регистрируется с помощью функции `CreateService` из библиотеки `advapi32.dll`.

Параметры, описывающие службы

Подраздел службы хранит общие сведения о службе, например имя и описание службы, ее исполняемый файл, способ запуска и т. д., а также настройки службы, если такие имеются. Общие сведения о работе служб хранятся в одних и тех же параметрах (с одинаковыми названиями), тогда как настройки службы могут описываться любыми параметрами, названия которых придумывают сами создатели службы. Кроме того, общие сведения о службах всегда располагаются непосредственно в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<название службы>`, тогда как параметры настройки службы могут находиться в любом подразделе данной ветви реестра (но чаще всего находятся в подразделе `Parameters`).

В данной главе мы рассмотрим параметры реестра, определяющие общие сведения о службах, а далее в этой книге будут приведены параметры настройки конкретных служб.

- `Group` — этот параметр строкового типа определяет группу служб или драйверов, к которой относится данная служба. От названия группы зависит время, когда данная служба будет запущена. Дело в том, что все группы служб запускаются последовательно: сначала службы, принадлежащие одной группе, потом службы, принадлежащие другой группе, и т. д. Если же служба не принадлежит ни одной из групп, то она запускается одной из самых последних.

  Сама последовательность запуска групп служб описана в параметре типа `REG_MULTI_SZ List`, расположенном в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder`.

ПРИМЕЧАНИЕ

Просмотреть список групп, зарегистрированных в операционной системе Windows Vista, можно с помощью класса Win32_LoadOrderGroup, принадлежащего пространству имен \\root\cimv2. Экземпляры данного класса описывают отдельную группу и поддерживают следующие свойства: DriverEnabled (определяет, могут ли в данную группу входить драйверы), GroupOrder (указывает очередность загрузки элементов данной группы), Name (ключевое свойство, определяющее название группы).

- `DependOnGroup` — этот параметр типа `REG_MULTI_SZ` определяет группы служб или драйверов, которые обязательно должны быть запущены перед запуском данной службы. Предполагается, что все группы служб, описанные

в этом параметре, необходимы для ее работы, поэтому без запуска любой описанной в параметре группы данная служба запущена не будет.

- DependOnService — имеет тип REG_MULTI_SZ и определяет службы, которые должны быть запущены перед запуском данной службы. Предполагается, что все службы, описанные в этом параметре, необходимы для ее работы, поэтому без запуска любой описанной в параметре службы данная служба запущена не будет.

ПРИМЕЧАНИЕ

Если служба зависит от группы, запускающейся позже той, в которую входит служба, то выдается сообщение об ошибке запуска. Эта же ошибка выдается, если служба зависит от другой службы, которая входит в группу, запускаемую позднее.

- DisplayName — этот параметр строкового типа определяет название службы, используемое для ее отображения в оснастке services.msc.
- Description — имеет строковый тип и определяет описание службы, используемое для отображения строки ее описания в оснастке services.msc.
- ObjectName — данный параметр строкового типа определяет учетную запись пользователя, с правами которого будет запущена данная служба. Может принимать следующие значения.
  - LocalSystem — служба запускается с правами локальной системы (данная учетная запись принадлежит администраторам компьютера со всеми вытекающими возможностями). Служба также запускается с правами локальной системы, если данный параметр отсутствует.

    Эта учетная запись хранит свои настройки в ветви реестра HKEY_USERS\.DEFAULT. Профиль же данной учетной записи содержится в каталоге %systemdrive%\Users\Default.
  - NT Authority\NetworkService — служба запускается с правами пользователя, которому разрешен доступ к сети.

    Данная учетная запись хранит свои настройки в ветви реестра HKEY_USERS\S-1-5-20. Профиль же данной учетной записи содержится в каталоге %systemroot%\ServiceProfiles\NetworkService.
  - NT AUTHORITY\LocalService — служба запускается с правами локального пользователя, который может взаимодействовать с сетью только с помощью нулевых сеансов (в остальном же данная учетная запись аналогична учетной записи NetworkService).

    Учетная запись хранит свои настройки в ветви системного реестра Windows HKEY_USERS\S-1-5-19. Профиль же ее содержится в каталоге %systemroot%\ServiceProfiles\LocalService.
  - .\<логин пользователя> — служба запускается с правами данного пользователя.

- `ErrorControl` — этот параметр типа `REG_DWORD` определяет поведение системы при возникновении ошибок во время запуска данной службы. Он может принимать следующие значения.
  - `0` — диспетчер ввода-вывода игнорирует возникшую ошибку, и загрузка операционной системы продолжается.
  - `1` — предупредить пользователя о возникшей ошибке и продолжить запуск операционной системы.
  - `2` — прекратить запуск операционной системы и выполнить перезагрузку компьютера для запуска последней удачной конфигурации. Если компьютер загружается именно с использованием последней удачной конфигурации, то ошибка игнорируется.
  - `3` — прекратить запуск операционной системы и выполнить перезагрузку компьютера для запуска последней удачной конфигурации. Если компьютер загружается именно с использованием последней удачной конфигурации, то отображается экран неустранимой ошибки BSOD.

  Последняя удачная конфигурация загружает операционную систему на основе ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\ControlSetX`, номер которой указан в параметре `REG_DWORD`-типа `LastKnownGood`, расположенном в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\Select`.

  По умолчанию значение параметра `LastKnownGood` изменяется после каждого успешного входа пользователя в операционную систему. Однако сторонние службы могут изменить условие, при котором загрузка операционной системы считается удачной, и значение параметра `LastKnownGood` изменяется.

  Для этого им достаточно описать новую программу верификации запуска системы с помощью ветви реестра Windows `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BootVerificationProgram`. Также им нужно будет присвоить параметру строкового типа `ReportBootOk`, расположенному в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`, значение `0`. Это необходимо сделать, чтобы операционная система не вызывала функцию `NotifyBootConfigStatus` при входе пользователя в систему (так как эта функция будет вызываться из новой программы верификации). Функция вызывается перед сохранением последней удачной конфигурации.
- `ImagePath` — этот параметр строкового типа определяет путь к исполняемому файлу службы. Именно этот файл представляет собой службу и будет запускаться при ее загрузке.
- `Start` — имеет тип `REG_DWORD` и определяет, когда именно будет запускаться данная служба. Он может принимать следующие значения.
  - `0` — запускать драйвер загрузчиком операционной системы (`NTLDR`) перед началом этапа инициализации ядра (во время загрузки драйвер будет находиться в памяти).
  - `1` — запускать драйвер при инициализации ядра (подсистемой ввода/вывода).

- 2 — запускать службу с помощью диспетчера управления службами (services.exe) после запуска окна приветствия winlogon.exe.
- 3 — запускать службу вручную, когда она понадобится какой-нибудь программе.
- 4 — запрещает запуск данной службы.

- DelayedAutoStart — этот параметр REG_DWORD-типа является нововведением операционной системы Windows Vista. Если его значение равно 1, то служба будет запускаться не сразу, а через определенный промежуток времени, чтобы не загружать операционную систему (с задержкой). Как правило, данный параметр используется в том случае, когда значение параметра Start равно 2.
- ServiceSidType — имеет тип REG_DWORD и является нововведением операционной системы Windows Vista. Он определят тип SID, который был присвоен соответствующей службе. Если значение данного параметра равно 1, то служба будет использовать неограниченный SID. А если значение равно 3, то ограниченный.
- Security — данный параметр REG_BINARY-типа содержит дескриптор защиты службы, определяющий права пользователей, которые могут получить доступ к службе.
- Type — имеет тип REG_DWORD и определяет тип службы. Возможны следующие значения этого параметра.
  - 0x1 — драйвер представляет устройство уровня ядра.
  - 0x2 — драйвер является драйвером файловой системы уровня ядра.
  - 0x4 — драйвер является аргументом для адаптера (данное значение является устаревшим).
  - 0x8 — драйвер используется для распознавания файловой системы.
  - 0x10 — служба является программой, запускающей свой процесс.
  - 0x20 — служба является программой, работающей в общем процессе. Работа нескольких служб в одном процессе позволяет экономить ресурсы компьютера.
  - 0x100 — данное значение параметра может добавляться к остальным значениям. Присутствие этого значения говорит о том, что службе разрешено взаимодействовать с Рабочим столом пользователя (то есть она может отображать свои окна). Использование данного значения параметра разрешено только для служб, запущенных от имени системы.

    По умолчанию службы, запущенные от имени системы или другой учетной записи, не могут взаимодействовать с Рабочим столом текущего пользователя. Это связано с особенностями работы операционной системы Windows: каждая учетная запись имеет свой собственный Рабочий стол и может взаимодействовать только с ним. При этом отображаться может только один Рабочий стол — текущего пользователя. Поэтому, даже если служба попытается отобразить какое-либо сообщение (за исключением диалогового сообщения, которое служба может отобразить на Рабочем

столе текущего пользователя, воспользовавшись специальными параметрами), пользователь этого сообщения не увидит.

Если же разрешить службе, запущенной от имени локальной системы, взаимодействовать с Рабочим столом, то она будет отображать окна не на своем Рабочем столе, а на Рабочем столе текущего пользователя.

ПРИМЕЧАНИЕ

Запретить работу служб в интерактивном режиме можно с помощью параметра типа REG_DWORD NoInteractiveServices, расположенного в ветви HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows.

- `FailureActions` — этот параметр `REG_BINARY`-типа определяет действия, которые будет выполняться в том случае, если в работе службы произошел сбой. При этом сначала в этом параметре описываются действия для первой неудачной попытки запуска, затем для второй, а потом для всех остальных.
- `RequiredPrivileges` — имеет тип `REG_MULTI_SZ` и определяет особые привилегии, которые необходимы для работы данной службы. Он впервые появился в операционной системе Windows Vista с целью повышения общей безопасности компьютера. Теперь службы, которым полностью не нужны системные права, но необходимо выполнять определенные системные операции, могут быть запущены с пониженными правами, однако при этом им будет предоставлено определенное системное право, необходимое для их работы.

ПРИМЕЧАНИЕ

Для получения сведений о службах, установленных в операционной системе, можно использовать класс Win32_Service, который принадлежит пространству имен root\cimv2 и является производным от классов Win32_BaseService и CIM_Service. Например, он поддерживает следующие свойства: AcceptPause (определяет, разрешено ли приостанавливать работу службы), AcceptStop (указывает, разрешено ли останавливать работу службы), Description (содержит строку описания службы), DesktopInteract (определяет, может ли служба взаимодействовать с Рабочим столом пользователя), DisplayName (указывает название службы), ErrorControl (определяет поведение операционной системы при возникновении ошибки во время запуска данной службы), Name (ключевое свойство, определяющее имя службы), PathName (указывает путь к исполняемому файлу службы), ProcessID (определяет PID процесса запущенной службы), Started (указывает, запущена ли служба в данный момент), StartName (определяет учетную запись, от имени которой запускается служба).

Класс также поддерживает следующие методы: Create (позволяет создать службу), Delete (позволяет удалить службу), Change (позволяет изменить настройки службы), ChangeStartMode (позволяет изменить режим запуска службы), InterrogateService (обновляет информацию о службе), PauseService (приостанавливает работу службы), ResumeService (продолжает работу службы), StartService (запускает работу службы), StopService (останавливает работу службы), UserControlService (посылает службе код управления).

Если вы знакомы с сервером инструментариев Windows (WMI), то, наверное, уже догадались, что параметр может хранить те же константы привилегий, что и сценарии WMI.

Некоторые параметры реестра, описывающие стандартные настройки службы, также хранятся в подразделе `Parameters`. К ним можно отнести два параметра: `ServiceDll` и `ServiceDllUnloadOnStop`. Первый имеет тип `REG_EXPAND_SZ` и определяет библиотеку, необходимую для работы данной службы. Второй же параметр имеет тип `REG_DWORD` и определяет, будут ли выгружаться из оперативной памяти компьютера библиотеки, необходимые для работы данной службы, если сама служба была остановлена.

Кроме того, некоторые службы и драйверы хранят в своей ветви реестра подразделы `Performance`. В данных подразделах описывается библиотека, в которой находятся счетчики производительности соответствующей службы, а также индивидуальные параметры работы этих счетчиков. Например, в данной ветви реестра может находиться параметр `REG_DWORD`-типа `Collect Timeout`, определяющий таймаут, в течение которого счетчики должны выполнить задание и ответить на запрос состояния.

Настройки служб svchost

Как вы уже узнали, служба может работать как в собственном процессе, так и в одном из общих процессов. Это позволяет экономить ресурсы компьютера. Хотя при этом появляется другая проблема: если возникнет ошибка в работе одной из служб, то будет завершена работа общего процесса, а вместе с ним и всех служб, которые в нем работали.

Одним из общих процессов для запуска служб является процесс `svchost.exe` (например, общим также является процесс `services.exe`). Он также называется «универсальным» процессом. Одновременно в операционной системе может существовать несколько запущенных процессов `svchost.exe`. При этом каждый из них содержит службы определенного типа (например, типа `netsvcs`). Данные типы служб указываются как параметр строки запуска службы, расположенной в параметре `ImagePath` ветви службы.

Все службы, исполняемый файл которых является частью файла `svchost.exe`, имеют несколько настраиваемых параметров, расположенных в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost`.

Эта ветвь реестра хранит набор параметров строкового типа. Их значения определяют службы, исполняемый файл которых является частью файла `svchost.exe`. Название же этих параметров определяет название дочернего подраздела ветви системного реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Svchost`, в котором расположены настройки для этих служб. Название этих параметров также соответствуют записи SCM, под которой эти службы исполняются.

В этих подразделах могут находиться три параметра, имеющие тип `REG_DWORD`, однако наиболее интересным из них является параметр `DefaultRpcStackSize`. Он определяет размер стека RPC, используемый соответствующими службами.

Основы работы драйверов

Как вы знаете, в ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services` описываются не только установленные в операционной системе службы, но и драйверы. При этом драйверы описываются с помощью тех же основных параметров реестра, что и службы. Хотя значения, присваиваемые данным параметрам, могут отличаться. Так, например, параметр `Type` для драйверов может использовать только значения `1`, `2` и `4`. А параметр `Start` — значения `0` и `1`.

Изменить тип запуска драйверов можно не только с помощью реестра, но и с помощью оснастки Диспетчер устройств (`devmgmt.msc`). Для этого вам нужно сначала включить отображение скрытых устройств (в меню Вид установить флажок Показать скрытые устройства), после чего перейти к разделу дерева оснастки Драйверы несамонастраиваемых устройств. Данный раздел содержит список всех установленных в операционной системе драйверов, которые не поддерживают технологию Plug and Play. При этом если вы отобразите окно Свойства (с помощью одноименной команды контекстного меню) любого из этих драйверов и перейдете на вкладку Драйвер, то в поле Загрузка сможете изменить тип запуска соответствующего драйвера.

ПРИМЕЧАНИЕ

По умолчанию оснастка Диспетчер устройств не отображает сведения о несуществующих в данный момент устройствах или драйверах (например, если драйвер устройства был установлен, а потом устройство было извлечено из компьютера). Если же вам нужно изменить параметры именно такого устройства, то достаточно создать системную переменную DEVMGR_SHOW_NONPRESENT_DEVICES и присвоить ей значение 1. После этого вы сможете увидеть несуществующие в данный момент устройства, если в меню Вид установите флажок Показать скрытые устройства.

Для создания данной системной переменной можно воспользоваться либо реестром (создать параметр строкового типа DEVMGR_SHOW_NONPRESENT_DEVICES в ветви HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment), либо окном Переменные среды (отображается после нажатия кнопки Переменные среды, расположенной на вкладке Дополнительно окна Свойства системы).

Список системных драйверов и их описание, а также драйверов, имеющих цифровую подпись, можно также просмотреть с помощью программы `msinfo32.exe`. Для этого достаточно запустить ее и перейти к разделам Программная среда ▸ Системные драйверы и Программная среда ▸ Подписанные драйверы.

ПРИМЕЧАНИЕ

Список мини-фильтров, установленных в операционной системе, можно просмотреть с помощью программы командной строки fltmc.exe. Если в поле напротив записи драйвера указано значение <Legacy>, то это фильтр. Иначе — мини-фильтр. При этом в поле Число экземпляров указано количество экземпляров данного мини-фильтра.

Диспетчер фильтров — это драйвер фильтра файловой системы. Он упрощает разработку дополнительных драйверов файловой системы от сторонних разработчиков, позволяя им пользоваться уже созданными и откорректированными функциями.

Мини-фильтр представляет собой драйвер, разработанный для модели диспетчера фильтров.

6.2. Работа со службами с помощью программ операционной системы

Естественно, что со службами можно работать не только с помощью реестра, но и используя специальные стандартные программы операционной системы Windows Vista. Одну из таких программ мы уже рассмотрели. Это оснастка `services.msc`, предоставляющая графический доступ к параметрам работы службы. Сейчас же рассмотрим дополнительные программы (или определенные команды программ) командной строки, с помощью которых в операционной системе Windows Vista также можно выполнять доступ к службам.

Возможности программы net.exe

С помощью программы `net.exe` можно не только работать со службами операционной системы, но и решать множество других задач. Однако в контексте данной главы мы рассмотрим лишь те команды этой программы, благодаря которым можно работать со службами.

- `Net statistics server` — отображает сведения о работе службы Сервер. Например, данная команда предоставляет следующие сведения: количество сеансов, размер принятых и переданных данных, количество ошибок при доступе к серверу (например, неправильно введенных паролей), количество обращений к файлам и принтерам, расположенным на сервере, и т. д.
- `Net statistics workstation` — выводит сведения о работе службы Рабочая станция. Например, данная команда предоставляет следующие сведения: размер переданных и принятых данных, количество успешных и запрещенных операций чтения и записи, количество подключений, запущенных сеансов, зависших сеансов и т. д.
- `Net config server` — отображает следующие сведения о работе службы Сервер: имя сервера, максимальное количество подключенных к серверу пользователей или открытых пользователями файлов, время простоя сеанса с сервером, по истечении которого сеанс будет автоматически завершаться.

- `Net config server /AUTODISCONNECT:<количество минут>` — устанавливает новое время простоя сеанса с сервером, после истечения которого данный сеанс будет автоматически завершен.

  Команда изменяет значение параметра `DWORD`-типа `autodisconnect`, расположенного в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters`.

- `Net config server /HIDDEN:<YES или NO>` — устанавливает или запрещает режим скрытого сервера.

  Команда изменяет значение параметра `DWORD`-типа `hidden` ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters`.

- `Net config workstation` — отображает следующие сведения о работе службы Рабочая станция: домен данного компьютера и его DNS-имя, отсчет передачи, таймаут передачи и интервал ожидания открытия COM-порта.

- `Net continue <имя службы>` — выполняет запуск службы, которая ранее была приостановлена.

- `Net pause <имя службы>` — приостанавливает работу данной службы.

- `Net start <имя службы>` — запускает работу данной службы.

- `Net stop <имя службы>` — останавливает работу данной службы.

Использование программы Sc.exe

Данная программа командной строки служит для выполнения основных работ по настройке служб. Ее особенностью является то, что все операции со службами вы можете выполнять как на локальном, так и на удаленном компьютере. Чтобы выполнить команду на удаленном компьютере, достаточно в ней после названия программы указать параметр `\\<имя компьютера>`.

Отображение сведений о службе

Следующие команды используются для вывода сведений о службах.

- `Sc enumdepend <имя службы>` — отображает список служб (и сведения о них), которые не смогут работать, если будет отключена данная служба.

- `Sc getdisplayname <имя службы>` — выводит общее имя данной службы.

- `Sc getkeyname <общее имя службы>` — отображает имя данной службы (название ее ветви реестра).

- `Sc qc <имя службы> [<размер буфера для вывода в байтах>]` — выводит такие сведения о службе, как ее имя, тип, способ запуска, действия при возникновении ошибки при запуске службы, файлы службы, ее описание и т. д. Если получаемые сведения будут иметь больший размер, чем указанный в команде буфер, то они будут обрезаться.

- `Sc qdescription <имя службы> [<размер буфера для вывода в байтах>]` — отображает строку описания службы.
- `Sc qfailure <имя службы> [<размер буфера для вывода в байтах>]` — выводит действия, которые будет выполнять система при возникновении ошибок во время запуска службы.
- `Sc sdshow <имя службы>` — отображает дескриптор безопасности данной службы.
- `sc showsid <имя службы>` — выводит идентификатор безопасности для соответствующей службы. Команда является нововведением Windows Vista. Идентификатор безопасности (SID) предназначен для идентификации данной службы среди остальных служб с целью определения ветвей реестра и папок файловой системы, к которым данная служба может получить доступ. В соответствии с концепцией безопасности по умолчанию, которую приводит в жизнь корпорация Microsoft, все меньше служб запускаются от имени локальной системы и со всеми привилегиями. Однако при этом возникает единственная проблема: многим службам нужен доступ к определенным ветвям реестра или каталогам, доступ к которым их учетной записи запрещен. В этом случае применяется SID службы с целью предоставить доступ только определенной службе, а не всем службам одной учетной записи.
- `sc qprivs <имя службы> <список привилегий>` — отображает список привилегий, предоставляемых соответствующей службе. Команда является нововведением Windows Vista.

Изменение сведений о службе

С помощью следующих команд можно изменить сведения о службе.

- `Sc config <имя службы> [type=<тип службы>] [start=<тип запуска>] [error=<действие при ошибке>] [binpath=<путь к исполняемому файлу службы>] [group=<имя группы>] [depend=<список служб и групп, которые должны быть запущены (пишутся через косую черту </>)>] [obj=<учетная запись пользователя, от имени которого запускается данная служба>] [displayname=<отображаемое имя службы>] [password=<пароль для указанной учетной записи пользователя>]` — изменяет настройки указанной службы локального или удаленного компьютера. Вы, наверное, уже поняли, что с помощью данной команды изменяются значения параметров ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<имя службы>`. Рассмотрим назначение основных параметров данной команды.

  Параметр `type=` определяет тип службы и может принимать следующие значения.

  - `Own` — служба является программой и выполняется в собственном процессе. Используется по умолчанию.
  - `Share` — является программой и использует общий процесс.

- `Kernel` — служба является драйвером.
- `Filesys` — является драйвером файловой системы и необходима для ее работы.
- `Rec` — служба является драйвером, определяющим доступные на компьютере файловые системы.
- `Adapt` — описывает работу устройства.

Параметр `start=` определяет способ запуска службы и может принимать следующие значения.

- `Boot` — служба запускается загрузчиком системы при инициализации ядра.
- `System` — запускается после инициализации ядра операционной системы.
- `Auto` — служба запускается автоматически после отображения окна приветствия (`winlogon.exe`).
- `Demand` — запускается вручную программами, когда она им необходима. Данное значение используется по умолчанию.
- `Disabled` — служба отключена.

Параметр `error=` определяет действия при неудачной попытке запуска службы и может принимать следующие значения.

- `Normal` — при возникновении ошибки записать сообщение о ней в журнале, после чего вывести пользователю предупреждение о возникшей проблеме.
- `Severe` — выполнить перезагрузку компьютера с использованием режима запуска последней удачной конфигурации.
- `Critical` — без работы данной службы невозможна работа операционной системы, поэтому прекратится загрузка операционной системы и компьютер перезагрузится.
- `Ignore` — продолжить загрузку операционной системы, не обращая внимания на возникшую ошибку.

- `Sc description <имя службы> <новая строка описания>` — изменяет строку описания для данной службы.
- `Sc failure <имя службы> reset=<интервал стабильной работы службы (в секундах)> reboot=<широковещательное сообщение> command=<команда, выполняемая при возникновении ошибки в работе службы> actions=<действия при ошибке>` — позволяет изменить поведение операционной системы в случае возникновения ошибки при запуске указанной в команде службы. Она поддерживает следующие значения своих параметров.

  Параметр `reset=` определяет интервал работы службы без ошибок, по истечении которого счетчик ошибок сбрасывается в `0` (на основе счетчика ошибок определяются действия, выполняемые при ошибке).

Параметр `reboot=` определяет широковещательное сообщение, которое будет посылаться всем компьютерам сети при сбое в работе службы.

Параметр `actions=` определяет действия (можно указать не больше трех), которые будет выполнять система при возникновении ошибки в работе службы. Возможны следующие значения данного параметра:

- `Run` — не обращать внимания на ошибку;
- `Restart` — выполнить перезапуск службы;
- `Reboot` — выполнить перезагрузку компьютера.

В этом параметре также указывается время в миллисекундах (после символа `/`), которое система будет ожидать, перед тем как выполнить указанное ранее действие.

Таким образом, общий формат значения параметра `actions=` следующий: `действие первое/интервал первый/действие второе/интервал второй/действие третье/интервал третий`.

- `sc privs <имя службы> <список привилегий>` — позволяет изменить список привилегий, предоставляемых соответствующей службе. Команда является нововведением Windows Vista.

Управление службами

Используя следующие команды с их параметрами, можно управлять службами.

- `Sc create <имя службы> [type=<тип службы>] [start=<тип запуска>] [error=<действие при ошибке>] [binpath=<путь к исполняемому файлу службы>] [group=<имя группы, которой принадлежит служба>] [depend=<список служб и групп, которые должны быть запущены перед данной (пишутся через косую черту </>)>] [obj=<учетная запись пользователя, от имени которого запускается данная служба>] [displayname=<отображаемое имя службы>] [password=<пароль к используемой учетной записи пользователя>]` — позволяет создать новую службу.
- `Sc continue <имя службы>` — запускает службу, которая ранее была приостановлена.
- `Sc control <имя службы> <управляющий код>` — посылает службе указанный в команде управляющий код. Возможны следующие стандартные управляющие коды: `paramchange`, `netbindadd`, `netbindremove`, `netbindenable`, `netbinddisable`. Можно также указывать пользовательские коды, если служба их поддерживает.
- `Sc delete <имя службы>` — удаляет указанную службу.
- `Sc pause <имя службы>` — приостанавливает работу данной службы.
- `Sc start <имя службы> [<аргументы запуска>]` — запускает службу.
- `Sc stop <имя службы>` — останавливает работу службы.

Другие команды

С помощью следующих команд можно выполнять другие действия над службами.

- `Sc boot <ok или bad>` — определяет, будет ли текущий сеанс работы компьютера сохраняться как последняя удачная конфигурация. Если в команде используется значение `ok`, то текущий сеанс работы компьютера будет сохраняться как последняя удачная конфигурация.
- `Sc interrogate <имя службы>` — с помощью данной команды можно обновить сведения о службе, получив новые сведения у диспетчера служб.
- `Sc lock` — блокирует работу диспетчера служб, после чего ни одна служба не сможет запуститься. Чтобы прекратить блокирование диспетчера служб, нужно нажать клавишу U.
- `Sc querylock` — определяет, заблокирована ли работа диспетчера служб, и если заблокирована, то кто именно и когда ее заблокировал.

6.3. Службы Windows Vista

Теперь, когда вы познакомились с общими понятиями, необходимыми для работы со службами операционной системы, рассмотрим сами службы, которые по умолчанию присутствуют в операционной системе Windows Vista.

Работа с файлами и файловой системой

Информация о совместимости приложений

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeTcbPrivilege, SeImpersonatePrivilege.

Файлы службы: `aelupsvc.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `AeLookupSvc`.

Службы, необходимые для работы данной: нет.

Данная служба обрабатывает запросы запущенных программ для проверки их совместимости с новой операционной системой. Как правило, большинство программ, созданных для операционной системы Windows XP, будут корректно работать и в новой операционной системе, поэтому эту службу можно отключить. Если же программа работает некорректно даже при настройке параметров, отображаемых на вкладке Совместимость окна Свойства исполняемого файла службы или ярлыка этого файла, то служба Информация о совместимости приложений сможет свести к нулю вредоносные последствия запуска данной программы (если такие

имеются) и даже попытается решить проблему некорректной работы программы, восстановив ее работоспособность.

Операционная система Windows Vista имеет несколько параметров реестра, которые можно использовать для настройки службы Информация о совместимости приложений. Все они имеют тип REG_DWORD и расположены в ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AeLookupSvc.

- MaximumThreadCount — определяет максимальное количество потоков, которые может создавать данная служба.
- EnableDebugCount — указывает, работает ли данная служба в режиме отладки.
- DebugOutputLevel — определяет общее количество сведений о работе службы, которые будут собираться.

Сведения о приложении

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeAssignPrimaryTokenPrivilege, SeIncreaseQuotaPrivilege, SeTcbPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeChangeNotifyPrivilege, SeImpersonatePrivilege.

Файлы службы: appinfo.dll.

Исполняемый файл: svchost.exe -k netsvcs.

Подраздел реестра: Appinfo.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (RpcSs), Служба профилей пользователей (ProfSvc).

Благодаря данной службе при запуске программ, требующих административных прав, перед вами отображается окно для ввода пароля администратора или подтверждения запуска программы от имени администратора. Если вы отключите эту службу, то не сможете запустить ни одну программу, требующую административных прав. Если же механизм UAC отключен, то острая необходимость в работе данной службы отсутствует.

Служба модуля архивации на уровне блоков

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeImpersonatePrivilege, SeBackupPrivilege, SeManageVolumePrivilege, SeRestorePrivilege.

Файлы службы: нет.

Исполняемый файл: `wbengine.exe`.

Подраздел реестра: `wbengine`.

Службы, необходимые для работы данной: нет.

Данная служба является основой служб, позволяющих выполнять архивирование и восстановление данных. По этой причине ее отключение приведет к невозможности выполнения архивирования файлов и каталогов.

Программный поставщик теневого копирования (Microsoft)

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeBackupPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeCreatePermanentPrivilege, SeImpersonatePrivilege, SeManageVolumePrivilege, SeRestorePrivilege, SeIncreaseBasePriorityPrivilege, SeTcbPrivilege.

Файлы службы: `swprv.dll`.

Исполняемый файл: `svchost.exe -k swprv`.

Подраздел реестра: `swprv`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Позволяет управлять теневыми копиями и службой теневого копирования, поэтому после отключения данной службы теневое копирование невозможно.

Автономные файлы

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: `cscsvc.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `CscService`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Управляет работой механизма создания автономных файлов. Отключение данной службы приведет к отключению самой возможности создания автономных файлов.

ПРИМЕЧАНИЕ

Поддержка автономных файлов недоступна в версиях Windows Vista Home Basic и Windows Vista Home Premium.

Superfetch

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeTcbPrivilege, SeProfileSingleProcessPrivilege, SeTakeOwnershipPrivilege, SeDebugPrivilege.

Файлы службы: `sysmain.dll`.

Исполняемый файл: `svchost.exe -k LocalSystemNetworkRestricted`.

Подраздел реестра: `SysMain`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), File Information FS MiniFilter (`Fileinfo`).

На смену механизма Prefetcher Windows XP пришла служба Superfetch операционной системы Windows Vista. Служба позволяет ускорить выполнение программ, с которыми вы часто работаете. Достигается это благодаря предварительному помещению в оперативную память компьютера файлов программ, которые вы часто используете. При этом, что является нововведением данной службы операционной системы Windows Vista, служба Superfetch ведет расписание и в зависимости от дня недели (или даже от времени суток) может подгружать в оперативную память файлы разных программ. Служба также занимается разделением ресурсов, уменьшая количество тех из них, что используются фоновыми программами, если это необходимо.

Если же оперативной памяти в вашем компьютере недостаточно, то служба Superfetch может использовать для своей работы флэш-память, карты памяти, которые медленнее оперативной памяти, но намного быстрее жестких дисков, либо даже гибридные диски. Для этого достаточно вставить флэш-память, после чего в появившемся окне Автозапуск выбрать команду Ускорить работу системы.

Основные настройки работы данной службы хранятся в ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters`. В основном параметры данной ветви имеют тип `REG_DWORD`.

- `EnableBootTrace` — определяет, будет ли выполняться трассировка работы службы Superfetch во время запуска операционной системы.
- `EnablePrefetcher` — указывает, будет ли операционной системой использоваться механизм предварительной выборки Prefetcher.

Чтобы полностью отключить возможность упреждающей выборки, установите значение этого параметра равным 0.

Чтобы включить возможность упреждающей выборки только запускаемых во время работы операционной системы приложений, установите его равным 1.

Чтобы включить возможность упреждающей выборки приложений только на этапе загрузки операционной системы, установите его значение равным 2.

По умолчанию используется значение равное 3, то есть включены обе возможности.

- EnableSuperfetch — определяет, будет ли операционной системой использоваться служба Superfetch.

Настройки работы службы Superfetch хранятся и в ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Prefetcher.

- BootFilesOptimized — этот параметр REG_DWORD-типа позволяет определить, будет ли выполняться оптимизация загрузки файлов при запуске операционной системы.
- LastDiskLayoutTimeString — имеет строковый тип и определяет дату последнего формирования данных службы Superfetch.
- Данные, которые служба помещает в память, находятся в следующем каталоге: %systemroot%\Prefetch. При этом в данном каталоге также содержится файл Layout.ini. Он хранит список программ, данные о работе которых находятся в каталоге %systemroot%\Prefetch. Вот именно дата последнего изменения файла Layout.ini и содержится в параметре LastDiskLayoutTimeString.

Как было сказано выше, файл Layout.ini расположен в каталоге %systemroot%\Prefetch. Однако это можно изменить с помощью ветви HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\OptimalLayout. Данная ветвь реестра содержит следующие параметры.

- LayoutFilePath — этот параметр строкового типа определяет путь к файлу Layout.ini.
- EnableAutoLayout — имеет тип REG_DWORD и определяет, будет ли выполняться автоматическое изменение содержимого файла Layout.ini.

Планировщик заданий

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: schedsvc.dll.

Исполняемый файл: svchost.exe -k netsvcs.

Подраздел реестра: Schedule.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (RpcSs).

Служба позволяет назначать задания, которые будут выполняться автоматически в указанное вами время.

Сведения о списке назначенных заданий содержатся в ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks.

Настройки службы Планировщик заданий хранятся в ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule. Например, здесь можно найти следующие параметры.

- MissedTasksStartupDelay — этот параметр REG_DWORD-типа определяет задержку при неудачной попытке запуска назначенного задания.
- TasksInMemoryQueue — имеет тип REG_DWORD и определяет количество назначенных заданий, которые разрешено помещать в очередь, хранящуюся в оперативной памяти. По умолчанию значение данного параметра равно 0x64.

Настройки агента службы Планировщик заданий находятся и в ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SchedulingAgent.

- LogPath — этот параметр строкового типа содержит путь к файлу журнала, хранящему сведения о запуске назначенных заданий.
- MaxLogSizeKB — имеет тип REG_DWORD и определяет максимальный размер файла журнала (в килобайтах).
- TasksFolder — этот параметр строкового типа содержит путь к каталогу, хранящему назначенные задания.
- NotifyOnTaskMiss — имеет тип REG_DWORD и определяет, будет ли отображаться сообщение при неудачной попытке запуска назначенного задания.
- ViewHiddenTasks — этот параметр REG_DWORD-типа определяет, будут ли отображаться скрытые задания.

Виртуальный диск

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: vds.exe.

Подраздел реестра: vds.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Plug and Play (`PlugPlay`).

Управляет работой дисков, файловых систем и т. д. Служба используется многими системными программами, например оснасткой Управление дисками.

Теневое копирование тома

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: `vssvc.exe`.

Подраздел реестра: `VSS`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Управляет работой службы теневого копирования. После отключения этой службы архивирование открытых данных может быть невыполнимым.

ПРИМЕЧАНИЕ

Теневое копирование недоступно в версиях Windows Vista Home Basic и Windows Vista Home Premium.

Параметры работы службы Теневое копирование тома хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VSS\Settings`. Большая часть этих параметров имеет тип `REG_DWORD`.

- `EnableRemoteSnapshots` — позволяет определить, разрешено ли создание удаленных снимков файловой системы компьютера.
- `MaxShadowCopies` — дает возможность определить максимальное количество создаваемых теневых копий файлов.

Архивация Windows

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: `SDRSVC.dll`.

Исполняемый файл: `svchost.exe -k SDRSVC`.

Подраздел реестра: SDRSVC.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (RpcSs).

Обеспечивает работу механизмов архивации и восстановления операционной системы.

Установщик Windows

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeTcbPrivilege, SeCreatePagefilePrivilege, SeLockMemoryPrivilege, SeIncreaseBasePriorityPrivilege, SeCreatePermanentPrivilege, SeAuditPrivilege, SeSecurityPrivilege, SeChangeNotifyPrivilege, SeProfileSingleProcessPrivilege, SeImpersonatePrivilege, SeCreateGlobalPrivilege, SeAssignPrimaryTokenPrivilege, SeRestorePrivilege, SeIncreaseQuotaPrivilege, SeShutdownPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege.

Файлы службы: нет.

Исполняемый файл: msiexec /V.

Подраздел реестра: msiserver.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (RpcSs).

Управляет работой с установочными MSI-пакетами. Основными особенностями установочных MSI-пакетов является то, что они поддерживают публикацию и назначение с помощью механизмов Active Directory, функции отката в случае возникновения сбоя при установке программы (возможность удаления всех внесенных в процессе установки изменений), возможности автоматической повторной установки файлов приложения, которые оказались поврежденными.

Сведения об установленном программном обеспечении MSI хранятся в следующих ветвях реестра.

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer — содержит сведения обо всех продуктах и компонентах, установленных на данный момент в операционной системе Windows Vista.
- HKEY_CLASSES_ROOT\Installer — хранит информацию о каталогах, из которых выполнялась установка приложений, список всех компонентов COM, определенных в пакете MSI, но не установленных в операционной системе, и т. д.

Параметры программы msiexec.exe

Программа msiexec.exe является как основным файлом службы Установщик Windows, так и установщиком программного обеспечения. При этом данная программа поддерживает набор параметров, с помощью которых можно установить,

удалить, восстановить или обновить определенное программное обеспечение. Подробное описание этих параметров можно просмотреть, если ввести команду `msiexec.exe /?`.

Настройка с помощью групповых политик

Параметры работы данной службы можно настроить с помощью групповых политик, описанных в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Установщик Windows. Эти политики изменяют следующие параметры `REG_DWORD`-типа, расположенные в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer`.

- `EnableAdminTSRemote` — если значение данного параметра равно `1`, то администраторам будет разрешено выполнять установку и настройку программ на удаленном компьютере (с помощью сеанса службы терминалов).
- `AlwaysInstallElevated` — при установке значения этого параметра равным `1` служба установщика Windows будет выполнять установку программ с системными привилегиями, а не с привилегиями текущего пользователя. Этот параметр доступен и в корневом разделе `HKEY_CURRENT_USER`.
- `MaxPatchCacheSize` — значение данного параметра определяет процент места на диске, который будет использоваться кэшем базисных файлов службы установщика Windows (каталог `%systemroot%\Installer`). Кэш базисных файлов хранит различные установленные обновления.
- `TransformsSecure` — если значение данного параметра равно `1`, то файлы преобразований, содержащие сведения об устанавливаемой программе, будут копироваться на локальный компьютер (эта политика актуальна при сетевой установке программы). Файл преобразования необходим при выполнении повторной установки приложения, поэтому, если он не будет найден на локальном компьютере, отобразится окно с просьбой указать расположение файла преобразований.
- `SafeForScripting` — при установке значения этого параметра равным `1` будет отключено отображение предупреждения при установке программы с помощью сценария, доступ к которому получен из Интернета.
- `DisableLoggingFromPackage` — если значение данного параметра равно `0`, то будет запрещено автоматическое создание файлов журнала (включаемое с помощью свойства `MsiLogging`) при установке программного обеспечения.
- `DisableMSI` — при установке значения этого параметра равным `1` пользователю будет разрешено устанавливать лишь программное обеспечение, назначенное или опубликованное администратором. Если же значение данного параметра равно `2`, то пользователю будет запрещено устанавливать любое программное обеспечение, использующее для своей инсталляции установщик Windows.
- `DisableBrowse` — если значение данного параметра равно `1`, то пользователю будет запрещено искать файлы установки при добавлении компонентов к установленной программе с помощью кнопки Обзор окна Использовать функцию.

- `EnableUserControl` — при установке значения этого параметра равным `1` пользователю будет разрешено выполнять настройку параметров установки программного обеспечения, которые по умолчанию доступны только администраторам (например, изменять каталог установки файлов).
- `AllowLockdownBrowse` — если значение данного параметра равно `1`, то при использовании режима установки с повышением привилегий пользователя (параметр `AlwaysInstallElevated`) будет разрешено выполнять поиск исходных файлов инсталляции с помощью кнопки Обзор окна Использовать функцию. По умолчанию только администраторы могут выполнять поиск с повышенными правами.
- `AllowLockdownPatch` — если присвоить этому параметру значение `1`, то установку обновлений программы можно будет выполнять при использовании режима установки с повышением привилегий.
- `AllowLockdownMedia` — если значение данного параметра равно `1`, то при использовании режима установки с повышением привилегий пользователя можно выполнять установку программ со съемных носителей. По умолчанию только администраторы могут выполнять установку со съемных носителей с повышенными правами.
- `DisableLUAPatching` — при установке значения этого параметра равным `1` для пользователей, не обладающих правами администраторов, будет запрещено выполнение установки обновлений программ, которые подписаны издателем. По умолчанию пользователи могут устанавливать такие обновления.
- `DisablePatch` — если значение данного параметра равно `1`, то возможность установки исправлений для программного обеспечения будет запрещена.
- `DisablePatchUninstall` — при установке значения этого параметра равным `1` будет запрещена возможность удаления установленных обновлений для программного обеспечения.
- `DisableRollback` — если значение данного параметра равно `1`, то возможность сохранения данных, с помощью которых можно выполнить откат установки программы, будет запрещена. Параметр доступен и в корневом разделе `HKEY_CURRENT_USER`.
- `DisableAutomaticApplicationShutdown` — значение данного параметра позволяет указать режим использования диспетчера перезапуска (диспетчер перезапуска применяется для сокращения количества перезагрузок при выполнении инсталляции программного обеспечения). Если значение данного параметра равно `1`, то диспетчер перезапуска будет отключен для всех программ. Если же значение равно `2`, то диспетчер перезапуска будет отключен только для программ, созданных с помощью более ранней версии установщика Windows, чем применяемая в операционной системе Windows Vista (в данной операционной системе применяется четвертая версия).
- `LimitSystemRestoreCheckpointing` — если значение данного параметра равно `1`, то создание точек восстановления при выполнении установки программного обеспечения будет запрещена.

Один параметр этой ветви реестра имеет строковый тип: `Logging`. С его помощью можно настроить типы событий, сведения о возникновении которых будут заноситься в файл журнала `Msi.log`, расположенный в каталоге `temp` системного раздела.

Настроить работу службы установщика можно и с помощью параметров ветви `HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Installer`.

- `DisableMedia` — если значение данного параметра `REG_DWORD`-типа равно `1`, то пользователю будет запрещено выполнять установку программного обеспечения, расположенного на съемных носителях.
- `SearchOrder` — имеет строковый тип. Он позволяет указать порядок поиска файлов установки. По умолчанию сначала выполняется поиск в сети, затем на съемных носителях, а потом в Интернете. Однако вы можете изменить порядок поиска с помощью указания последовательности трех символов: `n` (поиск в сети), `m` (на съемном носителе) и `u` (в Интернете).

Установщик модулей Windows

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: `%SystemRoot%\servicing\TrustedInstaller.exe`.

Подраздел реестра: `TrustedInstaller`.

Службы, необходимые для работы данной: Plug and Play (`PlugPlay`).

Управляет установкой и удалением обновлений операционной системы. Отключение данной службы может привести к невозможности установки обновлений операционной системы.

Поиск Windows

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeManageVolumePrivilege, SeImpersonatePrivilege, SeAssignPrimaryTokenPrivilege, SeIncreaseQuotaPrivilege, SeTcbPrivilege.

Файлы службы: нет.

Исполняемый файл: `SearchIndexer.exe /Embedding`.

Подраздел реестра: `WSearch`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Обеспечивает индексацию содержимого и кэширование файлов, электронной почты и других пользовательских данных. Данная служба позволяет внести в индекс изменения в пользовательских данных.

Работа с оборудованием

Распространение сертификата

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: `certprop.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `CertPropSvc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Эта служба распространяет сертификаты со смарт-карт. Параметры ее работы можно изменить с помощью групповых политик. Они определяются в файлах `smartcard.adml` и `smartcard.admx`.

ПРИМЕЧАНИЕ

Сведения о распространении сертификатов заносятся в журнал, расположенный в разделе Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ CertificateServicesClient-CredentialRoaming.

В операционной системе Windows Vista по умолчанию создано три задания, которые управляют распространением сертификатов. Они расположены в разделе Библиотека планировщика заданий ▸ Microsoft ▸ Windows ▸ CertificateServicesClient:

- SystemTask — запускается при включении компьютера;
- UserTask — запускается при входе любого пользователя в систему;
- UserTask-Roam — запускается при создании и завершении сетевого сеанса, а также при блокировании и разблокировании компьютера.

Факс

Тип запуска: вручную.

Учетная запись: сетевая служба.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: `fxssvc.exe`.

Подраздел реестра: `Fax`.

Службы, необходимые для работы данной: Телефония (`TapiSrv`), Удаленный вызов процедур (RPC) (`RpcSs`), Plug and Play (`PlugPlay`), Диспетчер печати (`Spooler`).

Позволяет отсылать и получать факсы с помощью оборудования данного компьютера или другого компьютера сети (например, с помощью соответствующего модема или факс-аппарата), а также выполняет мониторинг состояния факсов.

Операционная система Windows Vista позволяет просматривать сведения о работе данной службы с помощью счетчиков производительности объекта Служба факсов. Например, с помощью счетчиков данного объекта можно узнать следующие сведения о работе службы:

- общее количество минут, в течение которых служба отправляла и получала факсы (счетчик Всего минут приема и передачи), общее количество отправленных и полученных факсов (счетчик Всего отправлено и получено факсов), страниц (счетчик Всего страниц) и байт (счетчик Всего байт).
- количество страниц, факсов, байт или времени, в течение которого служба отправляла (соответственно, счетчики Отправлено страниц, Отправлено факсов, Отправлено байт, Минут передачи) или получала факсы (соответственно, счетчики Получено страниц, Получено факсов, Получено байт, Минут приема).

Настройки программы `fxssvc.exe` хранятся в ветви системного реестра Windows `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fax`.

Доступ к HID-устройствам

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: `hidserv.dll`.

Исполняемый файл: `svchost.exe -k LocalSystemNetworkRestricted`.

Подраздел реестра: `HidServ`.

Службы, необходимые для работы данной: нет.

Управляет работой дополнительных возможностей HID-совместимых устройств (клавиатур и мышей). Благодаря этой службе могут работать различные горячие клавиши данных устройств, дистанционное управление и другие мультимедийные возможности. Эти возможности некоторых манипуляторов могут работать и с отключенной службой Доступ к HID-устройствам.

Планировщик классов мультимедиа

Тип запуска: автоматически.

Учетная запись: система, но с привилегией SeIncreaseBasePriorityPrivilege.

Дополнительные привилегии: нет.

Файлы службы: `mmcss.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `MMCSS`.

Службы, необходимые для работы данной: нет.

Позволяет управлять приоритетом работы мультимедийных устройств. При отключении данной службы всегда будет использоваться приоритет, установленный по умолчанию устройству мультимедиа.

Настройки приоритетов хранятся в ветви `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Multimedia\SystemProfile\Tasks`. Эта ветвь включает в себя следующие дочерние подразделы: `Audio`, `Capture`, `Distribution`, `Games`, `Playback`, `Pro Audio`, `Window Manager`. Каждый из них содержит параметр `REG_DWORD`-типа `Priority`, который определяет приоритет данной категории задач. Также в данной ветви реестра содержится параметр строкового типа `Background Only`, который определяет, будет ли выполняться работа с данной категорией задач только в фоновом режиме.

Plug and Play

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeTcbPrivilege, SeSecurityPrivilege, SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeImpersonatePrivilege, SeAuditPrivilege, SeChangeNotifyPrivilege, SeUndockPrivilege, SeDebugPrivilege.

Файлы службы: `umpnpmgr.dll`.

Исполняемый файл: `svchost.exe -k DcomLaunch`.

Подраздел реестра: `PlugPlay`.

Службы, необходимые для работы данной: нет.

Управляет работой механизма Plug and Play и распознаванием новых Plug and Play-совместимых устройств. Данную службу нельзя остановить или отключить.

Перечислитель IP-шин PnP-X

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege, SeLoadDriverPrivilege.

Файлы службы: `ipbusenum.dll`.

Исполняемый файл: `svchost.exe -k LocalSystemNetworkRestricted`.

Подраздел реестра: `IPBusEnum`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Хост поставщика функции обнаружения (`fdPHost`).

Управляет энумерацией новых устройств, только что подключенных к сети и поддерживающих стандарт Plug and Play (управляет виртуальной сетевой шиной). После отключения данной службы не будет функционировать протокол SSDP/WS и, следовательно, не будут обнаруживаться новые Plug and Play устройства, подключенные к сети.

Провайдер, необходимый для работы данной службы, описывается в параметре ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Function Discovery\Categories\Provider\Microsoft.PnPX.Association`.

Диспетчер печати

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeTcbPrivilege, SeImpersonatePrivilege, SeAuditPrivilege, SeChangeNotifyPrivilege, SeLoadDriverPrivilege, SeAssignPrimaryTokenPrivilege.

Файлы службы: нет.

Исполняемый файл: `spoolsv.exe`

Подраздел реестра: `Spooler`.

Службы, необходимые для работы данной: Удаленный Вызов Процедур (RPC) (`RPCSS`).

Загружает в память компьютера файлы для дальнейшей печати с помощью принтера.

Определение оборудования оболочки

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: `shsvcs.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `ShellHWDetection`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Вызывает окно Автозапуск при обнаружении новых установленных устройств.

Данное окно, а также действия, выполняемые по умолчанию при обнаружении новых устройств или дисков определенного типа, можно настроить с помощью мастера Автозапуск, который вызывается с помощью одноименного значка папки Панель управления. Этот мастер состоит из флажка Использовать автозапуск для всех носителей и устройств и набора раскрывающихся списков. С помощью флажка можно запретить или разрешить выполнение каких-либо действий (отображение окна Автозапуск или выполнение действия по умолчанию) при обнаружении новых установленных устройств или дисков определенного типа. А с помощью раскрывающихся списков можно указать то действие по умолчанию, которое будет выполняться при обнаружении нового устройства.

Окно Автозапуск

Рассмотрим расположенные в этом окне раскрывающиеся списки. В основном здесь не будет описываться их назначение — оно понятно из названия. Вместо этого будут представлены подразделы реестра, в которых этих списки определяются.

- Звуковой CD — указывает действие, выполняемое при обнаружении нового компакт-диска в формате Audio CD. Данный раскрывающийся список определяется подразделом реестра `PlayCDAudioOnArrival`.
- Фильмы на DVD — определяется подразделом реестра `PlayDVDMovieOnArrival`.
- Звуковой улучшенный CD — указывает действие, выполняемое при обнаружении нового компакт-диска в формате Enhanced Audio CD. Данный раскрывающийся список определяется подразделом реестра `PlayEnhancedCDOnArrival`.
- Программы и игры — определяет действие, выполняемое при обнаружении нового диска, имеющего в корне файл `autorun.inf`. Данный список определяется подразделом реестра `AutorunINFLegacyArrival`.
- Чистый CD — определяется подразделом реестра `HandleCDBurningOnArrival`.
- Фильмы на улучшенном DVD — список определяется подразделом системного реестра `PlayEnhancedDVDOnArrival`.
- Звуковые файлы — определяется подразделом системного реестра Windows `PlayMusicFilesOnArrival`.
- Видеофайлы — этот раскрывающийся список определяется подразделом реестра `PlayVideoFilesOnArrival`.

- Изображения — определяется подразделом реестра `ShowPicturesOnArrival`.
- Чистый DVD — список определяется подразделом системного реестра Windows `HandleDVDBurningOnArrival`.
- Смешанное содержимое — этот раскрывающийся список определяется подразделом реестра `MixedContentOnArrival`.
- Фильмы на диске Blu-ray — определяется подразделом системного реестра Windows `PlayBluRayOnArrival`.
- Звуковой DVD — указывает действие, выполняемое при обнаружении нового DVD в формате Audio DVD. Данный раскрывающийся список определяется подразделом реестра `PlayDVDAudioOnArrival`.
- Фильмы на HD DVD — определяется подразделом реестра `PlayHDDVDOnArrival`.
- Супервидео CD — указывает действие, выполняемое при обнаружении нового диска в формате Super Video CD. Данный раскрывающийся список определяется подразделом реестра `PlaySuperVideoCDMovieOnArrival`.
- Видео CD — определяется подразделом реестра `PlayVideoCDMovieOnArrival`.

Каждый раскрывающийся список может включать в себя как минимум три значения: Не выполнять никаких действий, Спрашивать каждый раз и Открыть папку для просмотра файлов, используя Проводник. Остальные же значения, которые отображаются в выпадающем списке, определяются содержимым ветвей реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers\EventHandlers\<подраздел раскрывающегося списка>`. Здесь `подраздел раскрывающегося списка` представляет собой одно из описанных выше слов, которое определяет конкретный раскрывающийся список в системном реестре. Например, для раскрывающегося списка Видео CD это `PlayVideoCDMovieOnArrival`.

Данные ветви реестра содержат список параметров строкового типа. Их названия определяют команду, которая будет выполняться. Список всех возможных команд, а также их описание можно просмотреть в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\AutoplayHandlers\Handlers`. Существуют следующие команды.

- `EhomeMusicDropTarget` — определяет значение раскрывающегося списка Воспроизводить звуковой CD для воспроизведения в Windows Media Center. По умолчанию оно отображается в следующих раскрывающихся списках: Звуковой CD и Звуковой улучшенный CD.
- `MSOpenFolder` — указывает значение раскрывающегося списка Открыть папку для просмотра файлов. По умолчанию оно отображается во всех раскрывающихся списках.
- `MSTakeNoAction` — определяет значение списка Не выполнять никаких действий. По умолчанию оно отображается во всех раскрывающихся списках.
- `MSPromptEachTime` — указывает значение раскрывающегося списка Спрашивать каждый раз. По умолчанию оно отображается во всех раскрывающихся списках.

- MSAutoRun — определяет значение раскрывающегося списка Установить или выполнить программу. По умолчанию оно отображается в следующих раскрывающихся списках: Звуковой улучшенный CD, Программы и игры, Звуковой улучшенный DVD.
- EHomeVideosHandler — указывает значение раскрывающегося списка Воспроизводить видео для воспроизведения в Windows Media Center. По умолчанию оно отображается в списке Видеофайлы.
- MSShowPicturesOnArrival — определяет значение списка Просмотреть изображения для просмотра с помощью программы Фотоальбом Windows. По умолчанию оно отображается в раскрывающемся списке Изображения.
- EHomePhotosHandler — указывает значение раскрывающегося списка Просмотреть изображения для просмотра с помощью Windows Media Center. По умолчанию оно отображается в списке Изображения.
- MSPhotoAcquireDropHandler — определяет значение списка Импортировать изображения. По умолчанию оно отображается в следующих раскрывающихся списках: Видеофайлы, Изображения.
- MagicUSBCable — указывает значение раскрывающегося списка Перенос файлов и параметров настройки.
- MSDVDArrivalDvdMaker — определяет значение раскрывающегося списка Записать видео-DVD для записи с помощью программы DVD-студия Windows. По умолчанию оно отображается в раскрывающемся списке Чистый DVD.
- MSPlayMediaOnArrival — указывает значение раскрывающегося списка Воспроизводить для воспроизведения в Проигрывателе Windows Media.
- MSSHAudioDevHandler — определяет значение раскрывающегося списка Просмотреть музыкальные файлы.
- MSVideoCameraArrivalCaptureWizard — указывает значение раскрывающегося списка Импорт видео для импортирования видео из устройства с помощью одноименного компонента операционной системы.
- MSWPDNetworkConfigHandler — определяет значение раскрывающегося списка Настройка устройства для сетевого доступа.
- MSWPDShellNamespaceHandler — указывает значение списка Открыть устройство для просмотра файлов.

Например, если вы хотите, чтобы в раскрывающемся списке Звуковой DVD появилось значение Воспроизводить, то в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\AutoplayHandlers\EventHandlers\PlayDVDAudioOnArrival нужно создать параметр строкового типа MSPlayMediaOnArrival.

Если же вы хотите изменить саму команду, которая будет выполняться при обнаружении дисков определенного типа, то нужно воспользоваться параметром (По умолчанию) ветви реестра HKEY_CLASSES_ROOT\<идентификатор команды>\shell\play\DropTarget. Здесь <идентификатор команды> является значением параметра строкового типа InvokeProgId ветви реестра HKEY_LOCAL_MACHINE\

SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\AutoplayHandlers\Handlers.

Однако не все можно сделать с помощью мастера Автозапуск. Например, с его помощью нельзя определить те файлы, при обнаружении которых на вставленном диске будет подавляться любое действие, выполняемое по умолчанию (как не будет выполняться действие по умолчанию, так и не будет отображаться окно Автозапуск). Для этого применяются строковые параметры ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\AutoplayHandlers\CancelAutoplay\Files. Например, чтобы запретить автоматическое действие при обнаружении дисков, содержащих файл noauto.txt, нужно создать в данной ветви реестра параметр строкового типа noauto.txt. При определении параметра строкового типа можно также использовать такие шаблоны подстановки, как ? и *.

Настройка с помощью групповых политик

Некоторые параметры работы функции Автозапуск можно настроить и с помощью групповых политик, описанных в файле AutoPlay.admx и расположенных в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Политики автозапуска.

Политики данного раздела изменяют следующие параметры REG_DWORD-типа, расположенные в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer.

- NoDriveTypeAutoRun — если значение этого параметра равно 0xb5, то механизм автозапуска будет отключен для компакт-дисков и съемных носителей. А если значение равно 0xff, то механизм автозапуска будет отключен для всех устройств.
- DontSetAutoplayCheckbox — при установке значения этого параметра равным 1 по умолчанию будет снят флажок Всегда выполнять выбранное действие.
- NoAutorun — если значение данного параметра равно 1, то содержимое файла autorun.inf исполняться не будет. Если значение равно 2, то содержимое файла autorun.inf будет автоматически исполняться при запуске компакт-диска. По умолчанию же Windows Vista спрашивает у пользователя, запускать или нет команды файла autorun.inf.

Смарт-карта

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: нет.

Файлы службы: SCardSvr.dll.

Исполняемый файл: svchost.exe -k LocalService.

Подраздел реестра: SCardSvr.

Службы, необходимые для работы данной: Plug and Play (PlugPlay).

Реализует доступ к смарт-картам, подключенным к данному компьютеру. После отключения этой службы доступ к смарт-картам с помощью данного компьютера будет невозможен.

ПРИМЕЧАНИЕ

Управление смарт-картами недоступно в версиях Windows Vista Home Basic и Windows Vista Home Premium.

Служба ввода планшетного ПК

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeTcbPrivilege, SeImpersonatePrivilege, SeIncreaseQuotaPrivilege, SeAssignPrimaryTokenPrivilege, SeCreateGlobalPrivilege.

Файлы службы: TabSvc.dll.

Исполняемый файл: svchost.exe -k LocalSystemNetworkRestricted.

Подраздел реестра: TabletInputService.

Службы, необходимые для работы данной: Plug and Play (PlugPlay), Удаленный вызов процедур (RPC) (RpcSs).

Управляет работой механизма доступа к экрану компьютера с помощью пера.

ПРИМЕЧАНИЕ

Возможности работы с планшетными ПК недоступны в версии Windows Vista Home Basic.

Если значение параметра REG_DWORD-типа IsTabletPC, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Tablet PC, равно 1, то ваш компьютер является планшетным и работа этой службы на нем необходима.

Windows Audio

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeImpersonatePrivilege, SeIncreaseWorkingSetPrivilege.

Файлы службы: `Audiosrv.dll`.

Исполняемый файл: `svchost.exe -k LocalServiceNetworkRestricted`.

Подраздел реестра: `Audiosrv`.

Службы, необходимые для работы данной: Средство построения конечных точек Windows Audio (`AudioEndpointBuilder`), Удаленный вызов процедур (RPC) (`RpcSs`), Планировщик классов мультимедиа (`MMCSS`), Сервер упорядочения потоков (`ThreadOrder`).

Управляет работой аудиоподсистемы компьютера. После отключения данной службы программы не смогут работать со звуковыми устройствами.

Средство построения конечных точек Windows Audio

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeChangeNotifyPrivilege.

Файлы службы: `Audiosrv.dll`.

Исполняемый файл: `svchost.exe -k LocalSystemNetworkRestricted`.

Подраздел реестра: `AudioEndpointBuilder`.

Службы, необходимые для работы данной: Plug and Play (`PlugPlay`).

Управляет взаимодействием службы Windows Audio со звуковыми устройствами компьютера. После отключения службы работа со звуковыми устройствами невозможна.

Цветовая система Windows (WCS)

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: нет.

Файлы службы: `WcsPlugInService.dll`.

Исполняемый файл: `svchost.exe -k LocalService`.

Подраздел реестра: `WcsPlugInService`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Обеспечивает поддержку расширений третьего уровня (подключаемые модули, представляющие расширения модели устройства основных цветов из цветовой

схемы ОС и модели сопоставления палитры). При отключении данной службы операционная система сможет использовать только основную модель цветовой схемы, установленную по умолчанию.

Служба загрузки изображений Windows (WIA)

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: `wiaservc.dll`.

Исполняемый файл: `svchost.exe -k imgsvc`.

Подраздел реестра: `stisvc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Определение оборудования оболочки (`ShellHWDetection`).

Управляет получением изображения с подключенных к компьютеру цифровых камер и сканеров.

Безопасность операционной системы

Управление приложениями

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: `appmgmts.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `AppMgmt`.

Службы, необходимые для работы данной: нет.

Управляет установкой, удалением и перечислением приложений, которые были установлены с помощью групповых политик. Иными словами, после отключения данной службы пользователи не смогут устанавливать или удалять данные приложения.

Существует несколько параметров типа `REG_DWORD`, управляющих работой данной службы. Все они расположены в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Diagnostics`.

- `RunDiagnosticLoggingApplicationManagement` — определяет, будет ли выполняться запись сведений о работе данной службы.

- `AppMgmtDebugLevel` — указывает уровень слежения за работой данной службы (какая информация о работе службы будет сохраняться).
- `AppMgmtDebugBreak` — определяет, разрешено ли прекращать слежение за работой данной службы.

Кроме того, служба Управление приложениями также может записывать сведения о своей работе в файл журнала `appmgmt.log`, расположенный в каталоге `%SystemRoot%\Debug\UserMode`.

Служба базовой фильтрации

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: SeAuditPrivilege, SeImpersonatePrivilege.

Файлы службы: `bfe.dll`.

Исполняемый файл: `svchost.exe -k LocalServiceNoNetwork`.

Подраздел реестра: `BFE`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Эта служба управляет работой встроенного брандмауэра Windows и службы IPSec, а также пользовательскими фильтрами брандмауэра. Для отключения данной службы необходимо отключить и службы Маршрутизация и удаленный доступ, Агент политики IPSec, Брандмауэр Windows и Модули ключей IPSec для обмена ключами в Интернете и протокола IP с проверкой подлинности.

Изоляция ключей CNG

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: `lsass.exe`.

Подраздел реестра: `KeyIso`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Данная служба является частью процесса `lsass.exe` и выполняет изоляцию личных ключей пользователей от запущенных процессов в специальном хранилище.

Службы криптографии

Тип запуска: автоматически.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: `cryptsvc.dll`.

Исполняемый файл: `svchost.exe -k NetworkService`.

Подраздел реестра: `CryptSvc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Выполняет следующие действия: управляет базой данных каталога цифровых подписей всех файлов Windows (требуется для установки нового программного обеспечения), управляет восстановлением, добавлением и удалением сертификатов на данном компьютере, поддерживает работу протокола SSL. После отключения данной службы все эти возможности операционной системы будут работать некорректно.

Клиент групповой политики

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeImpersonatePrivilege, SeTcbPrivilege, SeTakeOwnershipPrivilege, SeIncreaseQuotaPrivilege, SeAssignPrimaryTokenPrivilege, SeSecurityPrivilege, SeChangeNotifyPrivilege, SeCreatePermanentPrivilege.

Файлы службы: `gpsvc.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `gpsvc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RPCSS`), Multiple UNC Provider (`Mup`).

Если раньше работа групповых политик осуществлялась с помощью процесса `winlogon.exe`, то теперь для этого предназначена отдельная служба. Она управляет применением групповых политик и определением медленного подключения (при низкой скорости подключения выполняется периодическое применение не всех групповых политик домена, а только основных из них). При этом также изменился способ определения медленного подключения (раньше применялся запрос протокола ICMP, однако это могло вызвать проблемы, так как многие администраторы блокируют передачу ответов на ICMP-запросы).

Кроме того, был изменен способ обнаружения контроллера домена. Теперь для этого применяется обработчик NLA 2.0, который оповещает службу Клиент групповой политики о доступности домена.

ПРИМЕЧАНИЕ

Поддержка групповой политики недоступна в версиях Windows Vista Home Basic и Windows Vista Home Premium.

После отключения данной службы групповые политики применяться не будут. Файл журнала работы данной службы хранится в каталоге `%systemroot%\Debug\UserMode` (файл `gpsvc.log`).

По умолчанию вы не сможете отключить данную службу, так как доступ на запись к ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\gpsvc` запрещен даже администраторам. Поэтому перед отключением данной службы нужно изменить доступ к ветви реестра службы.

В ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions` также хранится набор вложенных подразделов, описывающих расширения групповых политик, загружаемых данной службой при старте операционной системы.

Модули ключей IPSec для обмена ключами в Интернете и протокола IP с проверкой подлинности

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeAuditPrivilege, SeImpersonatePrivilege, SeTcbPrivilege.

Файлы службы: `ikeext.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `IKEEXT`.

Службы, необходимые для работы данной: Служба базовой фильтрации (`BFE`).

Данная служба управляет обменом ключей IPSec, и ее остановка может привести к невозможности установки одноранговых связей с помощью протокола IPSec (так как будет невозможен обмен ключами IKE и AuthIP).

Родительский контроль

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: нет.

Файлы службы: `wpcsvc.dll`.

Исполняемый файл: `svchost.exe -k wpcsvc`.

Подраздел реестра: `WPCSvc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Эта служба управляет работой механизма родительского контроля, и ее остановка приведет к отключению самого механизма родительского контроля.

Служба перечислителя переносных устройств

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: `wpdbusenum.dll`.

Исполняемый файл: `svchost.exe -k LocalSystemNetworkRestricted`.

Подраздел реестра: `WPDBusEnum`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Управляет установкой групповых политик для съемных устройств, а также позволяет Проигрывателю Windows Media и мастеру импорта рисунков передавать и синхронизировать контент, используя сменные устройства.

Защищенное хранилище

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: `lsass.exe`.

Подраздел реестра: `ProtectedStorage`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Управляет защищенным хранилищем, доступ к которому не может получить ни один процесс, кроме этой службы. Защищенное хранилище содержит такие данные пользователя (например, пароли), доступ к которым другим процессам должен быть ограничен.

Диспетчер учетных записей безопасности

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: `lsass.exe`.

Подраздел реестра: `SamSs`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Управляет локальными учетными записями пользователей (SAM) и сигнализирует о том, что база SAM готова к приему запросов. После отключения данной службы возможна некорректная работа других служб, которые не смогут обратиться к базе SAM.

Центр обеспечения безопасности

Тип запуска: автоматически с использованием механизма задержки запуска службы.

Учетная запись: система.

Дополнительные привилегии: SeChangeNotifyPrivilege и SeImpersonatePrivilege.

Файлы службы: `wscsvc.dll`.

Исполняемый файл: `svchost.exe -k LocalServiceNetworkRestricted`.

Подраздел реестра: `wscsvc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Инструментарий управления Windows (`WinMgmt`).

Управляет настройкой системы безопасности и выполняет наблюдение за ее корректностью.

Политика удаления смарт-карт

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: `certprop.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `SCPolicySvc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Управляет блокировкой Рабочего стола пользователя после извлечения смарт-карты, содержащей сертификат входа пользователя в операционную систему.

Основные службы доверенного платформенного модуля

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: нет.

Файлы службы: `tbssvc.dll`.

Исполняемый файл: `svchost.exe -k LocalService`.

Подраздел реестра: `TBS`.

Службы, необходимые для работы данной: нет.

Обеспечивает доступ к модулю TPM, хранящему все конфиденциальные данные системы и пользователя. После отключения данной службы доступ к чипу TPM и всем данным, защищенным с помощью ключей, содержащихся в чипе, будет невозможен.

ПРИМЕЧАНИЕ

Операционная система Windows Vista позволяет просматривать сведения о работе данной службы с помощью счетчиков производительности объекта TBS counters. Объект поддерживает два счетчика: CurrentContexts и CurrentResources.

Брандмауэр Windows

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege, SeIncreaseQuotaPrivilege.

Файлы службы: `mpssvc.dll`.

Исполняемый файл: `svchost.exe -k LocalServiceNoNetwork`.

Подраздел реестра: `MpsSvc`.

Службы, необходимые для работы данной: Драйвер авторизации брандмауэра Windows (`mpsdrv`), Служба базовой фильтрации (`BFE`).

Реализует работу встроенного брандмауэра операционной системы Windows Vista.

Центр обновления Windows

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeAuditPrivilege, SeCreateGlobalPrivilege, SeCreatePageFilePrivilege, SeTcbPrivilege, SeAssignPrimaryTokenPrivilege, SeImpersonatePrivilege, SeIncreaseQuotaPrivilege.

Файлы службы: `wuaueng.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `wuauserv`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Управляет автоматическим поиском, загрузкой и установкой обновлений операционной системы и всех программ, созданных Microsoft.

Работа в сети

Служба шлюза уровня приложения

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: нет.

Исполняемый файл: `alg.exe`.

Подраздел реестра: `ALG`.

Службы, необходимые для работы данной: нет.

Эта служба обеспечивает поддержку сторонних подключаемых модулей протокола для службы ICS (доступ к Интернету с помощью подключения другого компьютера).

Например, по умолчанию с помощью данной службы и содержимого ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ALG\ISV\{6E590D61-F6BC-4dad-AC21-7DC40D304059}` реализуется поддержка клиента FTP. Эта ветвь (а также другие дочерние подразделы подраздела `ISV`) может содержать следующие параметры.

- `Ports` — данный строковый параметр определяет порт, используемый этим модулем.

- `Product` — имеет строковый тип и определяет название модуля.
- `Protocol` — этот параметр типа `REG_DWORD` указывает, реализует ли данный модуль поддержку нового протокола.

Кроме того, с помощью ветви системного реестра Windows `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ALG\ISV` вы можете самостоятельно включать или отключать ненужные дополнительные модули службы ICS. Для этого в данной ветви реестра достаточно создать параметр, название которого соответствует CLSID-номеру модуля, а значение может быть словом `enable` или `disable`.

Фоновая интеллектуальная служба передачи (BITS)

Тип запуска: автоматически с использованием механизма задержки запуска службы.

Учетная запись: система.

Дополнительные привилегии: SeCreateGlobalPrivilege, SeImpersonatePrivilege, SeTcbPrivilege, SeAssignPrimaryTokenPrivilege, SeIncreaseQuotaPrivilege.

Файлы службы: `qmgr.dll`, `qmgrprxy.dll`, `bitsprx2.dll`, `bitsprx3.dll`, `bitsprx4.dll`, `bitsprx5.dll`, `bitsigd.dll` и `bitsperf.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `BITS`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Система событий COM+ (`EventSystem`).

Управляет фоновой передачей данных по сети (при ее бездействии) между клиентом и сервером. Служба используется для получения файлов такими приложениями, как, например, MSN Explorer или Служба обновления Windows, поэтому после отключения данной службы использующие ее приложения не смогут загружать файлы.

ПРИМЕЧАНИЕ

Сведения о работе службы BITS заносятся в журнал, расположенный в разделе Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Bits-Client.

Операционная система Windows Vista позволяет просматривать сведения о работе данной службы с помощью счетчиков производительности объекта Использование сети BITS. Например, с помощью счетчиков данного объекта можно узнать следующие сведения о работе службы.

- Предполагаемую скорость передачи данных от удаленного компьютера (счетчик Скорость удаленного сервера (бит/с)), предполагаемую скорость интернет-соединения (счетчик Скорость IGD (бит/с)), предполагаемую скорость локальной

сетевой карты (счетчик Скорость сетевой платы (бит/с)). Благодаря счетчику Расчетное значение пропускной способности, доступной для удаленной системы (бит/с) можно также узнать предполагаемую полосу пропускания, доступную службе BITS в удаленной системе.

- Процент использования интернет-соединения (счетчик Процент свободного IGD) и процент использования пропускной способности сетевой карты (счетчик Процент свободных ресурсов сетевой платы).
- Размер следующего блока данных, загружаемых службой BITS (счетчик BITS Размер загружаемого блока BITS (байт)), а также интервал отклика при загрузке данных (счетчик Интервал отклика BITS при загрузке (мсек)).

Служба BITS присутствовала и в предыдущих версиях Windows, но в Windows Vista она улучшена с целью снижения стоимости ее использования. Теперь другие компьютеры сети могут предоставлять для совместного доступа службам BITS уже загруженные ими файлы, чтобы другие службы повторно не скачивали их в случае необходимости из Интернета.

Файлы, скачиваемые данной службой, хранятся в каталоге `%systemdrive%\ProgramData\Microsoft\Network\Downloader`.

Настройки групповых политик

Некоторые параметры настройки службы Фоновая интеллектуальная служба передачи (BITS) можно изменить с помощью групповых политик. Все эти политики расположены в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Сеть ▸ Фоновая интеллектуальная служба передачи (BITS).

- `DisablePeerCachingClient` — если значение данного параметра равно `1`, то локальному компьютеру будет запрещено выступать в качестве клиента кэширования членов одноранговой группы BITS при загрузке файлов. Иначе говоря, данный компьютер сможет загружать файлы только с основного сервера одноранговой сети. В противном случае он также будет пытаться загружать файлы и из других компьютеров сети, которым разрешено быть серверами кэширования.
- `DisablePeerCachingServer` — при установке значения этого параметра равным `1` локальному компьютеру будет запрещено выступать в качестве сервера кэширования членов одноранговой группы BITS при загрузке файлов. Иными словами, данный компьютер не будет кэшировать загружаемые файлы и предоставлять их для загрузки другим компьютерам сети.
- `EnableBITSMaxBandwidth` — если значение данного параметра равно `1`, то пропускная способность сети, используемая службой BITS для фоновой передачи данных, будет ограничена значениями параметров `MaxBandwidthValidFrom`, `MaxBandwidthValidTo`, `MaxTransferRateOffSchedule`, `MaxTransferRateOnSchedule` и `UseSystemMaximum`.
- `MaxBandwidthValidFrom` — значение данного параметра определяет время, от которого будет ограничена пропускная способность канала, используемого службой BITS.

- `MaxBandwidthValidTo` — значение этого параметра определяет время, до которого будет ограничена пропускная способность канала, используемого службой BITS.
- `MaxTransferRateOffSchedule` — его значение определяет скорость передачи данных (в Кбайт/с) в часы, когда скорость передачи не ограничена.
- `MaxTransferRateOnSchedule` — значение данного параметра определяет скорость передачи данных (в Кбайт/с) в часы ограничения скорости передачи.
- `UseSystemMaximum` — если значение данного параметра равно `1`, то будет использоваться вся полоса пропускания сети в часы, когда скорость передачи не ограничена.
- `MaxBandwidthServed` — значение данного параметра определяет максимальную полосу пропускания, разрешенную для передачи кэшированных файлов другим компьютерам одноранговой сети. По умолчанию используется ограничение в 30 % от пропускной способности самого медленного соединения.
- `MaxRangesPerFile` — его значение указывает максимальное количество диапазонов, которые могут быть добавлены к файлу в задании BITS. По умолчанию максимальное количество диапазонов равно `500`.
- `MaxJobsPerUser` — значение этого параметра определяет максимальное количество заданий службы BITS, которые могут быть созданы одним пользователем. По умолчанию пользователь может создать только 60 заданий.
- `MaxJobsPerMachine` — его значение указывает максимальное количество заданий службы BITS, которые могут быть созданы всеми пользователями компьютера. По умолчанию значение данного параметра равно `300`.
- `MaxFilesPerJob` — значение параметра определяет максимальное количество файлов, которые можно загрузить в рамках одного задания. По умолчанию в рамках одного задания нельзя загружать больше 200 файлов.
- `MaxCacheSize` — значение указывает максимальный объем диска, который может использоваться для кэширования файлов, которые впоследствии будет разрешено скачивать другим клиентам одноранговой сети. По умолчанию размер кэша равен 1 % от общего объема диска.
- `MaxContentAge` — его значение определяет максимальное количество дней, в течение которых хранить данные в кэше разрешено (потом они будут удаляться). По умолчанию из кэша удалятся файлы, хранящиеся в нем более 14 дней.
- `EnablePeercaching` — если значение данного параметра равно `0`, то кэширование файлов для членов одноранговой группы будет запрещено.

BITS Administration Utility

Расположение: `%systemroot%\system32\bitsadmin.exe`.

Для настройки службы BITS предназначена специальная программа командной строки. Ее возможности очень подробно документированы в справке по программе, которая вызывается командой `bitsadmin /?`. Однако, чтобы вы понимали

хотя бы основные возможности данной программы, рассмотрим несколько способов ее использования.

Просмотр версии BITS и проверка корректности его работы. Для обеих задач применяется команда `bitsadmin /util /version /verbose`. После ее выполнения попробует запуститься служба, а также будет отображена следующая информация о ней: версии основных DLL-файлов службы, используемый ими язык, а также их имена, указание, используется ли в системе вспомогательная служба BITS, и если используется, то также отображается путь к ее библиотеке (он содержится в параметре строкового типа `ServiceDLL` ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\BITS`). Также будут отображены сведения о том, имеются ли незаконченные операции переименования файлов, принадлежащих BITS, и активирована ли политика слежения за временем бездействия службы.

Если по каким-то причинам служба BITS работает некорректно, то с помощью программы `bitsadmin.exe` можно попробовать восстановить основные параметры работы службы BITS и смежных с ней служб. Для этого используется команда `bitsadmin /util /repairservice /force`.

Настройка прокси-сервера браузера Internet Explorer для учетных записей системы, используемых службами. Если вы используете прокси-сервер, то для корректной работы служб и программ со службой BITS, возможно, придется самостоятельно настроить параметры прокси-сервера для следующих системных учетных записей: LOCAL SYSTEM, NETWORK SERVICE и LOCAL SERVICE. Для этого можно использовать программы `bitsadmin.exe`.

Перед самостоятельной настройкой прокси-сервера можно посмотреть его текущие настройки для определенной учетной записи. Для этого применяется команда `bitsadmin /util /getieproxy <системная учетная запись>`.

Если отображенные после применения предыдущей команды настройки неверны, то для их изменения нужно воспользоваться командой `bitsadmin /util /setieproxy <системная учетная запись> <настройки прокси>`. Здесь `<настройки прокси>` могут состоять из следующих параметров.

- `AUTODETECT` — при каждом соединении учетная запись будет самостоятельно выполнять поиск прокси-сервера.
- `NO_PROXY` — прокси-сервер не используется. Вместе с этим можно использовать параметр `/CONN <название соединения>`, чтобы указать имя конкретного соединения, которое будет использоваться учетной записью.
- `MANUAL_PROXY <адрес_прокси:порт, адрес_прокси:порт,…> <адрес прокси для локальных адресов>` — позволяет самостоятельно настроить параметры прокси-сервера, используемые данной учетной записью. Можно указывать как один, так и несколько прокси. Вместо адреса прокси для локальных адресов можно использовать значения `<Local>` или `NULL`.
- `AUTOSCRIPT <путь>` — указывает путь к сценарию, который будет использоваться для настройки параметров подключения.

Настройка аналитического канала BITS. С помощью программы `bitsadmin.exe` вы можете включить или отключить использование аналитического канала службы BITS. Он используется для записи аналитических сведений в стандартный журнал операционной системы. Для этого достаточно воспользоваться командой `bitsadmin /util /enableanalyticchannel <true или false>`.

Сведения об аналитическом канале службы BITS хранятся в ветви системного реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Bits-Client/Analytic`. Отключение канала приводит к тому, что параметру `REG_DWORD`-типа `Enabled` этой ветви присваивается значение `0`. Кроме того, это приводит к удалению подраздела, определяющего настройки создания стандартного журнала Windows, из ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger`.

Кроме параметра `Enabled`, ветвь реестра содержит другие параметры, некоторые из которых мы уже рассмотрели ранее в этой книге (в разд. 5.2 при рассмотрении оснастки `eventvwr.msc`).

ПРИМЕЧАНИЕ

Служба BITS создает еще один канал, параметры работы которого описаны в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Bits-Client/Operational. Параметры этого канала аналогичны параметрам аналитического канала.

Работа с записями кэша и областями службы BITS. Для работы с записями кэша службы BITS применяется команда вида `bitsadmin /cache <параметры>`. Можно указывать следующие параметры данной команды.

- `/LIST /VERBOSE` — отображает сведения о записях, которые расположены в кэше службы BITS.
- `/INFO <запись> /VERBOSE` — отображает полные сведения о конкретной записи кэша.
- `/DELETE <запись>` — удаляет запись из кэша.
- `/DELETEURL <URL-адрес>` — удаляет из кэша все записи, имеющие данный URL-адрес.
- `/CLEAR` — полностью очищает содержимое кэша службы.
- `/GETLIMIT` — отображает возможное максимальное количество записей в кэше службы.
- `/SETLIMIT <количество>` — устанавливает новое максимальное количество записей в кэше службы.
- `/GETEXPIRATIONTIME` — отображает время жизни записи в кэше.
- `/SETEXPIRATIONTIME <время в секундах>` — устанавливает новое время жизни записи в кэше.

- `/ENABLECLIENT <true или false>` — разрешает или запрещает помещение в кэш клиентских записей.
- `/ENABLESERVER <true или false>` — разрешает или запрещает помещение в кэш серверных записей.

Если же нужно просмотреть существующие области, то необходимо воспользоваться командой `bitsadmin /neighborhood <параметры>`. Можно указывать следующие параметры этой команды.

- `/LIST` — отображает сведения обо всех областях службы BITS.
- `/INFO <имя области>` — выводит сведения о конкретной области.
- `/CLEAR` — очищает список областей.
- `/DISCOVER` — снова выполняет поиск областей.
- `/GETLIMIT` — отображает возможное максимальное количество областей службы.
- `/SETLIMIT <количество>` — устанавливает новое максимальное количество областей.
- `/GETEXPIRATIONTIME` — отображает время жизни области в списке службы BITS.
- `/SETEXPIRATIONTIME <время в секундах>` — устанавливает новое время жизни области в списке службы BITS.
- `/SETAVAILABLE <FQDN-имя> <true или false>` — разрешает или запрещает использование данной области.
- `/SETAUTH <FQDN-имя> <true или false>` — разрешает или запрещает аутентификацию данной области.
- `/GETSEARCHCOUNT` — отображает количество возможных контактов при поиске в областях.
- `/SETSEARCHCOUNT <количество>` — устанавливает новое количество возможных контактов при поиске в областях. Указанное вами значение заносится в параметр `REG_DWORD`-типа `ContentDiscoverySearches` ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\BITS`.

Работа с заданиями службы BITS. Основным назначением службы BITS является выполнение заданий, которые ставят перед ней другие службы и программы, поэтому было бы странно, если бы с помощью программы `bitsadmin.exe` нельзя было управлять этими заданиями.

Вкратце рассмотрим основной список команд программы `bitsadmin.exe`, предназначенных для работы с заданиями.

- `Bitsadmin /list /allusers /verbose` — отображает список всех заданий от всех пользователей, которые находятся в очереди заданий. При этом отображаются следующие сведения о задании: его CLSID-номер, имя файла,

в передаче которого заключается задание, тип задания, его состояние выполнения, создатель, приоритет, ACL-флаги, время создания, список используемых для выполнения задания прокси-серверов и многое другое.

Кроме того, сведения об определенном задании можно вывести с помощью команды `Bitsadmin /info <CLSID-номер задания или его имя> /verbose`. Также можно отобразить только конкретные сведения об определенном задании. Для этого применяются следующие команды.

- `Bitsadmin /GETTYPE <CLSID-номер задания или его имя>` — отображает тип задания.
- `Bitsadmin /GETACLFLAGS <CLSID-номер задания или его имя>` — выводит ACL-флаги задания.
- `Bitsadmin /GETBYTESTOTAL <CLSID-номер задания или его имя>` — отображает общий размер задания.
- `Bitsadmin /GETBYTESTRANSFERRED <CLSID-номер задания или его имя>` — выводит количество переданных байт задания.
- `Bitsadmin /GETFILESTOTAL <CLSID-номер задания или его имя>` — отображает общее количество файлов в задании.
- `Bitsadmin /GETFILESTRANSFERRED <CLSID-номер задания или его имя>` — выводит количество переданных файлов задания.
- `Bitsadmin /GETCREATIONTIME <CLSID-номер задания или его имя>` — отображает дату создания задания.
- `Bitsadmin /GETSTATE <CLSID-номер задания или его имя>` — выводит состояние выполнения задания.
- `Bitsadmin /GETOWNER <CLSID-номер задания или его имя>` — отображает создателя задания.
- `Bitsadmin /GETPRIORITY <CLSID-номер задания или его имя>` — выводит приоритет задания.

Просматривать список заданий можно и в режиме мониторинга. Для этого применяется команда `Bitsadmin /monitor /allusers /refresh <время обновления в секундах>`. После ввода данной команды экран командной строки очистится и на нем будут отображаться сведения о только что добавленных заданиях (CLSID-номер задания и файл, в передаче которого заключается задание). Чтобы выйти из режима мониторинга, нужно нажать комбинацию клавиш Ctrl+C.

- `Bitsadmin /reset /allusers` — удаляет все задания от всех пользователей.

Можно удалить и конкретное задание. Для этого применяется такая команда, как `Bitsadmin /cancel <CLSID-номер задания или его имя>`.

- `Bitsadmin /TRANSFER <имя задания> <тип задания> <URL или UNC-имя удаленного компьютера> <локальное имя получаемого файла>` — создает задание и сразу же его выполняет.

- `Bitsadmin /create <тип задания> <имя задания>` — создает задание определенного типа. Для указания типа задания применяется один из следующих параметров.
  - `/DOWNLOAD` — задание заключается в загрузке файла на локальный компьютер. Данный тип задания используется по умолчанию.
  - `/UPLOAD` — заключается в загрузке файла на удаленный компьютер.
  - `/UPLOAD-REPLY` — задание заключается в ответе на загрузку файла.

После того как будет создано задание, можно настроить следующие параметры его работы.

- Файлы, передаваемые при выполнении задания. Для этого применяется одна из следующих команд.
  - `Bitsadmin /ADDFILE <CLSID-номер задания или его имя> <URL или UNC-имя удаленного компьютера> <локальное имя получаемого файла>` — добавляет определенный файл в задание.
  - `Bitsadmin /ADDFILESET <CLSID-номер задания или его имя> <URL или UNC-имя удаленного компьютера> <название и путь к текстовому файлу>` — указывает путь к текстовому файлу. В нем записан список файлов, которые нужно передать при выполнении задания.

    Формат данного файла довольно прост: в каждой строке нужно указывать одно URL- или UNC-имя удаленного компьютера и одно имя локального файла (разделенные пробелом). Строки, начинающиеся с символа #, считаются комментариями.
- ACL, распространяемое на передачу задания. Для этого применяется команда `Bitsadmin /setaclflags <CLSID-номер задания или его имя> <флаги ACL>`. Возможны следующие флаги ACL: `O` (владелец), `G` (группа), `D` (DACL), `S` (SACL). Можно указать сразу несколько флагов ACL. Например, `OGS`.
- Другие параметры задания.
  - `Bitsadmin /SETDESCRIPTION <CLSID-номер задания или его имя> <описание>` — изменяет описание данного задания.
  - `Bitsadmin /SETPRIORITY <CLSID-номер задания или его имя> <приоритет>` — меняет приоритет задания.
  - `Bitsadmin /SETMINRETRYDELAY <CLSID-номер задания или его имя> <задержка перед повторным выполнением задания>` — изменяет задержку перед повторным выполнением задания.

Можно также указать состояние выполнения задания. Для этого применяются следующие команды.

- `Bitsadmin /SUSPEND <CLSID-номер задания или его имя>` — приостанавливает выполнение задания.

- `Bitsadmin /RESUME <CLSID-номер задания или его имя>` — продолжает выполнение задания.
- `Bitsadmin /COMPLETE <CLSID-номер задания или его имя>` — завершает выполнение задания.

Обозреватель компьютеров

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `Browser`.

Службы, необходимые для работы данной: Рабочая станция (`LanmanWorkstation`), Сервер (`LanmanServer`).

Данная служба предоставляет пользовательским процессам сведения о других подключенных к сети компьютерах и принтерах. Если службы Обозреватель компьютеров на всех компьютерах сети будут отключены, то, например, вы не сможете увидеть список компьютеров сети с помощью значка Сетевого окружения, или любой мастер, отображающий список компьютеров и принтеров сети, не сможет найти ни одного компьютера или принтера. Это не говорит о том, что вы не сможете получить доступ к компьютерам сети: если вы знаете точное имя компьютера (или принтера) или его IP-адрес, то сможете получить к нему доступ.

Операционная система Windows Vista поддерживает набор счетчиков производительности, с помощью которых можно следить за состоянием работы данной службы. Они принадлежат объекту Обозреватель сети и позволяют просматривать следующие сведения.

- Частота, с которой домен или сервер извещают о своем существовании (счетчики Объявлений домена/сек, Объявлений сервера/сек и Всего объявлений/сек). Можно также просмотреть количество объявлений серверов, которые были потеряны (счетчик Промахов объявлений серверов) или не обработаны из-за нехватки памяти (счетчик Ошибок распределения объявлений сервера/сек), и количество ситуаций, когда один основной обозреватель обнаружил в том же домене еще один основной обозреватель (счетчик Дублирование объявлений основного обозревателя).
- Частота, с которой служба Обозреватель компьютеров обрабатывает запросы обзора серверов, доменов и прочих станций (счетчики Нумераций сервером/сек, Нумераций доменом/сек, Прочих нумераций/сек, Всего перечислений/сек). Можно также просмотреть количество обработанных (счетчик Запросов на список

серверов/сек) и необработанных (счетчик Промахов запросов на список серверов) запросов на получение списка обозревателей сети.

- Количество ошибок почтового слота, связанных с выделением буфера для размещения пользовательских данных (счетчик Ошибок распределения почтовых слотов) и с отсутствием почтового слота (счетчик Ошибок открытия почтового слота/сек), ошибок при транспортировке в почтовый слот (счетчик Ошибок приема в почтовый слот), ошибок записи в почтовый слот (Ошибок записи в почтовый слот), а также количество датаграмм почтовых слотов, отброшенных из-за нехватки памяти (счетчик Промахов датаграмм почтовых слотов). Можно также просмотреть количество успешных записей в почтовый слот (счетчик Операций записи в почтовый слот/сек).

Рекомендуется отключить службы Обозреватель компьютеров на всех компьютерах сети, кроме одного. В этом случае служба сможет работать нормально, и при этом не будет генерироваться лишний сетевой трафик (через определенный интервал времени все работающие службы выбирают основной обозреватель компьютеров, что порождает лишний трафик, если же в сети есть только одна служба, то она автоматически будет назначать себя основной).

Служба Обозреватель компьютеров поддерживает некоторые параметры реестра, хранящиеся в ветви `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BROWSER\Parameters`.

- `MaintainServerList` — если значение данного параметра строкового типа равно `yes`, то ваш компьютер может участвовать в выборах основного обозревателя компьютеров. Если вы не хотите отключать службу Обозреватель компьютеров на компьютерах сети, то можно просто присвоить значение `no` этому параметру для всех компьютеров сети, кроме одного. Тогда только один компьютер сможет участвовать в выборах, и только он всегда будет основным.
- `CacheResponseSize` — этот параметр типа `REG_DWORD` определяет размер кэша ответов, используемого службой Обозреватель компьютеров.
- `QueryDriverFrequency` — имеет тип `REG_DWORD` и определяет частоту опроса драйвера службой Обозреватель компьютеров.
- `DisableStopOnPortsClosed` — этот параметр типа `REG_DWORD` определяет, будет ли завершаться работа данной службы, если порты, используемые ею, закрыты.
- `AllowPassThrough` — имеет тип `REG_DWORD` и определяет, разрешена ли транзитная пересылка.

Модуль запуска процессов DCOM-сервера

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeDebugPrivilege, SeImpersonatePrivilege, SeIncreaseQuotaPrivilege, SeTcbPrivilege.

Файлы службы: rpcss.dll.

Исполняемый файл: svchost.exe -k DcomLaunch.

Подраздел реестра: DcomLaunch.

Службы, необходимые для работы данной: нет.

Обеспечивает запуск служб DCOM. Служба DCOM необходима для выполнения взаимодействия между COM-компонентами, установленными на разных компьютерах. Если ваш компьютер не подключен к сети или вы не хотите, чтобы приложения COM, установленные на вашем компьютере, могли взаимодействовать с приложениями COM удаленных компьютеров, то службу DCOM можно отключить. Однако вы не сможете это сделать с помощью оснастки services.msc, так как доступ к подразделу реестра DcomLaunch по умолчанию отсутствует даже у администраторов. По этой причине перед отключением службы нужно изменить права доступа к данной ветви реестра. Хотя отключать ее все-таки не стоит, так как это может привести к непредсказуемым последствиям.

Репликация DFS

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege, SeImpersonatePrivilege, SeTcbPrivilege, SeLoadDriverPrivilege.

Файлы службы: нет.

Исполняемый файл: DFSR.exe.

Подраздел реестра: DFSR.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (RpcSs), Система событий COM+ (EventSystem).

Синхронизирует файлы, которые требуют синхронизации, между компьютерами сети. При отключении данной службы не будет работать не только механизм синхронизации, но и автоматическое обновление содержимого открытого в данный момент сетевого каталога.

При первом запуске данной службы в оснастке eventvwr.msc создается новый стандартный журнал Репликация DFS, расположенный в подразделе Журналы приложений и служб.

База данных службы содержится в каталоге System Volume Information\DFSR.

Настройки службы Репликация DFS хранятся в ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\DFSR\Parameters. Например, данная ветвь реестра содержит параметр REG_DWORD-типа Enable Remote Namespace Access,

который определяет, разрешен ли удаленный доступ к пространству имен службы. А еще эта ветвь реестра может содержать параметр `REG_DWORD`-типа `Enable Verbose Event Logging`, который определяет, как много сведений будет заноситься в файл журнала службы Репликация DFS.

Эта ветвь реестра также включает в себя параметр расширенного строкового типа `Machine Configuration File`, который указывает путь к XML-файлу, хранящему настройки службы. Данные настройки применяются при запуске службы Репликация DFS. По умолчанию XML-файл содержит лишь настройки, влияющие на ведение файла журнала службы. Например, к ним относятся следующие настройки: каталог, хранящий файл журнала `dfsrXXXXX.log`, его размер, максимальное количество сообщений, а также указание, будет ли вообще выполняться запись сведений о работе службы в файл журнала (по умолчанию запись сведений не ведется).

Возможности репозитария CIM. Репозитарий CIM операционной системы Windows Vista стал включать в себя набор классов, с помощью которых можно просматривать сведения о работе службы Репликация DFS, а также управлять ее работой. Все эти классы расположены в пространстве имен `\\root\MicrosoftDfs`.

Класс DfsrConfig

Содержит описание параметров службы Репликация DFS. Свойства данного класса доступны только для чтения:

- `ProviderVersion`, тип: `string` — содержит версию провайдера DFS;
- `ServiceVersion`, тип: `string` — содержит версию службы Репликация DFS.

Класс также включает в себя метод `PollDsNow`. Он опрашивает доменную службу Active Directory и применяет изменения в конфигурации, если таковые вообще имеются.

Входящий параметр: строковый параметр, определяющий DNS-имя контроллера домена.

Возвращаемые параметры: нет.

Класс DfsrMachineConfig

Определяет конфигурацию службы Репликация DFS на локальном компьютере. Следующие свойства данного класса доступны как для чтения, так и для записи.

- `ConflictHighWatermarkPercent`, тип: `uint32` — может принимать значения от 80 до 100. Оно определяет процент, который должен превысить размер папки Conflict and Deleted, чтобы начался процесс очистки конфликтов.
- `ConflictLowWatermarkPercent`, тип: `uint32` — свойство может принимать значения от 10 до 80. Оно определяет процент, до которого должен опуститься размер папки Conflict and Deleted, чтобы процесс очистки конфликтов был остановлен.

- `DebugLogFilePath`, тип: `string` — не может содержать более чем 2600 символов. Оно определяет путь к файлу журнала.
- `DebugLogSeverity`, тип: `uint32` — может принимать значения от 1 до 5. Определяет уровень детальности записи в файл журнала.
- `Description`, тип: `string` — содержит описание текущих настроек компьютера.
- `DsPollingIntervalInMin`, тип: `uint32` — определяет интервал в минутах между окончанием одного цикла службы доменов Active Directory и началом другого.
- `EnableDebugLog`, тип: `boolean` — определяет, разрешена ли запись в файл журнала.
- `EnableLightDsPolling`, тип: `boolean` — определяет, будет ли периодически выполняться неполная проверка изменений в конфигурации службы доменов Active Directory. Это ускоряет начало некоторых типов изменений в конфигурации.
- `LastChangeNumber`, тип: `uint32` — доступно только для чтения. Оно определяет номер последних изменений в конфигурации и увеличивается на единицу при каждом обнаружении новых изменений.
- `LastChangeSource`, тип: `string` — доступно только для чтения. Оно содержит информацию об авторе изменения.
- `LastChangeTime`, тип: `datetime` — доступно только для чтения. Оно определяет время возникновения изменений в конфигурации.
- `MaxDebugLogFiles`, тип: `uint32` — определяет максимальный номер создаваемого файла журнала.
- `MaxDebugLogMessages`, тип: `uint32` — значение данного свойства не может быть меньше 1000. Оно определяет максимальное количество записей в каждом файле журнала.
- `MaxOfflineTimeInDays`, тип: `uint32` — определяет максимальное количество дней, которые реплицированный каталог может быть разъединен с партнерами. После истечения этого срока данный каталог считается неактуальным, и возникает состояние ошибки.
- `ReghostingRateInMin`, тип: `uint32` — значение данного свойства не может быть меньше 60. Оно определяет интервал в минутах между запусками процесса сканирования корня каталогов для поиска неизмененных файлов. Для экономии места на диске данные файлы перемещаются к своим теневым копиям.
- `RootHighWatermarkPercent`, тип: `uint32` — его значение не может быть меньше 40. Оно определяет процент занятого места в корневом каталоге, при котором начинается сканирование корня каталогов для поиска неизмененных файлов.
- `RootLowWatermarkPercent`, тип: `uint32` — может принимать значения от 10 до 40. Оно определяет процент занятого места в корневом каталоге, при достижении которого процесс сканирования корня каталогов завершается.

- `RpcPortAssignment`, тип: `uint32` — определяет порт, используемый RPC. По умолчанию значение данного свойства равно `0`, что говорит о том, что RPC может использовать любой порт. Для вступления в силу изменений необходимо перезапустить службу Репликация DFS.
- `StagingHighWatermarkPercent`, тип: `uint32` — может принимать значения от 80 до 100. Оно определяет процент использования каталога организации, при достижении которого начинается процесс очистки.
- `StagingLowWatermarkPercent`, тип: `uint32` — может принимать значения от 10 до 80. Оно определяет процент использования каталога организации, при достижении которого процесс очистки завершается.

Класс DfsrVolumeConfig

Класс хранит параметры настройки разделов компьютера, которые содержат реплицируемые папки. Следующие свойства данного класса доступны только для чтения.

- `DatabasePath`, тип: `string` — значение данного свойства не может содержать более 2600 символов. Оно определяет путь к каталогу, который хранит базу данных реплицируемых папок.
- `LastChangeNumber`, тип: `uint32` — определяет номер последних изменений в конфигурации и увеличивается на единицу при каждом обнаружении новых изменений.
- `LastChangeSource`, тип: `string` — содержит информацию об авторе изменения.
- `LastChangeTime`, тип: `datetime` — определяет время возникновения изменений в конфигурации.
- `MinNtfsJournalSizeInMb`, тип: `uint32` — определяет минимальный размер (в Мбайт) журнала номеров последовательности изменения (USN). Если журнал USN отсутствует, то служба Репликация DFS создает новый журнал с указанным в данном свойстве значением. Данное свойство доступно как для чтения, так и для записи. Оно может принимать значения от 4 до 10 000.
- `SerialNumber`, тип: `uint64` — содержит серийный номер раздела.
- `VolumeGuid`, тип: `string` — является ключевым. Оно определяет уникальный идентификатор раздела.
- `VolumePath`, тип: `string` — определяет путь к разделу.

Класс DfsrReplicatedFolderConfig

Данный класс определяет настройки конфигурации реплицируемой папки. Его свойства доступны только для чтения.

- `CacheObeyConnectionSchedule`, тип: `boolean` — определяет, удовлетворяет ли назначенное соединение репликации по требованию.
- `CompressedExtensions`, тип: `string` — определяет список расширений (разделенных между собой запятыми), файлы которых будут сжиматься.

- `ConflictPath`, тип: `string` — значение данного свойства не может состоять больше чем из 2600 символов. Оно определяет путь к локальному каталогу Conflict and Deleted.
- `ConflictSizeInMb`, тип: `uint32` — его значение не может быть меньше 10. Оно определяет размер квоты для каталога Conflict and Deleted в мегабайтах.
- `Description`, тип: `string` — содержит описание данной реплицируемой папки.
- `DirectoryFilter`, тип: `string` — определяет список каталогов-исключений, разделенных между собой запятыми. Значение данного свойства не может состоять больше чем из 2600 символов.
- `DisableReanimateDeletes`, тип: `boolean` — определяет, могут ли отдаленные удаления быть отменены при обновлении конфликтов.
- `DisableSaveDeletes`, тип: `boolean` — если значение данного свойства равно `true`, то удаленные файлы не будут перемещаться в каталог Conflict and Deleted.
- `Enabled`, тип: `boolean` — определяет, разрешена ли репликация каталога.
- `FileFilter`, тип: `string` — указывает список файлов-исключений, разделенных между собой запятыми. Значение данного свойства не может состоять больше чем из 2600 символов.
- `Ghosted`, тип: `boolean` — определяет, разрешено ли службе Репликация DFS использовать теневое копирование.
- `IsPrimary`, тип: `boolean` — указывает, было ли содержимое каталога при инициализации процесса репликации наиболее актуальным.
- `MaxAgeInCacheInMin`, тип: `uint32` — определяет максимальную продолжительность (в минутах) хранения ресурса в кэше, прежде чем начнется процесс его перезаписи.
- `MemberGuid`, тип: `string` — содержит уникальный идентификатор членства реплицируемого каталога.
- `MinAgeInCacheInMin`, тип: `uint32` — определяет минимальную продолжительность (в минутах) хранения теневого ресурса в кэше, после истечения которой ресурс будет поставлен на рассмотрение возможности помещения в хранилище теневых копий.
- `ReadOnly`, тип: `boolean` — определяет, можно ли изменять содержимое реплицируемого каталога.
- `ReplicatedFolderDn`, тип: `string` — определяет имя каталога, известное в службе доменов Active Directory.
- `ReplicatedFolderGuid`, тип: `string` — является ключевым. Оно определяет уникальный идентификатор реплицируемого каталога.
- `ReplicatedFolderName`, тип: `string` — определяет имя реплицируемого каталога.
- `ReplicationGroupGuid`, тип: `string` — указывает уникальный идентификатор группы, к которой принадлежит данный реплицируемый каталог.

- `RootPath`, тип: `string` — определяет локальный путь к реплицируемому каталогу. Значение данного свойства не может состоять больше чем из 2600 символов.
- `RootSizeInMb`, тип: `uint32` — указывает квоту в мегабайтах для папки, содержащей реплики данного каталога. Значение этого свойства не может быть меньше 10.
- `SharedStaging`, тип: `boolean` — определяет, может ли каталог организации быть общего доступа.
- `StagingPath`, тип: `string` — указывает путь к каталогу организации. Значение данного свойства не может состоять больше чем из 2600 символов.
- `StagingSizeInMb`, тип: `string` — определяет квоту в мегабайтах для каталога организации. Значение данного свойства не может быть меньше 10.
- `VolumeGuid`, тип: `string` — указывает уникальный идентификатор раздела, содержащего данную реплицируемую папку.

Класс DfsrReplicationGroupConfig

Определяет настройки группы репликации на данном компьютере. Свойства данного класса доступны только для чтения.

- `DefaultSchedule`, тип: массив значений `uint8` — определяет используемое по умолчанию расписание для данной группы репликации.
- `DefaultScheduleInUtc`, тип: `boolean` — определяет, на основе чего назначено расписание репликации группы: локального времени или другого UTC.
- `Description`, тип: `string` — содержит описание группы репликации.
- `LastChangeNumber`, тип: `uint32` — определяет номер последних изменений в конфигурации и увеличивается на единицу при каждом обнаружении новых изменений.
- `LastChangeSource`, тип: `string` — содержит информацию об авторе изменения.
- `LastChangeTime`, тип: `datetime` — определяет время возникновения изменений в конфигурации.
- `ReplicationGroupDn`, тип: `string` — содержит название группы репликации, используемое службой доменов Active Directory.
- `ReplicationGroupGuid`, тип: `string` — является ключевым. Оно определяет уникальный идентификатор группы репликации.
- `ReplicationGroupName`, тип: `string` — определяет имя группы репликации.
- `ReplicationGroupType`, тип: `uint32` — указывает тип группы репликации. Например, возможны следующие значения данного свойства: `0` (`OTHER`), `1` (`SYSVOL`), `2` (`PROTECTION`), `3` (`DISTRIBUTION`), `4` (`CLIENT`), `5` (`PEERNET`).
- `TombstoneExpiryInMin`, тип: `uint32` — определяет максимальное время жизни объектов (в минутах). Значение данного свойства не может быть меньше 60.

Класс DfsrLocalMemberConfig

Содержит описание класса членства групп репликации. Свойства данного класса доступны только для чтения.

- `Keywords`, тип: `string` — содержит ключевые слова, используемые для идентификации и группировки.
- `MemberDn`, тип: `string` — определяет имя данного членства, известное в службе доменов Active Directory.
- `MemberDns`, тип: `string` — содержит специальное имя членства, используемое сервером DNS.
- `MemberGuid`, тип: `string` — является ключевым. Оно содержит уникальный идентификатор членства.
- `MemberName`, тип: `string` — определяет имя членства.
- `MemberPeerNetGroupName`, тип: `string` — указывает имя членства для одноранговых сетей.
- `ReplicationGroupGuid`, тип: `string` — определяет уникальный идентификатор реплицируемой группы.

Класс DfsrConnectionConfig

Класс определяет настройки соединений для реплицируемых групп. Следующие свойства данного класса доступны только для чтения.

- `ConnectionDn`, тип: `string` — определяет имя соединения, известное в службе доменов Active Directory.
- `ConnectionGuid`, тип: `string` — является ключевым. Оно определяет уникальный идентификатор соединения.
- `Enabled`, тип: `boolean` — определяет, отключено ли данное соединение. Если соединение включено, то оно будет использоваться службой `Репликация DFS`.
- `Inbound`, тип: `boolean` — если значение данного свойства равно `true`, то соединение между локальным компьютером и партнером является входящим.
- `Keywords`, тип: `string` — содержит ключевые слова, используемые для идентификации и группировки.
- `MemberGuid`, тип: `string` — содержит идентификатор членства соединения.
- `PartnerDn`, тип: `string` — определяет имя партнера для данного соединения, известное в службе доменов Active Directory.
- `PartnerDns`, тип: `string` — определяет имя партнера для данного соединения, используемое сервером DNS.
- `PartnerGuid`, тип: `string` — указывает идентификатор партнера для данного соединения.
- `PartnerName`, тип: `string` — определяет имя партнера для данного соединения.

- `RdcEnabled`, тип: `boolean` — указывает, используется ли для данного соединения удаленная дифференциальная компрессия (RDC).
- `RdcMinFileSizeInKb`, тип: `uint32` — определяет минимальный размер передаваемого по соединению файла, который можно сжимать с помощью удаленной дифференциальной компрессии (RDC).
- `ReplicationGroupGuid`, тип: `string` — указывает уникальный идентификатор реплицируемой группы.
- `Schedule`, тип: массив значений `uint8` — содержит расписание репликаций для данного соединения.
- `ScheduleInUtc`, тип: `boolean` — определяет, расписание репликации для данного соединения назначено на основе локального времени или другого UTC.

Класс DfsrInfo

Определяет дополнительные параметры настройки провайдера службы Репликация DFS. Свойства данного класса доступны только для чтения.

- `LastDsPollTime`, тип: `datetime` — определяет время последнего проведения репликации службы доменов Active Directory.
- `LastErrorCode`, тип: `uint32` — указывает код ошибки при проведении репликации. Если значение свойства равно `0`, то ошибки не было.
- `LastErrorMessageId`, тип: `uint32` — определяет идентификатор последнего события, которое было описано в журнале.
- `ProviderVersion`, тип: `string` — содержит версию провайдера.
- `ServiceStartTime`, тип: `datetime` — определяет время последнего запуска службы Репликация DFS.
- `State`, тип: `uint8` — определяет текущее состояние работы службы Репликация DFS. Возможны следующие значения данного свойства: `0` (служба запускается), `1` (служба работает), `2` (деградация работы службы), `3` (служба завершает работу).

Класс DfsrVolumeInfo

Содержит информацию о каждом разделе, хранящем реплицируемые каталоги. Свойства данного класса доступны только для чтения.

- `DatabaseGuid`, тип: `string` — определяет уникальный идентификатор базы данных раздела.
- `LastConfigChangeTime`, тип: `datetime` — указывает последнее время возникновения изменений в конфигурациях раздела.
- `LastErrorCode`, тип: `uint32` — определяет код последней возникшей ошибки. Если значение свойства равно `0`, то ошибки не было.
- `LastErrorMessageId`, тип: `uint32` — указывает идентификатор последнего события, которое было описано в журнале.

- State, тип: uint8 — определяет текущее состояние тома. Данное свойство может содержать следующие значения: 0 (инициализация), 1 (отключение), 2 (состояние ошибки), 3 (автоматическое восстановление).
- VolumeGuid, тип: string — является ключевым. Оно определяет уникальный идентификатор тома.
- VolumePath, тип: string — указывает путь к тому в виде CLSID-номера или буквы диска.
- VolumeSerialNumber, тип: uint64 — определяет серийный номер раздела.

Класс DfsrLocalMemberInfo

Класс содержит информацию о каждом члене группы репликации. Свойства данного класса доступны только для чтения.

- LastConfigChangeTime, тип: datetime — определяет время возникновения изменений в конфигурации.
- LastErrorCode, тип: uint32 — указывает код последней возникшей ошибки. Если значение свойства равно 0, то ошибки не было.
- LastErrorMessageId, тип: uint32 — определяет идентификатор последнего события, которое было описано в журнале.
- MemberGuid, тип: string — является ключевым. Оно определяет уникальный идентификатор члена группы репликации.
- MemberName, тип: string — указывает имя члена группы репликации.
- ReplicationGroupGuid, тип: string — определяет уникальный идентификатор группы репликации.
- ReplicationGroupName, тип: string — указывает имя группы репликации.
- State, тип: uint8 — определяет текущее состояние для члена группы репликации. Данное свойство может содержать следующие значения: 0 (инициализация), 1 (отключение), 2 (состояние ошибки).

Класс DfsrConnectionInfo

Содержит информацию о соединении. Свойства данного класса доступны только для чтения.

- ConnectionGuid, тип: string — является ключевым. Оно определяет уникальный идентификатор соединения.
- Inbound, тип: boolean — если значение данного свойства равно true, то соединение между локальным компьютером и партнером является входящим.
- LastErrorCode, тип: uint32 — определяет код последней возникшей ошибки. Если значение свойства равно 0, то ошибки не было.
- LastErrorMessageId, тип: uint32 — указывает идентификатор последнего события, которое было описано в журнале.

- `LastSuccessfulSyncTime`, тип: `datetime` — определяет время начала последней успешной синхронизации.
- `LastSyncDuration`, тип: `uint32` — указывает длительность последней успешной синхронизации в секундах.
- `LastSyncTime`, тип: `datetime` — определяет время начала последней операции синхронизации.
- `MemberGuid`, тип: `string` — указывает уникальный идентификатор члена группы репликации.
- `MemberName`, тип: `string` — определяет имя члена группы репликации.
- `NextSyncTime`, тип: `datetime` — указывает следующую дату проведения синхронизации.
- `PartnerGuid`, тип: `string` — определяет уникальный идентификатор партнера.
- `PartnerName`, тип: `string` — указывает имя партнера.
- `ReplicationGroupGuid`, тип: `string` — определяет уникальный идентификатор группы репликации.
- `ReplicationGroupName`, тип: `string` — указывает имя группы репликации.
- `State`, тип: `uint32` — определяет текущее состояние соединения. Данное свойство может содержать следующие значения: `0` (начало соединения), `1` (доступ в режиме online), `2` (доступ в автономном режиме), `3` (состояние ошибки).

Данный класс также поддерживает следующие методы.

- `CheckConnectivity` — выполняет проверку соединения с партнером репликации.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.
- `ForceDownload` — начинает загрузку указанного ресурса.

  Входящие параметры:

  - строковый параметр, указывающий реплицируемый каталог;
  - строковый параметр, определяющий идентификатор.

  Возвращаемые параметры: нет.
- `ForceFolderReplication` — выполняет репликацию каталога.

  Входящие параметры.

  - Определяет время репликации в минутах. После истечения данного времени служба `Репликация DFS` возвращается к использованию расписания репликации. Имеет тип `uint32`.
  - Указывает ширину канала, используемую при репликации. Имеет тип `uint32`.
  - Строковый параметр, указывающий реплицируемый каталог.

  Возвращаемые параметры: нет.

- `ForceReplication` — выполняет или приостанавливает репликацию.

  Входящие параметры.

  - Определяет режим репликации. Имеет тип `uint32`.
  - Указывает время репликации в минутах. После истечения данного времени служба Репликация DFS возвращается к использованию расписания репликации. Имеет тип `uint32`.
  - Определяет ширину канала, используемую при репликации. Имеет тип `uint32`.

  Возвращаемые параметры: нет.

Класс DfsrSyncInfo

Содержит описание сессии синхронизации. Свойства данного класса доступны только для чтения.

- `BytesTransferred`, тип: `uint64` — определяет общее количество байт, переданных в процессе синхронизации.
- `ConflictsGenerated`, тип: `uint32` — указывает общее количество конфликтов столкновения при выполнении процесса обновления.
- `ConnectionGuid`, тип: `string` — содержит уникальный идентификатор соединения.
- `EndTime`, тип: `datetime` — определяет время окончания сессии синхронизации. Если сессия в данный момент еще установлена, то значение данного свойства соответствует 1 января 1601 года.
- `Inbound`, тип: `boolean` — если значение данного свойства равно `true`, то поток данных при синхронизации идет от партнера к члену группы репликации.
- `InitiationReason`, тип: `uint32` — определяет причину начала процесса синхронизации. Возможны следующие значения данного свойства: `0` (синхронизация по расписанию), `1` (синхронизация была начата пользователем самостоятельно), `2` (пауза в процессе синхронизации), `3` (синхронизация начата как ответ на команду Force Replication Until-In-Sync).
- `LastErrorCode`, тип: `uint32` — указывает код последней возникшей ошибки. Если значение свойства равно `0`, тогда ошибки не было.
- `LastErrorMessageId`, тип: `uint32` — определяет идентификатор последнего события, которое было описано в журнале.
- `MemberGuid`, тип: `string` — указывает уникальный идентификатор члена группы репликации.
- `MemberName`, тип: `string` — определяет имя члена группы репликации.
- `PartnerGuid`, тип: `string` — указывает уникальный идентификатор партнера.
- `PartnerName`, тип: `string` — определяет имя партнера.
- `ReplicationGroupGuid`, тип: `string` — указывает уникальный идентификатор группы репликации.

- `ReplicationGroupName`, тип: `string` — определяет имя группы репликации.
- `StartTime`, тип: `datetime` — указывает время начала синхронизации.
- `State`, тип: `uint32` — определяет текущее состояние процесса синхронизации. Данное свойство может содержать следующие значения: `0` (инициализация), `1` (подключение), `2` (синхронизация выполняется), `3` (синхронизация выполнена), `4` (состояние синхронизации), `5` (прерывание), `6` (состояние ошибки).
- `SyncGuid`, тип: `string` — является ключевым. Оно определяет уникальный идентификатор синхронизации.
- `TombstonesGenerated`, тип: `uint32` — определяет общее количество столкновений, обрабатываемых в процессе обновления.
- `UpdatesNotTransferred`, тип: `uint32` — содержит общее количество обновлений в очереди для передачи в процессе синхронизации.
- `UpdatesToBeTransferred`, тип: `uint32` — хранит общее количество обновлений, которые нужно синхронизировать с партнером.
- `UpdatesTransferred`, тип: `uint32` — содержит общее количество обновлений, которые были переданы после начала синхронизации.

Класс DfsrReplicatedFolderInfo

Содержит информацию о реплицируемых каталогах. Свойства данного класса доступны только для чтения.

- `CurrentConflictSizeInMb`, тип: `uint32` — содержит текущий размер каталога `Conflict and Deleted` в мегабайтах.
- `CurrentStageSizeInMb`, тип: `uint32` — хранит текущий размер каталога организации в мегабайтах.
- `LastConflictCleanupTime`, тип: `datetime` — определяет время последнего выполнения очистки каталога репликации от конфликтов.
- `LastErrorCode`, тип: `uint32` — указывает код последней возникшей ошибки. Если значение свойства равно `0`, то ошибки не было.
- `LastErrorMessageId`, тип: `uint32` — определяет идентификатор последнего события, которое было описано в журнале.
- `LastTombstoneCleanupTime`, тип: `datetime` — указывает время последнего выполнения очистки каталога репликации.
- `MemberGuid`, тип: `string` — определяет уникальный идентификатор члена каталога репликации.
- `MemberName`, тип: `string` — указывает имя члена каталога репликации.
- `ReplicatedFolderGuid`, тип: `string` — является ключевым. Оно определяет уникальный идентификатор каталога репликации.
- `ReplicatedFolderName`, тип: `string` — определяет имя каталога репликации.
- `ReplicationGroupGuid`, тип: `string` — указывает уникальный идентификатор группы репликации.
- `ReplicationGroupName`, тип: `string` — определяет имя группы репликации.

- `State`, тип: `uint8` — указывает текущее состояние члена каталога репликации. Свойство может принимать следующие значения: `0` (деинициализация), `1` (инициализация), `2` (инициализация процесса синхронизации), `3` (автоматическое восстановление), `4` (нормальная работа), `5` (состояние ошибки).

Данный класс также поддерживает следующие методы.

- `CleanupConflictDirectory` — выполняет очистку каталога Conflict and Deleted.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

- `Fence` — выполняет обмен репликами файла или каталога.

  Входящие параметры:

  - определяет режим репликации, имеет тип `uint8`;
  - строковый параметр, определяющий путь;
  - параметр, имеющий тип `boolean`, определяет, является ли репликация рекурсивной.

  Возвращаемые параметры: нет.

- `GetOutboundBacklogFileCount` — возвращает количество назначенных исходящих незавершенных репликаций файлов, имеющих указанную версию вектора.

  Входящий параметр: строковый параметр, определяющий версию вектора.

  Возвращаемые параметры:

  - определяет количество файлов, репликация которых не завершена, имеет тип `uint32`;
  - указывает индекс идентификатора записи, имеет тип `uint32`.

- `GetOutboundBacklogFileIdRecords` — возвращает список идентификаторов записей для назначенных исходящих незавершенных репликаций файлов, имеющих указанную версию вектора.

  Входящий параметр: строковый параметр, определяющий версию вектора.

  Возвращаемые параметры:

  - массив параметров типа `object`, определяющих идентификаторы незавершенных записей;
  - определяет индекс идентификатора записи, имеет тип `uint32`.

- `GetVersionVector` — возвращает версию вектора.

  Входящие параметры: нет.

  Возвращаемый параметр: строковый параметр, определяющий версию вектора.

- `Reghost` — запускает процесс сканирования корня каталогов для поиска неизмененных файлов.

  Входящий параметр: строковый параметр, определяющий путь к файлу.

  Возвращаемые параметры: нет.

Класс DfsrIdRecordInfo

Данный класс содержит информацию о записях таблицы идентификаторов, которая хранит сведения о каждом файле и каталоге, известном службе Репликация DFS. Кроме того, данная таблица хранит сведения об удаленных файлах и каталогах. Следующие свойства данного класса доступны только для чтения.

- `Attributes`, тип: `uint32` — содержит атрибуты файла или каталога.
- `Clock`, тип: `datetime` — определяет время назначения файла или папки.
- `CreateTime`, тип: `datetime` — указывает время создания файла или папки.
- `Fence`, тип: `string` — если значение свойства равно `1`, то выполняется начальная синхронизация. Если значение равно `2`, то выполняются предварительные выборы. Значение `3` определяет действие по умолчанию.
- `Fid`, тип: `uint64` — определяет уникальный идентификатор файла. Данные идентификаторы назначаются только файлам на томах NTFS.
- `FileHash`, тип: `string` — содержит значение хэша для содержимого данного файла.
- `FileName`, тип: `string` — хранит имя файла или каталога.
- `Flags`, тип: `uint8` — определяет флаги.
- `GVsn`, тип: `string` — указывает глобальную версию файла или каталога.
- `Index`, тип: `uint32` — определяет индекс записи, используемый для ускорения доступа.
- `ParentUid`, тип: `string` — содержит уникальный идентификатор родительского каталога.
- `ReplicatedFolderGuid`, тип: `string` — хранит уникальный идентификатор каталога репликации.
- `Uid`, тип: `string` — является ключевым. Оно определяет уникальный идентификатор и версию файла или каталога.
- `UpdateTime`, тип: `datetime` — указывает время последнего обновления записей службой Репликация DFS.
- `Usn`, тип: `string` — содержит последовательный номер обновления (USN), определяющий время обновления ресурса.
- `Volume`, тип: `string` — указывает том, в котором расположен файл или каталог.

Данный класс также поддерживает метод `GetFullFilePath`, который возвращает полный путь к данному файлу или каталогу.

Входящие параметры: нет.

Возвращаемый параметр: строковый параметр, содержащий полный путь.

Класс DfsrConflictInfo

Содержит сведения о файлах и папках, помещенных в каталог Conflict and Deleted из-за противоречивых обновлений. Свойства данного класса доступны только для чтения.

- `ConflictFileCount`, тип: `uint32` — определяет общее количество файлов в реплицируемом каталоге, в которых были найдены противоречия.
- `ConflictPath`, тип: `string` — указывает путь к противоречивому файлу или каталогу.
- `ConflictSizeInBytes`, тип: `uint64` — определяет размер файла или каталога в байтах.
- `ConflictTime`, тип: `datetime` — указывает время обнаружения противоречий в обновляемом файле или каталоге.
- `ConflictType`, тип: `uint8` — определяет тип конфликта. Например, возможны следующие значения этого свойства: `1` (конфликт имен), `2` (конфликт обновлений), `5` (файл на удаленном компьютере отсутствует).
- `FileAttributes`, тип: `uint32` — содержит атрибуты файла или каталога.
- `FileName`, тип: `string` — хранит имя файла или каталога после перемещения в папку Conflict and Deleted.
- `GVsn`, тип: `string` — является ключевым. Оно определяет глобальную версию файла или каталога.
- `MemberGuid`, тип: `string` — указывает уникальный идентификатор члена.
- `PartnerGuid`, тип: `string` — определяет уникальный идентификатор партнера в соединении.
- `ReplicatedFolderGuid`, тип: `string` — указывает уникальный идентификатор каталога репликации.
- `ReplicationGroupGuid`, тип: `string` — определяет уникальный идентификатор группы репликации.
- `Uid`, тип: `string` — содержит уникальный идентификатор и версию файла или каталога.

Класс также поддерживает метод `delete`, который удаляет данный конфликт из каталога вместе с записью.

Входящие параметры: нет.

Возвращаемые параметры: нет.

DHCP-клиент

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege.

Файлы службы: `dhcpcsvc.dll`.

Исполняемый файл: `svchost.exe -k LocalServiceNetworkRestricted`.

Подраздел реестра: `Dhcp`.

Службы, необходимые для работы данной: Служба интерфейса сохранения сети (`NSI`), Драйвер поддержки NetIO Legacy TDI (`Tdx`), Ancilliary Function Driver for Winsock (`Afd`).

Позволяет взаимодействовать с DHCP-сервером для автоматического получения IP-адреса. Данное взаимодействие происходит при включении компьютера, если IP-адрес локального компьютера не является статическим, а выделяется сервером DHCP. Также служба DHCP-клиент может выполнять обновление DNS для сетевых адаптеров, настроенных вручную или с помощью протокола DHCP.

Трассировка клиента DHCP

Вы можете включить или отключить трассировку для клиента DHCP с помощью команды вида `netsh dhcpclient trcace enable|disable`.

Настройка взаимодействия клиента DHCP с DNS

Основные параметры обновления DNS с помощью клиента DHCP имеют тип `REG_DWORD` и описаны для всех сетевых интерфейсов в ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` либо для конкретного сетевого интерфейса в ветви реестра вида `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<GUID-номер сетевого интерфейса>`.

- `DisableDynamicUpdate` — с помощью данного параметра можно запретить службе DHCP-клиент выполнять регистрацию в базе DNS записей прямого (тип A, предназначены для сопоставления имени компьютера IP-адресу) и обратного (тип PTR, предназначены для сопоставления IP-адреса имени компьютера) просмотра.

  Параметр имеет глобальный характер (для всех сетевых интерфейсов). Если же вам нужно отключить динамическую регистрацию для отдельного сетевого интерфейса, то можно воспользоваться не реестром, а стандартным окном операционной системы Windows Vista. Для этого нужно снять флажок Зарегистрировать адреса этого подключения в DNS, расположенный на вкладке DNS окна Дополнительные параметры TCP/IP. Это окно отображается после нажатия кнопки Дополнительно окна свойств протокола IPv4.

- `DisableReverseAddressRegistrations` — с помощью этого параметра можно запретить службе DHCP-клиент выполнять регистрацию в базе DNS записей обратного (тип PTR) просмотра.

- `DefaultRegistrationRefreshInterval` — позволяет изменить интервал динамической перерегистрации записей в базе DNS. Значение параметра указывается в секундах.

- DefaultRegistrationTTL — дает возможность изменить срок жизни динамически зарегистрированных записей базы данных DNS. Значение параметра указывается в секундах.
- MaxNumberOfAddressesToRegister — указывается для определенного сетевого адаптера и позволяет изменить количество IP-адресов сетевого интерфейса, которые клиент DHCP должен регистрировать в базе DNS. По умолчанию выполняется регистрация только первого IP-адреса сетевого адаптера. Если значение данного параметра равно 0, то IP-адреса сетевого адаптера регистрироваться в базе DNS не будут.
- UpdateSecurityLevel — позволяет определить, будет ли разрешено выполнять небезопасную регистрацию адресов в базе DNS. Он может принимать следующие значения.
  - 0x0 — для регистрации адресов использовать безопасное динамическое обновление только в том случае, если сервер DNS не разрешает использование небезопасного динамического обновления.
  - 0x10 — использовать только небезопасное динамическое обновление.
  - 0x100 — использовать только безопасное динамическое обновление. При безопасном динамическом обновлении сервер DNS регистрирует адреса только от авторизированных клиентов и серверов.
- DisableReplaceAddressesInConflicts — дает возможность запретить выполнение переопределения существующей записи PTR при возникновении конфликта адресов (когда клиент обнаруживает, что его IP-адрес сопоставлен с другим именем компьютера).

Клиент отслеживания изменившихся связей

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: trkwks.dll.

Исполняемый файл: svchost.exe -k netsvcs.

Подраздел реестра: TrkWks.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (RpcSs).

Данная служба управляет механизмом отслеживания связей между файлами локального компьютера (или компьютеров сети) и их ярлыками. Если обнаруживается, что ярлык указывает на несуществующий файл, то служба пытается найти его и изменить ссылку ярлыка на найденный файл.

Информация о найденных связях находится в файле tracking.log каталога %systemdrive%\System Volume Information.

DNS-клиент

Тип запуска: автоматически.

Учетная запись: сетевая служба.

Дополнительные привилегии: нет.

Файлы службы: `dnsrslvr.dll`.

Исполняемый файл: `svchost.exe -k NetworkService`.

Подраздел реестра: `DNSCache`.

Службы, необходимые для работы данной: Драйвер поддержки NetIO Legacy TDI (`Tdx`).

Выполняет подключение к серверу DNS, с помощью которого в обычной локальной сети или сети Active Directory можно присваивать компьютерам UNC-имена.

Некоторые параметры настройки службы DNS-клиент можно изменить с помощью групповых политик. Все они расположены в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Сеть ▸ DNS-клиент.

- `RegisterReverseLookup` — если значение данного параметра равно `0`, то клиенту будет запрещено выполнять автоматическую регистрацию записей типа PTR в базе DNS. Если же значение равно `1`, то разрешено. А если значение данного параметра равно `2` (по умолчанию), то регистрация записей будет разрешена только после успешной регистрации A-записей.
- `RegistrationEnabled` — при установке значения этого параметра равным `0` клиенту будет запрещено выполнять автоматическую регистрацию записей типа PTR и A в базе DNS.
- `AppendToMultiLabelName` — если значение данного параметра равно `0`, то компьютеру будет запрещено добавление суффиксов к несоответствующим составным именам (которые не заканчиваются точкой) перед повторной отправкой DNS-запросов (если предыдущий запрос не был удачным).
- `RegisterAdapterName` — если установить значение этого параметра равным `1`, то при использовании динамической регистрации записи ресурсов будут регистрироваться не только с помощью сцепления имени компьютера и основного DNS-суффикса, но и с помощью сцепления имени компьютера и DNS-суффикса подключения. По умолчанию сцепление выполняется только с основным DNS-суффиксом.
- `RegistrationRefreshInterval` — значение параметра определяет интервал перерегистрации записей типа A и PTR (в секундах) в базе DNS, если клиент и сервер DNS используют динамическую регистрацию. Данный параметр может принимать значения от 1800 до 4 294 967 200. Учтите, что значение не должно быть больше интервала обновления для зон, иначе сервер DNS в процессе сборки мусора будет удалять соответствующие записи.
- `RegistrationTtl` — его значение позволяет определить срок жизни записей типа A и PTR, который будет использовать клиент при динамической регистрации.

- SearchList — имеет строковый тип и определяет DNS-суффиксы (указываются через запятую), которые будут добавляться к неполному однокомпонентному имени (имени узла, не содержащему ни одной точки) перед выдачей DNS-запроса. По умолчанию используется основной DNS-суффикс и DNS-суффикс подключения. Если же значение параметра UseDomainNameDevolution равно 1, то также будет использоваться механизм регрессирования.
- UpdateSecurityLevel — значение данного параметра определяет, будет ли разрешено клиенту выполнять небезопасную регистрацию адресов в базе DNS.
- UpdateTopLevelDomainZones — если значение параметра равно 1, то клиент DNS может посылать динамические обновления в зоны доменов верхнего уровня. По умолчанию эта возможность запрещена.
- UseDomainNameDevolution — при установке значения этого параметра равным 1 клиенту DNS разрешено выполнять регрессирование DNS-суффикса (регрессирование можно выполнять только до двух суффиксов).
- EnableMulticast — если значение данного параметра равно 0, то работа протокола LLMNR, с помощью которого может выполняться разрешение имен с помощью базы DNS, будет запрещена. По умолчанию данный протокол разрешен для всех ненастроенных сетевых адаптеров.

Расширяемый протокол проверки подлинности (EAP)

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeTcbPrivilege, SeDebugPrivilege, SeImpersonatePrivilege.

Файлы службы: eapsvc.dll.

Исполняемый файл: svchost.exe -k netsvcs.

Подраздел реестра: EapHost.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (RpcSs).

Данная служба обеспечивает проверку подлинности в беспроводных сетях, VPN и NAP. Работа этой службы также необходима для работы службы Проводная автонастройка.

ReadyBoost

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeChangeNotifyPrivilege.

Файлы службы: emdmgmt.dll.

Исполняемый файл: svchost.exe -k LocalSystemNetworkRestricted.

Подраздел реестра: EMDMgmt.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), External Memory Devices Caching Driver (`Ecache`), Лицензирование программного обеспечения (`slsvc`).

Обеспечивает управление и поддержку внешних устройств памяти (флэш-память, внешние жесткие диски и т. д.), а также позволяет использовать их как дополнительную оперативную память. Для работы данной возможности необходимо, чтобы ваше USB-устройство удовлетворяло следующим требованиям:

- оно должно иметь интерфейс USB 2.0;
- иметь пропускную способность не меньше чем 3,5 Мбайт/с для объема 4 Кбайт (при произвольном равномерном считывании данных с устройства) и 2,5 Мбайт/с для 512 Кбайт (при произвольной равномерной записи данных на устройство);
- иметь не меньше 64 Мбайт свободного места.

Использование внешнего устройства в качестве дополнительной оперативной памяти

Чтобы использовать внешнее устройство, скорость доступа к которому больше, чем у жесткого диска, в качестве дополнительной оперативной памяти, достаточно подключить данное устройство к компьютеру. После того как оно будет распознано и отобразится окно Автозапуск, нужно выбрать в этом окне ссылку Ускорить работу системы.

После этого отобразится окно свойств внешнего устройства, в котором можно настроить параметры его использования как дополнительной оперативной памяти.

Если же с точки зрения операционной системы ваше внешнее устройство не соответствует требуемым скоростным характеристикам, чтобы использовать его в качестве дополнительной оперативной памяти, то можно вручную включить данную возможность с помощью параметров реестра, описанных далее.

Хранение настроек внешних устройств в реестре

Параметры работы службы ReadyBoost содержатся в ветви системного реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt`. В данной ветви реестра также могут находиться дочерние подразделы, каждый из которых определяет настройки одного внешнего устройства памяти, подключенного к компьютеру. Они могут содержать следующие параметры `REG_DWORD`-типа.

- `CacheSizeInMB` — определяет объем (в мегабайтах) внешнего устройства, который будет использоваться операционной системой как дополнительная оперативная память.
- `CacheStatus` — если значение данного параметра `REG_DWORD`-типа равно `1`, то данное внешнее устройство разрешено использовать как дополнительную оперативную память.
- `DoRetestDevice` — этот параметр `REG_DWORD`-типа позволяет определить, будет ли операционная система каждый раз заново тестировать подключаемое

внешнее устройство на возможность его использования в качестве дополнительной оперативной памяти.

Если операционная система Windows Vista не хочет использовать вашу флэш-память в качестве дополнительной оперативной памяти (аргументируя это тем, что она недостаточно быстрая), но вы хотите ее так использовать, то достаточно присвоить параметру `CacheStatus` значение `1`, а параметру `DoRetestDevice` значение `0`. После этого в окне свойств флэш-памяти появится вкладка, позволяющая использовать данное устройство в качестве дополнительной оперативной памяти.

- `PhysicalDeviceSizeMB` — определяет общий объем (в мегабайтах) внешнего устройства.
- `ReadSpeedKBs` — указывает скорость чтения с внешнего устройства в килобайтах, измеренную при его подключении.
- `USBVersion` — определяет версию USB, которая поддерживается устройством.
- `WriteSpeedKBs` — указывает скорость записи на внешнее устройство в килобайтах, измеренную при его подключении.

ПРИМЕЧАНИЕ

Сведения о работе данной службы заносятся в журнал, расположенный в разделе Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ ReadyBoost.

Настройки кэша службы ReadyBoost

Глобальные настройки службы ReadyBoost содержатся в ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ecache\Parameters`. Эта ветвь принадлежит драйверу `ecache.sys`, который управляет работой возможности использования внешней памяти для хранения кэша данных. Например, в данной ветви реестра могут присутствовать следующие параметры `REG_DWORD`-типа:

- `UseReadyBoot` — определяет, разрешено ли использование возможности службы ReadyBoost;
- `CompressionEnabled` — позволяет определить, разрешено ли выполнение сжатия данных в кэше службы ReadyBoost.

В данной ветви реестра также присутствует два дочерних подраздела.

- `DiskAssessment` — определяет параметры работы жесткого диска вашего компьютера. Например, в данном разделе можно встретить следующие параметры `REG_DWORD`-типа:
  - `DiskNumber` — указывает номер диска;
  - `RPM` — определяет количество оборотов в секунду;
  - `SizeInGb` — указывает реальный размер жесткого диска;
  - `VolumeSerialNumber` — определяет серийный номер жесткого диска.

- ReadyBootStats — указывает параметры работы механизма ReadyBoost, а также параметры определения пригодности внешней памяти для использования данного механизма.

Настройка с помощью групповых политик

Настроить параметры работы операционной системы с внешними носителями можно и с помощью групповых политик, расположенных в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Энергонезависимый кэш диска.

Политики данного раздела изменяют значения параметров REG_DWORD-типа, расположенных в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NvCache. Они позволяют настроить параметры работы операционной системы с гибридными жесткими дисками (эта возможность называется Windows ReadyDrive). Гибридный жесткий диск представляет собой новый вид жесткого диска, который также содержит определенный объем флэш-памяти, называемой NV-кэшем. Кэш NV используется операционной системой для хранения часто используемых файлов как в процессе работы системы, так и в момент ее выключения. Поскольку NV-кэш должен быть заведомо быстрее жесткого диска, это позволяет повысить скорость работы операционной системы, а также скорость включения компьютера (хотя скорость выключения компьютера может снизиться).

- OptimizeBootAndResume — если значение данного параметра равно 0, то операционная система не будет использовать NV-кэш гибридных жестких дисков для ускорения начальной загрузки компьютера и восстановления из спящего режима.
- EnablePowerModeState — при установке значения этого параметра равным 0 операционная система не будет использовать NV-кэш для хранения используемых данных (вместо жесткого диска) при переходе в энергосберегающий режим. Это может повысить время работы компьютера от батареи в энергосберегающем режиме.
- EnableNvCache — если значение данного параметра равно 0, то операционная система не будет использовать NV-кэш всех гибридных дисков.
- EnableSolidStateMode — при установке значения этого параметра равным 0 операционная система не будет записывать в NV-кэш такие часто применяемые файлы, как метаданные файловой системы и реестр.

Хост поставщика функции обнаружения

Тип запуска: вручную.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: fdPHost.dll.

Исполняемый файл: svchost.exe -k NetworkService.

Подраздел реестра: fdPHost.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (RpcSs), HTTP (http).

Является основным процессом провайдера функции обнаружения.

Публикация ресурсов обнаружения функции

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: fdrespub.dll.

Исполняемый файл: svchost.exe -k LocalService.

Подраздел реестра: FDResPub.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (RpcSs), HTTP (http).

Публикует ресурсы этого компьютера и сам компьютер в сети, благодаря чему пользователи других компьютеров могут увидеть данный компьютер и его ресурсы общего доступа. Даже если вы отключите данную службу, доступ к удаленному компьютеру и его общим ресурсам можно будет получить с помощью IP-адреса удаленного компьютера.

Управление сертификатами и ключом работоспособности

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeImpersonatePrivilege.

Файлы службы: kmsvc.dll.

Исполняемый файл: svchost.exe -k netsvcs.

Подраздел реестра: hkmsvc.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (RpcSs).

Данная служба используется NAP и управляет сертификатами X.509 и ключами.

Общий доступ к подключению к Интернету (ICS)

Тип запуска: отключена.

Учетная запись: система.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege, SeLoadDriverPrivilege, SeTakeOwnershipPrivilege.

Файлы службы: `ipnathlp.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `SharedAccess`.

Службы, необходимые для работы данной: Сетевые подключения (`Netman`), Инструментарий управления Windows (`WinMgmt`), Диспетчер подключений удаленного доступа (`RasMan`).

Обеспечивает работу механизма ICS, с помощью которого можно выполнить подключение к Интернету с помощью оборудования (модема), установленного на другом компьютере сети.

По умолчанию вы можете использовать ICS как на основе протокола Ipv4, так и на основе протокола Ipv6. Однако с помощью параметра `REG_DWORD`-типа `EnableICSIPv6`, расположенного в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tcpip6\Parameters`, можно запретить использование ICS на основе протокола IPv6. В этой ветви реестра также может находиться параметр `REG_DWORD`-типа `ICS_IPV6_Dhcp6ServerIDLen`, который определяет длину идентификатора сервера DHCP.

Параметры службы ICS хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters`. Например, данная ветвь реестра содержит следующие параметры.

- `ScopeAddress` — этот параметр строкового типа определяет IP-адрес, который должен использоваться компьютером, чтобы компьютер мог работать как сервер ICS. По умолчанию используется адрес 192.168.0.1.
- `ScopeAddressBackup` — имеет строковый тип и определяет IP-адрес, который должен использоваться компьютером, чтобы компьютер мог работать как резервный сервер ICS. По умолчанию используется адрес 192.168.0.1.
- `SharedAutoDial` — этот параметр `REG_DWORD`-типа определяет, будет ли разрешен общий доступ к удаленным подключениям.

Вспомогательная служба IP

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: `iphlpsvc.dll`.

Исполняемый файл: `svchost.exe -k NetSvcs`.

Подраздел реестра: `iphlpsvc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Драйвер поддержки NetIO Legacy TDI (`Tdx`), Инструментарий управления Windows (`WinMgmt`), Драйвер протокола TCP/IP (`tcpip`), Служба интерфейса сохранения сети (`NSI`).

Если вы используете протокол IPv6, то данная служба позволяет ему соединяться с компьютерами, работающими на основе протокола IPv4.

Настройки данной службы находятся в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\iphlpsvc\config`. Например, в ней могут быть следующие параметры.

- `Enable6to4` — этот параметр `REG_DWORD`-типа определяет, разрешено ли преобразование пакетов протокола IPv6 в пакеты протокола IPv4.
- `EnableRouting` — имеет тип `REG_DWORD` и определяет, разрешена ли маршрутизация.
- `EnableResolution` — этот параметр `REG_DWORD`-типа определяет, разрешена ли развязка.
- `ResolutionInterval` — имеет тип `REG_DWORD` и определяет интервал развязки.

Некоторые интересные параметры данной службы содержатся и в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\iphlpsvc\Teredo`.

- `AuthProvider` — этот параметр `REG_DWORD`-типа определяет провайдер аутентификации.
- `RefreshInterval` — имеет тип `REG_DWORD` и определяет интервал обновления.
- `Type` — этот параметр `REG_DWORD`-типа определяет тип.
- `ServerName` — имеет строковый тип и определяет имя сервера.
- `ClientPort` — этот параметр `REG_DWORD`-типа определяет номер порта клиента.

Агент политики IPSec

Тип запуска: автоматически.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeAuditPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: `ipsecsvc.dll`.

Исполняемый файл: `svchost.exe -k NetworkServiceNetworkRestricted`.

Подраздел реестра: `PolicyAgent`.

Службы, необходимые для работы данной: Драйвер протокола TCP/IP (`Tcpip`), Служба базовой фильтрации (`BFE`).

ПРИМЕЧАНИЕ

Сведения о работе IPSec заносятся в журнал, расположенный в разделе Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ IPSEC-SRV.

Данная служба управляет политикой безопасности протокола IP и содержит набор интерфейсов, основанных на удаленном вызове процедур. Она активирует механизмы протокола IKE, а также драйвер безопасности протокола IP.

Ветвь реестра службы хранит не только параметры, описывающие службу, но и параметры, определяющие ее настройки. Например, к ним можно отнести следующие параметры:

- `EnableRemoteMgmt` — этот параметр `REG_DWORD`-типа определяет, разрешено ли удаленное управление;
- `SAIdleTime` — имеет тип `REG_DWORD` и определяет время простоя SA.

Тополог канального уровня

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeImpersonatePrivilege, SeChangeNotifyPrivilege.

Файлы службы: `lltdsvc.dll`.

Исполняемый файл: `svchost.exe -k LocalService`.

Подраздел реестра: `lltdsvc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Link-Layer Topology Discovery Mapper I/O Driver (`lltdio`).

Создает топологию сети, включающую в себя компьютеры и другие устройства, подключенные к сети. При отключении данной службы компоненты операционной системы, требующие для своей работы карту сети, могут работать некорректно.

Некоторые параметры настройки службы Тополог канального уровня можно изменить и с помощью групповых политик. Все они расположены в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Сеть ▸ Обнаружение топологии связи (Link-Layer).

Политики данного подраздела изменяют параметры `REG_DWORD`-типа, расположенные в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD`.

- `AllowRspndrOnDomain` — если значение данного параметра равно `1`, то работа драйвера ответчика RSPNDR в домене будет разрешена. Он используется лишь тогда, когда параметру `EnableRspndr` присвоено значение `1`.
- `AllowRspndrOnPublicNet` — при установке значения этого параметра равным `1` работа драйвера ответчика RSPNDR в публичной сети будет разрешена. Он используется лишь тогда, когда параметру `EnableRspndr` присвоено значение `1`.
- `EnableRspndr` — если значение данного параметра равно `1`, то работа драйвера ответчика RSPNDR будет разрешена.
- `ProhibitRspndrOnPrivateNet` — при установке значения этого параметра равным `0` работа драйвера ответчика RSPNDR в частной сети будет разрешена. Он используется лишь тогда, когда параметру `EnableRspndr` присвоено значение `1`.
- `AllowLLTDIOOnDomain` — если значение данного параметра равно `1`, то работа драйвера отображения ввода/вывода LLTDIO в домене будет разрешена. Он используется лишь тогда, когда параметру `EnableLLTDIO` присвоено значение `1`.
- `AllowLLTDIOOnPublicNet` — при установке значения этого параметра равным `1` работа драйвера отображения ввода/вывода LLTDIO в публичной сети будет разрешена. Он используется лишь тогда, когда параметру `EnableLLTDIO` присвоено значение `1`.
- `EnableLLTDIO` — если значение данного параметра равно `1`, то работа драйвера отображения ввода/вывода LLTDIO будет разрешена.
- `ProhibitLLTDIOOnPrivateNet` — при установке значения этого параметра равным `0` работа драйвера отображения ввода/вывода LLTDIO в частной сети будет разрешена. Он используется лишь тогда, когда параметру `EnableLLTDIO` присвоено значение `1`.

Служба инициатора Майкрософт iSCSI

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeAuditPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeCreatePermanentPrivilege, SeImpersonatePrivilege, SeTcbPrivilege.

Файлы службы: `iscsiexe.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `MSiSCSI`.

Службы, необходимые для работы данной: нет.

Позволяет создавать сессии подключения к iSCSI-устройствам с помощью Интернета. После отключения данной службы вы не сможете установить связь с iSCSI-устройствами.

Настройки данной службы содержатся в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\iSCSI.

Служба общего доступа к портам Net.Tcp

Тип запуска: отключена.

Учетная запись: локальная служба.

Дополнительные привилегии: SeCreateGlobalPrivilege.

Файлы службы: нет.

Исполняемый файл: %systemroot%\WinFX\v3.0\Windows Communication Foundation\SMSvcHost.exe.

Подраздел реестра: NetTcpPortSharing.

Службы, необходимые для работы данной: нет.

Управляет возможностью совместного доступа к портам TCP с помощью протокола Net.TCP.

Сетевой вход в систему

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: lsass.exe.

Подраздел реестра: Netlogon.

Службы, необходимые для работы данной: Рабочая станция (LanmanWorkstation).

Управляет безопасным каналом между данным компьютером и контроллером домена, с помощью которого выполняется вход в систему.

Пароль безопасного канала хранится на каждом контроллере домена вместе с учетной записью компьютера. При этом пароль периодически изменяется и синхронизируется с данными LSA. В поставку операционной системы Windows XP входила программа командной строки Netdom.exe (она не устанавливалась по умолчанию), с помощью которой можно было переустановить безопасный канал. Для этого применялась команда Netdom.exe reset <компьютер> /domain:<домен>. Например, переустановка канала была необходима в том случае, если происходила рассинхронизация пароля безопасного канала с данными LSA.

Для просмотра состояния безопасного канала в операционной системе Windows XP также применялась программа командной строки nltest.exe, не устанавливающаяся по умолчанию при установке операционной системы.

Если ваш компьютер не подключен к домену Active Directory, то в данной службе нет необходимости. В противном случае благодаря ее использованию между вашим компьютером и контроллером домена создается аутентифицированное соединение RPC. Оно используется для проверки такой конфиденциальной информации, например, как идентификаторы безопасности (SID) пользователей и групп.

Настройка регистрации записей

Еще одной обязанностью службы Сетевой вход в систему при работе в домене является регистрация записей типа SRV, CNAME и A, определяющих домен и глобальный каталог, в базе DNS через определенные промежутки времени. При этом список регистрируемых службой записей хранится в файле `Netlogon.dns` каталога `%systemroot%\System32\Config`.

С помощью параметров `REG_DWORD`-типа ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters` можно настроить некоторые возможности регистрации записей в базе DNS.

- `UseDynamicDns` — применяется только на контроллерах домена. Он позволяет запретить службе Сетевой вход в систему автоматическую регистрацию записей, идентифицирующих данный контроллер домена, в базе DNS на этом контроллере домена.
- `RegisterDnsARecords` — используется только на контроллерах домена. Он позволяет запретить службе Сетевой вход в систему автоматическую регистрацию записей типа A (включая обязательные записи вида `gc._msdcs.имя_леса`, которые после отключения нужно будет регистрировать вручную). Если записи типа A регистрироваться не будут, то протокол LDAP, не поддерживающий записи типа SRV, не сможет обнаружить сервер LDAP на данном контроллере домена.

Настройка с помощью групповой политики

Настроить работу службы Сетевой вход в систему можно и с помощью групповых политик операционной системы. Для этого применяются политики, расположенные в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Сетевой вход в систему.

Следующие политики данного раздела изменяют параметры `REG_DWORD`-типа, расположенные в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters`.

- Обращение к PDS в случае неудачи входа в систему — изменяет значение параметра `AvoidPdcOnWan`. Данная политика позволяет определить, должен ли контроллер домена при вводе пользователем ошибочного пароля контактировать с PDC, чтобы проверить, не был ли пароль данного пользователя изменен, но еще не передан на контроллер домена.
- Ожидаемая задержка при удаленном входе — дает возможность изменить значение параметра `ExpectedDialupDelay`. Политика позволяет определить интервал ожидания ответа от контроллера домена при выполнении входа в систему.

- Окончательный интервал попыток обнаружения контроллера домена для фоновых клиентов — изменяет значение параметра `BackgroundRetryQuitTime`. Данная политика позволяет определить интервал времени, в течение которого клиент может пытаться обратиться к контроллеру домена, если ответа от контроллера не поступает. Если по истечении этого интервала контроллер домена так и не ответил, то клиент прекращает попытки связаться с ним.
- Начальный интервал попыток обнаружения контроллера домена для фоновых клиентов — меняет значение параметра `BackgroundRetryInitialPeriod`. Политика позволяет определить интервал времени, который должен пройти перед первой попыткой программы, пытающейся обратиться к контроллеру домена, выполнить повторное обращение к контроллеру домена (если на первое обращение контроллер домена не ответил).
- Уровень отладки файла журнала — изменяет значение параметра `dbFlag`. Данная политика позволяет определить информацию, которая будет помещаться в файл журнала регистрации `netlogon.log`, расположенный в каталоге `%windir%\debug`. По умолчанию файл журнала не ведется.
- Максимальный интервал повторных попыток обнаружения контроллера домена для фоновых клиентов — меняет значение параметра `BackgroundRetryMaximumPeriod`. Политика позволяет определить максимальный интервал времени между повторными обращениями к контроллеру домена программой, если на предыдущие обращения контроллер домена не ответил.
- Максимальный размер файла журнала — дает возможность изменить значение параметра `MaximumLogFileSize`. Данная политика позволяет определить максимальный размер файла `netlogon.log`, расположенного в каталоге `%windir%\debug`.
- Кэш-параметр негативного обнаружения контроллеров домена — меняет значение параметра `NegativeCachePeriod`. Политика позволяет определить интервал времени, в течение которого локатор домена все еще будет считать, что контроллер домена недоступен (если предыдущее обращение к контроллеру было неудачным). Иначе говоря, если после неудачного обращения к контроллеру домена и до истечения указанного данной политикой интервала локатору поступит еще одно требование обращения к контроллеру домена, то он автоматически ответит, что контроллер домена недоступен (без попытки обратиться к нему).
- Периодическое обновление кэша положительных ответов DC для фонового вызова — изменяет значение параметра `BackgroundSuccessfulRefreshPeriod`. Данная политика позволяет определить интервал обновления кэша успешных обращений к контроллеру домена для программ, обращающихся к контроллеру домена в фоновом режиме.
- Периодическое обновление кэша положительных ответов DC для нефонового вызова — меняет значение параметра `NonBackgroundSuccessfulRefreshPeriod`. Политика позволяет определить интервал обновления кэша успешных обращений к контроллеру домена для программ, обращающихся к контроллеру домена не в фоновом режиме.

- Интервал очистки — изменяет значение параметра `ScavengeInterval`. Эта политика позволяет определить интервал сбора мусора на контроллере домена.
- Имя сайта — меняет значение параметра строкового типа `SiteName`. Определяет имя сайта Active Directory, к которому принадлежит данный компьютер.
- Установка приоритета в DNS SRV-записях локатора контроллеров домена — изменяет значение параметра `LdapSrvPriority`. Политика позволяет определить значение поля приоритета в записях SRV, зарегистрированных диспетчером домена.
- Интервал обновления DNS-записей локатора контроллеров домена — меняет значение параметра `DnsRefreshInterval`. Данная политика позволяет определить интервал обновления локатором контроллера домена записей ресурсов.
- Попробовать следующий ближайший узел — дает возможность изменить значение параметра `TryNextClosestSite`. Политика позволяет определить, будет локатор контроллера домена искать контроллер домена только в текущем сайте или также и в ближайших сайтах (если в текущем сайте локатор не нашел контроллер домена).
- Набор TTL DNS-записей локатора контроллеров домена — меняет значение параметра `DnsTtl`. Эта политика позволяет определить значение поля Срок жизни в записях SRV, зарегистрированных диспетчером домена.
- Установка веса в DNS SRV-записях локатора контроллеров домена — изменяет значение параметра `LdapSrvWeight`. Политика позволяет определить значение поля веса в записях SRV, зарегистрированных диспетчером домена.

Агент защиты сетевого доступа

Тип запуска: вручную.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeImpersonatePrivilege.

Файлы службы: `qagentRT.dll`.

Исполняемый файл: `svchost.exe -k NetworkService`.

Подраздел реестра: `napagent`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Управляет работой компонента NAP.

ПРИМЕЧАНИЕ

Агент NAP недоступен в версиях Windows Vista Home Basic и Windows Vista Home Premium.

Сетевые подключения

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeImpersonatePrivilege, SeChangeNotifyPrivilege.

Файлы службы: `netman.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `netman`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Служба интерфейса сохранения сети (`NSI`).

Отображает содержимое папки Сеть и удаленный доступ к сети.

Служба списка сетей

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: SeImpersonatePrivilege, SeChangeNotifyPrivilege.

Файлы службы: `netprofm.dll`.

Исполняемый файл: `svchost.exe -k LocalService`.

Подраздел реестра: `netprofm`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Служба сведений о подключенных сетях (`Nlasvc`).

Выполняет сбор, хранение и предоставление другим программам данных о сетях, к которым подключен компьютер. Сведения обо всех доступных сетевых соединениях содержатся в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetworkProfiles`.

Служба сведений о подключенных сетях

Тип запуска: автоматически.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeCreateGlobalPrivilege, SeImpersonatePrivilege, SeAuditPrivilege.

Файлы службы: `nlasvc.dll`.

Исполняемый файл: `svchost.exe -k NetworkService`.

Подраздел реестра: `NlaSvc`.

Службы, необходимые для работы данной: Служба интерфейса сохранения сети (NSI), Удаленный вызов процедур (RPC) (RpcSs), Драйвер протокола TCP/IP (TcpIp).

Собирает и хранит информацию о конфигурации сети, к которой подключен ваш компьютер, с целью уведомления программ об изменениях в ней.

Настройки данной службы содержатся в ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet:

- EnableActiveProbing — этот параметр REG_DWORD-типа указывает, разрешено ли службе выполнять активное зондирование;
- PassivePollPeriod — имеет тип REG_DWORD и определяет период пассивного опроса;
- ActiveProbingResetTime — этот параметр REG_DWORD-типа указывает время сброса активного зондирования;
- MinimumInternetHopCount — имеет тип REG_DWORD и определяет минимальное количество переходов между маршрутизаторами;
- TransparentProxyHopLimit — этот параметр REG_DWORD-типа указывает лимит переходов между прозрачными маршрутизаторами;
- ActiveDnsProbeHost — имеет строковый тип и определяет DNS-имя для активного зондирования.

Настройки службы содержатся и в ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters:

- DelayQueueMin — этот параметр REG_DWORD-типа определяет минимальную задержку в очереди информации о сети;
- DelayQueueMax — имеет тип REG_DWORD и определяет максимальную задержку в очереди информации о сети.

Служба интерфейса сохранения сети

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: nsisvc.dll.

Исполняемый файл: svchost.exe -k LocalService.

Подраздел реестра: nsi.

Службы, необходимые для работы данной: NSI proxy service (NSIProxy).

Передает уведомления сети пользовательским клиентам. Остановка данной службы приведет к отключению сетевого соединения. Вы не сможете пользоваться мастером Подключиться к сети, а также мастером Центр управления сетями и общим доступом.

Протокол PNRP

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: `p2psvc.dll`.

Исполняемый файл: `svchost.exe -k LocalServiceNetworkRestricted`.

Подраздел реестра: `PNRPsvc`.

Службы, необходимые для работы данной: Диспетчер удостоверения сетевых участников (`p2pimsvc`).

Поддерживает механизм бессерверного однорангового разрешения имен через Интернет. Без этого механизма некоторые приложения, функционирующие с одноранговыми сетями (например, Windows Messenger), не будут работать.

Настройки групповой политики

Операционная система Windows Vista содержит ряд настроек групповой политики, с помощью которых можно изменить параметры работы в одноранговых сетях. Все они находятся в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Сеть ▸ Службы одноранговых сетей Microsoft и во вложенных в него подразделах.

Данные политики изменяют значения следующих параметров `REG_DWORD`-типа, расположенных в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Peernet`.

- `IgnoreDomainPasswordPolicyForNewGroups` — если значение этого параметра равно `1`, то при создании одноранговой группы и указании пароля он не будет проверяться согласно требованиям надежности, определенным операционной системой локального компьютера (то есть можно будет указывать любой пароль).
- `Disabled` — если значение параметра равно `1`, то службы одноранговой сети, реализованные в операционной системе Windows, будут запрещены.

Вы также можете воспользоваться параметрами `REG_DWORD`-типа `DisableMulticastBootstrap` и строкового типа `SeedServer`, чтобы отключить возможность использования протокола PNRP для поиска компьютеров в сети и оповещения, а также для задания сервера инициализации. Эти параметры в зависимости от области действия могут находиться в одном из следующих подразделов ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Peernet\Pnrp`: `IPv6-Global` (настройки для глобального облака), `IPv6-LinkLocal` (настройки для локального облака связи) и `IPv6-SiteLocal` (настройки для локального облака узла).

Параметры настройки службы

Параметры настройки протоколов PNRP, обслуживаемых данной службой, хранятся в подразделах ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\PeerNet\PNRP\IPV6-LinkLocal. Например, ниже перечислены самые интересные параметры REG_DWORD-типа.

- Disabled — позволяет отключить сетевое подключение.
- DisableMulticastPublish — дает возможность отключить использование широковещательных пакетов при публикации.
- DisableMulticastSearch — позволяет отключить использование широковещательных пакетов при поиске.
- NumPeersToFlood — дает возможность указать количество одноранговых соединений, превышение которого будет считаться переполнением.
- PeriodBetweenMaintenanceInSecond — позволяет указать интервал (в секундах) между сохранением.
- MaxStartupTimeInMillisecond — дает возможность указать максимальное время загрузки в миллисекундах.
- MaxDelayForCPAAuthorizationInSecond — позволяет указать максимальную задержку (в секундах) авторизации CPA.
- MinCPALigeTime — дает возможность указать минимальное время жизни CPA.

Еще один параметр имеет строковый тип: SeedServer. Он содержит список начальных серверов, перечисленных через запятую.

Параметры работы данной службы можно найти и в ветви HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PNRPsvc\parameters. Например, здесь может находиться описанный выше параметр SeedServer.

Группировка сетевых участников

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: p2psvc.dll.

Исполняемый файл: svchost.exe -k LocalServiceNetworkRestricted.

Подраздел реестра: p2psvc.

Службы, необходимые для работы данной: Диспетчер удостоверения сетевых участников (p2pimsvc), Протокол PNRP (PNRPSvc).

Управляет групповыми службами одноранговой сети.

Диспетчер удостоверения сетевых участников

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: `p2psvc.dll`.

Исполняемый файл: `svchost.exe -k LocalServiceNetworkRestricted`.

Подраздел реестра: `p2pimsvc`.

Службы, необходимые для работы данной: нет.

Управляет службой идентификации одноранговых сетей.

Служба публикации имен компьютеров PNRP

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: `p2psvc.dll`.

Исполняемый файл: `svchost.exe -k LocalServiceNetworkRestricted`.

Подраздел реестра: `PNRPAutoReg`.

Службы, необходимые для работы данной: Протокол PNRP (`PNRPSvc`).

Эта служба публикует имена компьютеров, использующих протокол PNRP.

Quality Windows Audio Video Experience Service

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege.

Файлы службы: `qwave.dll`.

Исполняемый файл: `svchost.exe -k LocalService`.

Подраздел реестра: `QWAVE`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Драйвер QWAVE (`QWAVEdrv`), Link-Layer Topology Discovery Mapper I/O Driver (`LLTDIO`).

Представляет собой новую сетевую платформу qWave, предназначенную для просмотра аудио и видео в домашней сети. В частности, с помощью данной платформы можно назначать приоритет для сетевого мультимедийного трафика.

ПРИМЕЧАНИЕ

Сведения об отладке данной службы заносятся в журнал, расположенный в разделе Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ QoS-qWAVE.

Диспетчер автоматических подключений удаленного доступа

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeImpersonatePrivilege, SeIncreaseQuotaPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeAssignPrimaryTokenPrivilege.

Файлы службы: `rasauto.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `RasAuto`.

Службы, необходимые для работы данной: Диспетчер подключений удаленного доступа (`RasMan`), Телефония (`TapiSrv`).

Создает сетевое соединение с удаленной сетью всякий раз, когда программа ссылается на удаленное DNS- или NetBIOS-имя либо на IP-адрес удаленного компьютера.

Диспетчер подключений удаленного доступа

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeImpersonatePrivilege, SeIncreaseQuotaPrivilege, SeTcbPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeAssignPrimaryTokenPrivilege.

Файлы службы: `rasmans.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `RasMan`.

Службы, необходимые для работы данной: Телефония (`TapiSrv`).

Данная служба управляет подключениями удаленного доступа (с помощью модема) и созданием VPN.

Операционная система Windows Vista позволяет просматривать сведения о работе данной службы с помощью счетчиков производительности объектов Всего RAS и Порт RAS. Данные объекты поддерживают одни и те же счетчики, только первый объект содержит общие сведения о работе службы, а второй — сведения отдельно для каждого порта. Например, с помощью счетчиков данного объекта можно узнать следующие сведения о работе службы.

- О возникших при передаче данных ошибках четности (счетчик Ошибок CRC), выравнивания (Ошибок выравнивания), переполнения порта (Переполнений посл. порта), истечения таймаута ожидания данных (Ошибок таймаута), переполнения буфера (Переполнений буфера), общем количестве ошибок (Всего ошибок). Можно также воспользоваться счетчиком Всего ошибок/сек, чтобы просмотреть сведения о количестве возникших за последнюю секунду ошибок.
- О байтах и кадрах, переданных или полученных либо во время работы данной службы (соответственно, счетчики Передано байт, Кадров передано, Получено байт, Получено кадров), либо за последнюю секунду (соответственно, счетчики Передано байт/сек, Передано кадров/сек, Получено байт/сек, Получено кадров/сек). Можно также просмотреть сведения о проценте полученных или переданных сжатых данных (счетчики Процент сжатия на выходе и Процент сжатия на входе).
- Об общем количестве соединений, обработанных службой (счетчик Всего подключений).

Удаленный вызов процедур (RPC)

Тип запуска: автоматически.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeAuditPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: `rpcss.dll`.

Исполняемый файл: `svchost.exe -k rpcss`.

Подраздел реестра: `RpcSs`.

Службы, необходимые для работы данной: Модуль запуска процессов DCOM-сервера (`DcomLaunch`).

Представляет собой менеджер контроля обслуживания COM. Если эта служба будет остановлена, то программы, использующие COM или RPC, будут работать некорректно.

ПРИМЕЧАНИЕ

Сведения об отладке данной службы заносятся в журналы, расположенные в разделах Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ RPC и Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Rpcss-EndpointMapper.

Локатор удаленного вызова процедур (RPC)

Тип запуска: вручную.

Учетная запись: сетевая служба.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: `locator.exe`.

Подраздел реестра: `RpcLocator`.

Службы, необходимые для работы данной: нет.

Управляет базой данных службы имен RPC.

Удаленный реестр

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: нет.

Файлы службы: `regsvc.dll`.

Исполняемый файл: `svchost.exe -k regsvc`.

Подраздел реестра: `RemoteRegistry`.

Службы, необходимые для работы данной: Удаленный Вызов Процедур (RPC) (`RPCSS`).

Предоставляет доступ к реестру данного компьютера удаленным пользователям и программам. После отключения данной службы сетевой доступ к реестру компьютера будет невозможен. По этой причине отключение данной службы повышает не только производительность компьютера, но и безопасность вашего компьютера.

Маршрутизация и удаленный доступ

Тип запуска: отключена (если данная служба используется, то она запускается автоматически при входе пользователя в систему).

Учетная запись: система.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeLoadDriverPrivilege, SeImpersonatePrivilege, SeAuditPrivilege.

Файлы службы: `mprdim.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `RemoteAccess`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Диспетчер подключений удаленного доступа (`RasMan`), Служба базовой фильтрации (`BFE`).

Позволяет использовать ваш компьютер в качестве программного маршрутизатора между двумя сетями, к которым он подключен. Она также используется при удаленном доступе к компьютеру с помощью модема.

Вторичный вход в систему

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: `seclogon.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `seclogon`.

Службы, необходимые для работы данной: нет.

Позволяет пользователям компьютера запускать программы от имени другого пользователя. Например, после отключения данной службы программа `runas.exe` не будет работать.

Использование программы runas.exe. Программа командной строки `runas.exe` позволяет выполнить любую команду от имени другого пользователя. При этом загрузится его профиль, после чего программа попытается запуститься в контексте соответствующего пользователя.

Основной синтаксис данной программы следующий: `runas /user:<логин пользователя> <команда, которую нужно выполнить от имени этого пользователя>`. После выполнения данной команды перед вами отобразится запрос на ввод пароля к учетной записи соответствующего пользователя (если учетная запись не защищена паролем, то вы не сможете запустить команду от ее имени с помощью программы `runas.exe`). Вводите пароль внимательно, так как на экране при этом не будет отображаться не только то, что вы вводите, но и звездочки, которыми обычно заменяют символы пароля при вводе.

Список параметров, которые поддерживает данная программа, можно просмотреть с помощью команды `runas.exe /?`.

Сервер

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: `srvsvc.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `LanmanServer`.

Службы, необходимые для работы данной: Диспетчер учетных записей безопасности (`SamSs`), драйвер `srv.sys` (`Srv`).

Управляет созданием папок общего доступа данного компьютера, а также доступом к файлам и папкам данного компьютера по сети. После отключения этой службы доступ к компьютеру по сети будет невозможен.

Сведения обо всех папках общего доступа компьютера хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\Shares`.

Настройки службы Сервер содержатся в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters`. Например, в данной ветви могут находиться следующие параметры.

- `Autodisconnect` — этот параметр типа `REG_BINARY` определяет интервал простоя сетевого сеанса, после истечения которого соответствующий сетевой сеанс будет автоматически завершен.
- `EnableForcedLogOff` — при установке значения данного параметра типа `REG_DWORD` равным `1` операционная система будет отключать сетевое соединение пользователя, если отведенное ему время работы истекло. Например, значение данного параметра используется службой SMB.
- `Enablesecuritysignature` — если значение данного параметра `REG_DWORD`-типа равно `1`, то использование SMB-подписей сетевых пакетов будет разрешено.
- `Enableextendedsignature` — если значение этого параметра `REG_DWORD`-типа равно `1`, то использование расширенных сигнатур для сетевых пакетов будет разрешено.
- `NullSessionPipes` — этот параметр `REG_MULTI_SZ`-типа определяет службы, которым будет разрешен анонимный доступ к именованным каналам.
- `NullSessionShares` — имеет тип `REG_MULTI_SZ` и определяет службы, которым будет разрешен анонимный доступ к общим папкам.
- `Requiresecuritysignature` — если значение данного параметра `REG_DWORD`-типа равно `1`, то операционная система будет отбрасывать все сетевые пакеты, которые не имеют SMB-подписи.
- `Requireextendedsignature` — при установке значения этого параметра `REG_DWORD`-типа равным `1` операционная система будет отбрасывать все сетевые пакеты, которые не имеют расширенной подписи.
- `RestrictNullSessAccess` — если значение данного параметра `REG_DWORD`-типа равно `1`, то операционная система будет запрещать сетевой доступ к нулевым каналам.
- `DontNotifyIcf` — этот параметр `REG_DWORD`-типа определяет, будет ли уведомляться служба ICF.

Настройки службы Сервер, относящиеся к безопасности компьютера, также хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity`. Например, настройки управления папками общего доступа содержатся в параметре `SrvsvcShareFileInfo` типа `REG_BINARY`, а настройки управления принтерами общего доступа — в параметре `REG_BINARY`-типа `SrvsvcSharePrintInfo`.

Ловушка SNMP

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege.

Файлы службы: нет.

Исполняемый файл: `snmptrap.exe`.

Подраздел реестра: `SNMPTRAP`.

Службы, необходимые для работы данной: нет.

Получает сообщения от агентов SNMP и передает их программам, управляющим работой агентов SNMP или реализующим наблюдение за сообщениями от них.

Модуль поддержки NetBIOS через TCP/IP

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: SeCreateGlobalPrivilege.

Файлы службы: `lmhsvc.dll`.

Исполняемый файл: `svchost.exe -k LocalServiceNetworkRestricted`.

Подраздел реестра: `lmhosts`.

Службы, необходимые для работы данной: NETBT (`NetBT`), Ancilliary Function Driver for Winsock (`Afd`).

Обеспечивает поддержку служб, работающих с протоколом NetBT, а также разрешение имен NetBIOS для клиентов сети.

ПРИМЕЧАНИЕ

Просмотреть сведения о работе соединения NBT можно с помощью объекта Подключение NBT. С его помощью можно узнать количество отправленных (счетчик Отправлено байт/сек), полученных (счетчик Получено байт/сек) или общее количество прошедших через соединение байт за последнюю секунду (счетчик Всего байт/сек).

Как и раньше, в поставку операционных систем семейства Windows входит программа для просмотра сведений о работе протокола NetBIOS. Например, с ее помощью можно узнать, под каким NetBIOS-именем сервер зарегистрирован в сети, для чего нужно применить команду `nbtstat -n`. Это бывает необходимо при неполадках в работе сервера, при которых не удается обратиться к серверу с помощью NetBIOS-имени.

Программа `nbtstat.exe` позволяет также отобразить кэшированные записи удаленных компьютеров, которые отмечены префиксом `#PRE` в файле `Lmhosts`.

Телефония

Тип запуска: вручную.

Учетная запись: сетевая служба.

Дополнительные привилегии: нет.

Файлы службы: `tapisrv.dll`.

Исполняемый файл: `svchost.exe -k NetworkService`.

Подраздел реестра: `TapiSrv`.

Службы, необходимые для работы данной: Plug and Play (`PlugPlay`), Удаленный вызов процедур (RPC) (`RpcSs`).

Обеспечивает работу TAPI, реализующего доступ к локальному компьютеру или сети с помощью телефона (через модем).

Операционная система Windows Vista позволяет просматривать сведения о работе данной службы с помощью счетчиков производительности объекта Телефония. Например, с помощью счетчиков данного объекта можно узнать следующие сведения о работе службы:

- количество телефонных линий, обслуживаемых службой (счетчик Линий), и активных в данный момент линий (Активных линий);
- количество телефонов, обслуживаемых службой (Телефонных устройств), и активных в данный момент телефонов (Активных телефонов);
- частоту входящих и исходящих звонков в секунду, на которые отвечает служба (Исходящих звонков/сек и Входящих звонков/сек), а также текущее количество входящих и исходящих звонков (Текущих исходящих звонков и Текущих входящих звонков);
- количество приложений, работающих с данной службой (Приложений-клиентов).

Службы терминалов

Тип запуска: автоматически.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege, SeIncreaseQuotaPrivilege.

Файлы службы: `termsrv.dll`.

Исполняемый файл: `svchost.exe -k NetworkService`.

Подраздел реестра: `TermService`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Драйвер устройства терминала (`TermDD`).

Позволяет пользователям удаленно подключаться к данному компьютеру, используя окно терминала (например, программу `mstsc.exe`).

ПРИМЕЧАНИЕ

Операционная система Windows Vista позволяет просматривать сведения о работе данной службы с помощью счетчиков производительности объекта Службы терминалов. Например, с помощью счетчиков данного объекта можно узнать сведения об общем количестве сессий (счетчик Всего сеансов), количестве активных сессий (Активных сеансов), а также количестве неактивных сессий (Неактивных сеансов).

Настройка служб терминалов

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeImpersonatePrivilege.

Файлы службы: `sessenv.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `SessionEnv`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Рабочая станция (`LanmanWorkstation`).

Отвечает за работу всех служб удаленного доступа и поддерживает сессии, запущенные с правами системы.

Перенаправитель портов пользовательского режима служб терминалов

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeAuditPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege, SeIncreaseQuotaPrivilege, SeCreatePermanentPrivilege, SeLoadDriverPrivilege.

Файлы службы: umrdp.dll.

Исполняемый файл: svchost.exe -k LocalSystemNetworkRestricted.

Подраздел реестра: UmRdpService.

Службы, необходимые для работы данной: Службы терминалов (TermService).

Позволяет выполнять переназначение принтеров, драйверов и портов для всех программ, использующих протокол RDP.

Узел универсальных PNP-устройств

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: upnphost.dll.

Исполняемый файл: svchost.exe -k LocalService.

Подраздел реестра: upnphost.

Службы, необходимые для работы данной: Обнаружение SSDP (SSDPSRV), HTTP (http).

Позволяет данному компьютеру работать с устройствами UPnP. После отключения службы работа с устройствами UPnP будет невозможна.

Веб-клиент

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: нет.

Файлы службы: webclnt.dll.

Исполняемый файл: svchost.exe -k LocalService.

Подраздел реестра: WebClient.

Службы, необходимые для работы данной: WebDav Client Redirector Driver (MRxDAV).

Позволяет программам и компонентам операционной системы получать доступ к файлам, хранящимся в Интернете.

Немедленные подключения Windows — регистратор настройки

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeImpersonatePrivilege и SeChangeNotifyPrivilege.

Файлы службы: `wcncsvc.dll`.

Исполняемый файл: `svchost.exe -k LocalService`.

Подраздел реестра: `wcncsvc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Данная служба используется для выдачи сетевых удостоверений подписчикам (выступает в роли регистратора).

Параметры работы мастеров Windows Connect Now (WCN) можно настроить с помощью групповых политик, расположенных в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Сеть ▸ Windows Connect Now. Данные политики изменяют значения следующих параметров `REG_DWORD`-типа, расположенных в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\UI`.

- `DisableFlashConfigRegistrar` — если значение данного параметра равно 1, то конфигурирование беспроводных «флэшек» с помощью мастера будет запрещено.
- `DisableUPnPRegistrar` — при установке значения данного параметра равным 1 конфигурирование устройств UPNP с помощью мастера будет запрещено.

ПРИМЕЧАНИЕ

Универсальный стандарт Plug and Play (UPnP) призван упростить установку новых сетевых устройств и управление ими. При подключении к сети устройства, поддерживающего стандарт UPNP, оно самостоятельно объявляет о себе всем компьютерам сети, описывает свои возможности, а также возможности управления параметрами своей работы.

Работа стандарта UPNP основана на протоколе SSDP — именно с его помощью выполняется взаимодействие устройств с операционными системами семейства Windows. Реализация стандарта UPNP в операционной системе поддерживается благодаря следующим файлам: Upnpcont.exe, Upnphost.dll (выполняет подключение устройств UPNP), Upnp.dll (содержит основные API UPNP), Ssdpsrv.dll (используется протоколом SSDP в качестве ведущего узла).

- `DisableWPDRegistrar` — если значение параметра равно 1, то конфигурирование портативных устройств с помощью мастера будет запрещено.
- `EnableRegistrars` — при установке значения этого параметра равным 1 конфигурирование любых устройств с помощью мастера будет запрещено.
- `MaxWCNDeviceNumber` — значение данного параметра определяет максимальное количество устройств, которые можно конфигурировать с помощью мастера.

- DisableWcnUi — если значение параметра равно 1, то запуск задач мастера будет запрещен. Параметр можно создавать и в ветви корневого раздела HKEY_CURRENT_USER.

Защитник Windows

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeImpersonatePrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeChangeNotifyPrivilege, SeSecurityPrivilege.

Файлы службы: %ProgramFiles%\Windows Defender\mpsvc.dll.

Исполняемый файл: svchost.exe -k secsvcs.

Подраздел реестра: WinDefend.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (RpcSs).

Управляет работой программы Защитник Windows. После отключения службы работа этой программы будет невозможна.

Windows Driver Foundation — User-mode Driver Framework

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: SeCreateGlobalPrivilege.

Файлы службы: WUDFSvc.dll.

Исполняемый файл: svchost.exe -k LocalService.

Подраздел реестра: wudfsvc.

Службы, необходимые для работы данной: Plug and Play (PlugPlay).

Управляет драйверами в пользовательском режиме.

Служба общих сетевых ресурсов проигрывателя Windows Media

Тип запуска: вручную.

Учетная запись: сетевая служба.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: %ProgramFiles%\Windows Media Player\wmpnetwk.exe.

Подраздел реестра: `WMPNetworkSvc`.

Службы, необходимые для работы данной: Узел универсальных PNP-устройств (`UPnPHost`), HTTP (`http`).

Разделяет библиотеку Проигрывателя Windows Media с другими пользователями сети.

Служба удаленного управления Windows (WS-Management)

Тип запуска: вручную.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: `WsmSvc.dll`.

Исполняемый файл: `svchost.exe -k NetworkService`.

Подраздел реестра: `WinRM`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RPCSS`), HTTP (`http`).

Служба удаленного управления Windows (WS-Management) реализует работу протокола для защищенного удаленного управления компьютером. Она прослушивает сеть с целью получения запросов удаленного управления и выполняет их. Благодаря этому администраторы могут легко запускать сценарии и выполнять другие задачи на удаленном компьютере. С помощью данной службы также реализуется возможность подписывания на события с помощью оснастки Просмотр событий.

Служба автоматического обнаружения веб-прокси WinHTTP

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: `winhttp.dll`.

Исполняемый файл: `svchost.exe -k LocalService`.

Подраздел реестра: `WinHttpAutoProxySvc`.

Службы, необходимые для работы данной: DHCP-клиент (`Dhcp`).

Обеспечивает программный интерфейс Win32 API для передачи запросов HTTP и приема ответов на них. Кроме того, данная служба обеспечивает поддержку автоматического обнаружения прокси с помощью протокола Web Proxy Auto-Discovery (WPAD).

Проводная автонастройка

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeImpersonatePrivilege, SeAuditPrivilege, SeTcbPrivilege.

Файлы службы: `dot3svc.dll`.

Исполняемый файл: `svchost.exe -k LocalSystemNetworkRestricted`.

Подраздел реестра: `dot3svc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), NDIS Usermode I/O Protocol (`Ndisuio`), Расширяемый протокол проверки подлинности (EAP) (`Eaphost`).

Управляет установкой подлинности на сетевых интерфейсах стандарта IEEE 802.1X.

ПРИМЕЧАНИЕ

Сведения о работе данной службы заносятся в журнал, расположенный в разделе Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Wired-AutoConfig.

Служба автонастройки WLAN

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeImpersonatePrivilege, SeAuditPrivilege, SeTcbPrivilege, SeDebugPrivilege.

Файлы службы: `wlansvc.dll`.

Исполняемый файл: `svchost.exe -k LocalSystemNetworkRestricted`.

Подраздел реестра: `Wlansvc`.

Службы, необходимые для работы данной: NativeWiFi Filter (`nativewifip`), Удаленный вызов процедур (RPC) (`RpcSs`), NDIS Usermode I/O Protocol (`Ndisuio`), Расширяемый протокол проверки подлинности (EAP) (`Eaphost`).

Выполняет энумерацию беспроводных устройств и реализует их обнаружение.

ПРИМЕЧАНИЕ

Сведения о работе данной службы заносятся в журнал, расположенный в разделе Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ WLAN-AutoConfig.

Рабочая станция

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: `srvsvc.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `LanmanWorkstation`.

Службы, необходимые для работы данной: нет.

Обеспечивает и поддерживает соединение с удаленным сервером на основе протокола SMB.

Операционная система Windows Vista позволяет просматривать сведения о работе редиректора с помощью счетчиков производительности объекта Перенаправитель. Например, с помощью счетчиков данного объекта можно узнать следующие сведения о работе службы.

- Количество записанных или считанных за последнюю секунду измененных страничных (или нестраничных) данных, используемых приложениями (счетчики Прочитано страничных байт/сек, Прочитано не страничных байт/сек, Записано страничных байт/сек, Записано не страничных байт/сек). Страничные данные после передачи по сети помещаются в страничную память и выгружаются из нее только в том случае, когда они больше не нужны. Нестраничные данные представляют собой обычные файловые запросы на запись/чтение данных, расположенных на другом компьютере.
- Общее количество данных, записанных приложениями с помощью редиректора в кэш (Прочитано из кэша байт/сек) или считанных из него (Записано в кэш байт/сек). Использование редиректором кэша позволяет повысить скорость работы с сетевыми данными, которые периодически требуется загрузить из сети.
- Количество переданных или принятых из сети данных (данных, которые не были помещены в кэш-память), требуемых приложениями (Прочитано сетевых байт/сек и Записано сетевых байт/сек), а также общее количество данных (Получено байт/сек и Передано байт/сек).

Объект также поддерживает множество других счетчиков, позволяющих следить за функционированием рабочих элементов и передачей «сырых» данных.

Настройки службы Рабочая станция хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworkstation\parameters`. Среди интересных параметров `REG_DWORD`-типа можно выделить следующие.

- `EnablePlainTextPassword` — если значение данного параметра равно `1`, то службам SMB будет разрешено передавать незашифрованные пароли. Это может быть необходимо для некоторых сетевых служб UNIX.

- EnableSecuritySignature — при установке значения этого параметра равным 1 использование SMB-подписей сетевых пакетов будет разрешено.
- MaxCmds — определяет количество команд, которые могут находиться в буфере для сетевых операций. Значение данного параметра может находиться в диапазоне от 0 до 255. Чем больше значение параметра, тем больше оперативной памяти будет использовано.
- MaxCollectionCount — указывает размер буфера, который будет использоваться для записи через именованные каналы, работающие в символьном режиме. Значение параметра может находиться в диапазоне от 0 до 65 535. Чем больше значение данного параметра, тем больше оперативной памяти будет использовано.
- MaxThreads — определяет количество потоков, которые могут находиться в буфере для сетевых операций. Значение может находиться в диапазоне от 0 до 255. Чем больше значение, тем больше оперативной памяти будет использовано.
- RequireSecuritySignature — если значение данного параметра равно 1, то операционная система будет подписывать все передаваемые пакеты с помощью SMB-подписи.
- UseEncryption — определяет, будет ли использоваться шифрование передаваемых пакетов.

Другие службы

Система событий COM+

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeImpersonatePrivilege.

Файлы службы: es.dll.

Исполняемый файл: svchost.exe -k LocalService.

Подраздел реестра: EventSystem.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (RpcSs).

Выполняет поддержку службы SENS (Служба уведомления о системных событиях). При отключении службы Система событий COM+ не сможет работать и служба SENS (Служба уведомления о системных событиях), а следовательно, не смогут выполняться такие операции, как уведомления о входе в систему и выходе из нее.

Параметры работы данной службы хранятся в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EventSystem. Кроме того, один из разделов данной ветви реестра содержит дочерний подраздел EventClass, определяющий классы событий, которые управляются службой Система событий COM+. С его помощью вы можете запретить обработку некоторых классов событий или изменить SID, с которым они выполняются.

Системное приложение COM+

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeDebugPrivilege, SeImpersonatePrivilege, SeIncreaseQuotaPrivilege.

Файлы службы: нет.

Исполняемый файл: `dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}`.

Подраздел реестра: `COMSysApp`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Система событий COM+ (`EventSystem`), Служба уведомления о системных событиях (`SENS`).

Управляет работой компонентов COM (по сути, ActiveX-объекты операционной системы). После отключения данной службы многие компоненты COM не будут работать или будут работать некорректно.

Запустить данную службу можно, воспользовавшись программой командной строки `mtstocom.exe`.

Диспетчер сеансов диспетчера окон рабочего стола

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: `uxsms.dll`.

Исполняемый файл: `svchost.exe -k UxSvcGroup`.

Подраздел реестра: `UxSms`.

Службы, необходимые для работы данной: нет.

Обеспечивает запуск и обслуживание компонента операционной системы Desktop Window Manager (DWM). Если служба Диспетчер сеансов диспетчера окон рабочего стола будет отключена, то интерфейс Windows Aero будет запрещен.

Служба политики диагностики

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeAssignPrimaryTokenPrivilege, SeImpersonatePrivilege.

Файлы службы: `dps.dll`.

Исполняемый файл: `svchost.exe -k LocalServiceNoNetwork`.

Подраздел реестра: `DPS`.

Службы, необходимые для работы данной: нет.

Отслеживает проблемы в работе запущенных процессов и сетевых компонентов. При их обнаружении служба пытается решить проблему.

Например, именно благодаря данной службе можно использовать команду Диагностика и восстановление контекстного меню значка Сетевого окружения в области уведомления для определения неисправности сети. Но это не единственная заслуга данной службы — загляните в раздел групповой политики Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Диагностика. Все политики данного раздела и его подразделов настраивают возможности, реализация которых основана на службе Служба политики диагностики.

ПРИМЕЧАНИЕ

Информация о диагностике заносится во множество журналов, расположенных в дочерних подразделах раздела Журналы приложений и служб ▸ Microsoft ▸ Windows. Например, к ним относятся следующие: CorruptedFileRecovery-Client, CorruptedFileRecovery-Server, Diagnosis-DPS, Diagnosis-PLA, DiskDiagnosis, MemoryDiagnostics-Results, Diagnosis-WDI и т. д.

Список компонентов, диагностику которых можно проводить в операционной системе, определяется диагностическими модулями, доступными службе. Сведения о диагностических модулях, которые доступны операционной системе Windows Vista и службе Служба политики диагностики, описаны в ветви `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WDI\DiagnosticModules`. Данная ветвь реестра хранит набор подразделов, названных в честь CLSID-номера диагностического модуля. Каждый такой подраздел может содержать следующие параметры.

- `NeverUnload` — этот параметр `REG_DWORD`-типа определяет, может ли выгружаться данный модуль после использования.
- `IsReentrant` — имеет тип `REG_DWORD` и указывает, является ли модуль повторно используемым.
- `ModuleName` — этот параметр строкового типа определяет название модуля.
- `ExecutionContext` — имеет строковый тип и указывает контекст выполняемого модуля. Если значение данного параметра равно `LocalSystemNetworkRestricted`, то для диагностики будет использоваться дополнительная

служба Узел системы диагностики. Если же значение равно `LocalServiceNoNetwork`, то для диагностики будет использоваться дополнительная служба Узел службы диагностики.

Настройки диагностики компонентов операционной системы содержатся и в ветви системного реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\Performance`.

Кроме того, в каталоге `%systemroot%\system32\WDI` содержатся файлы трассировки и системные файлы настройки диагностики, создаваемые службой Служба политики диагностики.

Узел службы диагностики

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeImpersonatePrivilege.

Файлы службы: `wdi.dll`.

Исполняемый файл: `svchost.exe -k LocalService`.

Подраздел реестра: `WdiServiceHost`.

Службы, необходимые для работы данной: нет.

Данная служба отслеживает проблемы в работе запущенных процессов и компонентов операционной системы. При их обнаружении она пытается решить проблему.

Узел системы диагностики

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeImpersonatePrivilege, SeTcbPrivilege, SeDebugPrivilege, SeProfileSingleProcessPrivilege.

Файлы службы: `wdi.dll`.

Исполняемый файл: `svchost.exe -k LocalSystemNetworkRestricted`.

Подраздел реестра: `WdiSystemHost`.

Службы, необходимые для работы данной: нет.

Эта служба также отслеживает проблемы в работе запущенных процессов и компонентов операционной системы. При их обнаружении она пытается решить проблему.

Координатор распределенных транзакций

Тип запуска: вручную.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: нет.

Исполняемый файл: `msdtc.exe`.

Подраздел реестра: `MSDTC`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Диспетчер учетных записей безопасности (`SamSs`).

Управляет транзакциями баз данных, очередей сообщений и различных файловых систем, что существенно снижает количество ошибок файловой системы. При отключении данной службы транзакции работать не будут.

Операционная система Windows Vista позволяет просматривать сведения о работе данной службы с помощью счетчиков производительности объекта Координатор распределенных транзакций. Например, с помощью счетчиков данного объекта можно узнать следующие сведения о работе службы:

- количество активных, совершенных, прерванных и неопределенных транзакций, выполненных данной службой во время ее работы (соответственно, счетчики Активных транзакций, Завершенные транзакции, Прерванные транзакции, Транзакций под сомнением) или за последнюю секунду (Транзакций в секунду, Зафиксированных транзакций в секунду, Прерванных транзакций в секунду);
- минимальный, средний и максимальный интервал времени между началом и завершением транзакции (соответственно, счетчики Время ответа: минимальное, Время ответа: среднее, Время ответа: максимальное).

Параметры работы данной службы хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDTC`.

Обнаружение интерактивных служб

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeTcbPrivilege, SeAssignPrimaryTokenPrivilege, SeIncreaseQuotaPrivilege.

Файлы службы: нет.

Исполняемый файл: `UI0Detect.exe`.

Подраздел реестра: `UI0Detect`.

Службы, необходимые для работы данной: нет.

Поддерживает возможность отображения интерактивными службами уведомлений и окон для взаимодействия с пользователем.

KtmRm для координатора распределенных транзакций

Тип запуска: автоматически с использованием механизма задержки запуска службы.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeImpersonatePrivilege.

Файлы службы: `msdtckrm.dll`.

Исполняемый файл: `svchost.exe -k NetworkService`.

Подраздел реестра: `KtmRm`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`), Диспетчер учетных записей безопасности (`SamSs`).

Управляет транзакциями между MSDTC и ядром менеджера транзакций (KTM).

Журналы и оповещения производительности

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeImpersonatePrivilege.

Файлы службы: `pla.dll`.

Исполняемый файл: `svchost.exe -k LocalServiceNoNetwork`.

Подраздел реестра: `pla`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Собирает и хранит данные производительности и оповещений от локального компьютера и других компьютеров сети, после чего позволяет сохранять их или оповещать пользователя о возникшем событии. После отключения этой службы данные производительности и оповещения собираться не будут.

Поддержка элемента панели управления «Отчеты о проблемах и их решениях»

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: SeImpersonatePrivilege и SeTcbPrivilege.

Файлы службы: `wercplsupport.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `wercplsupport`.

Службы, необходимые для работы данной: нет.

Управляет получением и передачей сообщений о проблемах в системных компонентах.

Служба помощника по совместимости программ

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeDebugPrivilege.

Файлы службы: `pcasvc.dll`.

Исполняемый файл: `svchost.exe -k LocalSystemNetworkRestricted`.

Подраздел реестра: `PcaSvc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Управляет работой помощника по совместимости программ. После отключения данной службы помощник совместимости программ работать не сможет.

Служба уведомлений лицензирования программного обеспечения

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeImpersonatePrivilege.

Файлы службы: `SLUINotify.dll`.

Исполняемый файл: `svchost.exe -k LocalService`.

Подраздел реестра: `SLUINotify`.

Службы, необходимые для работы данной: Лицензирование программного обеспечения (`slsvc`), Служба списка сетей (`netprofm`).

Управляет работой службы лицензирования и отображением уведомлений о необходимости активации. Она также управляет загрузкой и установкой цифровых лицензий для программ, созданных Microsoft. Если данная служба будет

отключена, то программы, требующие установки лицензий, будут работать в ограниченном режиме.

Настройки данной службы хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL\Activation`. Например, здесь могут содержаться следующие параметры `REG_DWORD`-типа:

- `ActivationInterval` — определяет интервал, с которым служба пытается выполнить активацию операционной системы;
- `NotificationDisabled` — если значение параметра равно `1`, то уведомления о необходимости активации отображаться не будут;
- `Manual` — определяет, будет ли использоваться ручная активация.

Лицензирование программного обеспечения

Тип запуска: автоматически.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeAuditPrivilege, SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: нет.

Исполняемый файл: `SLsvc.exe`.

Подраздел реестра: `slsvc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Данная служба управляет загрузкой и установкой лицензий на операционную систему Windows и программы. Отключение данной службы может привести к отключению некоторых возможностей программ и операционной системы.

Вы можете удалить эту службу, воспользовавшись командой `slsvc -Delete`. Удаление произойдет после перезагрузки компьютера. А с помощью команды `slsvc -Install` службу можно установить заново. Названия параметров должны обязательно начинаться с большой буквы.

Для работы со службой активации также предназначен новый класс `SoftwareLicensingService` пространства имен `\\root\cimv2` инструментария управления Windows. Описание его свойств и методов приведены в гл. 7.

Обнаружение SSDP

Тип запуска: вручную.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege.

Файлы службы: `ssdpsrv.dll`.

Исполняемый файл: `svchost.exe -k LocalService`.

Подраздел реестра: `SSDPSRV`.

Службы, необходимые для работы данной: HTTP (`http`).

Определяет сетевые службы и устройства, которые используют протокол SSDP, а также предоставляет сведения о сетевых службах и устройствах, работающих с протоколом SSDP на локальном компьютере (например, UPnP).

Служба уведомления о системных событиях

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: `sens.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `SENS`.

Службы, необходимые для работы данной: Система событий COM+ (`EventSystem`).

Контролирует системные события и уведомления от подписчиков на систему событий COM+.

Темы

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeAssignPrimaryTokenPrivilege, SeDebugPrivilege, SeImpersonatePrivilege.

Файлы службы: `shsvcs.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `Themes`.

Службы, необходимые для работы данной: нет.

Обеспечивает работу пользовательских тем. Новый интерфейс Windows Vista также считается темой, поэтому после отключения данной службы можно будет использовать только стандартный интерфейс операционной системы.

Сервер упорядочения потоков

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: нет.

Файлы службы: `mmcss.dll`.

Исполняемый файл: `svchost.exe -k LocalService`.

Подраздел реестра: `THREADORDER`.

Службы, необходимые для работы данной: нет.

Обеспечивает упорядоченное выполнение для групп и потоков в определенный промежуток времени.

Служба профилей пользователей

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeBackupPrivilege, SeRestorePrivilege, SeTakeOwnershipPrivilege, SeDebugPrivilege.

Файлы службы: `profsvc.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `ProfSvc`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Управляет загрузкой и выгрузкой профилей пользователей, а также взаимодействием приложений с данными пользователей. После отключения данной службы нормальный вход и выход из системы будут невозможны.

Windows CardSpace

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: `%systemroot%\WinFX\v3.0\Windows Communication Foundation\infocard.exe`.

Подраздел реестра: `idsvc`.

Службы, необходимые для работы данной: нет.

Управляет созданием и работой электронных пластиковых карт, которые можно создать при использовании программы, вызываемой с помощью значка Windows CardSpace папки Панель управления. Данная программа была рассмотрена ранее в этой книге.

Служба регистрации ошибок Windows

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: SeDebugPrivilege, SeTcbPrivilege, SeImpersonatePrivilege, SeAssignPrimaryTokenPrivilege.

Файлы службы: `WerSvc.dll`.

Исполняемый файл: `svchost.exe -k WerSvcGroup`.

Подраздел реестра: `WerSvc`.

Службы, необходимые для работы данной: нет.

Хранит сведения о возникших в процессе работы операционной системы и программ ошибках, а также пытается отправить их корпорации Microsoft и получить сведения и решения возникшей проблемы. Служба также управляет созданием журналов для служб диагностики и восстановления.

Сборщик событий Windows

Тип запуска: вручную.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeAuditPrivilege, SeChangeNotifyPrivilege, SeImpersonatePrivilege.

Файлы службы: `wecsvc.dll`.

Исполняемый файл: `svchost.exe -k NetworkService`.

Подраздел реестра: `Wecsvc`.

Службы, необходимые для работы данной: нет.

Собирает сведения от программ и оборудования локального и удаленных компьютеров. Например, данная служба необходима для работы механизма подписки на события, реализованного в оснастке Просмотр событий.

ПРИМЕЧАНИЕ

Сведения о работе данной службы заносятся в журнал, расположенный в разделе Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ EventCollector.

Настройки данной службы хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\EventCollector`, которая была описана в разд. 5.2 (при описании оснастки Просмотр событий).

Журнал событий Windows

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege и SeImpersonatePrivilege.

Файлы службы: `wevtsvc.dll`.

Исполняемый файл: `svchost.exe -k LocalServiceNetworkRestricted`.

Подраздел реестра: `Eventlog`.

Службы, необходимые для работы данной: нет.

Реализует работу системных журналов событий, доступ к которым можно получить с помощью оснастки Просмотр событий.

Инструментарий управления Windows

Тип запуска: автоматически.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: `%SystemRoot%\system32\wbem\WMIsvc.dll`.

Исполняемый файл: `svchost.exe -k netsvcs`.

Подраздел реестра: `Winmgmt`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Обеспечивает общий интерфейс и объектную модель доступа для получения полной информации об операционной системе, службах и устройствах.

Служба медиаприставки Windows Media Center

Тип запуска: отключена.

Учетная запись: локальная служба.

Дополнительные привилегии: нет.

Файлы службы: `Mcx2Svc.dll`.

Исполняемый файл: `svchost.exe -k LocalService`.

Подраздел реестра: `Mcx2Svc`.

Службы, необходимые для работы данной: Обнаружение SSDP (`SSDPSRV`), Перечислитель IP-шин PnP-X (`IPBusEnum`), Службы терминалов (`TermService`).

Позволяет устройствам Windows Media Center Extender (медиаприставке) соединяться с данным компьютером.

Служба ресивера Windows Media Center

Тип запуска: вручную.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: нет.

Исполняемый файл: `%systemroot%\ehome\ehRecvr.exe`.

Подраздел реестра: `ehRecvr`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Управляет работой передачи телевидения и радиовещания с помощью компонента Windows Media Center операционной системы (то есть управляет работой с TV-тюнером).

Служба планировщика Windows Media Center

Тип запуска: вручную.

Учетная запись: сетевая служба.

Дополнительные привилегии: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeImpersonatePrivilege.

Файлы службы: нет.

Исполняемый файл: `%systemroot%\ehome\ehsched.exe`.

Подраздел реестра: `ehSched`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Позволяет управлять записью телепередач на компьютер с помощью компонента Windows Media Center операционной системы. Настройки данной службы хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Media Center\Service\Scheduler`.

Модуль запуска службы Windows Media Center

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: SeChangeNotifyPrivilege.

Файлы службы: `%SystemRoot%\ehome\ehstart.dll`.

Исполняемый файл: `svchost.exe -k LocalServiceNoNetwork`.

Подраздел реестра: `ehstart`.

Службы, необходимые для работы данной: Удаленный вызов процедур (RPC) (`RpcSs`).

Управляет запуском служб Служба ресивера Windows Media Center и Служба планировщика Windows Media Center.

Кэш шрифтов Windows Presentation Foundation 3.0.0.0

Тип запуска: вручную.

Учетная запись: локальная служба.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: `%systemroot%\WinFX\v3.0\WPF\PresentationFontCache.exe`.

Подраздел реестра: `FontCache3.0.0.0`.

Службы, необходимые для работы данной: нет.

Ускоряет работу приложений Windows Presentation Foundation (WPF) путем кэширования данных шрифтов.

Служба времени Windows

Тип запуска: автоматически.

Учетная запись: локальная служба.

Дополнительные привилегии: нет.

Файлы службы: `w32time.dll`.

Исполняемый файл: `svchost.exe -k LocalService`.

Подраздел реестра: `W32Time`.

Службы, необходимые для работы данной: нет.

Управляет синхронизацией времени локального компьютера с удаленным сервером времени (либо с сервером в локальной сети домена Active Directory).

W32tm.exe

Расположение: `%systemroot%\system32\w32tm.exe`.

Для настройки возможностей синхронизации локального времени компьютера можно использовать программу командной строки `w32tm.exe`. Она также присут-

ствовала в операционной системе Windows XP, поэтому рассмотрим ее возможности лишь поверхностно. Описание же всех параметров данной программы можно отобразить, воспользовавшись командой `w32tm /?`. Итак, она поддерживает следующие параметры.

- `/register` — устанавливает стандартные параметры реестра, предназначенные для настройки службы Служба времени Windows.
- `/unregister` — удаляет сведения о службе Служба времени Windows.
- `/tz` — отображает текущую настройку часового пояса.
- `/resync /nowait` — немедленно выполняет ресинхронизацию локальных часов компьютера. Эта команда обычно применяется на компьютерах, входящих в состав домена.
- `w32tm /config /syncfromflags:manual /manualpeerlist:<список DNS-имен или IP-адресов соответствующих источников времени, разделенный запятыми>` — устанавливает внешние серверы точного времени, с которыми нужно выполнять синхронизацию.
- `/config /computer:<имя компьютера> /update` — согласует параметры работы службы Служба времени Windows локального и удаленного компьютера.

Настройки групповой политики

Настройки синхронизации времени можно изменить с помощью групповых политик, расположенных в разделе Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Служба времени Windows. Данные политики изменяют параметры `REG_DWORD`-типа, расположенные в подразделах ветви системного реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\W32Time`.

- Глобальные параметры конфигурации — позволяет выполнить конфигурирование глобальных параметров работы службы Служба времени Windows.
- Настроить NTP-клиент Windows — дает возможность выполнить конфигурирование параметров работы клиента NTP, осуществляющего синхронизацию с сервером точного времени. Например, с ее помощью можно изменить значения следующих параметров, расположенных либо в подразделе `Parameters`, либо в подразделе `TimeProviders\NtpClient` ветви реестра.
  - `NtpServer` — определяет NTP-сервер (название его сайта), а также порт, который нужно использовать при подключении.
  - `Type` — указывает тип сервера NTP. Возможны следующие типы серверов: `NoSync` (не выполнять синхронизацию), `NTP` (синхронизация с сервером времени Интернета), `NT5DS` (синхронизация с сервером времени домена Active Directory), `AllSync` (оба типа синхронизации).
  - `CrossSiteSyncFlags` — определяет, может ли клиент NTP синхронизировать время с сервером точного времени, который находится за пределами его сайта Active Directory.
  - `EventLogFlags` — указывает степень подробности протоколирования событий, связанных с работой клиента NTP.

- `SpecialPollInterval` — определяет интервал синхронизации клиента NTP с сервером точного времени.

- Включить NTP-клиент Windows — изменяет значение параметра `Enabled`, расположенного в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpClient`. Политика позволяет запретить или разрешить использование клиента NTP на локальном компьютере (то есть определить, может ли данный компьютер получать сведения точного времени).
- Включить NTP-сервер Windows — изменяет значение параметра `Enabled`, расположенного в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpServer`. Политика дает возможность запретить или разрешить использование сервера NTP на локальном компьютере (то есть определить, может ли данный компьютер предоставлять сведения точного времени).

WMI Performance Adapter

Тип запуска: вручную.

Учетная запись: система.

Дополнительные привилегии: нет.

Файлы службы: нет.

Исполняемый файл: `%systemroot%\system32\wbem\WmiApSrv.exe`.

Подраздел реестра: `wmiApSrv`.

Службы, необходимые для работы данной: нет.

Обеспечивает работу библиотеки WMI для клиентов сети.

Глава 7

Администрирование Windows Vista

- **Настройка разрешений и аудит доступа**
- **Архивирование и восстановление**
- **Диагностика компонентов операционной системы**
- **Шифрование**
- **Работа с драйверами**
- **Работа с файловой системой**
- **Работа с принтерами**
- **Другие вопросы администрирования**

В предыдущих главах мы рассмотрели основные программы операционной системы Windows Vista, оснастки, а также службы данной операционной системы. Сейчас же будут более подробно рассмотрены способы решения некоторых задач, которые могут возникнуть перед администратором Windows Vista.

7.1. Настройка разрешений и аудит доступа

По сравнению с предыдущими версиями операционных систем семейства Windows, настройка разрешений на доступ к файлам и ветвям реестра в Windows Vista совершенно не изменилась: окна операционной системы и механизмы изменения остались те же, настройки безопасности по-прежнему основаны на SID учетной записи пользователя.

ПРИМЕЧАНИЕ

SID представляет собой 48-битный код, который идентифицирует такие объекты операционной системы, как учетные записи пользователей, группы, компьютеры, домены и члены доменов. SID компьютера генерируется при инсталляции операционной системы и используется при генерации SID учетных записей локального компьютера: для создания SID учетной записи к SID компьютера добавляется уникальный на компьютере RID. При этом существует несколько RID, которые на любом компьютере идентифицируют одну и ту же учетную запись. Например, RID 500 идентифицирует учетную запись администратора, а RID 501 — учетную запись гостя.

Каждый SID начинается с буквы S, после которой указываются следующие элементы, разделенные дефисом: номер версии (как правило, 1), код агента идентификатора (как правило, 5), четыре кода субагентов, идущие подряд, и на последнем месте RID.

Однако теперь права администраторов на доступ к файлам и ветвям реестра по умолчанию несколько урезаны.

Реализация защиты

Подсистема защиты в операционных системах семейства Windows основана на SID, маркерах и дескрипторах защиты. Описание SID было приведено выше, сейчас же мы рассмотрим реализацию двух других терминов.

Маркер доступа

Маркер доступа представляет собой набор сведений, присваиваемых любому процессу при его создании и определяющих те операции, которые процесс может выполнять. Он содержит следующую информацию.

- Привилегии, которые предоставлены процессу или потоку (эта информация необходима для определения тех операций, которые может выполнять процесс в операционной системе).
- Тип олицетворения, если маркер является олицетворяющим (эта информация необходима для определения тех прав, которые будут заимствоваться процессом у другого процесса).

ПРИМЕЧАНИЕ

Олицетворение позволяет одному процессу заимствовать права другого (как будто он имеет маркер доступа другого процесса). Например, олицетворение часто применяется в клиент-серверных приложениях, где сервер может применять олицетворение для получения доступа к ресурсам компьютера от имени клиента (и с его правами доступа). При этом процесс, получивший олицетворяющий маркер (в нашем примере сервер), не может передавать его другому процессу.

Существует несколько уровней олицетворения: anonymous (олицетворение запрещено), identification (можно получать SID и привилегии клиента, но олицетворять клиента запрещено), impersonation (можно как идентифицировать, так и олицетворять клиента) и delegation (позволяет олицетворять клиента как на локальном, так и на удаленном компьютере). Вы уже встречались с этими уровнями при описании оснастки Службы компонентов.

- Информацию о том, кто создал данный маркер (диспетчер сеансов, RPC-сервер и т. д.).
- DACL по умолчанию (эта информация необходима для определения тех атрибутов защиты, которые будут присваиваться создаваемым с помощью данного маркера объектам, если дескриптор защиты для создаваемого объекта не определен, и объект не наследует DACL родительского объекта).
- Сведения об учетной записи, которой принадлежит маркер, и группах, в которые входит данная учетная запись (эта информация необходима для определения прав доступа процесса к требуемым ему объектам).

Поскольку маркер содержит переменные сведения (набор привилегий и групп), его длина не является постоянной.

Начальный маркер доступа создается во время входа пользователя в систему и присваивается начальному процессу `userinit.exe`. Этот процесс запускает все основные процессы пользователя, а поскольку маркер доступа родительского процесса передается и процессам, которые он создает (дочерним процессам), все процессы, создаваемые пользователем, имеют один и тот же маркер доступа.

Кроме основных маркеров доступа и маркеров олицетворения, в операционных системах семейства Windows могут использоваться ограниченные маркеры. Ограниченным называется такой маркер, выданный дочернему процессу, в котором отсутствует какая-нибудь привилегия родительского маркера.

Дескрипторы защиты

Если маркер доступа выдается процессу и определяет те права, которыми обладает запущенный процесс, то дескриптор защиты выдается объектам операционной системы (файлы, каталоги) и определяет тех пользователей, которые могут получить доступ к объекту, а также права, которыми эти пользователи обладают. Дескриптор защиты состоит из следующих элементов.

- DACL (список управления избирательным доступом) — определяет пользователей, которые могут получить доступ к данному объекту, и их права. Каждый ACE (элемент списка DACL) содержит SID учетной записи пользователя или группы,

маску доступа, а также флаги наследования (определяют, был ли данный ACE унаследован от DACL родительского объекта и будет ли он наследоваться DACL дочерних объектов). При этом ACE может быть четырех основных типов.

- Доступ разрешен (access allowed). Разрешает пользователю, определенному SID, права доступа к объекту, определенные в маске доступа.
- Доступ отклонен (access denied). Запрещает пользователю, определенному SID, права доступа к объекту, определенные в маске доступа.
- Разрешенный объект (allowed-object). Данный тип ACE используется в Active Directory и применяется для разрешения доступа к объектам и подобъектам каталога.
- Запрещенный объект (denied-object). Данный тип ACE используется в Active Directory и применяется для запрещения доступа к объектам и подобъектам каталога.

Если дескриптор защиты не содержит DACL, то любой пользователь может получить доступ к данному объекту. Если же дескриптор защиты содержит пустой DACL (не имеющий ни одной записи ACE), то доступ к объекту запрещен всем пользователям.

Если же DACL включает в себя множество ACE, определяющих доступ одному и тому же пользователю, то определить, сможет ли в результате пользователь получить доступ к объекту, бывает очень сложно. В этом случае проще воспользоваться вкладкой Действующие разрешения окна Дополнительные параметры безопасности. С ее помощью можно просуммировать все запрещающие и разрешающие ACE для учетной записи пользователя и групп, в которые он входит, и определить текущие разрешения для данного пользователя.

- SACL (системный список управления доступом) — определяет пользователей, для которых установлен аудит доступа, а также те операции, совершаемые пользователем над объектом, которые будут подлежать аудиту. Список SACL может содержать ACE двух типов: системного аудита и объекта системного аудита. Каждый ACE включает в себя SID учетной записи пользователя, GUID-объекта, к которому применим ACE, а также флаги наследования.

  Если дескриптор защиты не содержит SACL, то аудит работы с объектом не ведется.

DACL и SACL являются составными частями списка управления доступом (ACL). Данный список (а также DACL и SACL) состоит из элементов, называемых ACE. Работа с DACL и SACL в операционной системе Windows Vista будет описана далее в этой главе.

Привилегии и права

При описании маркеров доступа мы определили, что они могут содержать информацию о привилегиях, предоставляемых процессу. Привилегии — это права определенной учетной записи (или службы, о чем было описано в гл. 6), позволяющие ей выполнять те операции в операционной системе, которые по умолчанию выполнять запрещено.

Мы уже сталкивались с привилегиями, когда рассматривали оснастку Редактор объектов групповой политики, хотя тогда было упомянуто о них лишь мельком, даже не говорилось о том, что это привилегии.

Привилегии операционной системы

Добавлять и удалять привилегии можно как с помощью API-функций, так и с помощью оснастки Редактор объектов групповой политики. Для этого применяется подраздел оснастки Конфигурация компьютера ▸ Конфигурация Windows ▸ Параметры безопасности ▸ Локальные политики ▸ Назначение прав пользователя. Данный подраздел содержит следующие элементы (сначала указано системное название привилегии, потом ее название в оснастке и в самом конце ее описание).

- SeBackupPrivilege (архивация файлов и каталогов) — разрешает службе или учетной записи выполнять операции резервного копирования. Данная привилегия позволяет учетной записи или службе открывать файлы и каталоги независимо от того, разрешена для них эта операция с помощью DACL или нет. Привилегия позволяет обходить проверку таких разрешений, как Обзор папок/Выполнение файлов, Содержимое папки/Чтение данных, Чтение атрибутов, Чтение расширенных атрибутов, Чтение разрешений. При этом DACL обходится только в том случае, если установлен флаг `FILE_FLAG_BACKUP_SEMANTIC`.

  Привилегия предоставлена группам: Администраторы, Операторы архива и Операторы сервера.

- SeChangeNotifyPrivilege (обход перекрестной проверки) — разрешает службе или учетной записи не проходить все проверки прав доступа пользователя при проходе многоуровневых каталогов (проверки прав доступа к вложенным каталогам). Она не предоставляет прав на просмотр содержимого каталога, если эти права вам не предоставлены DACL, однако позволяет выполнять обзор каталога.

  Привилегия предоставлена группам: Администраторы, Операторы архива, Пользователи, Все, а также учетной записи локальной службы, учетной записи сетевой службы.

- SeCreateGlobalPrivilege (создание глобальных объектов) — позволяет процессу создание разделов и символьных ссылок во время сеанса службы терминалов.

  Привилегия предоставлена: группе Администраторы, учетной записи локальной службы, учетной записи сетевой службы.

- SeCreatePagefilePrivilege (создание файла подкачки) — разрешает службе или учетной записи создание файла подкачки с помощью специальных API-функций.

  Привилегия предоставлена группе Администраторы.

- SeCreateSymbolicLinkPrivilege (создание символических ссылок) — позволяет пользователю создавать символические ссылки. Определить, какие виды символьных ссылок доступны в операционной системе, можно с помощью команды программы командной строки `fsutil behavior set`.

  Привилегия предоставлена группе Администраторы.

- SeDebugPrivilege (отладка программ) — разрешает службе или учетной записи производить отладку системного процесса с помощью подключаемого отладчика программ. Это позволяет процессам получать доступ к другим процессам, минуя проверку их дескриптора защиты.

  Привилегия предоставлена группе Администраторы.

- SeImpersonatePrivilege (имитация клиента после проверки подлинности) — позволяет процессам выполнять олицетворение других процессов.

  Привилегия предоставлена группе Администраторы, учетной записи локальной службы, учетной записи сетевой службы.

- SeIncreaseBasePriorityPrivilege (увеличение приоритета выполнения) — разрешает службе или учетной записи увеличивать приоритет, с которым выполняются процессы. Например, пользователь сможет сделать это с помощью окна диспетчера задач.

  Привилегия предоставлена группе Администраторы.

- SeIncreaseQuotaPrivilege (настройка квот памяти для процесса) — позволяет службе или учетной записи увеличивать квоту на доступный объем памяти, назначенную запущенному процессу.

  Привилегия предоставлена группе Администраторы, учетной записи локальной службы, учетной записи сетевой службы.

- SeLoadDriverPrivilege (загрузка и выгрузка драйверов устройств) — разрешает службе или учетной записи загружать и выгружать драйверы устройств режима ядра. Данная привилегия не относится к драйверам, поддерживающим Plug and Play.

  Привилегия предоставлена группе Администраторы.

- SeManageVolumePrivilege (выполнение задач по обслуживанию томов) — необходима для выполнения проверки диска или его дефрагментации.

  Привилегия предоставлена группе Администраторы.

- SeProfileSingleProcessPrivilege (профилирование одного процесса) — разрешает службе или учетной записи собирать информацию о профилях одиночного процесса. Данная привилегия необходима для работы службы предвыборки данных. В частности, эта привилегия необходима для использования средства мониторинга производительности несистемных процессов.

  Привилегия предоставлена группе Администраторы.

- SeRemoteShutdownPrivilege (принудительное удаленное завершение работы) — необходима, чтобы процесс `winlogon.exe` разрешил удаленно завершить работу компьютера.

  Привилегия предоставлена группе Администраторы.

- SeRestorePrivilege (восстановление файлов и каталогов) — разрешает службе или учетной записи выполнять операции восстановления. Данная привилегия позволяет учетной записи или службе открывать файлы и каталоги независимо от того, разрешена для них эта операция с помощью DACL или нет. При этом она

позволяет обходить проверку таких разрешений, как Обзор папок/Выполнение файлов и Запись. Однако DACL обходится только в том случае, если установлен флаг FILE_FLAG_BACKUP_SEMANTIC.

Привилегия предоставлена группам Администраторы и Операторы архива.

- SeSecurityPrivilege (управление аудитом и журналом безопасности) — необходима для доступа к SACL дескриптора защиты, а также для чтения и очистки журнала событий безопасности. Она идентифицирует своего владельца в качестве оператора системы безопасности.

  Привилегия предоставлена группе Администраторы.

- SeShutdownPrivilege (завершение работы системы) — разрешает службе или учетной записи завершать работу операционной системы.

  Привилегия предоставлена группам Администраторы, Операторы архива, Пользователи.

- SeSystemEnvironmentPrivilege (изменение параметров среды изготовителя) — необходима для чтения переменных окружения микрокода из энергонезависимой памяти компьютеров с помощью HAL. Эта привилегия применима только к компьютерам с архитектурой, отличной от x86 — единственное, к чему можно получить доступ с помощью этой привилегии на компьютерах x86, так это к сведениям о последней удачной конфигурации. Также эта привилегия требуется для установки и модернизации операционной системы.

  Привилегия предоставлена группе Администраторы.

- SeSystemProfilePrivilege (профилирование производительности системы) — проверяется API-функцией NtCreateProfile. Данная привилегия необходима для использования средства мониторинга производительности системных процессов.

  Привилегия предоставлена группе Администраторы.

- SeSystemtimePrivilege (изменение системного времени) — разрешает изменять на компьютере время и дату.

  Привилегия предоставлена группе Администраторы, учетной записи локальной службы.

- SeTakeOwnershipPrivilege (смена владельцев файлов и других объектов) — позволяет службе или учетной записи получать права владельца на любой объект файловой системы (объекты Active Directory, файлы и папки, принтеры, разделы реестра, процессы и потоки), но не предоставляет полного доступа к объекту.

  Привилегия предоставлена группе Администраторы.

- SeTimeZonePrivilege (изменение часового пояса) — разрешает пользователю изменять временную зону, установленную в операционной системе.

  Привилегия предоставлена группе Администраторы, учетной записи локальной службы.

- SeTcbPrivilege (работа в составе операционной системы) — повышает общие права службы или учетной записи до уровня операционной системы (идентифицирует

владельца привилегии как часть доверенного блока компьютеров). Например, это позволяет создавать новый сеанс от имени любого локального пользователя, относящегося к любой группе (позволяет олицетворять любого пользователя локального компьютера без аутентификации и получать доступ к тем ресурсам, к которым может получить доступ другой пользователь).

Привилегия предоставлена: никому.

- SeUndockPrivilege (отключение компьютера от стыковочного узла) — необходима, чтобы режим Plug and Play разрешил извлечение компьютера из стыковочного устройства.

  Привилегия предоставлена группам Администраторы, Пользователи.

Если же вам необходимо узнать, какие привилегии предоставлены текущему пользователю, то можно воспользоваться новой программой командной строки операционной системы Windows Vista `Whoami.exe`. Для этого применяется следующий синтаксис программы: `Whoami /priv`.

Права учетной записи

Подраздел Конфигурация компьютера ▸ Конфигурация Windows ▸ Параметры безопасности ▸ Локальные политики ▸ Назначение прав пользователя оснастки Редактор объектов групповой политики содержит также набор прав, которые могут предоставляться пользователю.

Список большинства этих прав приведен ниже.

- SeAssignPrimaryTokenPrivilege (замена маркера уровня процесса) — позволяет процессам использовать API-функцию `CreateProcessAsUser` для запуска других процессов, не используя свой маркер доступа. Например, эта привилегия может использоваться одной службой для запуска другой. В частности, она используется планировщиком заданий.

  Право предоставлено учетным записям сетевой и локальной службы.

- SeAuditPrivilege (управлять аудитом и журналом безопасности) — разрешает службе или учетной записи создание записей в стандартном журнале безопасности системы (`eventvwr.msc`) с помощью API-функции `ReportEvent`.

  Право предоставлено учетным записям сетевой и локальной службы.

- SeCreatePermanentPrivilege (создание постоянных общих объектов) — позволяет службе или учетной записи создавать постоянные объекты (объекты, не удаляемые при отсутствии ссылок на них). Например, создавать объекты каталога с помощью диспетчера объектов.

  Право предоставлено: никому.

- SeCreateTokenPrivilege (создание маркерного объекта) — разрешает службе или учетной записи создавать первичные маркеры. Иначе говоря, учетная запись может создать маркер, содержащий любые SID и привилегии, и запустить с его помощью процесс.

  Право предоставлено: никому.

- SeEnableDelegationPrivilege (разрешить доверия к учетным записям компьютеров и пользователей при делегировании) — используется в Active Directory для делегирования учетных записей и определяет, может ли данная учетная запись устанавливать параметр Делегирование разрешено для пользовательского или компьютерного объекта. Этот параметр можно устанавливать только для тех учетных записей пользователей или компьютеров, для которых снят флажок Учетная запись не может быть делегирована.

  Право предоставлено: никому.

- SeLockMemoryPrivilege (блокировка страниц в памяти) — разрешает службе или учетной записи выполнять блокировку физических страниц памяти. Блокировка физических страниц памяти запрещает сброс блокированных страниц в файл подкачки, то есть они всегда будут находиться в оперативной памяти.

  Право предоставлено: никому.

- SeMachineAccountPrivilege (добавление рабочих станций к домену) — необходимо, чтобы диспетчер учетных данных безопасности SAM разрешил добавление компьютера к домену. Если пользователь обладает данным правом, он может добавить до десяти компьютеров в домен.

  Право предоставлено пользователям, прошедшим проверку.

- SeSyncAgentPrivilege (синхронизировать данные службы каталогов) — позволяет пользователям выполнять синхронизацию Active Directory. Данное право позволяет читать объекты и свойства каталога Active Directory, даже если их атрибуты защиты это запрещают.

  Право предоставлено: никому.

Редактирование DACL объекта

По умолчанию, если вы еще не отключили механизм UAC, большинство ветвей реестра подраздела HKEY_LOCAL_MACHINE и системных файлов доступны администраторам только для чтения. Полный же доступ на них имеет пользователь TrustedInstaller, который также является и их владельцем. Поэтому администраторы не смогут изменить права доступа на ветвь реестра или файл, пока не сменят владельца на него.

Операция смены владельца проходит так же, как и в Windows XP. Например, для смены владельца файла нужно отобразить окно Свойства данного файла, перейти на вкладку Безопасность и нажать кнопку Изменить. После этого отобразится копия окна Безопасность, в которой нужно нажать кнопку Дополнительно, чтобы отобразилось еще одно окно, имеющее вкладку Владелец. Чтобы сменить владельца файла, нужно перейти на данную вкладку и в поле Изменить владельца на: выбрать нового владельца. После нажатия кнопки OK владелец файла будет изменен, и вы сможете изменить разрешения на доступ к файлу. Похожим образом выполняется изменение владельца ветви реестра.

Программа для работы с DACL icacls.exe

Вы, наверное, знаете, что в предыдущих версиях операционной системы Windows присутствовала программа командной строки cacls.exe, с помощью которой

можно изменять DACL определенного файла. Данная программа присутствует и в Windows Vista, однако, кроме нее, в новой операционной системе есть еще одна программа для работы с DACL — `icacls.exe`. Основные возможности данной программы лучше всего рассмотреть на примерах ее использования. Полное же описание ее возможностей можно увидеть, введя в командной строке команду `icacls /?`.

Архивирование и восстановление DACL файла или нескольких файлов и каталогов

Интересной возможностью данной программы является возможность архивирования DACL файлов или каталогов с целью их дальнейшего восстановления на локальном или удаленном компьютере.

Для архивирования DACL файла достаточно воспользоваться командой `icacls.exe <путь к файлу и его имя> /save <путь к архиву и его имя>`. Например:

- `Icacls c:\windows\system32\cmd.exe /save d:\cmd_ACL_old` — копирует ACL файла `cmd.exe` в файл `cmd_ACL_old`;
- `Icacls c:\windows\system32\* /save d:\System32_ACL_old` — копирует ACL всех файлов и каталогов папки `%systemroot%\system32` в файл `System32_ACL_old`.

Не забывайте, что если какая-нибудь программа, DACL которой нужно скопировать, в данный момент открыта другой программой, то `icacls.exe` не сможет получить к ней доступ и завершит свою работу. В этом случае, если вы копируете DACL содержимого целого каталога, нужно использовать параметр `/C`, чтобы программа `icacls.exe` не завершала свою работу, а продолжила, не копируя DACL занятого файла. Также при копировании DACL содержимого каталога можно использовать параметр `/T`, чтобы также копировалось содержимое всех вложенных в выбранный каталог подкаталогов.

Если же вы хотите восстановить DACL из созданного ранее файла, то нужно воспользоваться командой `icacls.exe <путь к файлу и его имя> /restore <путь к архиву и его имя>`.

Например, `Icacls c:\windows\system32\ /restore d:\System32_ACL_old /C`. Команда восстанавливает DACL для всех файлов, подкаталогов и содержимого подкаталогов папки `%systemroot%\system32` из файла `System32_ACL_old`. Если какой-то файл в данный момент заблокирован, то он будет пропущен программой (благодаря параметру `/C`). Заметьте, что в команде при указании каталога не нужно указывать маску `*`.

Смена владельца файлов и каталогов

С помощью данной программы также очень легко сменить владельца для определенного файла или для всего содержимого каталога. Для этого применяется команда `icacls.exe <путь к файлу и его имя или путь к каталогу> /setowner <логин нового владельца>`.

Например, `Icacls c:\windows\system32\* /setowner administrator /C`. Команда изменяет владельца всего содержимого каталога `%systemroot%` на владельца Администратор. Заметьте, что в команде применяется параметр `/C`. Он имеет такое же действие, что и в предыдущих командах. При смене владельца можно также использовать параметр `/T`. Точнее, параметры `/C` и `/T` можно использовать во всех командах программы `icacls.exe`.

Поиск файлов, в DACL которых есть упоминание о SID определенного пользователя

Для реализации этой возможности используется команда `icacls.exe <путь к файлу и его имя или путь к каталогу> /findsid <SID пользователя или группы>`. В ней вы можете также использовать параметры `/C` и `/T`.

Изменение DACL

Изменение DACL можно выполнить не только с помощью программы `cacls.exe`, но и с помощью новой программы `icacls.exe`. Но перед изменением DACL сначала вспомним обозначения прав пользователей, которые применяются в программах `cacls.exe` и `icacls.exe`:

- `F` — определяет право на полный доступ к объекту;
- `M` — указывает право на изменение объекта;
- `RE` — определяет право на чтение и выполнение объекта;
- `R` — указывает право только на чтение объекта;
- `W` — определяет право на запись объекта;
- `D` — указывает право на удаление объекта;
- `RC` — определяет разрешение на чтение разрешения;
- `WDAC` — указывает разрешение на запись DAC;
- `WO` — определяет разрешение на смену владельца;
- `S` — указывает разрешение на синхронизацию;
- `AS` — определяет разрешение на доступ к системе безопасности;
- `MA` — указывает разрешение на полный доступ к объекту;
- `RD` — определяет разрешение на просмотр содержимого папок и чтение данных;
- `WD` — указывает разрешение на создание файлов и запись данных;
- `AD` — определяет разрешение на создание папок и дозапись данных;
- `REA` — указывает разрешение на чтение дополнительных атрибутов;
- `WEA` — определяет разрешение на запись дополнительных атрибутов;
- `EX` — указывает разрешение на обзор папок и выполнение файлов;
- `DC` — определяет разрешение на удаление;
- `RA` — указывает разрешение на чтение атрибутов;
- `WA` — определяет разрешение на запись атрибутов.

Для добавления DACL, разрешающих определенное действие, нужно использовать команду icacls.exe <путь к файлу и его имя или путь к каталогу> /grant <SID пользователя>:(разрешения через запятую). В этом случае указанное DACL будет добавляться к уже существующему. Если же нужно заменить существующий DACL, то вместо /grant необходимо воспользоваться /grant:r.

Например, такая команда, как Icacls c:\windows\system32* /grant:r administrator:(D,WO) /C, изменяет разрешения для администратора на разрешение удаления и разрешение смены владельца всех файлов и папок каталога %systemroot%\system32. Как обычно при изменении DACL нескольких файлов, в команде используется параметр /C.

Для добавления DACL, запрещающих определенное действие, нужно использовать команду icacls.exe <путь к файлу и его имя или путь к каталогу> /deny <SID пользователя>:(разрешения через запятую).

Например, Icacls c:\windows\system32* /deny administrator:(D,WO) /C. Данная команда запрещает администратору удалять или изменять владельца для всех файлов и папок каталога %systemroot%\system32. Как обычно при изменении DACL нескольких файлов, в команде используется параметр /C.

Для удаления DACL используется команда icacls.exe <путь к файлу и его имя или путь к каталогу> /remove <SID пользователя>.

Например, Icacls c:\windows\system32* /remove administrator /C. Удаляет DACL, упоминающий SID учетной записи Администратор, для всех файлов и папок каталога %systemroot%\system32.

Вы также можете сбросить DACL всех файлов определенного каталога или только определенного файла. В этом случае для него будет применяться наследуемый DACL. Для этого применяется команда icacls.exe <путь к файлу и его имя или путь к каталогу> /reset.

Программа смены владельца takeown.exe

Наверное, вам знакома ситуация, когда после запрещения полного доступа к файлу вы больше не можете изменить его DACL, так как это запрещено вами же. В этом случае можно попробовать заново получить файл во владение, чтобы сбросить все элементы DACL. Для этого можно использовать программу takeown.exe.

С помощью данной программы администраторы могут сменить владельца определенного файла или каталога локального или удаленного компьютера на группу Администраторы или пользователя, от имени которого было выполнено подключение к компьютеру.

Синтаксис данной программы следующий: takeown /s <удаленный компьютер> /u <пользователь, от имени которого выполняется подключение к компьютеру> /p <пароль> /F <путь к файлу или каталогу, владельца которых нужно изменить> <дополнительные параметры>.

- /A — по умолчанию владельцем указанных в команде файлов становится пользователь, от имени которого выполнено подключение к компьютеру. Если же вы укажете этот параметр, то владельцем станет группа Администраторы.
- /R — по умолчанию владелец файлов сменяется только в файлах указанного в команде каталога. Если же нужно, чтобы владелец сменился для всех файлов, каталогов и содержимого вложенных каталогов, необходимо использовать данный параметр.
- /D <Y или N> — если значение данного параметра равно Y, то в случае отказа в доступе к файлу будет выполняться смена разрешений. Иначе данный файл будет пропущен.

Работа с SACL объекта

Как вы, наверное, уже знаете, включить аудит доступа к различным категориям объектов операционной системы можно с помощью оснастки Редактор объектов групповой политики, которая также входит в стандартную консоль gpedit.msc. Для этого нужно перейти в ее подраздел Конфигурация компьютера ▸ Конфигурация Windows ▸ Параметры безопасности ▸ Локальные политики ▸ Политика аудита.

После этого можно указать определенный файл или ветвь реестра, аудит доступа к которым будет отслеживаться (если соответствующий тип аудита установлен в групповых политиках). Например, включить аудит для файла можно следующим образом. После отображения окна Свойства файла нужно перейти на вкладку Безопасность и нажать кнопку Дополнительно. Это приведет к отображению нового окна, содержащего вкладку Аудит. Вам достаточно перейти на нее и нажать кнопку Добавить. После этого отобразится окно Выбор: "Пользователь" или "Группа" для выбора учетной записи пользователя, для которого нужно установить аудит доступа к файлу. А после этого отобразится окно Элемент аудита для, с помощью которого можно выбрать действия над файлом, сведения о выполнении которых пользователем будут заноситься в стандартный журнал Windows Vista. Похожим образом устанавливается аудит доступа к ветвям реестра.

Просмотреть же события аудита можно в стандартном журнале операционной системы Безопасность, отображаемом в оснастке Просмотр событий (входит в консоль eventvwr.msc).

Однако это не единственный способ работы с функциями аудита операционной системы.

В состав операционной системы Windows Vista входит программа командной строки, назначением которой является аудит доступа к объектам и его настройкам. Эта программа является нововведением операционной системы Windows Vista, однако мы не будем полностью описывать ее параметры, так как о них всегда можно прочитать, введя в командной строке auditpol.exe /? или auditpol.exe <команда> /?. Рассмотрим лишь основные способы применения данной программы.

Просмотр состояния аудита доступа к компонентам операционной системы

С помощью данной программы можно определить, включен или нет аудит доступа к тем или иным категориям или подкатегориям доступа операционной системы.

Для просмотра состояния аудита подкатегорий определенной категории доступа используется команда `auditpol.exe /get /Category:"категория"`. Здесь вместо категории можно использовать следующие значения.

- `Account Logon` — определяет аудит событий аутентификации пользователей в системе. В нее входят следующие подкатегории:
  - `Kerberos Ticket Events` — аудит использования билетов Kerberos;
  - `Other Account Logon Events` — аудит других событий;
  - `Credential Validation` — аудит входа в систему с использованием учетных записей.
- `Account Management` — определяет аудит событий изменения параметров настройки учетных записей пользователей. Например, изменения членства в группах, создание и удаление новых учетных записей. В нее входят следующие подкатегории:
  - `Computer Account Management` — изменение системных учетных записей;
  - `Security Group Management` — смена системных групп пользователей;
  - `Distribution Group Management` — изменение в распределении групп пользователей;
  - `Application Group Management` — смена групп приложений;
  - `Other Account Management Events` — изменение других групп пользователей;
  - `User Account Management` — смена пользовательских учетных записей.
- `Object Access` — определяет аудит событий доступа к объектам (файлам, папкам, принтерам, разделам реестра, системным службам и т. д.). Именно к этой категории относится аудит, который назначается с помощью вкладки Аудит окна Дополнительные параметры безопасности (данное окно отображается после нажатия кнопки Дополнительно окна Свойства папки, файла, принтера или подраздела реестра). В нее входят следующие подкатегории:
  - `File System` — объекты файловой системы;
  - `Registry` — ветви реестра;
  - `Kernel Object` — объекты ядра;
  - `SAM` — объекты базы данных локальной безопасности SAM;
  - `Certification Services` — объекты служб сертификации;

- Application Generated — объекты генерирования приложений;
- Handle Manipulation — объекты работы с указателями на окна;
- File Share — объекты доступа к общим файлам и папкам;
- Filtering Platform Packet Drop — список утерянных пакетов;
- Filtering Platform Connection — список соединений;
- Other Object Access Events — другие объекты операционной системы.

- Policy Change — определяет аудит изменения настроек безопасности операционной системы. Например, таких настроек, как изменение доверительных отношений, политики Kerberos, файловой системы EFS и параметров работы протокола QoS. В нее входят следующие подкатегории:
  - Authentication Policy Change — изменение политик аутентификации;
  - Authorization Policy Change — смена политик авторизации;
  - MPSSVC Rule-Level Policy Change — изменение политик MPSSVC;
  - Filtering Platform Policy Change — смена политик фильтрации пакетов;
  - Other Policy Change Events — изменение других политик;
  - Audit Policy Change — смена политик аудита.
- DS Access — определяет аудит изменения объектов Active Directory и их свойств. Поскольку в Active Directory учетные записи пользователей и группы также считаются объектами, некоторые события аудита, заносимые в категорию Account Management, могут заноситься и в эту категорию. В нее входят следующие подкатегории:
  - Directory Service Changes — события изменения служб каталога;
  - Directory Service Replication — события репликации каталога;
  - Detailed Directory Service Replication — расширенные сведения о событиях репликации каталога;
  - Directory Service Access — события доступа к службам каталога.
- Logon/Logoff — определяет события аудита входа и выхода из системы, а также регистрации в ней. В отличие от категории Account Logon, которая также содержит информацию об аутентификации, Logon/Logoff хранит события, позволяющие определить протекание всего сеанса регистрации в операционной системе. В нее входят следующие подкатегории:
  - Logoff — события выхода из системы;
  - Account Lockout — события политики блокировки окна входа при неправильном введении пароля учетной записи;
  - IPSec Main Mode — события использования основного режима IPSec;
  - IPSec Quick Mode — события использования быстрого режима IPSec;

  - `IPSec Extended Mode` — события использования расширенного режима IPSec;
  - `Special Logon` — события специального входа в систему;
  - `Other Logon/Logoff Events` — другие события данной категории;
  - `Logon` — события входа в систему.
- `Privilege Use` — определяет аудит использования привилегий, предоставленных службе или пользователю. К данной категории относятся события, описывающие применение пользователем конкретной привилегии, а также описание этой привилегии (некоторые привилегии могут использоваться очень часто, поэтому они генерируют лишь событие при первом использовании). В нее входят следующие подкатегории:
  - `Non Sensitive Privilege Use` — использование редко изменяемых привилегий;
  - `Other Privilege Use Events` — применение других привилегий;
  - `Sensitive Privilege Use` — использование часто изменяемых привилегий.
- `Detailed Tracking` — определяет категорию аудита отслеживания работы процессов и служб. Например, к данной категории относятся события создания служб и назначенных заданий, а также открытие и закрытие процессов. В нее входят следующие подкатегории:
  - `Process Termination` — завершение работы процесса;
  - `DPAPI Activity` — активация DPAPI;
  - `Other Detailed Tracking Events` — другие изменения в процессах;
  - `Process Creation` — создание процесса.
- `System` — определяет категорию слежения за системными событиями, касающимися системы безопасности Windows. Например, в данную категорию входят события о процессах начальной загрузки, выключения компьютера, аутентификации пользователя. В нее входят следующие подкатегории:
  - `Security System Extension` — аудит расширений безопасности;
  - `System Integrity` — аудит целостности системы;
  - `IPSec Driver` — аудит драйвера IPSec;
  - `Other System Events` — аудит других компонентов системы;
  - `Security State Change` — аудит изменения параметров безопасности.

Подкатегории категорий аудита описывались выше не только для того, чтобы было более точно понятно, аудит чего именно выполняют данные категории. Вы можете просмотреть непосредственно состояние определенной подкатегории аудита. Для этого применяется команда `auditpol /get /SubCategory:"подкатегория"`.

Кроме того, в командах просмотра состояния аудита вы можете использовать параметр /r. При его использовании будет отображаться не только состояние аудита, но и такие дополнительные параметры, как имя компьютера, CLSID-номер подкатегории (его можно использовать в командах вместо названия подкатегории).

Можно также использовать параметр /user:, чтобы определить пользователя, состояние аудита для которого будет отображаться.

Например, чтобы просмотреть состояние аудита системных событий для пользователя Администратор (в расширенном варианте), нужно воспользоваться командой auditpol /get /user:administrator /category:"system" /r.

Редактирование состояния категорий аудита

С помощью данной программы можно не только просматривать состояние аудита категорий, но и устанавливать новое состояние. Для этого применяются команды auditpol /set /category:"категория" или auditpol /set /subcategory:"подкатегория". При этом будет устанавливаться аудит успеха применения определенных категорией или подкатегорией прав.

Если же нужно установить аудит неудачных попыток применения определенных категорией или подкатегорией прав, то нужно воспользоваться следующими командами: auditpol /set /category:"категория" /failure:enable или auditpol /set /subcategory:"подкатегория" /failure:enable.

Если нужно установить аудит как удачных, так и неудачных попыток применения определенных категорией или подкатегорией прав, то нужно воспользоваться следующими командами: auditpol /set /category:"категория" /success:enable /failure:enable или auditpol /set /subcategory:"подкатегория" /success:enable /failure:enable.

Кроме того, можно отключить состояние определенных категорий аудита. Для этого в параметрах /success и /failure вместо значения enable нужно указать значение disable.

Вы также можете использовать параметр /user:, чтобы указать пользователя, для которого устанавливается данное состояние аудита.

Работа с дополнительными параметрами аудита

С помощью данной программы можно также включать или отключать дополнительные настройки работы аудита. Для этого применяются следующие значения параметра /option программы.

- CrashOnAuditFail — определяет, будет ли выполняться перезагрузка компьютера при невозможности записи события аудита. Это значение определяет значение параметра REG_DWORD-типа CrashOnAuditFail ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.
- FullPrivilegeAuditing — указывает, будет ли производиться аудит операций архивирования и восстановления. Данное значение определяет значение

параметра REG_BINARY-типа FullPrivilegeAuditing ветви системного реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.

- AuditBaseObjects — определяет, будет ли выполняться аудит доступа глобальных системных объектов. Оно определяет значение параметра REG_DWORD-типа AuditBaseObjects ветви системного реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.
- AuditBaseDirectories — указывает, будет ли выполняться расширенный аудит доступа к каталогам. Определяет значение параметра REG_DWORD-типа AuditBaseDirectories ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.

Чтобы просмотреть текущее значение одного из приведенных выше параметров, нужно воспользоваться командой auditpol /get /option:"параметр".

Чтобы установить новое значение параметра, нужно воспользоваться командой auditpol /set /option:"параметр" /value:значение. Если значение параметра /value равно enable, то данный параметр аудита будет включен. Если же значение равно disable, то параметр аудита будет отключен.

Архивирование и восстановление настроек аудита

Программа auditpol.exe позволяет сохранить текущее состояние аудита доступа в файл, чтобы потом восстановить их из этого файла.

Для сохранения настроек аудита в файл применяется команда auditpol /backup /file:путь к файлу с расширением CSV. Настройки аудита доступа сохраняются в обычный текстовый файл, в котором они разделяются между собой запятой.

Для восстановления настроек аудита из файла применяется команда auditpol /restore /file:путь к файлу с расширением CSV.

Удаление политик аудита

Последней возможностью данной программы является возможность удаления настроек аудита для определенных учетных записей пользователей.

Чтобы очистить состояние всех категорий и подкатегорий аудита доступа для всех пользователей, нужно воспользоваться командой auditpol /clear. При этом очищается состояние как категорий аудита, так и параметров аудита ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.

7.2. Архивирование и восстановление

Одной из повседневных задач администратора является создание архивных копий файлов, необходимых пользователям. Если раньше, в Windows XP, для этого существовало только одно средство (Ntbackup.exe, который в Windows Vista отсутствует), то теперь ему на смену пришли сразу несколько мастеров и программ командной строки. Именно о них и будет рассказано в этом разделе.

Мастер Центр архивации и восстановления

Данный мастер можно отобразить с помощью одноименного значка папки Панель управления. Основное окно мастера представлено на рис. 7.1.

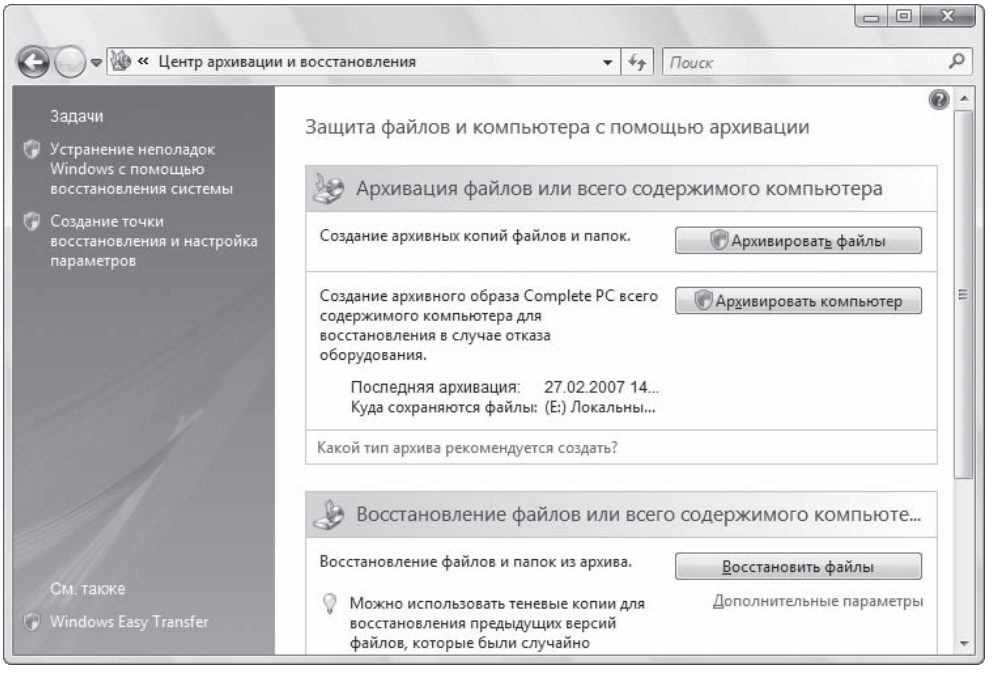


Рис. 7.1. Основное окно мастера Центр архивации и восстановления

Основное окно мастера Центр архивации и восстановления разделено на две части: Архивация файлов или всего содержимого компьютера и Восстановление файлов или всего содержимого компьютера.

ПРИМЕЧАНИЕ

Информация о процессе архивирования и восстановления данных заносится в журнал подраздела Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Backup.

Архивация файлов или всего содержимого компьютера

С помощью раздела Архивация файлов или всего содержимого компьютера можно создать архивную копию определенных файлов или содержимого всего компьютера на основе службы теневого копирования файлов (поэтому в архив войдут даже те файлы, доступ к которым в данный момент запрещен запущенными программами). При этом происходит не просто одноразовое архивирование, а создается задание, которое будет выполняться в определенное время. Обратите на это внимание. Иными словами, для работы с мастером архивирования необходимо, чтобы служба Планировщик заданий была запущена.

Чтобы сделать архивную копию файлов, нужно нажать кнопку Архивировать файлы. После этого отобразится одноименный мастер, первым шагом которого будет выбор места хранения архива. Можно выбрать один из локальных разделов компьютера либо общую папку. После этого мастер предложит вам выбрать разделы диска, которые войдут в архив. При этом системный раздел диска всегда входит в архив, и его архивирование нельзя отключить. На этом шаге нельзя выбрать отдельный файл. А вот следующим шагом мастера будет выбор файлов, которые войдут в архив. Можно поместить в архив следующие файлы: файлы изображений, музыкальные, видео, документы. И последним шагом мастера является создание расписания для запуска данного задания архивирования файлов. Вы можете выбрать не только день архивирования, но и час. После нажатия кнопки Сохранить параметры и начать архивацию перед вами отобразится окно с вопросом о том, хотите ли вы немедленно начать архивирование файлов.

Чтобы сделать архивную копию всего содержимого компьютера, нужно нажать кнопку Архивировать компьютер. После этого отобразится мастер Архивация CompletePC Windows, первым шагом которого будет выбор места хранения архива. Можно выбрать один из локальных разделов компьютера либо привод DVD для записи содержимого на DVD. После этого мастер предложит вам выбрать разделы диска, которые войдут в архив. При этом системный и загрузочные разделы диска (содержащие системные файлы операционных систем, которые установлены на вашем компьютере) всегда входят в архив, и их архивирование нельзя отключить. После выбора разделов диска мастер отобразит выбранные вами диски-источники и диск назначения. Нажав кнопку Сохранить параметры и начать архивацию, можно начать процесс архивирования файлов.

Восстановление файлов или всего содержимого компьютера

Благодаря разделу Восстановление файлов или всего содержимого компьютера вы можете выполнить восстановление файлов из созданных вами ранее архивов. Для этого нужно нажать кнопку Восстановить файлы, после чего запустится мастер Восстановление файлов. Он предложит вам установить переключатель в одно из следующих положений: Файлы из последнего архива и Файлы из более ранних архивов. Если вы установите переключатель в первое положение, то следующим шагом мастера будет восстановление файлов из последней созданной архивной копии файлов. В противном случае мастер отобразит список существующих архивов, из которого вы можете выбрать нужный вам.

Кроме кнопки Восстановить файлы, в разделе Восстановление файлов или всего содержимого компьютера есть ссылка Дополнительные параметры. Вы можете щелкнуть на ней кнопкой мыши, чтобы запустить мастер настройки архивирования Состояние и настройка архивации. Данный мастер будет описан далее в этом разделе.

Можно также воспользоваться кнопкой Восстановить компьютер, чтобы выполнить восстановление файлов на основе архивов, созданных с помощью мастера Windows CompletePC Backup.

Но это еще не все возможности данного раздела. Он также содержит ссылку Используйте восстановление системы для устранения проблем и отмены нежелательных

изменений Windows. После щелчка на ней кнопкой мыши отобразится мастер Восстановление системы. На первом шаге данного мастера вы можете либо выбрать ссылку открыть Защиту системы, чтобы отобразилось окно Свойства системы, открытое на вкладке Защита системы, либо нажать кнопку Далее. Во втором случае перед вами отобразится список доступных точек восстановления, из которого вы можете выбрать нужную вам точку восстановления. Более подробно о восстановлении системы будет рассказано далее.

Настройка мастера Центр архивации и восстановления

Сведения, необходимые для построения содержимого мастера Центр архивации и восстановления, расположены в реестре. Для этого предназначена ветвь реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\BRCpl\BackupApps`. Она включает в себя два подраздела: `{77916c00-866d-4575-a371-74831d3e2285}` и `{a763bfc4-73b8-428b-87d0-9248112f4183}`. Первый из них определяет настройки кнопки Архивировать компьютер раздела Архивация файлов или всего содержимого компьютера и кнопки Восстановить компьютер раздела Восстановление файлов или всего содержимого компьютера. Второй же определяет настройки кнопки Архивировать файлы раздела Архивация файлов или всего содержимого компьютера и кнопки Восстановить файлы раздела Восстановление файлов или всего содержимого компьютера. Оба эти подраздела могут содержать одинаковые параметры, отдельные из которых описаны ниже.

- `BackupDescription` — этот параметр строкового типа хранит описание, отображаемое напротив соответствующей кнопки раздела Архивация файлов или всего содержимого компьютера.
- `RestoreDescription` — имеет строковый тип и содержит описание, отображаемое напротив соответствующей кнопки раздела Восстановление файлов или всего содержимого компьютера.
- `BackupIcon` — этот параметр строкового типа хранит путь к значку, отображаемому напротив соответствующей кнопки раздела Архивация файлов или всего содержимого компьютера.
- `RestoreIcon` — имеет строковый тип и содержит путь к значку, отображаемому напротив соответствующей кнопки раздела Восстановление файлов или всего содержимого компьютера.
- `RestoreAlwaysEnabled` — если значение данного параметра `REG_DWORD`-типа равно `1`, то соответствующая кнопка раздела Восстановление файлов или всего содержимого компьютера будет всегда активирована (по умолчанию она не активна, если вы не делали архивной копии).

Приведенные выше подразделы также включают в себя вложенный подраздел `Commands`, определяющий команды, которые выполняются при выборе соответствующей кнопки или ссылки. Этот подраздел содержит другие подразделы, которые определяют описание отдельных кнопок и ссылок. Эти подразделы, в свою очередь, могут хранить следующие параметры.

- `Executable` — этот параметр строкового типа определяет команду, которая будет выполняться при нажатии соответствующей кнопки или ссылки.

- CommandText — данный параметр строкового типа содержит текст, отображаемый на соответствующей кнопке.
- Arguments — если для работы команды, описанной в параметре Executable, необходимо также указывать аргументы, то они записываются в данном параметре строкового типа.
- RequirePrivilege — этот параметр REG_DWORD-типа определяет, необходимы ли административные привилегии для запуска указанной в параметре Executable команды. Если его значение равно 1, то при нажатии соответствующей кнопки будет активизироваться механизм UAC для запроса подтверждения на запуск команды. Если же значение данного параметра равно 0, то механизм UAC активизироваться не будет. По умолчанию значение данного параметра практически для всех команд равно 1.

Если же вам интересен способ хранения задания автоматического архивирования файлов, то необходимо взглянуть на ветвь реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsBackup\ScheduleParams\Rules. Она содержит набор вложенных подразделов с именами 1, 2, 3 и т. д. Каждый из этих подразделов определяет один раздел диска, содержимое которого будет входить в архив. Для этого данные подразделы включают в себя строковый параметр Root. Они также содержат параметр REG_DWORD-типа Flags. Он может принимать значения вида 40000XXX, где XXX является битовой маской и определяет типы файлов, которые будут архивироваться.

И последнее, о чем хотелось бы рассказать. Как вы уже знаете, с помощью мастера Центр архивации и восстановления можно выполнить архивирование только разделов каталога, а не отдельных его файлов. Однако с помощью реестра можно более тонко настроить процесс архивирования. Например, для этого можно воспользоваться ветвью HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore. Она включает в себя следующие подразделы.

- FilesNotToBackup — содержит список параметров типа REG_MULTI_SZ, значения которых определяют каталоги или файлы, которые нельзя будет архивировать. Например, по умолчанию нельзя архивировать файл подкачки, временные файлы, файлы службы System Restore и службы BITS и т. д.
- FilesNotToSnapshot — хранит список параметров типа REG_MULTI_SZ, значения которых определяют каталоги или файлы, которые не будут входить в создаваемый снимок. По умолчанию в него не входят файлы, принадлежащие RAC.
- KeysNotToRestore — содержит список параметров типа REG_MULTI_SZ, значения которых определяют ветви реестра, содержимое которых не будет восстанавливаться при восстановлении настроек компьютера с помощью ASR.

Мастер Состояние и настройка архивации

Расположение: %systemroot%\system32\sdclt.exe.

Приведенный выше мастер Центр архивации и восстановления является лишь оболочкой для команд мастера Состояние и настройка архивации. Далее будут описа-

ны эти команды, а сейчас рассмотрим сам мастер Состояние и настройка архивации (рис. 7.2).

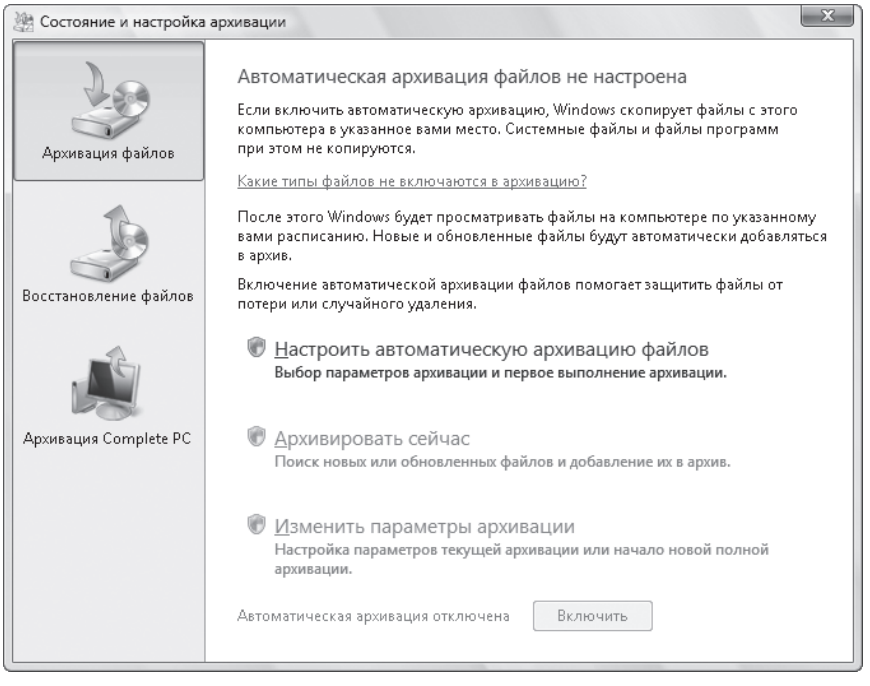


Рис. 7.2. Мастер Состояние и настройка архивации

ПРИМЕЧАНИЕ

Мастер Состояние и настройка архивации можно отобразить и с помощью кнопки Выполнить архивацию, расположенной на вкладке Сервис окна Свойства диска. Команда, которая выполняется после нажатия этой кнопки, указана в параметре (По умолчанию) ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\MyComputer\BackupPath.

Данный мастер состоит из трех разделов: Архивация файлов, Восстановление файлов и Архивация Complete PC.

Архивация файлов

Если вы уже настраивали автоматическое архивирование файлов с помощью кнопки Архивация файлов раздела Архивация файлов или всего содержимого компьютера мастера Центр архивации и восстановления и при этом служба Планировщик заданий в данный момент запущена, то данный раздел будет содержать сведения о времени последнего архивирования файлов и дату следующего архивирования. Кроме того, с помощью данного раздела можно отключить/включить автоматическое архивирование файлов (кнопка Выключить/Включить) или немедленно запустить процесс архивирования (ссылка Архивировать сейчас).

Раздел также содержит ссылку Изменить параметры архивации, с помощью которой можно изменить настройки автоматического архивирования. После выбора данной ссылки отобразится мастер Архивация файлов и вы сможете пройти все шаги настройки архивирования заново.

Восстановление файлов

Данный раздел включает в себя две кнопки: Специальное восстановление и Восстановление файлов.

С помощью кнопки Восстановление файлов можно отобразить одноименный мастер, то есть тот же мастер, что и с помощью кнопки Восстановление файлов раздела Восстановление файлов или всего содержимого компьютера мастера Центр архивации и восстановления.

А с помощью кнопки Специальное восстановление можно отобразить мастер Восстановление файлов (для опытных).

Архивация Complete PC

Данный раздел отображает сведения о дате последнего создания архива содержимого компьютера, а также раздел диска, на котором был создан архив. Если же при последней попытке архивирования произошла ошибка, то с помощью ссылки подробно можно отобразить сведения об этой ошибке.

Раздел также содержит кнопку Архивировать сейчас, с помощью которой можно вызвать мастер Архивация CompletePC Windows, то есть тот же мастер, что и с помощью кнопки Архивация компьютера раздела Архивация файлов или всего содержимого компьютера мастера Центр архивации и восстановления.

Параметры мастера

Данный мастер можно запускать, используя следующие параметры. Именно с этими параметрами он запускается при использовании мастера Центр архивации и восстановления.

- `/RUNONCE` — отображает мастер Архивация файлов. Для его вызова можно также использовать параметр `/STARTBACKUPS`.
- `/CONFIGURE` — выводит мастер Архивация файлов для изменения текущих настроек задания автоматического архивирования файлов.
- `/BLBBACKUPWIZARD` — отображает мастер Архивация CompletePC Windows.
- `/RESTOREWIZARDADMIN` — выводит мастер Восстановление файлов (для опытных).
- `/RESTOREWIZARD` — отображает Восстановление файлов.
- `/UIMODE` — выводит в области уведомлений оповещение, при выборе которого будет вызван мастер Состояние и настройка архивации.
- `/ENABLEJOB` — включает задания автоматического архивирования системы.
- `/DISABLEJOB` — отключает задания автоматического архивирования системы.
- `/KICKOFFJOB` — завершает запущенные в данный момент задания автоматического архивирования системы.

Групповые политики

Параметры работы мастера Состояние и настройка архивации можно ограничить с помощью групповых политик. Для этой цели применяются политики файлов UserDataBackup.admx и WindowsBackup.admx, расположенные в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Архивация данных.

Часть политик данного подраздела расположена в параметрах ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Backup\Client. Они имеют тип REG_DWORD:

- DisableBackupLauncher — если значение данного параметра равно 1, то возможность использования средств архивирования и восстановления данных, реализованных в операционной системе Windows Vista, будет запрещена;
- DisableBackupToDisk — при установке значения этого параметра равным 1 архивирование данных на жесткий диск компьютера будет запрещено (хотя на съемные жесткие диски архивировать данные будет можно);
- DisableBackupToNetwork — если значение данного параметра равно 1, то архивирование данных на общие папки компьютеров сети будет запрещено;
- DisableBackupToOptical — при установке значения этого параметра равным 1 архивирование данных на компакт-диски будет запрещено;
- DisableBackupUI — если значение данного параметра равно 1, то архивирование данных с помощью мастера Центр архивации и восстановления будет запрещено;
- DisableRestoreUI — при установке значения этого параметра равным 1 восстановление данных с помощью мастера Центр архивации и восстановления будет запрещено.
- DisableSystemBackupUI — если значение данного параметра равно 1, то возможность архивации компьютера будет отключена.

Другая же часть политик данного подраздела расположена в ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Backup\Server. Они также имеют тип REG_DWORD:

- OnlySystemBackup — если значение данного параметра равно 1, то администраторам и операторам архива будет запрещено выполнение архивирования данных, расположенных на несистемных разделах диска;
- NoBackupToDisk — при установке значения этого параметра равным 1 администраторам и операторам архива будет запрещено выполнение архивирования данных на локальный компьютер с помощью мастера архивации Windows Server;
- NoBackupToNetwork — если значение данного параметра равно 1, то администраторам и операторам архива будет запрещено выполнение архивирования данных на общие папки компьютеров сети с помощью мастера архивации Windows Server;

- NoBackupToOptical — при установке значения этого параметра равным 1 администраторам и операторам архива будет запрещено выполнение архивирования данных на компакт-диски с помощью мастера архивации Windows Server;
- NoRunNowBackup — если значение данного параметра равно 1, то администраторам и операторам архива будет запрещен однократный запуск мастера архивации Windows Server.

Служба Восстановление системы

Выше уже упоминалась возможность восстановления файлов системы из созданной ранее точки восстановления. Для этого применяется служба Восстановление системы, которая входит в состав как операционной системы Windows Vista, так и более ранних ее версий. Служба Восстановление системы предназначена для создания точек восстановления системы (их еще называют точками отката), которые используются для возврата к предыдущей конфигурации компьютера, если система стала работать некорректно. После создания точки восстановления вы можете в любой момент откатить систему к этой точке. При этом все файлы, содержащиеся в точке восстановления, заменят собой более новые версии.

Для своей работы служба Восстановление системы использует привилегии SeManageVolumePrivilege, SeTakeOwnershipPrivilege, SeSecurityPrivilege, SeRestorePrivilege, SeBackupPrivilege.

ПРИМЕЧАНИЕ

В операционной системе по умолчанию создано задание SR, расположенное в разделе Библиотека планировщика заданий Microsoft ▸ Windows ▸ SystemRestore. Данное задание запускается при старте системы, а также каждый день в 12 часов ночи и выполняет команду rundll32.exe /d srrstr.dll,ExecuteScheduledSPPCreation.

Все точки восстановления хранятся в каталоге <буква диска>\System Volume Information (каждый раздел диска имеет свой каталог System Volume Information, в котором содержатся только точки восстановления файлов, расположенных на соответствующем разделе диска) как файлы без расширения.

В точку восстановления входит копия реестра, локальных профилей, базы данных COM, файла метабазы IIS, базы данных WMI.

По умолчанию операционная система создает точки восстановления в следующих случаях: в начале дня, перед установкой программ (если программы вызывают создание точки восстановления с помощью специальных API-функций) и неподписанных драйверов, перед восстановлением или обновлением системы, а также перед откатом к определенной точке восстановления.

Вкладка Защита системы

Как и раньше, настроить параметры защиты системы можно с помощью вкладки Защита системы окна Свойства системы. Данное окно можно отобразить либо с по-

мощью ссылки Защита системы окна Система (отображается при нажатии комбинации клавиш Alt+Pause Break), либо с помощью одноименной ссылки мастера Восстановление системы. Мастер же Восстановление системы мы раньше вызывали с помощью ссылки Используйте восстановление системы для устранения проблем и отмены нежелательных изменений Windows раздела Восстановление файлов или всего содержимого компьютера мастера Центр архивации и восстановления. Также мастер Восстановление системы можно вызвать, введя команду `rstrui.exe`.

ПРИМЕЧАНИЕ

Вкладка Защита системы отображается только в том случае, если значения параметров REG_DWORD-типа DisableConfig и DisableSR, расположенных в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore, не равно 1. Также, если значение данных параметров равно 1, доступ к мастеру Восстановление системы будет запрещен.

Эти параметры системного реестра изменяются с помощью групповых политик файла SystemRestore.admx, расположенных в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Восстановление системы. Правда, в описаниях этих политик говорится о том, что они не влияют на операционную систему Windows Vista.

Репозитарий CIM операционных систем семейства Windows содержит два класса: `SystemRestoreConfig` и `SystemRestore`, предназначенных для работы со службой Восстановление системы. Они находятся в пространстве имен `root\default`.

Класс `SystemRestoreConfig` хранит основную информацию о параметрах настройки службы и включает в себя следующие свойства: `DiskPercent` (определяет объем диска, резервируемый службой под хранение точек восстановления), `RPGlobalInterval` (определяет интервал между созданиями точек восстановления в секундах), `RPLifeInterval` (определяет время хранения точек восстановления в секундах), `MyKey` (ключевое свойство, идентифицирующее `SystemRestore`).

Экземпляры класса `SystemRestore` определяют информацию о хранящихся на компьютере точках восстановления. Данный класс поддерживает следующие свойства: `CreationTime` (определяет дату создания точки восстановления), `Description` (определяет описание данной точки восстановления), `RestorePointType` (определяет тип данной точки восстановления, например значение `11` говорит о системной точке), `SequenceNumber` (ключевое свойство, содержащее идентификатор точки восстановления).

Кроме того, класс `SystemRestore` поддерживает набор методов, позволяющих работать с точками восстановления. Например, к ним можно отнести следующие методы: `CreateRestorePoint` (создает новую точку восстановления), `Disable` (отключает создание точек восстановления на определенном разделе), `Enable` (включает создание точек восстановления на определенном разделе), `Restore` (восстанавливает систему с помощью определенной точки восстановления).

Вкладка Защита системы содержит список существующих разделов компьютера. Если напротив раздела установлен флажок, то службе Восстановление системы разрешено создавать точки восстановления данного раздела. Справа же от названия раздела отображается дата последнего создания точки восстановления.

ПРИМЕЧАНИЕ

С помощью команды rundll32.exe SRCORE.dll SysprepGeneralize можно отключить службу Восстановление системы на всех дисках.

Кроме того, в операционной системе Windows Vista вкладка Защита системы также содержит две кнопки: Восстановление и Создать. С помощью первой из них можно вызвать мастер Восстановление системы. Вторая же кнопка создает точку восстановления. При этом перед вами отобразится окно Защита системы с просьбой указать описание точки восстановления. Следует заметить, что создание точки восстановления с помощью кнопки Создать основано на работе службы Планировщик заданий, поэтому для корректного создания точки восстановления данная служба должна быть запущена.

ПРИМЕЧАНИЕ

С помощью команды rundll32.exe SRCORE.dll SysprepCleanup можно удалить все созданные точки восстановления.

Мастер Восстановление системы

Расположение: `%systemroot%\system32\rstrui.exe`.

Мастер Восстановление системы, который представляет собой файл `rstrui.exe`, позволяет восстановить состояние компьютера на основе созданной ранее точки восстановления. Использование мастера не является сложным делом — он состоит всего лишь из одного шага, на котором нужно выбрать конкретную точку восстановления из списка созданных ранее точек.

После того как вы нажмете кнопку Готово, отобразится сообщение о том, что идет подготовка к восстановлению, после которой компьютер начнет перезагружаться. Если восстановление из точки отката прошло успешно, то при следующем входе в систему перед вами отобразится сообщение от службы Восстановление системы об этом.

Программа `rstrui.exe` также поддерживает два параметра: `/RUNONCE` и `/OFFLINE:<точка отката>`. Первый отображает сведения о дате последнего восстановления системы из точки восстановления. Второй же восстанавливает систему на основе точки восстановления.

Настройка службы Восстановление системы с помощью реестра

Служба Восстановление системы хранит параметры своей работы в двух ветвях системного реестра: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\`

CurrentVersion\SPP\Clients и HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore.

Настройки создания точек восстановления

В первой из этих ветвей описываются параметры создания точки восстановления. Например, список всех разделов, для которых службе Восстановление системы разрешено создавать точки восстановления, содержится в параметре REG_MULTI_SZ-типа {09F7EDC5-294E-4180-AF6A-FB0E6A0E9513}, расположенном в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SPP\Clients. Кроме того, в первой ветви реестра могут присутствовать следующие параметры REG_DWORD-типа.

- CreateTimeout — определяет интервал ожидания создания теневой копии (в миллисекундах) при создании новой точки восстановления. Если по истечении данного интервала теневая копия нужных файлов создана не будет, то создание точки восстановления будет завершено ошибкой.
- DisableOptimizedRPCreation — позволяет отключить выполнение оптимизации при создании точки восстановления.

Настройки службы Восстановление системы

В ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore содержатся параметры настройки службы Восстановление системы. Большинство из них имеют тип REG-DWORD.

- RPGlobalInterval — определяет интервал между созданиями точек восстановления в секундах (по умолчанию используется интервал в 24 часа).
- RPLifeInterval — указывает время хранения точек восстановления в секундах.

В подразделе cfg данной ветви реестра может присутствовать параметр REG_DWORD-типа DiskPercent. Он определяет процент места на диске, который будет забирать под свои нужды служба Восстановление системы.

На работу службы Восстановление системы также влияют настройки создания теневых копий. Но о них мы поговорим далее в этой книге.

Инструмент командной строки архивации

Расположение: %systemroot%\system32\wbadmin.exe.

Выполнить архивирование файлов можно и с помощью новой программы командной строки wbadmin.exe. Программа поддерживает следующие параметры:

- START BACKUP -backuptarget:<буква диска или UNC-имя общего ресурса, в который нужно выполнить архивирование> -include:<буквы дисков, содержимое которых нужно архивировать, написанные через запятую> — выполняет архивацию содержимого дисков, указанных в параметре -include, на диск или в общий каталог, указанный в параметре -backuptarget.

- `STOP JOB` — отменяет текущую операцию архивирования или восстановления системы.
- `GET VERSIONS -backuptarget:<буква диска или UNC-имя общего ресурса>` — отображает даты создания архивов (в формате `MM/DD/YYYY-HH:MM`), расположенных на указанном в параметре `-backuptarget` диске или общем ресурсе.
- `GET ITEMS -version <дата создания архива> -backuptarget:<буква диска или UNC-имя общего ресурса>` — отображает содержимое архива, расположенного на указанном в параметре `-backuptarget` диске или общем ресурсе и имеющего указанную в параметре `-version` дату создания.
- `GET STATUS` — отображает статус выполнения текущей операции архивирования или восстановления.

Работа с теневыми копиями

Как было сказано выше, архивирование файлов основано на службе теневого копирования. Некоторые параметры работы службы теневого копирования можно также настроить с помощью специальных окон операционной системы.

Вкладка Предыдущие версии

В операционной системе Windows Vista окно Свойства любых файлов и папок содержит новую вкладку: Предыдущие версии. С ее помощью вы можете просмотреть список копий данных файлов или папок, созданных ранее с помощью службы теневого копирования. При этом с помощью той же вкладки можно открыть конкретную теневую копию файла или каталога (с помощью кнопки Открыть), создать новую теневую копию файла на основе существующей теневой копии (с помощью кнопки Копировать), а также восстановить содержимое файла или каталога на основе конкретной теневой копии (с помощью кнопки Восстановить).

Для примера попробуйте создать теневую копию раздела с помощью рассмотренной выше программы `vssuirun.exe`. А после этого посмотрите на содержимое вкладки Предыдущие версии окна Свойства файла или каталога, расположенного на разделе, теневую копию которого вы только что создали.

Теневая копия всех каталогов определенного раздела также создается во время создания точки восстановления с помощью службы Восстановление системы.

Содержимое вкладки Предыдущие версии можно ограничить с помощью групповых политик. Для этого применяются политики файла `PreviousVersions.admx`, расположенные в подразделе Конфигурация пользователя ▸ Административные шаблоны ▸ Компоненты Windows ▸ Проводник Windows ▸ Предыдущие версии.

Политики данного подраздела изменяют значения параметров `REG_DWORD`-типа, расположенных в ветви реестра `HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions`.

- `DisableBackupRestore` — если значение данного параметра равно `1`, то восстановление файла из резервной копии будет запрещено.

- DisableLocalPage — при установке значения этого параметра равным 1 вкладка Предыдущие версии не будет отображаться в окне Свойства для файлов и папок, расположенных на локальном компьютере.
- DisableLocalRestore — если значение данного параметра равно 1, то восстановление файла с помощью копий, расположенных на локальном диске компьютера, будет запрещено.
- DisableRemotePage — при установке значения этого параметра равным 1 вкладка Предыдущие версии не будет отображаться в окне Свойства для файлов и папок, расположенных в общих каталогах.
- DisableRemoteRestore — если значение данного параметра равно 1, то восстановление файла с помощью копий, расположенных в общих каталогах, будет запрещено.
- HideBackupEntries — при установке значения этого параметра равным 1 восстановление файла из копий, хранящихся на архивных носителях, будет запрещено. По умолчанию восстанавливать файлы можно как из теневых копий, расположенных на диске, так и из копий, хранящихся на архивных носителях.

Работа с WMI

Работать с теневыми копиями и просматривать параметры работы провайдера теневого копирования можно также с помощью инструментария управления Windows. Для этого в пространство имен \\root\cimv2 были добавлены новые классы: Win32_ShadowProvider, Win32_ShadowCopy, Win32_ShadowStorage, Win32_ShadowContext.

Класс Win32_ShadowProvider

Данный класс содержит описание провайдеров теневого копирования. Он включает в себя следующие свойства.

- Caption, тип: string — определяет короткое описание провайдера (не более 64 символов).
- CLSID, тип: string — указывает CLSID-номер COM-класса провайдера теневого копирования.
- Description, тип: string — определяет описание провайдера.
- ID, тип: string — является ключевым. Определяет уникальный идентификатор провайдера теневого копирования.
- InstallDate, тип: datetime — указывает дату установки провайдера.
- Name, тип: string — определяет имя провайдера теневого копирования.
- Status, тип: string — указывает статус работы провайдера теневого копирования. Например, возможны следующие значения данного свойства: OK, Error, Degraded, Unknown, Pred Fail, Starting, Stopping, Service, NonRecover, No Contact, Lost Comm.
- Type, тип: uint32 — определяет тип провайдера теневого копирования. Например, провайдер может иметь следующий тип: «неизвестно», «системный», «программное обеспечение», «оборудование».

- `Version`, тип: `string` — указывает версию провайдера.
- `VersionID`, тип: `string` — определяет идентификатор версии провайдера.

Класс Win32_ShadowCopy

Экземпляры данного класса определяют теневые копии файлов. Класс содержит следующие свойства.

- `Caption`, тип: `string` — определяет короткое описание теневой копии (не больше 64 символов).
- `ClientAccessible`, тип: `boolean` — указывает, была ли данная теневая копия создана с помощью компонента Windows Предыдущие версии.
- `Count`, тип: `uint32` — определяет номер теневой копии файла.
- `Description`, тип: `string` — указывает описание теневой копии.
- `DeviceObject`, тип: `string` — определяет название менеджера объектов Windows.
- `Differential`, тип: `boolean` — указывает, была ли создана данная копия отличительным провайдером теневых копий.
- `ExposedLocally`, тип: `boolean` — определяет, была ли данная теневая копия выставлена на локальном компьютере. Если значение данного свойства равно `false`, то данная теневая копия скрыта.
- `ExposedName`, тип: `string` — указывает имя отображаемой теневой копии.
- `ExposedPath`, тип: `string` — определяет путь к отображаемой теневой копии.
- `ExposedRemotely`, тип: `boolean` — указывает, была ли теневая копия выставлена на удаленной машине. Если значение данного свойства равно `false`, то данная теневая копия скрыта.
- `HardwareAssisted`, тип: `boolean` — определяет, была ли данная теневая копия создана провайдером теневых копий оборудования.
- `ID`, тип: `string` — является ключевым. Оно определяет уникальный идентификатор теневой копии на локальном компьютере.
- `Imported`, тип: `boolean` — определяет, была ли данная теневая копия импортирована на данный компьютер, а не создана на нем.
- `InstallDate`, тип: `datetime` — содержит дату создания теневой копии.
- `Name`, тип: `string` — определяет метку теневой копии.
- `NoAutoRelease`, тип: `boolean` — значение свойства указывает, будет ли данная теневая копия удалена автоматически в момент завершения работы процесса, который запросил ее создание. Если значение свойства равно `true`, то теневая копия удалена не будет.
- `NotSurfaced`, тип: `boolean` — определяет, является ли данная теневая копия текущей в пространстве локального компьютера.
- `NoWriters`, тип: `boolean` — указывает, является ли данная теневая копия созданной с теневой копии записывающего компонента.

- `OriginatingMachine`, тип: `string` — определяет имя компьютера, на котором находится оригинал для данной теневой копии.
- `Persistent`, тип: `boolean` — указывает, является ли данная теневая копия постоянной.
- `Plex`, тип: `boolean` — определяет, была ли данная теневая копия создана с помощью провайдера расщепления зеркала.
- `ProviderID`, тип: `string` — указывает уникальный идентификатор провайдера, создавшего данную теневую копию.
- `ServiceMachine`, тип: `string` — определяет идентификатор компьютера, обслуживающего данную теневую копию.
- `SetID`, тип: `string` — указывает идентификатор набора теневых копий, в который входит данная теневая копия.
- `State`, тип: `uint32` — определяет состояние теневой копии. Например, если значение данного свойства равно `1`, то теневая копия подготавливается, а если значение равно `3`, то она уже готова. Если же значение равно `9`, то теневая копия создана. Если значение свойства равно `11`, то она уже удалена.
- `Status`, тип: `string` — указывает описание статуса создания данной теневой копии. Например, возможны следующие значения данного свойства: `OK`, `Error`, `Degraded`, `Unknown`, `Pred Fail`, `Starting`, `Stopping` и т. д.
- `Transportable`, тип: `boolean` — определяет, может ли данная теневая копия быть перенесена на другой компьютер. Если значение данного свойства равно `false`, то теневая копия может работать только на локальном компьютере.
- `VolumeName`, тип: `string` — указывает раздел. На этом разделе находится оригинальный файл, теневую копию которого описывает данный экземпляр класса.

Класс `Win32_ShadowCopy` также поддерживает несколько методов.

- `Create` — создает теневую копию, используя строку окружения.

  Входящие параметры:

  - строковый параметр, определяющий раздел диска;
  - параметр строкового типа, определяющий окружение, по умолчанию его значение равно `ClientAccessible`.

  Возвращаемый параметр: строковый параметр, идентифицирующий созданную теневую копию.

- `Revert` — восстанавливает оригинальный файл на основе данной теневой копии. После этого все более новые теневые копии, чем та, на основе которой содержимое оригинального файла было восстановлено, будут удалены.

  Входящий параметр: определяет, будет ли насильно происходить отключение тома перед восстановлением содержимого оригинального файла из теневой копии. Имеет тип `boolean`.

  Возвращаемые параметры: нет.

Класс Win32_ShadowStorage

Содержит параметры работы хранилища теневых копий. Поддерживает следующие свойства.

- `AllocatedSpace`, тип: `uint64` — определяет размер хранилища.
- `DiffVolume`, тип: указатель на объект `Win32_Volume` — является ключевым. Оно определяет название раздела, присвоенное данному хранилищу теневых копий.
- `MaxSpace`, тип: `uint64` — определяет максимальный размер хранилища. Данное свойство доступно как для чтения, так и для записи.
- `UsedSpace`, тип: `uint64` — указывает используемый размер хранилища.
- `Volume`, тип: указатель на объект `Win32_Volume` — является ключевым. Оно определяет оригинальный раздел диска, на котором было создано хранилище теневых копий.

Класс также поддерживает метод `Create`, который создает новое хранилище теневых копий на указанном разделе.

Входящие параметры:

- строковый параметр, определяющий раздел, на котором создается хранилище теневых копий;
- параметр строкового типа, определяющий название нового раздела, которое будет использоваться для идентификации данного хранилища теневых копий;
- параметр, определяющий максимальный размер хранилища теневых копий, имеет тип `uint64`.

Возвращаемые параметры: нет.

Класс Win32_ShadowContext

Содержит описание окружения теневой копии. Класс содержит следующие свойства.

- `Caption`, тип: `string` — содержит короткое (не больше 64 символов) описание класса `CIM_Setting`.
- `ClientAccessible`, тип: `boolean` — определяет, была ли теневая копия создана с помощью компонента операционной системы Windows Предыдущие версии.
- `Description`, тип: `string` — содержит описание объекта `CIM_Setting`.
- `Differential`, тип: `boolean` — определяет, была ли создана данная теневая копия отличительным провайдером теневых копий.
- `ExposedLocally`, тип: `boolean` — указывает, была ли данная теневая копия выставлена на локальном компьютере. Если значение данного свойства равно `false`, то теневая копия скрыта.

- `ExposedRemotely`, тип: `boolean` — определяет, была ли теневая копия выставлена на удаленной машине. Если значение данного свойства равно `false`, то данная теневая копия скрыта.
- `HardwareAssisted`, тип: `boolean` — указывает, была ли данная теневая копия создана провайдером теневых копий оборудования.
- `Imported`, тип: `boolean` — определяет, была ли данная теневая копия импортирована на данный компьютер, а не создана на нем.
- `Name`, тип: `string` — является ключевым. Оно определяет имя окружения.
- `NoAutoRelease`, тип: `boolean` — значение свойства указывает, будет ли данная теневая копия удалена автоматически в момент завершения работы процесса, который запросил ее создание. Если значение свойства равно `true`, то теневая копия удалена не будет.
- `NotSurfaced`, тип: `boolean` — определяет, является ли данная теневая копия текущей в пространстве локального компьютера.
- `NoWriters`, тип: `boolean` — указывает, является ли данная теневая копия созданной с теневой копии записывающего компонента.
- `Persistent`, тип: `boolean` — определяет, является ли данная теневая копия постоянной.
- `Plex`, тип: `boolean` — указывает, была ли данная теневая копия создана с помощью провайдера расщепления зеркала.
- `SettingID`, тип: `string` — определяет идентификатор объекта `CIM_Setting`. Идентификатор не может быть больше 256 символов.
- `Transportable`, тип: `boolean` — указывает, может ли данная теневая копия быть перенесена на другой компьютер. Если значение данного свойства равно `false`, то теневая копия может работать только на локальном компьютере.

Утилита теневого копирования тома

Расположение: `%systemroot%\system32\vssadmin.exe`.

Еще одной программой для настройки процесса создания теневых копий является стандартная программа командной строки `vssadmin.exe`. Данная программа не является чем-то новым, она присутствовала и в операционной системе Windows XP, поэтому мы рассмотрим ее лишь поверхностно.

Она поддерживает следующие возможности.

- `vssadmin.exe list providers` — выводит список провайдеров теневого копирования (имя провайдера, его тип, идентификатор и версию).
- `vssadmin.exe list shadows` — отображает список существующих теневых копий файлов, а также следующие сведения о них: идентификатор копии, раздел диска и имя компьютера, на котором расположен файл, атрибуты файла, а также имя провайдера, создавшего данную теневую копию.

Можно также воспользоваться дополнительными параметрами `/For=<раздел диска>`, `/Shadow=<идентификатор теневой копии>` или `/Set=<идентификатор набора теневых копий>`. Параметры используются, соответственно, для указания раздела диска, список теневых копий которого нужно отобразить, идентификатора теневой копии для вывода сведений только о ней или идентификатора набора теневых копий для отображения только теневых копий из этого набора.

- `vssadmin.exe list writers` — выводит список всех компонентов системы, которые могут создавать теневые копии. При этом отображается имя компонента, его идентификатор, состояние и описание последней возникшей в работе компонента ошибки.

Кроме того, программа `vssadmin.exe` операционной системы Windows Vista поддерживает следующие новые возможности.

- `vssadmin.exe list shadowstorage` — отображает список всех существующих на компьютере хранилищ теневых копий. Также выводится используемый хранилищами объем диска и максимальный объем диска, который может использовать данное хранилище.

  Команда поддерживает два дополнительных параметра: `/For=<хранилища для данного раздела диска>` и `/On=<хранилища на данном разделе диска>`.

- `vssadmin.exe resize shadowstorage /For=<хранилище для данного раздела диска> /On=<хранилище на данном разделе диска> /MaxSize=<новый максимальный размер хранилища>` — изменяет максимальный размер данного хранилища.
- `vssadmin.exe list volumes` — отображает список всех существующих на компьютере разделов.

7.3. Диагностика компонентов операционной системы

В Windows Vista много внимания уделено средствам диагностики неполадок в работе компонентов операционной системы и способам устранения этих неполадок или передачи информации о них компании Microsoft. Для этого были как улучшены стандартные средства операционной системы Windows XP, так и добавлены совершенно новые возможности.

Окно Отчеты о проблемах и их решениях

Расположение: `%systemroot%\system32\wercon.exe`.

Например, был существенно улучшен механизм передачи информации корпорации Microsoft об ошибках в работе стандартных программ и самой операционной системы. Теперь для настройки данного механизма применяется диалог `Отчеты`

о проблемах и их решениях, получить доступ к которому можно с помощью одноименного значка папки Панель управления.

Основное окно диалога Отчеты о проблемах и их решениях (рис. 7.3) состоит из панели ссылок, с помощью которой можно выполнить переход между вкладками. При запуске же диалога в нем отображаются сведения об ошибках, которые возникли за последнее время. Для этого используется два поля: Устанавливаемые решения и Информация о других проблемах. Первое из них отображает ошибки, возникшие на этапах установки или удаления программ. Второе же отображает сведения о других ошибках.

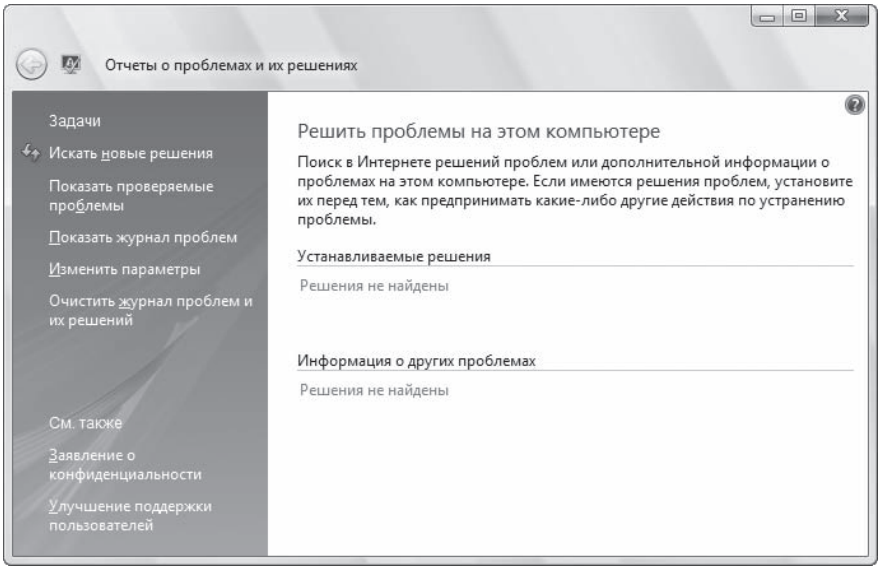


Рис. 7.3. Основное окно диалога Отчеты о проблемах и их решениях

Панель ссылок

Панель ссылок содержит следующие ссылки.

Искать новые решения. Данная ссылка позволяет выполнить поиск исправлений, которые смогли бы устранить возникшие ранее ошибки. После ее выбора отобразится окно передачи информации об ошибках, в процессе которого сведения об ошибках будут записаны в текстовый файл `sysdata.xml`. После этого перед вами отобразится окно с вопросом о том, хотите ли вы передать файл `sysdata.xml` и дополнительные данные на сервер корпорации Microsoft. Если вы нажмете кнопку Передать информацию, то соответствующие файлы будут переданы. Также можно выбрать ссылку Просмотр временной копии файлов, чтобы просмотреть список файлов, которые будут переданы, а также их содержимое.

После того как вы передадите сведения об ошибках корпорации Microsoft, будет получен отчет о том, для решения каких из возникших в работе проблем существуют исправления.

Показать проверяемые проблемы. После выбора данной ссылки перед вами отобразится список всех возникших проблем, отсортированных по названию процесса, в работе которого возникла проблема. При этом будут отображены такие сведения о проблемах, как краткое описание проблемы и дата ее возникновения. Кроме того, с помощью ссылки Показать подробности можно отобразить полные сведения о конкретной проблеме. Среди них можно встретить более детальное описание проблемы, код ошибки, код события, INF-файл, а также список файлов, описывающих возникшую ошибку (например, временные файлы, дампы памяти и т. п.), и т. д.

Обратите также внимание на кнопку Искать решения. С ее помощью можно выполнить поиск только для выбранных вами ошибок. Чтобы выбрать ошибку, достаточно установить флажок напротив нее.

Показать журнал проблем. После выбора данной ссылки перед вами отобразится список всех возникших проблем, отсортированный по названию процесса, в работе которого возникла проблема. Данный список похож на тот, что отображается с помощью ссылки Показать проверяемые проблемы. Однако также с его помощью можно определить, было ли найдено исправление для возникшей ошибки.

Изменить параметры. После щелчка кнопкой мыши на данной ссылке перед вами отобразится окно, с помощью которого можно определить, будет ли автоматически выполняться поиск исправлений для возникших ошибок или же перед этим будет задан вопрос пользователю. Однако это не все параметры, которые можно настроить с помощью ссылки Изменить параметры — обратите внимание на ссылку Дополнительные параметры. После ее выбора перед вами отобразится дополнительное окно, с помощью которого можно изменить следующие параметры работы механизма отправки сообщений об ошибках.

- С помощью переключателя Для моих программ отчеты о проблемах, установленного в положение вкл. или выкл., можно включить или отключить механизм отправки сообщений об ошибках. Действительно, если у вас нет Интернета или вы просто не хотите хранить и передавать сведения о возникших в работе программ ошибках, то лучше всего будет отключить данный механизм.
- С помощью кнопки Изменить параметры можно установить переключатель Выберите настройку отчетности для всех пользователей в одно из положений, влияющих на работу механизма отправки сообщений.
    - Разрешить пользователям выбирать индивидуальные параметры отчетов — позволить каждому пользователю отдельно для своей учетной записи изменять настройки работы механизма отправки сообщений о возникших ошибках.
    - Запрашивать при каждом возникновении проблемы — спрашивать об отправке сообщений и поиске исправлений при каждом возникновении ошибки.
    - Автоматически проверять наличие решений (рекомендуется) — автоматически отправлять сообщения о возникших ошибках и выполнять поиск исправлений, не спрашивая об этом пользователя.

- Автоматически проверять наличие решений и отправлять дополнительную информацию — автоматически отправлять сообщения о возникших ошибках и выполнять поиск исправлений, не спрашивая об этом пользователя. При передаче сообщений об ошибке также будут передаваться дополнительные файлы, которые могут понадобиться серверу Microsoft.

- С помощью поля Список блокировок можно указать программы, сведения об ошибках в которых не будут отправляться на сервер корпорации Microsoft.

Очистить журнал проблем и их решений. С помощью данной ссылки можно удалить информацию о возникших ошибках, а также сведения о состоянии операционной системы и памяти при возникновении данных ошибок. Следует понимать, что хранение данной информации занимает определенный объем свободного места на диске.

Улучшение поддержки пользователей. В самом низу панели ссылок расположена ссылка, с помощью которой можно отобразить окно Программа по улучшению качества программного обеспечения.

Данное окно содержит переключатель, который можно установить в одно из следующих положений: Присоединиться к программе улучшения поддержки пользователей Windows или Не присоединиться к этой программе. Выбрав одно из этих положений, можно вступить или выйти из программы улучшения работы операционной системы Windows Vista и стандартных программ. По этой программе корпорация Microsoft может следить за вариантами использования операционной системы и программ с целью определения необходимых улучшений в программах.

ПРИМЕЧАНИЕ

По умолчанию в операционной системе присутствует два назначенных задания, относящихся к программе Программа по улучшению качества программного обеспечения: Consolidator и OptinNotification. Они расположены в разделе Библиотека планировщика заданий ▸ Microsoft ▸ Windows ▸ Customer Experience Improvement Program.

Задание Consolidator отправляет данные (если они есть), относящиеся к программе улучшения работы операционной системы, в корпорацию Microsoft. Данное задание запускается через каждые 19 часов и выполняет программу wsqmcons.exe.

Задание OptinNotification запускается при каждом входе любого пользователя в систему и выполняет команду wsqmcons.exe -n 0x1C577FA2B69CAD0.

Дополнительные параметры программы Wercon.exe

Кроме того что программа `Wercon.exe` отображает окно Отчеты о проблемах и их решениях, она имеет дополнительные параметры, некоторые из которых описаны ниже.

- `-solutioncheck` — после отображения окна начнется поиск решений проблем, возникших при работе с операционной системой.
- `-signoff` — отображает только окно Поиск решений для этих проблем окна Отчеты о проблемах и их решениях.

- `-problemhistory` — выводит только окно Отчеты о проблемах и их решениях одноименного окна.
- `-showweropts` — отображает только окно Выберите способ проверки на наличие решений в случае неполадок компьютера окна Отчеты о проблемах и их решениях.
- `-showsqmopts` — выводит окно Программа по улучшению качества программного обеспечения.

Настройка механизма с помощью групповых политик

С помощью групповых политик можно изменить многие настройки работы мастера Отчеты о проблемах и их решениях. Для этого применяются политики, описанные в файле `ErrorReporting.admx` и расположенные в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Отчеты об ошибках Windows и его подразделах.

Данные политики изменяют значения следующих параметров, расположенных в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting` и имеющих тип `REG_DWORD`.

- `Disabled` — если значение данного параметра равно `1`, то механизм отчетов об ошибках будет запрещен.
- `LoggingDisabled` — при установке значения этого параметра равным `1` ведение системного журнала ошибок будет запрещено.
- `DontSendAdditionalData` — если значение данного параметра равно `1`, то при передаче сведений о возникшей ошибке будет запрещена передача любых дополнительных данных.
- `MaxArchiveCount` — значение данного параметра определяет максимальное количество отчетов об ошибках, которые могут находиться в хранилище операционной системы.
- `ConfigureArchive` — если значение данного параметра равно `1`, то в хранилище будут помещаться только параметры возникшей ошибки. Если же значение равно `2`, то в хранилище будут помещаться все возможные данные о возникшей ошибке.
- `CorporateWerPortNumber` — значение данного параметра определяет номер порта, по которому будут передаваться данные на сервер обработки отчетов об ошибках.
- `CorporateWerServer` — параметр имеет строковый тип. Его значение указывает имя сервера, на который будут передаваться отчеты об ошибках.
- `CorporateWerUseSSL` — если значение данного параметра равно `1`, то сведения об ошибках будут передаваться на сервер с помощью протокола SSL.
- `ForceQueue` — после установки значения этого параметра равным `2` проверять исправления для отчетов об ошибках сможет только администратор. Если же значение данного параметра равно `1`, то эту операцию может выполнять не только администратор, но и обычный пользователь. А если значение равно `0`, то проверка исправлений будет выполняться автоматически.

- `MaxQueueCount` — значение данного параметра определяет максимально возможное количество отчетов в очереди.
- `QueuePesterInterval` — определяет интервал (в днях) автоматической проверки исправлений для ошибок, находящихся в очереди. По истечении данного интервала будет либо выполняться автоматическая проверка исправлений (если значение параметра `ForceQueue` равно `0`), либо отображаться уведомление с предложением проверки.
- `DefaultConsent` — расположен в подразделе `Consent` указанной ветви реестра. С его помощью можно настроить разрешения на отправку отчетов по умолчанию. Например, если значение параметра равно `1`, то перед отправкой любых данных операционная система будет запрашивать у пользователя подтверждение. Если значение данного параметра равно `2`, то отправка основных сведений об ошибке будет выполняться автоматически, а вот если сайт Microsoft запросит дополнительные данные об ошибке, то перед их отправкой операционная система запросит подтверждение у пользователя. Если же значение равно `3`, то автоматически будут передаваться как основные, так и дополнительные данные, не содержащие личной информации о пользователе. Когда же значение параметра равно `4`, без запроса будут передаваться любые данные.

ПРИМЕЧАНИЕ

По умолчанию содержимое очереди хранится в сжатом виде в каталоге %userprofile%\AppData\Local\Microsoft\Windows\WER\ReportQueue. Вы можете изменить расположение каталога с помощью параметра строкового типа StoreLocation, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug.

По умолчанию в операционной системе присутствует задание QueueReporting, расположенное в разделе Библиотека планировщика заданий ▸ Microsoft ▸ Windows ▸ Windows Error Reporting. Данное задание запускается при каждом входе пользователей в систему с промежутком в 13 минут. При этом, если задание будет выполнено, следующее задание будет назначено только через месяц. Данное задание выполняет команду wermgr.exe -queuereporting.

Параметры реестра

Напоследок рассмотрим некоторые параметры реестра, с помощью которых можно настроить дополнительные свойства работы механизма отправки сведений о возникших ошибках. Все эти параметры расположены в ветви системного реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\Windows Error Reporting` (или в ветви подраздела `HKEY_LOCAL_MACHINE`, если запрещено использование отдельных настроек механизма отправки сообщений об ошибках для каждого пользователя) и имеют тип `REG_DWORD`.

- `DisableArchive` — дает возможность запретить хранение сведений о возникших в работе программ ошибках.
- `DisableQueue` — позволяет запретить использование очередей отправки сведений об ошибках.

- `DontShowUI` — если значение данного параметра равно `1`, то при возникновении ошибки не будет отображаться окно ошибки, содержащее описание ошибки и кнопки завершения программы, вызвавшей ошибку, либо открытия сайта корпорации Microsoft для поиска исправлений возникшей ошибки.

ПРИМЕЧАНИЕ

В ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\Windows Error Reporting\Consent может находиться параметр REG_DWORD-типа APPCRASH. Если его значение равно 0, то окно Microsoft Windows, отображаемое при возникновении ошибки, не будет содержать описание ошибки и кнопку открытия сайта корпорации Microsoft для поиска исправлений возникшей ошибки.

Окно Microsoft Windows может отобразиться не сразу. Например, если значение одного из параметров REG_DWORD-типа WaitOnStart или WaitonExceptionRecord, расположенных в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug, равно 1, то окно Microsoft Windows не будет отображаться до тех пор, пока значение этого параметра не станет равным 0.

- `MaxArchiveCount` — определяет максимальное количество архивируемых сведений об ошибках.
- `MaxQueueCount` — указывает максимальный размер очереди.
- `CorporateWerUseAuthentication` — определяет способ аутентификации при передаче данных о возникшей ошибке на сервер.
- `SendEFSFiles` — указывает, разрешено ли посылать на сервер зашифрованные файлы.

Мастер Средство диагностики технической поддержки Майкрософт

Расположение: `%systemroot%\system32\msdt.exe`.

Данный мастер предназначен для диагностики неисправностей в работе компьютера. С его помощью можно отослать сведения о неисправности профессионалам корпорации Microsoft, чтобы они подсказали решение возникшей проблемы.

ПРИМЕЧАНИЕ

Информация о процессе работы с мастером Средство диагностики технической поддержки Майкрософт заносится в журнал подраздела Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Diagnosis-MSDT.

На первом шаге данного мастера можно выбрать компьютер (локальный или удаленный), на котором возникла неисправность. После этого необходимо указать идентификатор возникшей ошибки, затем начнется соединение с сервером Microsoft для поиска решения возникшей проблемы.

Работу данного мастера можно ограничить с помощью групповых политик файла MSDT.admx, расположенных в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Диагностика ▸ Средство диагностики технической поддержки Майкрософт.

Данные политики изменяют значения параметров REG_DWORD-типа, расположенных в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WDI\{C295FBBA-FD47-46ac-8BEE-B1715EC634E5}.

- Средство диагностики технической поддержки Майкрософт: ограничить загрузку служебных средств — политика изменяет значения параметров DownloadToolsEnabled и DownloadToolsLevel. Если значение параметра DownloadToolsEnabled равно 0, то мастер Средство диагностики технической поддержки Майкрософт не будет предлагать скачивать дополнительные программы для диагностики (если специалисты корпорации определяют, что для решения возникшей проблемы (или для ее диагностики) необходимо использование дополнительных программ, то по умолчанию вам будет предложено их скачать). Если же значение параметра DownloadToolsEnabled равно 1, то с помощью параметра DownloadToolsLevel можно определить дополнительные настройки загрузки программ. Если значение этого параметра равно 1, то загружать дополнительные программы можно только при решении проблем с работой удаленных компьютеров.
- Средство диагностики технической поддержки Майкрософт: настройка режима работы — изменяет значение параметров EnabledScenarioExecutionLevel и ScenarioExecutionEnabled.

Если политика Средство диагностики технической поддержки Майкрософт: настройка режима работы установлена, то использование мастера Средство диагностики технической поддержки Майкрософт будет разрешено. При этом значение параметра EnabledScenarioExecutionLevel равно 2, а значение параметра ScenarioExecutionEnabled равно 1.

Если политика отключена, то использование мастера Средство диагностики технической поддержки Майкрософт будет запрещено. При этом значение параметра EnabledScenarioExecutionLevel равно 2, а значение параметра ScenarioExecutionEnabled равно 0.

Средство диагностики DirectX

Расположение: %systemroot%\system32\dxdiag.exe.

Никуда не исчезла и стандартная программа предыдущих версий операционной системы Windows, предназначенная для диагностики таких компонентов компьютера, как монитор, видеокарта, звуковая плата и манипуляторы.

Как и раньше, перед своим запуском данная программа спрашивает, нужно ли проверить цифровые подписи всех драйверов системы. При использовании проверки цифровых подписей запуск программы займет намного больше времени.

Окно программы состоит из четырех вкладок.

- Система — отображает общие сведения об операционной системе и компьютере: версию операционной системы и BIOS, используемый язык, текущее время, имя компьютера, количество оперативной памяти, общий размер файла подкачки и используемый в данный момент, а также версию DirectX. С операционной системой Windows Vista поставляется десятая версия DirectX.
- Дисплей — выводит общие сведения о параметрах монитора и видеокарты, а также список используемых ими драйверов, указывает, поддерживают ли драйверы стандарт WHQL Logo и имеются ли проблемы в работе данных устройств.
- Звук — отображает общие сведения о звуковой карте вашего компьютера или колонках. Также выводится список используемых звуковой картой драйверов и имеющиеся в работе звуковой платы проблемы.
- Ввод — выводит общие сведения о мыши и клавиатуре, используемых в системе.

Собственно, это все, что позволяет программа `dxdiag.exe` в операционной системе Windows Vista.

Непонятно, почему программа поддерживает так мало возможностей, ведь в предыдущих операционных системах с ее помощью можно было тестировать компоненты операционной системы, отключать различные варианты ускорения работы видеокарты, просматривать список драйверов DirectX, список сетевых протоколов и выполнять другие операции. Сейчас же программу `dxdiag.exe` никак нельзя назвать диагностическим средством.

Диагностика и восстановление томов дисков

Расположение: `%systemroot%\system32\fsutil.exe`.

В операционной системе Windows Vista появилась новая функция автоматической диагностики состояния томов дисков, по умолчанию включенная. Однако найти, где она настраивается, не так-то просто. Все дело в том, что возможности ее настройки были добавлены к стандартной программе командной строки `fsutil.exe`. Для этого данная программа стала поддерживать новый параметр `repair`, который можно использовать следующим образом.

- Чтобы просмотреть состояние работы функции диагностики на определенном томе, нужно воспользоваться командой `fsutil repair query <раздел диска>`. После ее ввода перед вами отобразится флаг диагностики для данного тома. Например, если флаг равен `1`, то будет автоматически происходить общее восстановление поврежденных данных. А если флаг равен `8`, то будет выдаваться предупреждение о возможной потере данных. Описание значений флагов также отображается после ввода данной команды.
- Для установки нового флага состояния работы функции диагностики на определенном томе нужно воспользоваться командой `fsutil repair set <раздел диска> <флаг>`. Описание всех возможных флагов отображается при

вводе команды `fsutil repair set /?`. Вы можете складывать флаги, чтобы выполнялось сразу несколько действий при обнаружении ошибок.

- Чтобы попробовать восстановить содержимое файла определенного тома, можно воспользоваться командой `fsutil repair initiate <раздел диска> <ссылка на файл>`. Описание данной команды можно просмотреть, введя команду `fsutil repair initiate /?`.
- Можно также воспользоваться командой `fsutil repair wait <раздел диска> <0 или 1>` для ожидания завершения восстановления файлов. Если в команде указать `0`, то будет ожидаться завершение всех восстановлений. А если указать `1`, то только текущего восстановления.

7.4. Шифрование

В операционной системе Windows Vista также появились новые возможности по шифрованию файлов и папок, а также целых разделов жесткого диска. Поэтому нельзя не упомянуть об этих возможностях в книге, посвященной нововведениям операционной системы Windows Vista.

Работа с системой шифрования EFS

Как и раньше, в операционной системе присутствует дополнительная файловая система EFS, предназначенная для шифрования файлов и каталогов, находящихся на разделах NTFS жесткого диска. Вы можете выполнить шифрование как с помощью окна Свойства файла или каталога, так и с помощью программы командной строки `cipher.exe`.

Этапы шифрования EFS

Процесс шифрования файла с помощью EFS можно разделить на следующие этапы.

1. Загрузка профиля

Если профиль пользователя еще не загружен (например, такое бывает, когда шифрование или дешифрование файла происходит с помощью программы командной строки `runas.exe`), то он загружается.

2. Создание файла журнала

Начинается процесс шифрования. На этом этапе создается файл журнала шифрования с именем формата `efsX.log`, где `X` определяет номер файла, который был зашифрован в текущий сеанс шифрования процессом `lsasrv.exe`. Данный файл создается в каталоге System Volume Information.

3. Генерация FEK

Выполняется генерация случайного 128-битного числа, используемого в качестве FEK.

FEK используется операционной системой для шифрования содержимого файла по определенному алгоритму, после чего значение FEK добавляется к самому

зашифрованному файлу. Однако перед тем как добавить FEK к файлу, операционная система выполняет шифрование FEK с помощью алгоритма RSA, используя при этом открытый пользовательский ключ. После выполнения всех этих операций файл считается зашифрованным. Чтобы просмотреть его, нужно расшифровать его с помощью FEK, а FEK расшифровывается только с применением ключей, которые можно получить лишь после загрузки учетной записи пользователя, зашифровавшего файл (или тех пользователей, которым разрешен доступ к зашифрованному файлу).

Как было сказано выше, FEK используется для шифрования содержимого файла по определенному алгоритму. Если вопрос защиты информации для вас не является праздным и вы постоянно выполняете шифрование с помощью EFS, то операционная система Windows позволяет вам изменить алгоритм, используемый при шифровании файла (на 3DES). Для этого нужно воспользоваться одним из двух приведенных ниже способов.

- Чтобы установить шифрование на основе 3DES для всех криптографических сервисов операционной системы Windows Vista, нужно запустить оснастку `gpedit.msc` и перейти к подразделу Конфигурация компьютера ▸ Конфигурация Windows ▸ Параметры безопасности ▸ Локальные политики ▸ Параметры безопасности. В данном подразделе есть элемент Системная криптография: Использовать FIPS-совместимые алгоритмы для шифрования, хэширования и подписывания. Состояние данного элемента нужно установить в Отключен. Не забывайте, что использование алгоритма 3DES может замедлить процесс шифрования.
- Можно также установить использование алгоритма 3DES только службой EFS. Для этого нужно параметру `REG_DWORD`-типа `AlgorithmID`, расположенному в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS`, присвоить значение `0x6603`.

Однако это все произойдет на следующих этапах шифрования файла.

4. Получение открытого и закрытого пользовательского ключа

Если раньше пользователь никогда не выполнял шифрование файлов, то генерируется пара пользовательских ключей (закрытый и открытый пользовательские ключи).

В противном случае открытый пользовательский ключ берется из параметра типа `REG_BINARY CertificateHash`, расположенного в ветви системного реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\EFS\CurrentKeys`. На основе данных этой ветви реестра создается сигнатура открытого ключа пользователя.

Закрытые же ключи находятся в каталоге `%userprofile%\AppData\Roaming\Microsoft\Crypto\RSA`. Содержимое этого каталога зашифровано на основе симметричного ключа, который называется мастер-ключом пользователя.

Мастер-ключ содержится в каталоге `%userprofile%\AppData\Roaming\Microsoft\Protect`. Он также зашифрован — с помощью алгоритма 3DES и пароля пользователя.

5. Создание DDF

Для шифруемого файла создается связка ключей DDF (совокупность нескольких DDF, определяющих пользователей, которые могут расшифровать данный файл). DDF хранит информацию о пользователе, который может открыть данный файл, а также о его правах доступа к файлу. В эту информацию входит SID-пользователя, имя контейнера, имя провайдера, зашифровавшего файл, хэш сертификата EFS, используемый при расшифровке, а также зашифрованный FEK.

6. Создание DRF

Для шифруемого файла создается связка ключей DRF. Связка DRF содержит информацию обо всех агентах восстановления, которые могут открыть данный зашифрованный файл. Информация, помещаемая в DRF, аналогична информации, помещаемой в DDF.

Агенты восстановления представляют собой учетные записи пользователей, которые могут открыть зашифрованный файл, даже если они не входят в группу пользователей, которым разрешен доступ к файлу. Как правило, агентом восстановления является администратор. Это сделано для того, чтобы можно было открыть зашифрованные файлы при потере пароля от основного профиля пользователя, который зашифровал файл, или при его повреждении.

Описание работы с агентами восстановления будет приведено далее в этом разделе книги.

7. Шифрование

Создается резервная копия шифруемого файла с именем `efs0.tmp`. В дальнейшем шифрование будет применяться именно к резервному файлу, после чего его содержимое будет скопировано в исходный файл. И в самом конце произойдет удаление резервного файла, а также файла журнала шифрования.

Окно Дополнительные атрибуты

Использование окна Свойства файла или каталога является очень простой задачей. Для шифрования в этом случае достаточно нажать кнопку Другие, после чего в появившемся окне Дополнительные атрибуты установить переключатель Атрибуты сжатия и шифрования в положение Шифровать содержимое для защиты данных. После этого, как только вы нажмете кнопку OK, попытавшись тем самым закрыть окно Свойства, перед вами отобразится еще одно окно, название которого зависит от того, шифруете вы файл или каталог. Независимо от названия, данное окно имеет одну и ту же цель. С помощью его переключателей вы можете определить, будет ли шифроваться только выбранный вами файл или каталог или также родительский каталог (при шифровании файла) либо вложенные в папку файлы и каталоги (при шифровании папки).

Обратите внимание на кнопку Подробно окна Дополнительные атрибуты. По умолчанию она неактивна, но если вы зашифруете файл и опять откроете это окно, то сможете воспользоваться этой кнопкой, чтобы отобразить окно Пользовательский доступ к. С помощью этого окна можно добавить пользователей, которые смогут

открывать данный зашифрованный файл. По умолчанию его можете открывать только вы (так как в атрибутах файла присутствуют сведения о ключе только для вашей учетной записи). Однако если вы нажмете кнопку Добавить данного окна, то сможете выбрать файл сертификата других пользователей, которые смогут открывать этот зашифрованный файл. А с помощью кнопки Удалить можно удалить добавленных ранее пользователей.

Обратите также внимание на кнопку Архивация ключей, которая активируется при выборе из списка одного из пользователей. С ее помощью можно отобразить окно Мастер экспорта сертификатов, позволяющее экспортировать сертификат выбранного пользователя в файл.

Программа cipher.exe

Если же вы захотите использовать программу командной строки `cipher.exe`, то заметите, что ее возможности несколько расширились, а параметры изменились.

Как и раньше, основной синтаксис программы следующий: `cipher [/E | /D | /C] /S:<путь к каталогу> <дополнительные параметры> <файл, каталог или шаблон>`. С помощью данного синтаксиса можно выполнить шифрование (параметр `/E`), дешифровку (`/D`) или просмотреть состояние объектов (`/C`), удовлетворяющих шаблону и расположенных в каталоге, указанном в параметре `/S`. Дополнительных параметров теперь всего два (раньше было пять): `/B` и `/H`. Если указан параметр `/B`, то при ошибке в процессе шифрования файлов программа прекратит свою работу (по умолчанию она продолжает шифрование, просто пропуская проблемный файл). А с помощью параметра `/H` можно определить, будут ли отображаться скрытые и системные файлы.

Дополнительные возможности программы

Никуда не исчезли и следующие дополнительные варианты синтаксиса программы.

- `Cipher` — отображает сведения о состоянии файлов и каталогов, расположенных в данной папке.
- `Cipher /K` — создает новый ключ шифрования для текущего пользователя.
- `Cipher /R:<путь и имя файла>` — создает новый ключ шифрования пользователя и сертификат агента восстановления EFS. После этого созданная информация записывается в два файла с указанным вами именем, но с разными расширениями: PFX (содержит ключ и сертификат агента восстановления) и CER (содержит только сертификат агента восстановления).

  После того как вы введете данную команду, перед вами отобразится запрос с просьбой ввода пароля, который будет защищать файл с расширением PFX. Затем введенный вами пароль нужно ввести еще раз — для подтверждения.
- `Cipher /U /N` — отображает список всех зашифрованных файлов, расположенных на вашем жестком диске. Если вы не укажете параметр /N, то также будет изменен ключ шифрования для найденных файлов (если вы его только что изменили).

- `Cipher /W:<путь к папке>` — удаляет всю информацию в неиспользуемом дисковом пространстве на указанном томе.
- `Cipher /R:<путь и имя EFS-файла> <путь и имя файла архива>` — архивирует сертификат EFS и ключ шифрования в файл с указанным именем.

Новые возможности программы

Но, кроме этого, программа командной строки `cipher.exe` обзавелась и новыми вариантами синтаксиса.

- `Cipher /Y` — отображает набросок текущего сертификата EFS для вашего компьютера.
- `Cipher /ADDUSER [/CERTHASH:<хэш сертификата> | /CERTFILE:<путь к файлу сертификата>] /S:<путь к каталогу> <дополнительные параметры> <файл, каталог или шаблон>` — добавляет нового пользователя, которому разрешено открывать данный зашифрованный файл.
- `Cipher /REMOVEUSER /CERTHASH:<хэш сертификата> /S:<путь к каталогу> <дополнительные параметры> <файл, каталог или шаблон>` — удаляет пользователя из списка пользователей, которым разрешено открывать данный зашифрованный файл.
- `Cipher /REKEY <файл, каталог или шаблон>` — заново шифрует указанные шаблоном файлы, используя текущий ключ шифрования файлов пользователя.

Создание сертификата шифрования

Расположение: `%systemroot%\system32\rekeywiz.exe`.

Мы уже рассмотрели несколько способов создания EFS-сертификата для текущего пользователя и помещение его в файл. Однако это еще не все способы создания сертификата. Для этого также можно воспользоваться специальным мастером операционной системы Windows Vista, который называется Шифрующая файловая система EFS. Данный мастер можно вызвать либо с помощью программы `rekeywiz.exe`, либо с помощью ссылки Управление сертификатами шифрования файлов, отображаемой в мастере Учетные записи пользователей, открыть который можно с помощью одноименного значка папки Панель управления.

Особенностью использования данного мастера является то, что вы можете указать способ хранения создаваемого файла сертификата. Можно выбрать либо хранение сертификата на жестком диске компьютера, либо хранение на смарт-карте, либо хранение в центре сертификации домена Active Directory.

После того как вы выберете место хранения сертификата, нужно будет указать имя файла (если файл сертификата будет храниться на компьютере), а также пароль.

И последним шагом мастера будет указание разделов диска, зашифрованные файлы и каталоги которых будут заново перезашифрованы с использованием нового сертификата (если с помощью мастера Шифрующая файловая система EFS вы создавали

новый сертификат пользователя, а не выбрали на первом шаге мастера один из старых сертификатов).

Работа с агентами восстановления

Как было сказано выше, сведения об агентах восстановления заносятся в поле DRF шифруемого файла. Но как же можно добавить нового агента восстановления? Для этого нужно воспользоваться командой Добавить агент восстановления данных контекстного меню раздела Конфигурация компьютера ▸ Конфигурация Windows ▸ Параметры безопасности ▸ Политики открытого ключа ▸ Шифрующая файловая система EFS оснастки `gpedit.msc`. После выбора данной команды перед вами отобразится Мастер добавления агента восстановления, первым шагом которого будет выбор CER-файла агента восстановления, добавляемого в систему. После этого перед вами появится информация о файле, и после нажатия кнопки Готово новый агент восстановления будет создан. Теперь пользователь, CER-файл которого был добавлен в качестве агента восстановления, сможет расшифровывать любые зашифрованные файлы любого пользователя данной операционной системы.

Напомним, что CER-файл, необходимый для добавления агента восстановления, создается соответствующим пользователем с помощью команды `cipher /R:<путь к каталогу и имя CER-файла>`.

Настройка системы шифрования EFS

Как и другие компоненты операционной системы Windows Vista, параметры системы шифрования можно изменить либо с помощью стандартных окон операционной системы, либо непосредственно с помощью реестра.

Настройка с помощью оснастки gpedit.msc

Оснастка `gpedit.msc` содержит специальный подраздел Конфигурация компьютера ▸ Конфигурация Windows ▸ Параметры безопасности ▸ Политики открытого ключа ▸ Шифрующая файловая система EFS. С помощью команды Свойства контекстного меню данного подраздела можно отобразить окно Свойства: Шифрующая файловая система (EFS), позволяющее настроить основные параметры работы шифрования EFS. Данное окно состоит всего из двух вкладок, с помощью которых можно редактировать значения параметров ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion\EFS`. Большинство элементов данного окна редактируют биты параметра `REG_DWORD`-типа `EfsOptions`.

- Общие — сразу же обратите внимание на переключатель Шифрование файлов с помощью шифрующей файловой системы (EFS). Пока данный переключатель не будет установлен в положение Разрешить, параметры, изменяемые с помощью окна Свойства: Шифрующая файловая система (EFS), активными не будут. После того как вы сделаете все параметры окна активными, можно изменить настройки EFS, устанавливаемые с помощью следующих флажков:
  - Шифровать содержимое папки "Документы" пользователя — указывает, что содержимое каталога Документы пользовательского профиля должно автоматически шифроваться;

- Требовать смарт-карту для EFS — определяет, разрешено ли шифровать содержимое смарт-карт с помощью EFS;
- Создать кэшируемый пользовательский ключ из смарт-карты — указывает, будут ли создаваться пользовательские ключи шифрования, поддерживающие хранение зашифрованных данных на смарт-картах;
- Включить шифрование файла подкачки — определяет, будет ли шифроваться содержимое файла подкачки;
- Отображать уведомления об архивации ключа при создании или изменении пользовательского ключа — указывает, будет ли отображаться уведомление в области уведомлений при создании или изменении пользовательского ключа шифрования.

На вкладке Общие также присутствует поле Сертификаты, которое позволяет указать, разрешено ли EFS создавать пользовательские сертификаты, а также указать размер ключа, используемого при шифровании алгоритмом RSA. Размер ключа хранится в параметре REG_DWORD-типа RsaKeyLength.

- Кэш — позволяет определить события, при которых кэш, содержащий расшифрованный FEK, будет очищаться. По умолчанию операционная система Windows Vista помещает сгенерированный FEK в специальный кэш, чтобы не генерировать его при каждом выполнении процесса шифрования (генерация FEK является сложной и ресурсоемкой операцией).

Можно указать очистку кэша при блокировке сеанса, а также после истечения определенного времени, в течение которого операция шифрования больше не выполнялась. Время, после истечения которого кэш будет очищен, хранится в параметре REG_DWORD-типа CacheTimeout.

Настройка параметров шифрования с помощью реестра

После того как вы зашифруете каталог или файл, его название станет зеленого цвета. Вы можете и сами указать цвет, который примет название зашифрованного файла. Для этого достаточно воспользоваться параметром REG_BINARY-типа AltEncryptionColor, расположенным в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer. Он имеет следующий формат: RGB 0, где R, G и B представляют собой красную, зеленую и синюю компоненты цвета, на которые отводится по одному байту параметра. Операционная система также позволяет вообще отключить изменение цвета зашифрованных файлов. Для этого вам не понадобится знание реестра. Достаточно снять флажок Отображать сжатые или зашифрованные файлы NTFSдругим цветом в поле Дополнительные параметры вкладки Вид окна Свойства папки. Данное окно можно вызвать с помощью одноименной команды меню Упорядочить любой папки.

По умолчанию операционная система Windows Vista автоматически шифрует все файлы и каталоги, перемещаемые в уже зашифрованный каталог. Чтобы отключить такое поведение операционной системы, нужно параметру REG_DWORD-типа NoEncryptOnMove, расположенному в ветви реестра HKEY_LOCAL_MACHINE\

SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer, присвоить значение 1.

Можно также полностью отключить подсистему EFS на данном компьютере. Для этого достаточно присвоить значение 1 параметру REG_DWORD-типа NtfsDisableEncryption ветви системного реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem. Данный параметр можно изменить и с помощью программы командной строки fsutil.exe, которую мы рассмотрели в разд. 7.3.

Работа с механизмом BitLocker Drive Encryption

Нововведением операционной системы Windows Vista является мастер Шифрование диска BitLocker, доступ к которому можно получить с помощью одноименного значка папки Панель управления. Данный мастер позволяет зашифровать не отдельный файл, а весь раздел диска, после чего на лету расшифровывать его содержимое, если к содержимому данного диска обращается аутентифицированный пользователь. Шифрование содержимого диска выполняется с помощью 128- или 256-разрядного алгоритма шифрования Advanced Encryption Standard (AES). При этом вы можете пользоваться как знакомым по предыдущим операционным системам Windows способом шифрования файлов и папок на основе файловой системы EFS, так и механизмом Шифрование диска BitLocker. Например, файлы и папки на разделах диска, которые не являются загрузочными, можно шифровать с помощью EFS, а загрузочный раздел — с помощью механизма Шифрование диска BitLocker. При этом, поскольку ключи шифрования EFS хранятся на загрузочном разделе, безопасность их хранения будет повышена.

Работа мастера Шифрование диска BitLocker тесно связана с чипом TPM, однако вы можете использовать его и на компьютерах, не имеющих данного чипа. В этом случае необходимо использовать USB-носитель.

ПРИМЕЧАНИЕ

По умолчанию использование BitLocker на компьютерах без чипа TPM запрещено. Однако это можно изменить с помощью специальной групповой политики. Данная политика будет описана ниже.

Основное окно мастера состоит из списка разделов жесткого диска компьютера, напротив которых отображается информация о том, зашифровано ли содержимое данного раздела. Если мастер Шифрование диска BitLocker может выполнить шифрование содержимого данного раздела, то под ним отображается ссылка Включить BitLocker. После выбора этой ссылки перед вами отобразится мастер Шифрование диска BitLocker, представленный на рис. 7.4. В операционной системе Windows Vista с помощью мастера Шифрование диска BitLocker можно выполнить шифрование только загрузочного раздела операционной системы, хотя с помощью сценариев можно зашифровать и другие разделы.

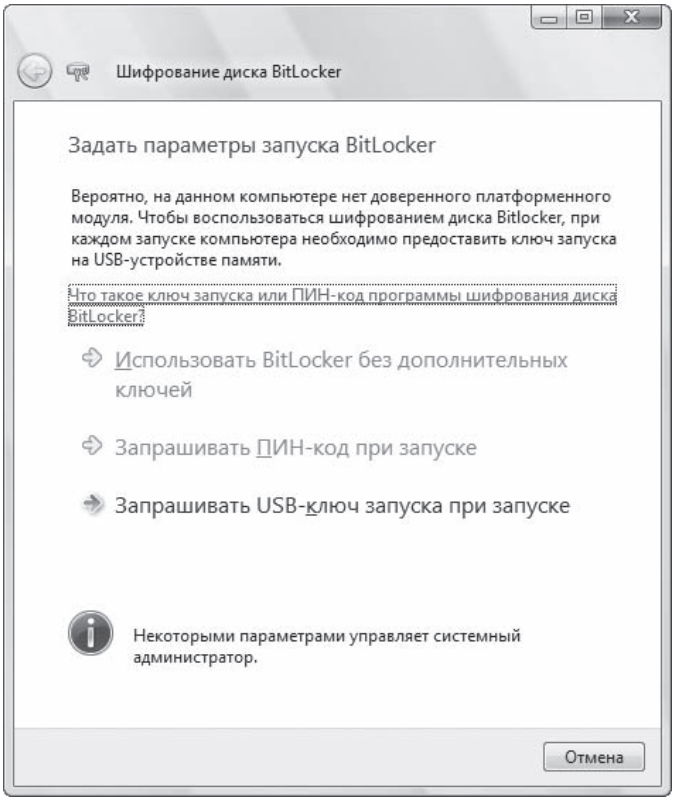


Рис. 7.4. Мастер шифрования содержимого раздела диска

Мастер содержит следующие возможности.

- Запрашивать USB-ключ запуска при запуске — если вы решили зашифровать содержимое раздела, то необходимо воспользоваться данной кнопкой, чтобы сохранить загрузочный ключ (он будет запрашиваться при попытке запуска операционной системы, если вы шифруете загрузочный раздел) на USB-носителе, который нужно будет выбрать из списка USB-носителей, подключенных к компьютеру.

  После того как вы нажмете кнопку Сохранить, загрузочный ключ будет сохранен на USB-носителе, а вам будет предложено установить пароль восстановления. Пароль восстановления создается автоматически (вы его не вводите), а вы можете также сохранить его на USB-носителе или в папке, отобразить на экране либо распечатать на принтере.

  Это последний шаг мастера шифрования выбранного раздела диска. После того как вы сохраните пароль восстановления и нажмете кнопку Зашифровать, начнется процесс шифрования раздела диска. Учтите, что в случае большого объема раздела диска процесс шифрования может занять много времени (шифруются не только используемые кластеры раздела диска, а полностью весь раздел

диска, независимо от того, сколько места на нем используется). Также учтите, что для работы механизма Шифрование диска BitLocker операционная система обязательно создает дополнительный раздел объемом 1,5 Гбайт.

- Запрашивать PIN-код при запуске — позволяет установить загрузочный PIN.
- Использовать BitLocker без дополнительных ключей — разрешает отключить механизм использования загрузочного ключа или ПИН-кода при выполнении загрузки с зашифрованного раздела.

Программа fveupdate.exe

Расположение: `%systemroot%\system32\fveupdate.exe`.

В операционной системе Windows Vista присутствует программа командной строки, предназначенная для работы с механизмом Шифрование диска BitLocker и чипом TPM. К сожалению, ее параметры недокументированны, поэтому для их работы необходимо, чтобы механизм Шифрование диска BitLocker был включен, а на материнской плате присутствовал чип TPM.

Данная программа имеет следующие параметры, выполняющие запрос на обслуживание.

- `/memtest` — программы `memtest.exe`.
- `/bootmgr` — загрузочного меню.
- `/windowsbootenvironment` — программ загрузки операционной системы `winload.exe` и `winresume.exe`.

Работа с WMI

Для работы с BitLocker можно также использовать новый класс репозитария управления CIM. Он содержит обширный набор методов, которые предоставляют доступ к основным возможностям работы механизма Шифрование диска BitLocker. Он находится в пространстве имен `\\.\root\cimv2\Security\MicrosoftVolumeEncryption` и называется `Win32_EncryptableVolume`. Класс поддерживает следующие свойства.

- `DeviceID`, тип: `string` — является ключевым. Оно определяет уникальный идентификатор раздела.
- `DriveLetter`, тип: `string` — содержит букву раздела, который описывается данным экземпляром класса.
- `PersistentVolumeID`, тип: `string` — хранит постоянный идентификатор раздела.

Данный класс также поддерживает следующие методы.

- `ClearAllAutoUnlockKeys` — очищает все ключи разблокировки.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

- `Decrypt` — расшифровывает зашифрованный файл.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

- `DeleteKeyProtector` — удаляет ключ защиты.

  Входящий параметр: строковый параметр, определяющий идентификатор метки ключа защиты.

  Возвращаемые параметры: нет.

- `DeleteKeyProtectors` — удаляет ключи защиты.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

- `DisableAutoUnlock` — запрещает выполнение автоматической разблокировки.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

- `DisableKeyProtectors` — запрещает ключи защиты.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

- `EnableAutoUnlock` — разрешает выполнение автоматической разблокировки.

  Входящий параметр: строковый параметр, определяющий идентификатор метки ключа защиты.

  Возвращаемые параметры: нет.

- `EnableKeyProtectors` — разрешает ключи защиты.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

- `Encrypt` — шифрует файл.

  Входящий параметр: определяет метод шифрования, имеет тип `uint32`.

  Возвращаемые параметры: нет.

- `GetConversionStatus` — возвращает статус конверсии файла.

  Входящие параметры: нет.

  Возвращаемые параметры:

  - определяет статус конверсии, имеет тип `uint32`;
  - определяет процент шифрования, имеет тип `uint32`.

- `GetEncryptionMethod` — возвращает используемый метод шифрования.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет метод шифрования, имеет тип `uint32`.

- `GetExternalKeyFileName` — возвращает путь к файлу, содержащему внешний ключ.

  Входящий параметр: строковый параметр, определяющий идентификатор метки ключа защиты.

  Возвращаемый параметр: строковый параметр, определяющий путь к файлу.

- `GetExternalKeyFromFile` — возвращает внешний ключ, полученный из файла.

  Входящий параметр: строковый параметр, определяющий путь к файлу.

  Возвращаемые параметры: массив параметров типа `uint8`, определяющих внешний ключ.

- `GetKeyProtectorExternalKey` — возвращает ключ защиты для внешнего ключа.

  Входящий параметр: строковый параметр, определяющий идентификатор метки ключа защиты.

  Возвращаемые параметры: массив параметров типа `uint8`, определяющих внешний ключ.

- `GetKeyProtectorFriendlyName` — возвращает имя ключа защиты.

  Входящий параметр: строковый параметр, определяющий идентификатор метки ключа защиты.

  Возвращаемый параметр: строковый параметр, определяющий имя ключа защиты.

- `GetKeyProtectorNumericalPassword` — возвращает пароль ключа защиты.

  Входящий параметр: строковый параметр, определяющий идентификатор метки ключа защиты.

  Возвращаемый параметр: строковый параметр, определяющий пароль ключа защиты.

- `GetKeyProtectorPlatformValidationProfile` — возвращает платформы аутентификации профиля, поддерживаемые ключом защиты.

  Входящий параметр: строковый параметр, определяющий идентификатор метки ключа защиты.

  Возвращаемый параметр: массив параметров типа `uint8`, определяющих платформы аутентификации профиля.

- `GetKeyProtectors` — возвращает ключи защиты.

  Входящий параметр: определяет тип ключа защиты, имеет тип `uint32`.

  Возвращаемый параметр: массив строковых параметров, определяющий идентификаторы метки ключа защиты.

- `GetKeyProtectorType` — возвращает тип ключа защиты.

  Входящий параметр: строковый параметр, определяющий идентификатор метки ключа защиты.

  Возвращаемый параметр: определяет тип ключа защиты, имеет тип `uint32`.

- `GetLockStatus` — возвращает статус блокировки.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет статус блокировки, имеет тип `uint32`.

- `GetProtectionStatus` — возвращает статус защиты.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет статус защиты, имеет тип `uint32`.

- `IsAutoUnlockEnabled` — указывает, разрешена ли автоматическая разблокировка.

  Входящие параметры: нет.

  Возвращаемые параметры:

  - определяет, разрешена ли автоматическая разблокировка, имеет тип `boolean`;
  - строковый параметр, определяющий идентификатор метки ключа защиты.

- `IsAutoUnlockKeyStored` — указывает, разрешена ли автоматическая разблокировка хранилища ключей.

  Входящие параметры: нет.

  Возвращаемый параметр: определяет, разрешена ли автоматическая разблокировка хранилища ключей, имеет тип `boolean`.

- `IsKeyProtectorAvailable` — определяет, разрешен ли ключ защиты.

  Входящий параметр: определяет тип ключа защиты, имеет тип `uint32`.

  Возвращаемый параметр: определяет, разрешен ли ключ защиты, имеет тип `boolean`.

- `IsNumericalPasswordValid` — указывает, является ли пароль истинным.

  Входящий параметр: содержит пароль, имеет тип `uint32`.

  Возвращаемый параметр: определяет, является ли пароль истинным, имеет тип `boolean`.

- `Lock` — выполняет блокировку.

  Входящий параметр: определяет, будет ли выполняться принудительная блокировка, имеет тип `boolean`.

  Возвращаемые параметры: нет.

- `PauseConversion` — приостанавливает конверсию.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

- `ProtectKeyWithExternalKey` — ключ защиты с внешним ключом.

  Входящие параметры:

  - строковый параметр, определяющий имя;
  - массив параметров типа `uint8`, определяющих внешний ключ.

Возвращаемый параметр: строковый параметр, определяющий идентификатор метки ключа защиты.

- `ProtectKeyWithNumericalPassword` — ключ защиты с паролем.

  Входящие строковые параметры, определяющие:

  - имя;
  - пароль.

  Возвращаемый параметр: строковый параметр, определяющий идентификатор метки ключа защиты.

- `ProtectKeyWithTPM` — ключ защиты с TPM.

  Входящие параметры:

  - строковый параметр, определяющий имя;
  - массив параметров типа `uint8`, определяющих платформы, поддерживаемые профилем.

  Возвращаемый параметр: строковый параметр, определяющий идентификатор метки ключа защиты.

- `ProtectKeyWithTPMAndPIN` — ключ защиты с TPM и ПИН-код.

  Входящие параметры:

  - строковый параметр, определяющий имя;
  - массив параметров типа `uint8`, определяющих платформы, поддерживаемые профилем;
  - строковый параметр, определяющий ПИН-код.

  Возвращаемый параметр: строковый параметр, определяющий идентификатор метки ключа защиты.

- `ProtectKeyWithTPMAndStartupKey` — ключ защиты с TPM и загрузочным ключом.

  Входящие параметры:

  - строковый параметр, определяющий имя;
  - массив параметров типа `uint8`, определяющих платформы, поддерживаемые профилем;
  - массив параметров типа `uint8`, определяющих внешний ключ.

  Возвращаемый параметр: строковый параметр, определяющий идентификатор метки ключа защиты.

- `ResumeConversion` — продолжает конверсию.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

- `SaveExternalKeyToFile` — сохраняет внешний ключ в файле.

  Входящие строковые параметры, определяющие:

  - идентификатор метки ключа защиты;
  - путь к файлу.

  Возвращаемые параметры: нет.

- `UnlockWithExternalKey` — выполняет разблокировку на основе внешнего ключа.

  Входящие параметры: массив параметров типа `uint8`, определяющих внешний ключ.

  Возвращаемые параметры: нет.

- `UnlockWithNumericalPassword` — выполняет разблокировку на основе пароля.

  Входящий параметр: строковый параметр, определяющий пароль.

  Возвращаемые параметры: нет.

Групповые политики

Параметры работы механизма шифрования Шифрование диска BitLocker можно настроить с помощью групповых политик файла `VolumeEncryption.admx`, расположенных в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Шифрование диска BitLocker.

Данные политики изменяют значения следующих параметров типа `REG_DWORD`, расположенных в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE`.

- `ActiveDirectoryBackup` — если значение данного параметра равно `1`, то будет разрешено выполнять архивирование важных данных механизма BitLocker (пароль восстановления, различные идентификационные данные и ключ шифрования) на контроллер домена. Архивирование данных BitLocker на контроллере домена позволяет повысить отказоустойчивость механизма шифрования.
- `RequireActiveDirectoryBackup` — при установке значения этого параметра равным `1` перед выполнением шифрования система должна выполнить архивирование данных BitLocker на контроллере домена. Если архивирование данных не будет выполнено, то шифрование данных будет отменено.
- `ActiveDirectoryInfoToStore` — если значение данного параметра равно `1`, то на контроллере домена будет архивироваться вся дополнительная информация, необходимая для восстановления. Если значение равно `2`, то на контроллере домена будет архивироваться только пароль восстановления.
- `DefaultRecoveryFolderPath` — имеет тип `REG_EXPAND_SZ`. Параметр содержит путь к папке для сохранения паролей восстановления по умолчанию.

- `UseRecoveryDrive` — если значение данного параметра равно `1`, то перед шифрованием необходимо сохранить ключ шифрования на съемном носителе. Это позволяет повысить отказоустойчивость механизма шифрования.
- `UseRecoveryPassword` — при установке значения этого параметра равным `1` перед шифрованием необходимо указать пароль шифрования и сохранить его. Это позволяет повысить отказоустойчивость механизма шифрования.
- `EnableNonTPM` — если значение данного параметра равно `1`, то использование механизма BitLocker на компьютерах без чипа TPM будет разрешено.
- `UsePartialEncryptionKey` — при установке значения этого параметра равным `0` TPM при запуске компьютера не будет требовать предъявления «флэшки», содержащей ключ запуска. Если значение равно `1`, то значение параметра `UsePIN` должно быть равно `0`.
- `UsePIN` — если значение данного параметра равно `0`, то TPM при запуске компьютера не будет требовать ввод ПИН-кода (от 2 до 20 символов). Если значение равно `1`, то значение параметра `UsePartialEncryptionKey` должно быть равно `0`.
- `EncryptionMethod` — значение параметра определяет алгоритм шифрования, который будет использоваться при следующем выполнении шифрования. Если значение равно `1` (по умолчанию), то будет использоваться шифрование с помощью 128-битного ключа алгоритма AES с диффузором. Если значение равно `2`, то будет использоваться шифрование с помощью 256-битного ключа алгоритма AES с диффузором. Если же значение параметра равно `3`, будет использоваться шифрование с помощью 128-битного ключа алгоритма AES без диффузора. Ну, а если значение параметра равно `4` — 256-битного ключа алгоритма AES без диффузора.
- `MorBehavior` — при установке значения этого параметра равным `1` при перезагрузке компьютера не будет выполняться перезапись содержимого памяти. Это позволяет повысить скорость перезагрузки компьютера, хотя безопасность работы BitLocker будет понижена.

Вы также можете изменить профиль проверки целостности компьютера, используемый чипом TPM по умолчанию для определения применяемых способов защиты ключа шифрования BitLocker. Для этого нужно изменить значения параметров `REG_DWORD`-типа, расположенных в подразделе `PlatformValidation` указанной ветви реестра.

По умолчанию используется проверка изменений базовой точки начала доверительных измерений (CRTM), BIOS и расширений платформы (регистр PCR 0), кода `Option ROM` (PCR 2), основной загрузочной записи (MBR) (PCR 4), загрузочного сектора NTFS (PCR 8), загрузочного блока NTFS (PCR 9), диспетчера загрузки (PCR 10) и управления доступом BitLocker (PCR 11). Если какой-то из этих компонентов окажется измененным, то TPM запретит расшифровку данных механизмом BitLocker и начнет процесс восстановления.

7.5. Работа с драйверами

Драйвер представляет собой программу в специальном формате, которая управляет работой определенного устройства или, в некоторых случаях, программы. Как правило, драйвер работает в нулевом кольце защиты, поэтому он может выполнить любую операцию в системе.

Установка драйверов

Если только что установленное оборудование компьютера не распознается, то, скорее всего, операционная система не смогла найти драйвер для него. Чтобы проверить эту догадку, нужно запустить оснастку Диспетчер устройств (`devmgmt.msc`) и посмотреть список найденного операционной системой оборудования. По умолчанию после запуска данной оснастки вы сразу же заметите неработающее оборудование — оно будет отображаться в списке Другие устройства, который будет раскрыт, и в нижней части значка каждого неработающего оборудования будет отображаться восклицательный или вопросительный знак.

ПРИМЕЧАНИЕ

Информация о загруженных и выгруженных драйверах пользовательского режима заносится в журнал подраздела Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ DriverFrameworks-UserMode.

Если установленное вами оборудование выводится в оснастке `devmgmt.msc` и напротив него действительно отображается восклицательный знак, то зайдите в свойства данного оборудования (команда Свойства контекстного меню значка оборудования) и посмотрите на поле Состояние устройства. Если в нем написано, что драйвер оборудования не установлен, то проблему нераспознавания оборудования мы нашли.

Процесс установки

Используем оболочку

Чтобы установить драйвер для оборудования (если у вас есть диск с драйвером), нужно нажать кнопку Обновить драйверы окна свойств неработающего оборудования. После этого перед вами отобразится мастер Обновление драйверов, содержащий две ссылки.

- Автоматический поиск обновленных драйверов — выполняет поиск файлов драйвера в стандартном каталоге операционной системы, содержащем драйверы устройств, или в Интернете на сайте Microsoft. Если вы не установили переключатель Хотите, чтобы при подключении новых устройств выполнялся поиск подходящих драйверов в Центре обновления Windows? (расположен в окне Параметры поиска драйверов в Центре обновления Windows, которое можно отобразить с помощью одноименной кнопки вкладки Оборудование окна Свойства системы)

в положение Не выполнять поиск драйверов при подключении новых устройств, то после выбора данной ссылки перед вами откроется еще ряд ссылок:

- Да, всегда выполнять поиск в Интернете (рекомендуется) — выполнить поиск драйвера для устройства на сайте Microsoft и в будущем всегда сначала выполнять поиск драйверов на сайте Microsoft;
- Да, выполнить поиск в Интернете только в этот раз — выполнить поиск драйвера для устройства на сайте Microsoft;
- Не выполнять поиск в Интернете — не выполнять поиск драйвера для устройства на сайте Microsoft, а сразу же перейти к поиску в стандартном каталоге драйверов операционной системы.

ПРИМЕЧАНИЕ

Окно Параметры поиска драйверов в Центре обновления Windows, содержащее переключатель Хотите, чтобы при подключении новых устройств выполнялся поиск подходящих драйверов в Центре обновления Windows?, можно вызвать и с помощью команды rundll32.exe newdev.dll, WindowsUpdateDriverSearchingPolicyUi.

- Выполнить поиск драйверов на этом компьютере — позволяет указать путь к папке или диску, в котором нужно выполнить поиск драйвера. Если у вас действительно есть диск с драйвером для устройства, то его нужно поместить в привод и воспользоваться данной ссылкой для поиска драйвера на диске.

Вы также можете вручную выполнить поиск среди всех обнаруженных драйверов. Для этого нужно выбрать ссылку Установка оборудования, выбранного из списка вручную. После этого нужно выбрать спецификацию оборудования (например, модем, видеокарта, монитор и т. д.) и в появившемся списке драйверов — необходимый драйвер. Обратите также внимание на кнопку Установить с диска, с помощью которой можно указать файл драйвера на диске. Этот способ установки аналогичен использованию мастера Установка оборудования, доступ к которому можно получить с помощью одноименного значка папки Панель управления.

После того как операционная система обнаружит драйвер, она автоматически начнет устанавливать его. Если же на диске будет обнаружено сразу несколько драйверов, то перед вами отобразится их список и будет предложено выбрать один из них.

Используем программу PnPutil.exe

Установить драйвер или пакет драйвера (сам драйвер и спецификацию для работы с ним) можно и с помощью программы командной строки `PnPutil.exe`. Она поддерживает следующие возможности.

- `pnputil.exe -a <путь к INF-файлу и его имя>` — добавляет указанный пакет драйвера. Вместо имени INF-файла можно указать шаблон, чтобы было добавлено сразу несколько пакетов, находящихся в каталоге.

- `pnputil.exe -i -a <путь к INF-файлу и его имя>` — добавляет указанный пакет драйвера, а также устанавливает сам драйвер.
- `s` — отображает список всех пакетов, установленных после инсталляции операционной системы.
- `pnputil.exe -d <название INF-файла>` — удаляет данный пакет. Можно также использовать дополнительный параметр `-f`, чтобы пакет был удален даже в том случае, если он необходим компонентам операционной системы.

Откат драйвера

Иногда возникают ситуации, когда только что переустановленный драйвер устройства приводит к непредсказуемому поведению операционной системы. В таких ситуациях особо не стоит отчаиваться.

Если после установки нового драйвера операционная система не может корректно загрузиться, отображая «синий экран смерти» на одном из этапов загрузки, для восстановления работоспособности системы достаточно воспользоваться загрузкой последней удачной конфигурации (при отображении загрузочного меню нажать клавишу F8 и в появившемся меню альтернативных способов загрузки выбрать пункт Последняя удачная конфигурация (дополнительно)).

Если же ошибки возникают уже после входа в операционную систему, то можно попробовать откатить установку драйвера. Эта операция приведет к установке прежней версии драйвера.

Чтобы сделать откат драйвера, нужно отобразить окно Свойства устройства (с помощью оснастки Диспетчер устройств (`devmgmt.msc`)), перейти на вкладку Драйвер и нажать на кнопку Откатить.

Групповые политики

Благодаря групповым политикам вы можете настроить некоторые параметры установки драйверов и новых устройств компьютера. Для этого применяются политики подразделов Установка устройства и Установка драйвера раздела Конфигурация компьютера ▸ Административные шаблоны ▸ Система, а также политики подраздела Установка драйвера раздела Конфигурация пользователя ▸ Административные шаблоны ▸ Система. Все эти политики описаны в файле `DeviceInstallation.admx`.

Групповые политики из указанных подразделов влияют на параметры, имеющие тип `REG_DWORD` и расположенные в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Settings`.

- `InstallTimeout` — значение данного параметра определяет максимальное время установки нового устройства (в секундах). Если по истечении данного времени устройство так и не было установлено, его установка будет прекращена. По умолчанию устройство может устанавливаться не более пяти минут.
- `DisableSendGenericDriverNotFoundToWER` — если значение данного параметра равно `1`, то операционной системе будет запрещено отсылать сообщения

Windows Error Reporting в том случае, если вместо драйвера производителя выполняется установка универсального драйвера операционной системы. По умолчанию такие сообщения отсылаются.

- `AllSigningEqual` — при установке значения этого параметра равным `1` операционная система не будет различать драйверы, подписанные Microsoft, и драйверы, подписанные другими производителями. По умолчанию система отдает предпочтение драйверам, подписанным корпорацией Microsoft, даже если драйверы производителя более новые.
- `DisableBalloonTips` — если значение данного параметра равно `1`, то при обнаружении нового устройства уведомление Найдено новое оборудование не будет отображаться в области уведомлений.
- `DisableSystemRestore` — если установить значение этого параметра равным `1`, то при установке нового драйвера устройства создание точки восстановления выполняться не будет.
- `AllowRemoteRPC` — если значение данного параметра равно `1`, то удаленное подключение к инфраструктуре Plug and Play с помощью протокола RPC будет разрешено.

Политики же подраздела Установка драйвера изменяют значения параметров типа `REG_DWORD`, расположенных в ветви `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DriverSearching`.

Отключить запрос на поиск драйверов устройств на веб-узле Windows Update — эта политика изменяет значение параметра `DontPromptForWindowsUpdate`. Установка значения данного параметра равным `1` приводит к тому, что при установке драйвера не будет отображаться окно, предлагающее произвести поиск подходящих для данного устройства драйверов в Интернете.

Другие операции

Теперь рассмотрим стандартные программы операционной системы Windows Vista, предназначенные для работы с драйверами.

Просмотр списка загруженных драйверов

Еще одной программой командной строки, присутствующей в стандартной поставке операционных систем семейства Windows, является программа `driverquery.exe`, позволяющая просмотреть сведения о работающих в данный момент драйверах. Вот некоторые команды этой программы.

- `Driverquery` — отображает такие сведения об установленных в системе драйверах, как имя драйвера, его тип и дату создания.
- `Driverquery /fo LIST /v` — с помощью данной команды можно просмотреть расширенные сведения об установленных в системе драйверах. В них входят также сведения о режиме запуска драйвера (автоматически или вручную), указания, работает ли драйвер в данный момент, разрешено ли останавливать работу драйвера, размер занимаемого драйвером файла подкачки, путь к файлу драйвера и т. д. Все сведения отображаются в виде списка.

- `Driverquery /S <компьютер> /U <пользователь> /P <пароль> /fo LIST /si` — отображает сведения о драйверах удаленного компьютера NOUT. Обратите внимание на параметр `/si` — при его использовании также отображается информация о цифровой подписи драйверов (параметр `/si` не может применяться вместе с параметром `/v`).

Просмотр загруженных драйверов, относящихся к группе Фильтр

Расположение: `%systemroot%\system32\fltMC.exe`.

Операционная система Windows Vista также содержит программу `fltMC.exe`, предназначенную для работы с драйверами фильтров. С ее помощью можно выполнить следующие операции (для просмотра дополнительной информации о параметрах команд введите команду вида `fltMC.exe help <команда>`).

- Отображение списка загруженных драйверов фильтров. Эту операцию можно выполнить либо с помощью команды `fltMC.exe`, либо с помощью команды `fltMC.exe filters`. Можно также воспользоваться командой `fltMC.exe instances`, чтобы отобразить список всех экземпляров драйверов. А с помощью команды `fltMC.exe volumes` можно вывести список разделов диска и экземпляры драйверов, которые работают с этими разделами.
- Загрузка и выгрузка драйвера фильтра. Для загрузки драйвера фильтра нужно воспользоваться командой `fltMC.exe load <имя драйвера>`. Чтобы выгрузить драйвер фильтра, нужно воспользоваться командой `fltMC.exe unload <имя драйвера>`.

  Вы также можете подключить или отключить определенный экземпляр драйвера фильтра к конкретному разделу диска. Для этого применяются команды `fltMC.exe attach|detach <имя драйвера> <раздел диска>`.

Диспетчер проверки драйверов

Расположение: `%systemroot%\system32\verifier.exe`.

В операционной системе Windows Vista присутствует программа, с помощью которой можно следить за работой драйверов. С ее помощью можно вывести такие сведения об использовании драйвером резидентного и нерезидентного пула, как текущее и максимальное количество используемых байт, текущий и максимальный номер размещений.

Работа программы `verifier.exe` основана на настройках, которые вы должны предварительно выполнить. Иначе говоря, основной способ работы с программой следующий: сначала настраиваются такие параметры, как список библиотек и параметры их работы, за которыми нужно следить; потом выполняется перезагрузка компьютера; а после этого когда вы опять запустите программу `verifier.exe`, с ее помощью можно следить за параметрами выбранных вами на первом шаге библиотек.

После запуска программы `verifier.exe` перед вами отобразится мастер Диспетчер проверки драйверов, содержащий переключатель Выберите действие, который можно установить в одно из следующих положений.

- Создать стандартные параметры — переключатель нужно установить в это положение на первом шаге для настройки списка библиотек, за которыми нужно следить. При этом будет выполняться слежение только за стандартными параметрами (параметры работы с резидентным и нерезидентным пулом).

  После того как вы выберете это положение и нажмете кнопку Далее, мастер предложит вам выбрать библиотеки, за которыми нужно следить. Для этого нужно установить переключатель Выбор проверяемых драйверов в одно из следующих положений.

  - Автоматически выбирать неподписываемые драйверы — следить за всеми библиотеками, не имеющими цифровой подписи.
  - Автоматически выбирать драйверы для прошлых версий Windows — следить за всеми библиотеками, созданными для более старых версий операционной системы Windows, чем установленная на вашем компьютере.
  - Автоматически выбирать все драйверы, установленные на этом компьютере — следить за всеми драйверами.
  - Выберите имя драйвера из списка — следить только за выбранными драйверами. После установки переключателя в это положение и нажатия кнопки Далее перед вами отобразится список всех установленных в операционной системе драйверов. Чтобы выбрать драйвер из данного списка, достаточно установить флажок напротив него.

- Создать не стандартные параметры (для кода программ) — также используется на первом шаге, но при этом вы можете более тонко настроить параметры работы библиотек, сведения о которых будут отображаться. В частности, после установки переключателя в это положение и нажатия кнопки Далее вам будет предложено выбрать те из параметров, за значениями которых нужно следить. После этого вам нужно будет выбрать список библиотек, за которыми нужно следить, для чего используется переключатель Выбор проверяемых драйверов с возможностями установки его в те же положения, что описаны выше. И последним шагом мастера будет настройка дополнительных параметров слежения за работой драйверов. Например, если будет выбрано слежение за значениями параметра Проверка целостности диска, то также нужно будет выбрать жесткий диск из списка установленных на компьютере.

- Удалить существующие параметры — после того как вы проследите за работой необходимых вам драйверов, не забудьте установить переключатель в это положение, чтобы удалить созданные на первом шаге настройки. Иначе при каждой перезагрузке компьютера будет автоматически запускаться слежение за выбранными вами драйверами, что сказывается на общей производительности компьютера.

- Вывести существующие параметры — отображает текущие настройки слежения за работой драйверов: список драйверов, за работой которых нужно следить, а также список параметров, за значениями которых нужно следить.

- Вывести сведения о текущих проверенных драйверах — в это положение переключатель нужно устанавливать уже после настройки слежения, перезагрузки ком-

пьютера и повторного запуска программы `verifier.exe`. После того как вы установите переключатель в это положение и нажмете кнопку Далее, перед вами отобразятся сведения о настройках слежения за драйверами: список драйверов, а также список параметров, за значениями которых нужно следить. Заметьте, что с помощью кнопок Изменить, Добавить и Удалить данного шага мастера вы можете изменить список параметров, а также список библиотек, за которыми нужно следить.

На следующем шаге мастера перед вами уже отобразятся глобальные значения выбранных вами параметров. А если вы еще раз нажмете кнопку Далее, то сможете просмотреть значения параметров для конкретного драйвера. При этом драйвер, значения которого нужно отобразить, можно выбрать с помощью списка Драйвер.

7.6. Работа с файловой системой

Операционная система Windows Vista поддерживает множество операций, относящихся к работе с жесткими дисками и файловой системой. Это и стандартные возможности сжатия и шифрования данных, и изменение или монтирование новых разделов, и запись дисков, и проверка, форматирование, дефрагментация дисков, и еще многое другое.

Работа с разделами жесткого диска

Перед тем как мы рассмотрим операции, которые можно выполнить над разделами диска, расскажу о некоторых возможностях настройки разделов диска.

Прежде всего, следует обратить внимание на содержимое вкладки Политика окна Свойства, отобразить которое можно с помощью команды Свойства контекстного меню вашего диска в оснастке Диспетчер устройств (является частью консоли `devmgmt.msc`). На данной вкладке содержится переключатель Кэширование записи и безопасное удаление, значения которого изменяют параметры `REG_DWORD`-типа, расположенные в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\IDE\<диск>\<ID диска>\Device Parameters\Disk`. Его можно установить в следующие положения.

- Оптимизировать для быстрого удаления — используется по умолчанию для всех съемных дисков. При установке переключателя в это положение вы сможете отключать съемный диск без использования значка съемного диска в области уведомления (без использования безопасного отключения). Однако при этом понижается производительность работы со съемным диском.

  Установка переключателя в это положение приводит к изменению значения параметра `UserRemovalPolicy`.

- Оптимизировать для выполнения — применяется по умолчанию для всех локальных дисков. При этом выполняется оптимизация работы с диском, однако отключение диска без использования значка съемного диска, расположенного в области уведомления, может привести к потере данных.

При установке переключателя в это положение также становятся активными следующие флажки.

- Разрешить кэширование записи на диск — если он установлен, то будет разрешено кэширование данных на диск.

  Установка переключателя в данное положение приводит к изменению значения параметра `UserWriteCacheSetting`.

- Включить повышенную производительность — если флажок установлен, то будет выполнено дополнительное повышение производительности доступа к данным. Это следует делать только в том случае, если у вас есть источник бесперебойного питания, так как при установке данного флажка может произойти потеря данных, если питание компьютера неожиданно прекратится.

Установка переключателя в это положение приводит к изменению значения параметра `CacheIsPowerProtected`.

Общая информация о жестких дисках

Перед тем как погрузиться в описание возможностей файловой системы NTFS и работы с дисками с помощью операционной системы Windows Vista, повторим некоторые теоретические сведения, которые должен знать каждый опытный пользователь.

Как и предыдущие версии операционной системы, Windows Vista поддерживает два вида дисков: базовые (используются по умолчанию, кроме того, на портативных компьютерах могут применяться только базовые диски) и динамические.

Базовые диски

Базовыми дисками можно назвать диски, которые используют разбиение разделов по схемам MBR или GPT.

ПРИМЕЧАНИЕ

Существует три вида разбиения диска на разделы: MBR, GPT и LDM.

Разбиение диска с помощью MBR используется на большинстве компьютеров. Это сложилось исторически, ведь чтобы BIOS смогла запустить операционную систему, она сначала должна обратиться к первому сектору основного диска, чтобы считать из него главную загрузочную запись (MBR), а уже код, записанный в MBR, инициирует процесс загрузки операционной системы. Иными словами, на x86-совместимых компьютерах основной раздел диска обязательно должен быть разбит с помощью MBR.

Метод разбиения GPT используется по умолчанию (по спецификации EFI) на x64-совместимых компьютерах. Основное отличие данного метода от метода MBR состоит в том, что GPT вместо таблицы разделов использует таблицу разделов GUID. Кроме того, GPT поддерживает контрольную сумму CRC для таблицы разделов GUID, а также создание ее резервной копии, поэтому риск повреждения этой таблицы снижен.

На страницах данной книги мы рассмотрим только метод разбиения MBR.

Главная загрузочная запись MBR содержит не только код, инициирующий запуск операционной системы, но и таблицу разделов. Таблица разделов определяет все разделы, на которые разбит жесткий диск, а также раздел, на котором установлена операционная система. Вы, наверное, слышали о таких понятиях, как дополнительный раздел (extended partition) или логический диск. Эти понятия сформировались именно благодаря особенностям (или, скорее, недостаткам) таблицы разделов MBR, поэтому на их основе опишем саму структуру таблицы разделов.

Главные разделы (primary partition). Максимальное количество разделов, которые могут содержаться в таблице разделов одного MBR, равно четырем. Именно эти разделы называются **главными**.

Дополнительные разделы (extended partition). Естественно, что такое ограничение, как максимальное количество разделов, описываемых в таблице разделов, равное четырем, существенно уменьшает достоинства самого механизма MFT. Именно поэтому таблица разделов может содержать в себе главные разделы особого типа, которые как раз и называются **дополнительными разделами**.

Дополнительный раздел — это главный раздел, который содержит не описание файловой системы раздела, а еще одну главную загрузочную запись MBR, которая хранит еще одну таблицу разделов.

Логический диск (Logical Drive). Как вы, наверное, догадались, таблица разделов, хранящаяся на **дополнительном диске**, может состоять из четырех разделов. Именно эти четыре раздела и называются **логическими дисками**.

Активный раздел представляет собой главный раздел, содержащий в своем первом секторе код, который выполняет MBR с целью запуска операционной системы. Первый сектор активного раздела называется загрузочным.

Но это теория, а как же можно проверить ее на практике? Для этого достаточно лишь запустить консоль `diskmgmt.msc` (оснастка Управление дисками). Данная консоль включат в себя список разделов, из которых состоит жесткий диск. Причем для каждого раздела указывается его объем, используемая на нем файловая система и, что нам и необходимо, в самом низу в скобках указывается, является раздел активным, главным, расширенным или логическим.

Динамические диски

Тип разбиения на разделы, используемый динамическими дисками, называется LDM. Данный тип был разработан компанией VERITAS Software для операционных систем семейства UNIX, после чего лицензирован Microsoft для своей операционной системы.

ПРИМЕЧАНИЕ

Повторю, что нельзя создавать динамические диски на ноутбуках; если диск подключен к шине IEEE 1394 или USB (то есть если диск не является фиксированным); если диск совместно используется серверным кластером.

База данных LDM. LDM поддерживает единственную базу данных, которая содержит информацию обо всех динамических дисках, подключенных к компьютеру, а также о конфигурации составных томов. База данных LDM помещается в последнем мегабайте пространства каждого динамического диска (именно поэтому при преобразовании базового диска в динамический необходимо, чтобы последний мегабайт базового диска был пуст). База данных LDM состоит из пяти областей.

- Сектор заголовка — содержит GUID-номер динамического диска, указатель на начало таблицы оглавления, а также имя дисковой группы (операционные системы семейства Windows поддерживают только одну динамическую группу, поэтому эта информация не представляется важной).
- Таблица оглавления — хранит сведения о структуре базы данных и имеет длину в 16 секторов.
- Записи базы данных — существует четыре типа записей базы данных.
  - Раздел — описывает нежесткие разделы (непрерывные области на диске, которые содержат (или могут содержать) том), хранит идентификаторы, которые связывают раздел с диском и компонентом.
  - Диск — описывает динамический диск, состоящий в группе, и хранит его GUID-номер.
  - Компонент — связывает раздел с томом, который на нем хранится.
  - Том — содержит GUID-номер тома, его размер, атрибуты и букву. Именно этот GUID-номер используется операционной системой для идентификации тома.
- Журнал транзакций — хранит резервную копию информации базы данных, которая была изменена или изменяется в данный момент.
- Копия сектора заголовка — содержит GUID-номер динамического диска, указатель на начало таблицы оглавления, а также имя дисковой группы.

Кроме базы данных, LDM также создает таблицу разделов, используемую MBR (или GPT), чтобы процесс загрузки операционной системы прошел корректно, а также для того, чтобы программы, созданные для базовых дисков, смогли работать и с динамическими дисками.

Составные тома. Основным плюсом динамических дисков является то, что они поддерживают создание составных томов, которые являются более производительными и более надежными. Составной том представляет собой один раздел диска, созданный из нескольких физических дисков. От того, как именно будут взаимодействовать несколько физических дисков, являющихся частью составного тома, зависит название составного тома. Операционная система Windows Vista поддерживает следующие составные тома.

- Перекрытый том — составной том, состоящий из нескольких жестких дисков, которые логически объединены в один.

  Отличительной особенностью данного типа составных томов при использовании файловой системы NTFS является возможность их расширения без потери данных. Это достигается благодаря тому, что все сведения о свободном

пространстве перекрытого тома, жестких дисках, из которых он состоит, расположении файлов на этих жестких дисках, находятся в отдельном файле, называемом битовой картой. Операционная система обращается к битовой карте для выполнения любых операций с перекрытым томом. Например, для определения свободного места на перекрытом томе. Или при чтении файла с целью определения, какие его части находятся на каких жестких дисках, входящих в перекрытый том.

- Чередующийся том, или RAID-0, — составной том, состоящий из нескольких жестких дисков, данные на которые записываются по очереди. При этом единица записи равна 64 Кбайт, то есть первые 64 Кбайт файла записываются на первый жесткий диск чередующегося тома, вторые 64 Кбайт файла — на второй жесткий диск, следующие 64 Кбайт файла — на первый жесткий диск чередующегося тома, и так по очереди.

  Отличительной особенностью данного типа составных томов является существенный прирост в скорости чтения записанных данных: поскольку чтение происходит сразу с двух дисков (отдельно двумя контроллерами диска), скорость чтения может быть в два раза больше, чем с одного диска.

- Зеркальный том, или RAID-1, — составной том, состоящий из нескольких жестких дисков, данные на которых дублируются. При записи данных на зеркальный том данные записываются одновременно как на первый жесткий диск, входящий в зеркало, так и на второй.

  Отличительной особенностью данного типа составных томов является повышенная надежность: если выйдет из строя один из жестких дисков, входящих в зеркало, данные все еще будут доступны на втором жестком диске. Кроме того, не стоит забывать и о том, что скорость считывания данных с зеркального тома, как правило, выше, чем с обычного. Ведь данные находятся сразу на двух дисках, и операционная система может считывать их одновременно с двух дисков. Правда, стоит упомянуть, что скорость записи на зеркальных томах, как правило, ниже, чем на других томах, и занимает больше системных ресурсов из-за необходимости двойной записи.

- Чередующийся том с записью четности, или RAID-5, — составной том, состоящий из трех жестких дисков, два из которых представляют собой один обычный чередующийся том, а на третий диск заносится контрольная сумма (значение, представляющее логическую сумму (XOR) данных, записанных на чередующийся том).

  Отличительной особенностью данного типа составных томов является существенный прирост в скорости чтения записанных данных (из-за того, что данные считываются параллельно с двух дисков). Кроме того, данный тип составных томов характеризует повышенная надежность по сравнению с обычным чередующимся томом: если один из жестких дисков выйдет из строя, данные все равно можно будет прочитать на основе контрольной суммы, хранящейся на третьем диске.

Подводим итоги: использование программы diskpart.exe

Выше вы узнали о том, что такое базовый и динамический диск, что такое NTFS, какие бывают виды разделов.

Главным образом, вы узнали это лишь потому, что вся эта информация необходима для работы с дисками с помощью программы командной строки `diskpart.exe`. Она представляет собой оболочку, то есть перед тем как пользоваться ее возможностями, нужно запустить программу `diskpart.exe`, чтобы войти в ее оболочку. После этого можно применять следующие возможности программы.

Просмотр сведений о дисках, разделах и томах. Данную возможность программы `diskpart.exe` вы будете использовать очень часто, ведь, чтобы выполнить любую другую операцию, нужно сначала выбрать конкретный диск, раздел или том. Чтобы сделать такой выбор, нужно знать порядковый номер необходимого диска, раздела или тома.

Итак, для просмотра сведений о структуре диска используется команда `list`. Она имеет следующий синтаксис.

- `List disk` — отображает следующую информацию о дисках, подключенных к компьютеру: порядковый номер диска, его объем, количество неразмеченного пространства, является ли диск динамическим, а также сведения о GPT.

ВНИМАНИЕ

Это, наверное, единственная команда программы diskpart.exe, которую можно выполнять без выбора конкретного диска. Все же остальные команды можно выполнять только после того, как будет выбран диск, к которому обращается команда. Чтобы выбрать диск, нужно воспользоваться командой select disk <номер диска>. Номер нужного диска можно узнать с помощью команды list disk.

- `List partition` — выводит следующую информацию о разделах, на которые разбит конкретный диск (выбранный с помощью команды `select disk <номер диска>`): номер раздела, тип раздела (главный, дополнительный, логический диск), объем раздела, а также смещение раздела относительно начала диска.
- `List volume` — отображает следующую информацию о томах, которые присутствуют в операционной системе: номер тома, его буква и метка, тип файловой системы, тип тома (раздел диска, съемный диск, оптический носитель), размер тома, указание, является он системным или загрузочным.

Еще одной командой, с помощью которой можно отобразить сведения о дисках, разделах или томах, является команда `Detail`. Она выводит сведения о выбранном вами диске, партиции или томе. Иными словами, сначала требуемый элемент нужно выбрать с помощью команды вида `select disk|partition|volume <номер объекта>`.

- `Detail disk` — отображает сведения о томах, расположенных на диске (те же сведения, что и команда `list volume`), а также следующую информацию: название диска, его идентификатор, тип и номер шины, LUN и Target (последние два элемента используются для описания SCSI-дисков).

- `Detail partition` — выводит сведения о томе, который расположен в разделе (те же сведения, что и команда `list volume`), а также следующую информацию: тип раздела, указания, является ли раздел скрытым и является ли раздел активным.
- `Detail volume` — отображает сведения о диске, на котором находится том (те же сведения, что и команда `list disk`), а также следующую информацию: доступен ли том для записи, скрыт ли он, размонтирован ли он, зашифрован ли он с помощью BitLocker, используется ли он теневым копированием, количество доступного на томе пространства.

Кроме того, вы можете просмотреть такую информацию о томах, как файловые системы, которые они поддерживают, а также размер кластера, используемый по умолчанию, и те размеры кластеров, которые поддерживают файловые системы. Для этого достаточно выбрать том и ввести команду `filesystems`.

Работа с диском. В данном разделе мы рассмотрим очень страшную команду программы `diskpart.exe`: `clean`. Существует две разновидности данной команды.

- `Clean` — удалить MBR на конкретном диске.
- `Clean all` — удалить всю информацию на диске, заполнив каждый сектор нулями.

Работа с разделом. Теперь опишем те операции, которые можно выполнить с разделами диска.

Вы уже знаете, что такое активный раздел. Так вот, чтобы изменить активный раздел, достаточно выбрать нужный раздел и воспользоваться командой `active`. С помощью команды `inactive` вы также можете удалить активный раздел, не назначая нового.

Кроме того, вы можете создать новый раздел. Для этого применяется команда вида `create partition efi|EXTENDED|LOGICAL|MSR|PRIMARY size=<размер нового раздела> offset=<смещение относительно начала диска>`. Либо удалить существующий раздел, для чего нужно применять команду `delete partition`.

Работа с томом. С помощью программы `diskpart.exe` можно также работать с отдельными томами.

Например, можно изменить букву тома или примонтировать его к каталогу (создать точку подключения). Для этого достаточно выбрать нужный том, после чего воспользоваться командой вида `ASSIGN LETTER=<новая буква диска> MOUNT=<путь к каталогу для создания точки подключения>`. Если же вам нужно удалить букву тома, то воспользуйтесь командой `remove letter=<буква дома>`.

При использовании команды `Detail volume` можно отобразить такие атрибуты тома, как, например, указание, является ли он скрытым. Значения этих атрибутов можно установить или сбросить с помощью команды вида `ATTRIBUTES VOLUME SET|CLEAR HIDDEN|READONLY|NODEFAULTDRIVELETTER|SHADOWCOPY`. Если

вы используете параметр SET, то значение атрибута будет установлено. Если же в команде используется параметр CLEAR, то значение атрибута будет сброшено.

Работа с динамическими дисками. И напоследок рассмотрим несколько команд, применяемых для работы с динамическими дисками (вообще, для работы с динамическими дисками, объединенными в массив RAID, используется программа командной строки diskraid.exe).

- ADD DISK=<номер второго диска> ALIGN=<выравнивание RAID> WAIT — объединяет два диска в зеркало.
- BREAK DISK=<номер второго диска> — разбивает зеркало.
- CREATE PARTITION PRIMARY SIZE=<размер диска> OFFSET=<смещение относительно начала диска> ID=<GUID-номер динамического диска> — создает новый раздел на динамическом диске.
- convert dynamic — преобразует базовый диск в динамический.
- RETAIN — подготавливает динамический диск для использования в качестве системного или загрузочного.

Просмотр сведений о жестком диске

Наверное, каждый пользователь знает, где можно просмотреть сведения об общем объеме раздела, оставшемся свободном месте, а также о файловой системе, используемой на разделе диска. Для этого достаточно воспользоваться вкладкой Общие окна Свойства раздела диска. Однако это далеко не вся информация о разделах жесткого диска, которую может предоставить операционная система Windows Vista.

Просмотр сведений о жестком диске с помощью msinfo32.exe

Основные сведения о жестком диске и его разделах можно просмотреть с помощью программы msinfo32.exe. После запуска данной программы отобразится окно Сведения о системе, в дереве которого нужно перейти к подразделу Компоненты ▸ Запоминающие устройства ▸ Диски. После этого в основном окне программы вы сможете найти следующую информацию о вашем жестком диске:

- количество байт в одном секторе, количество секторов, цилиндров, дорожек, а также общий объем жесткого диска;
- общее количество партиций, присутствующих на жестком диске, их названия и занимаемый ими размер;
- если ваш диск имеет SCSI-интерфейс, то шину SCSI, к которой диск подключен, логическую единицу и порт SCSI, а также идентификатор цели SCSI.

Просмотр сведений о файловой системе разделов с помощью Fsutil.exe

Операционная система Windows Vista также содержит в своем составе программу fsutil.exe, с помощью которой можно просмотреть исчерпывающую информацию о файловой системе, используемой на разделе диска, а также о самих разделах диска. Специально для этого программа fsutil.exe поддерживает отдельную команду fsinfo. Ее использование предельно просто.

- `fsutil fsinfo drives` — отображает буквы доступных разделов диска.
- `fsutil fsinfo drivetype <буква диска и двоеточие>` — выводит тип раздела диска (фиксированный, съемный, сетевой или динамический).
- `fsutil fsinfo volumeinfo <буква диска и двоеточие>` — отображает общую информацию о разделе диска. С помощью данной команды можно узнать не только о том, какая файловая система используется на разделе диска и какой максимальный размер имени файла ею поддерживается, но и сведения о том, поддерживаются ли:
  - верхний регистр в именах файлов;
  - символы Unicode в именах файлах;
  - сведения ACL;
  - механизм сжатия;
  - раздел квоты;
  - разреженные файлы;
  - точки повторного разбора;
  - идентификаторы объектов;
  - файловая система EFS;
  - именованные потоки файлов;
  - файловая система транзакции.
- `fsutil fsinfo ntfsinfo <буква диска и двоеточие>` — выводит сведения о файловой системе NTFS. С помощью данной команды можно узнать о следующих параметрах NTFS.
  - Версия.
  - Количество секторов, на которые разбит раздел. Общее количество кластеров, количество свободных кластеров, а также количество зарезервированных операционной системой кластеров.
  - Размер одного сектора, кластера и сегмента в байтах.
  - Информация о главной записи MFT.
- `fsutil fsinfo statistics <буква диска и двоеточие>` — отображает информацию о текущем использовании соответствующего раздела диска (количество потоков чтения или записи, количество считываемых и записываемых байт и т. д.).

ПРИМЕЧАНИЕ

Как раньше, репозитарий CIM ОС Windows содержит два класса, предназначенных для просмотра сведений о диске: Win32_DiskPartition и Win32_LogicalDisk. Оба расположены в пространстве имен root\cimv2.

Например, класс Win32_DiskPartition поддерживает следующие, наиболее интересные, свойства: BlockSize (определяет размер одного блока для данной партиции), Bootable (указывает, является ли партиция загрузочной), BootPartition (определяет,

является ли партиция активной), DeviceID (ключевое свойство), NumberOfBlocks (определяет количество блоков, на которые разбита партиция), Size (указывает размер партиции в байтах), StartingOffset (определяет смещение партиции в байтах).

Транзакции

Запись данных на диск, использующий файловую систему NTFS, основана на атомарных транзакциях. Суть атомарных транзакций можно охарактеризовать фразой «все или ничего». Все изменения на диске, определенные одной транзакцией (одной операцией записи), происходят атомарно. Иначе говоря, запись не будет считаться успешной, пока транзакция не будет полностью завершена. Если в процессе записи произойдет сбой, все уже записанные данные будут удалены (так называемый откат), система перейдет в состояние, которое было до начала транзакции, и, если это возможно, транзакция начнется заново.

Управлять транзакциями ядра операционной системы можно с помощью программы командной строки `ktmutil.exe`. Она поддерживает следующие параметры.

- `Resolve <параметр> <GUID-транзакции>` — предназначена для управления выполнением транзакции. В команде можно использовать один из следующих параметров:
  - `Complete` — закончить транзакцию;
  - `Commit` — начать транзакцию;
  - `Rollback` — отменить транзакцию.
- `Force <commit или rollback> <GUID-транзакции>` — насильно начинает неопределенную транзакцию.
- `List <тип транзакции>` — отображает список транзакций. В качестве типа транзакции можно указывать одно из следующих значений: `commit` или `rollback`.

Возможности данной программы можно использовать и с помощью команды `fsutil transaction`.

Создание меток

Метка диска представляет собой произвольный текст, отображаемый напротив буквы диска (по умолчанию, слева от нее). В основном метка диска служит для облегчения работы с дисками, особенно если в вашей операционной системе присутствует больше шести разделов.

Чтобы создать метку диска, достаточно в окне Свойства этого диска на вкладке Общие воспользоваться специальным полем, расположенным в самом верху этой вкладки.

ПРИМЕЧАНИЕ

Создать метку раздела можно и с помощью программы командной строки label.exe. Ее синтаксис предельно прост: label <буква диска и двоеточие> <новая метка>.

Монтирование дисков и создание точек подключения

Вы часто пользуетесь такой возможностью операционных систем семейства Windows, как создание ссылок? А ведь это не единственный способ облегчения доступа к файлам и изменения логической структуры файловой системы компьютера.

Работа с виртуальными дисками

Виртуальный диск представляет собой своеобразную ссылку на сетевой или локальный ресурс. После создания виртуального диска вы сможете получить доступ к сетевому или локальному ресурсу не с помощью его полного пути, а просто введя букву виртуального раздела, которую вы указали для соответствующего сетевого или локального пути.

Создание виртуального диска с помощью оболочки. С помощью оболочки Windows Vista можно создать виртуальные разделы, которые будут указывать на каталоги других компьютеров. Для этого достаточно воспользоваться командой Подключить сетевой диск меню Сервис старой строки меню (которая отображается после нажатия клавиши Alt) любой папки. После выбора данной команды перед вами отобразится одноименный мастер, который позволяет указать новую букву диска и сетевой каталог, на который он будет указывать. Обратите также внимание на флажок Восстанавливать при входе в систему данного мастера. Если он установлен, то будет создаваться виртуальный диск, то есть диск, подключение к которому операционная система будет создавать всякий раз после перезагрузки. По умолчанию данный флажок установлен, однако если присвоить параметру строкового типа `SaveConnections`, расположенному в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Network\Persistent Connections`, значение `No`, то он будет снят.

Сведения обо всех виртуальных дисках, созданных таким образом, хранятся в ветвях реестра вида `HKEY_CURRENT_USER\Network\<буква виртуального диска>`. Значение параметра строкового типа `RemotePath` данной ветви реестра определяет путь, к которому ведет виртуальный диск. А значение параметра `REG_DWORD`-типа `ConnectionType` определяет, является ли данный виртуальный диск постоянным (будет ли выполняться автоматическое подключение к нему или после перезагрузки данный виртуальный диск будет удален).

Если же вам нужно удалить созданный ранее виртуальный раздел, то воспользуйтесь командой Отключить сетевой диск меню Сервис или командой Отключить контекстного меню соответствующего виртуального раздела.

Создание виртуального диска с помощью программы subst.exe. Создать виртуальный диск можно и с помощью программы командной строки `subst.exe`. Она поддерживает два основных синтаксиса.

- `subst <буква диска и двоеточие> <путь к каталогу>` — создает новый раздел диска с указанной буквой, который будет открывать соответствующий каталог.
- `subst <буква диска и двоеточие> /D` — удаляет созданный ранее виртуальный диск, имеющий соответствующую букву.

Обратите внимание, что с помощью такого способа создания виртуального диска вы можете создавать диски, указывающие не только на сетевые общие папки, но и на локальные каталоги. Кроме того, созданные с помощью программы `subst.exe` разделы нельзя удалить с помощью команды Отключить сетевой диск оболочки.

Работа с точками подключения

С помощью точек подключения можно к содержимому каталога или раздела добавить содержимое другого раздела. Иными словами, фактически точки подключения противоположны виртуальным разделам: если сутью создания виртуального раздела является создание нового раздела на основе содержимого каталога, то сутью точек подключения является создание нового каталога, указывающего на содержимое уже существующего раздела.

Программа mountvol.exe. Для работы с точками подключения используется программа командной строки `mountvol.exe`. Она управляет работой драйвера `mountmgr.sys`, описанного в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MountMgr`.

Программа поддерживает следующие стандартные возможности.

- `mountvol.exe <раздел или путь к каталогу> <точка подключения>` — подключает указанную точку подключения (список доступных точек подключения отображается после ввода команды `mountvol.exe`) к указанному каталогу. Каталог, к которому подключается точка подключения, должен быть пуст.
- `mountvol.exe <раздел или путь к каталогу> /D` — удаляет все точки подключения, которые подключены к соответствующему разделу или его каталогам.

Программа `mountvol.exe` операционной системы Windows Vista также поддерживает следующие новые возможности.

- `mountvol.exe /N` — отменяет автоматическое подключение к разделам новых точек подключения. Чтобы заново установить автоматическое подключение новых точек подключения, нужно вместо параметра `/N` воспользоваться параметром `/E`.

  Эти команды изменяют значение параметра `REG_DWORD`-типа `NoAutoMount`, расположенного в ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MountMgr`.

ПРИМЕЧАНИЕ

Отключить или включить автоматическое монтирование можно и с помощью программы diskpart. Для этого сначала нужно войти в данную программу, введя в командной строке diskpart, а после этого в появившейся строке приветствия ввести команду automount enable|disable.

- `mountvol.exe /R` — отключает все точки подключения.

Оснастка Управление дисками. Можно также создать точку подключения на основе свободного пространства на диске. Для этого нужно воспользоваться оснасткой Управление дисками, которую можно отобразить с помощью консоли `diskmgmt.msc`.

После запуска данной оснастки нужно выделить свободное пространство на диске, после чего в его контекстном меню выбрать команду Создать простой том. Это приведет к отображению мастера Мастер создания простых томов, на втором шаге которого нужно установить переключатель Назначение буквы диска или пути в положение Подключить том как пустую NTFS-папку и в поле под данным переключателем указать путь к папке, к которой будет примонтировано данное свободное пространство.

ПРИМЕЧАНИЕ

Создать точку подключения можно и с помощью программы командной строки diskpart.exe. Для этого нужно войти в оболочку данной программы, выбрать нужную партицию диска с помощью команды select partition <номер партиции, начиная с 1>, а потом ввести команду ASSIGN MOUNT=<каталог>.

Точки повторного разбора

Механизм точек подключения, которые мы рассмотрели выше, основан на точках повторного разбора. Точкой повторного разбора является каталог или файл, который хранит данные повторного разбора. Данные повторного разбора содержат команду, а также тег, определяющий создателя точки повторного разбора. Если программа или компонент операционной системы обнаруживает точку повторного разбора, он просматривает ее тег. И если тег указывает, что точку повторного разбора создал именно данный компонент, то он выполняет заложенную в точке повторного разбора команду. Например, именно так и работают точки подключения: в качестве команды, заложенной в точке повторного разбора, выступает раздел, в который нужно перенаправить пользователя, обратившегося к данной точке повторного разбора.

Для работы с точками повторного разбора используются следующие команды.

- `fsutil reparsepoint query <путь к каталогу или файлу>` — отображает сведения о точке повторного разбора (тег точки повторного разбора, длину, а также записанные в точку данные), которая присвоена данному каталогу или файлу. Например, можно создать точку подключения, после чего просмотреть сведения о точке повторного разбора, созданной в каталоге, который мы определили как точку подключения.
- `fsutil reparsepoint delete <путь к каталогу или файлу>` — удаляет точку повторного разбора в указанном каталоге или файле. Удаление точки повторного разбора приводит к удалению точки подключения.

Жесткие ссылки

Жесткие ссылки позволяют отображать один и тот же файл в разных каталогах файловой системы и под различными именами. Иначе говоря, в чем-то жесткие

ссылки похожи на обычные ссылки. Однако есть некоторые существенные различия.

- Жесткая ссылка никак не отличается от оригинального файла. Например, она весит столько же, сколько и оригинальный файл. Жесткая ссылка выглядит точно так же, как и оригинальный файл.
- Отличие от обычной ссылки состоит и в том, что, если удалить оригинальный файл, жесткая ссылка все равно будет работать и хранить содержимое оригинального файла.
- Результат изменения содержимого жесткой ссылки заносится в файл-оригинал. Результат изменения в оригинальном файле заносится в жесткую ссылку. При этом, как уже говорилось выше, жесткая ссылка и файл-оригинал не взаимосвязаны. Иными словами, повторюсь, если удалить файл-оригинал, то жесткая ссылка все равно будет содержать его данные. Однако после удаления файла-оригинала жесткая ссылка автоматически преобразуется в обычный файл.

Чтобы создать жесткую ссылку, достаточно воспользоваться командой `fsutil hardlink Create <путь к создаваемой жесткой ссылке и ее имя> <путь к файлу оригиналу, на который создается жесткая ссылка>`.

Проверка диска

Проверку диска в операционной системе Windows Vista можно выполнить тремя способами. Первый из них — это использование программы командной строки `chkdsk.exe` во время работы операционной системы. Второй же — назначение выполнения проверки диска при перезагрузке операционной системы. А третьим способом является использование оболочки операционной системы.

Использование программы chkdsk.exe

Программа `chkdsk.exe` является стандартной консольной программой всех версий операционной системы Windows, однако в Windows Vista данная программа стала поддерживать новый параметр `/B`. Он используется вместе с параметрами `/R` и `/F` и говорит программе о том, что она должна заново проверить количество сбойных кластеров на томе.

Теперь рассмотрим основные способы использования данной программы.

- `Chkdsk <буква диска> /L` — отображает сведения о текущей файловой системе диска, используемом размере файла журнала, а также о размере файла журнала, который используется по умолчанию для данного раздела.
- `Chkdsk <буква диска> /L:<размер файла журнала>` — устанавливает новый размер файла журнала (в килобайтах) для данного раздела диска.
- `Chkdsk` — выполнить проверку системного диска. При этом режим восстановления сбойных кластеров отключен и выполняется стандартная проверка диска, состоящая из трех этапов (проверка структуры файлов, индексов и дескрипторов безопасности).

  Для ускорения процесса проверки диска вы можете использовать параметры `/I` и `/C`. Первый отключает подробную проверку структуры индексов на диске. Второй отключает циклическую проверку структуры каталогов на диске.

- Chkdsk <буква диска, метка или точка подключения> /V — выполнить стандартную проверку соответствующего раздела и отобразить подробную информацию о результатах проверки.

По умолчанию программа Chkdsk при обнаружении сбойных секторов не пытается как-то их обработать, однако вы можете указать специальные параметры, с помощью которых можно заставить программу выполнить следующие операции по работе со сбойными секторами.

- /F — определяет сбойные секторы на диске.
- /R — при обнаружении сбойного сектора пытаться выполнить чтение неразрешенной информации из него. Может использоваться вместе с параметром /F.

ПРИМЕЧАНИЕ

Если вы обнаружили сбойные секторы на диске, информацию из которых не получается прочитать с помощью параметра /R программы chrdsk.exe, то можно попробовать воспользоваться программой командной строки recover.exe.

Проверка при перезагрузке компьютера

Проверку диска можно выполнить и при перезагрузке компьютера. Данная проверка выполняется быстрее, чем проверка с помощью программы Chkdsk. Кроме того, при данном виде проверки не возникает таких проблем, как отказ в доступе к файлу или неудачная попытка размонтирования диска.

Чтобы установить проверку раздела диска при следующей перезагрузке компьютера, достаточно выполнить команду fsutil dirty set <буква диска, метка или точка подключения>. Тогда при следующей перезагрузке компьютера запустится программа autochk.exe. При этом по умолчанию перед запуском проверки диска операционная система будет ожидать десять секунд нажатия пользователем любой клавиши (если пользователь нажмет любую клавишу в течение этого времени, проверка диска будет отменена). Это время ожидания можно изменить. Для этого достаточно указать новое время в параметре REG_DWORD-типа AutoChkTimeout, расположенном в ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager.

ПРИМЕЧАНИЕ

В ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager также присутствует параметр REG_MULTI_SZ-типа BootExecute. Именно с помощью его значения и запускается программа проверки диска autochk.exe. Например, если удалить из этого параметра строку autocheck autochk *, то проверка диска при перезагрузке компьютера больше выполняться не будет.

Использование вкладки Сервис

Еще одним способом проверки диска является кнопка Выполнить проверку, расположенная на вкладке Сервис окна Свойства диска. После нажатия данной кнопки

отобразится окно, в котором можно указать проверку диска с обнаружением и восстановлением поврежденных секторов. После того как вы нажмете кнопку Запуск данного окна, начнется проверка диска, результат которой отобразится в отдельном окне.

Дефрагментация диска

Программа dfrgui.exe

На смену оснастке `dfrg.msc` в операционной системе Windows Vista пришла программа `dfrgui.exe`.

ПРИМЕЧАНИЕ

Данную программу можно запустить как с помощью окна Запуск программы, так и с помощью кнопки Выполнить дефрагментацию, расположенной на вкладке Сервис окна Свойства диска. Команда, которая выполняется после нажатия данной кнопки, определена в параметре (По умолчанию) ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\MyComputer\DefragPath.

После запуска данной программы начнется анализ дисков. Если она обнаружит, что дефрагментация действительно нужна, то предложит ее выполнить.

Основное окно программы просто поражает своей функциональностью. Оно обладает всего двумя возможностями: собственно кнопкой запуска процесса дефрагментации, а также возможностью разрешения или запрещения автоматического запуска дефрагментации в указанное время (по умолчанию один раз в неделю). Для использования возможности автоматического запуска дефрагментации необходимо, чтобы служба Планировщик заданий была запущена. Собственно, если эта служба не запущена, то вы вообще не сможете запустить программу `dfrgui.exe`.

ПРИМЕЧАНИЕ

По умолчанию операционная система имеет задание ScheduledDefrag, расположенное в разделе Библиотека планировщика заданий ▸ Microsoft ▸ Windows ▸ Defrag. Данное задание выполняет команду defrag.exe -c -i каждое воскресенье в час ночи.

Параметры дефрагментации

Немного больше возможностей настройки дефрагментации предоставляет реестр операционной системы. Сведения, необходимые для работы дефрагментации диска, хранятся в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Dfrg`. Среди них можно встретить следующие параметры.

- `LogFilePath` — этот параметр строкового типа позволяет задать путь к файлу журнала, в который программа `dfrgui.exe` будет записывать сведения о процессе своей работы. В частности, туда заносятся сведения анализа диска. Следует только учитывать, что размер данного файла будет очень большой. Ско-

рее всего, это вина самой программы dfrgui.exe (ошибка в ней), так как результат анализа диска состоит всего из нескольких десятков строк и заносится в самый конец файла, а размер создаваемого файла равен примерно 10 Мбайт.

- CreateLogFile — имеет тип REG_DWORD и определяет, будет ли создаваться файл журнала работы программы дефрагментации диска.
- DoNoOptimizeForVolsnap — этот параметр REG_DWORD-типа определяет, будет ли выполняться оптимизация доступа к снимкам системы во время дефрагментации раздела диска.
- FreeSpaceErrorLevel — по умолчанию дефрагментация диска не начнется, если на диске, содержимое которого дефрагментируется, нет как минимум 15 % свободного места. Это место нужно программе дефрагментации для хранения временных файлов, необходимых в процессе дефрагментации. Однако вы можете изменить процент свободного места, необходимый программе дефрагментации, изменив значение данного параметра.

Программа defrag.exe

Однако лучше всего для дефрагментации и анализа использовать программу командной строки defrag.exe, которая входит в поставку операционной системы Windows Vista (как и предыдущих версий Windows). При анализе она отображает не только сведения о том, нужна дефрагментация или нет, но и полные сведения о фрагментации файлов на указанном томе.

Программа поддерживает следующие возможности.

- Defrag <буква диска, метка или точка подключения> -a -v — анализирует фрагментацию файлов на указанном разделе диска и отображает подробные сведения о результатах анализа.
- Defrag -c — выполняет дефрагментацию всех разделов диска.
- Defrag <буква диска, метка или точка подключения> — выполняет дефрагментацию на указанном разделе диска.

При выполнении дефрагментации можно также использовать параметры -r или -w. Если используется первый параметр (он используется по умолчанию), то будет произведена частичная дефрагментация. При этом будет выполнена попытка объединения фрагментов, размер которых меньше 64 Мбайт. Если же используется параметр -w, то будет выполняться объединение фрагментов любого размера.

Возможности WMI

Выполнить дефрагментацию теперь можно и с помощью WMI. Для этого предназначен специальный метод Defrag класса Win32_Volume, расположенного в пространстве имен \\root\cimv2. Данный метод после выполнения дефрагментации возвращает указатель на экземпляр класса Win32_DefragAnalysis.

Настройка квот

Квота — это объем пространства на разделе жесткого диска, которое может использовать определенный пользователь. Если администратор указал квоту для

пользователя, то в зависимости от настроек квоты пользователь либо не сможет использовать больший объем раздела диска, чем указан в квоте, либо при превышении квоты для пользователя будет постоянно отображаться предупреждение о необходимости удаления ненужных пользователю данных.

Установка квоты с помощью оболочки Windows

Самым простым способом работы с квотами является использование вкладки Квота окна Свойства определенного раздела диска. Данная вкладка содержит следующие флажки.

- Включить управление квотами — именно с помощью этого флажка можно включить или отключить квоту на соответствующем разделе диска. Для включения квоты достаточно установить данный флажок.
- Не выделять место на диске при превышении квоты — если флажок установлен, то пользователю будет запрещено использовать большее пространство раздела диска, чем указано в квоте.
- Регистрация превышения квоты пользователем — при установке этого флажка каждое превышение пользователем квоты будет заноситься в файл журнала.
- Регистрация превышения порога предупреждения — если флажок установлен, то каждое предупреждающее сообщение, которое получит пользователь, будет заноситься в файл журнала.

  На вкладке также расположен переключатель Квота по умолчанию для нового пользователя этого тома. Он позволяет указать объем раздела диска, после использования которого пользователю будет выдаваться предупреждающее сообщение, а также максимальный объем раздела диска, который может использовать пользователь.

  Здесь также присутствует кнопка Записи квот. Как вы, наверное, догадались, с помощью предыдущих элементов вкладки Квота настраивалась квота для всех пользователей соответствующего раздела диска. С помощью же кнопки Записи квот можно настроить квоты для отдельных пользователей.

  После нажатия данной кнопки отобразится окно, содержащее список всех пользователей компьютера, для которых установлена квота (также с помощью колонок данного списка можно определить саму квоту и уже использованный пользователем объем раздела диска). Чтобы изменить объем квоты для определенного пользователя, нужно в контекстном меню соответствующего элемента списка выбрать команду Свойства и в появившемся окне ввести новую квоту.

  Обратите также внимание на команду Создать запись квоты меню Квота открытого окна. С помощью данной команды можно указать квоту для нового пользователя, который не отображается в списке окна Записи квоты.

ПРИМЕЧАНИЕ

Как и раньше, репозитарий CIM операционной системы Windows содержит класс Win32_QuotaSetting (в пространстве имен root\cimv2). Он позволяет просмотреть

и изменить значения тех параметров, которые изменяются с помощью вкладки Квота окна Свойства.

Например, данный класс поддерживает следующие свойства: DefaultLimit (определяет размер доступной пользователю квоты), DefaultWarningLimit (указывает предел превышения квоты, после которого будут выдаваться предупреждающие сообщения), ExceededNotification (определяет, будут ли сведения о превышении квоты заноситься в журнал), VolumePath (ключевое свойство, определяющее диск, квоты которого мы просматриваем), WarningExceededNotification (указывает, будут ли сведения о выдаче предупреждающих сообщений заноситься в журнал).

Работа с квотами с помощью программы fsutil.exe

Управлять квотами можно и с помощью программы командной строки `fsutil.exe`. Специально для этого данная программа поддерживает команду `quota`.

- `Fsutil quota track <буква диска>` — включает квоту для соответствующего раздела диска.
- `Fsutil quota enforce <буква диска>` — включает квоту для соответствующего раздела диска, а также устанавливает флажок Не выделять место на диске при превышении квоты.
- `Fsutil quota disable <буква диска>` — отключает квоту для данного раздела диска.
- `Fsutil quota violations` — отображает все записи из файла журнала, хранящего сведения о превышении квот.
- `Fsutil quota query <буква диска>` — выводит такие сведения о квоте для соответствующего раздела диска, как размер квоты по умолчанию, а также размер квоты для каждого отдельного пользователя компьютера, использованный им объем квоты и дату ее установки.
- `Fsutil quota modify <буква диска> <порог квоты> <предел> <имя пользователя>` — изменяет настройки квоты для соответствующего пользователя.

Работа с квотами с помощью групповых политик

Настроить параметры работы квот можно и с помощью групповых политик. Для этого применяются политики файла `DiskQuota.admx`, расположенные в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Дисковые квоты.

Данные политики изменяют значения параметров `REG_DWORD`-типа, расположенных в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DiskQuota`.

- Заносить событие превышения уровня предупреждения квоты — политика изменяет значение параметра `LogEventOverThreshold`. Если он присутствует в реестре, то флажок Регистрация превышения порога предупреждения, расположенный на вкладке Квота, будет снят и заблокирован.

- Вести журнал даже при превышении предела квоты — меняет значение параметра `LogEventOverLimit`. Если он присутствует в реестре, тогда флажок Регистрация превышения квоты пользователем, расположенный на вкладке Quota, будет сброшен и заблокирован.
- Задать предел дисковой квоты — политика изменяет значение параметра `Enforce`. Если он присутствует в реестре, то флажок Не выделять место на диске при превышении квоты, расположенный на вкладке Квота, будет снят и заблокирован.
- Включить дисковые квоты — изменяет значение параметра `Enable`. Если данный параметр присутствует в реестре, тогда использование квот будет запрещено.
- Предел квоты по умолчанию и уровень предупреждения — с помощью данной политики можно определить предел квоты, а также предел для выдачи предупреждающего сообщения. Политика изменяет значения следующих параметров.
  - `Limit` — значение данного параметра определяет предел для квоты. При этом единицы, в которых исчисляется данный предел, определяются значением параметра `LimitUnits`.
  - `LimitUnits` — указывает единицы, в которых исчисляется предел для квоты. Параметр может принимать следующие значения: `1` (Кбайт), `2` (Мбайт), `3` (Гбайт), `4` (Тбайт), `5` (Пбайт), `6` (Эбайт).
  - `Threshold` — значение данного параметра определяет предел для выдачи предупреждающего сообщения. При этом единицы, в которых исчисляется данный предел, определяются значением параметра `ThresholdUnits`.
  - `ThresholdUnits` — указывает единицы, в которых исчисляется предел для выдачи предупреждающего сообщения. Данный параметр может принимать следующие значения: `1` (Кбайт), `2` (Мбайт), `3` (Гбайт), `4` (Тбайт), `5` (Пбайт), `6` (Эбайт).

Работа с WMI

Репозитарий CIM операционной системы Windows Vista включает в себя несколько новых классов, описывающих настройки разделов диска и позволяющих работать с ним. Данный класс принадлежит к пространству имен `\\.\root\cimv2`.

Класс Win32_Volume

Данный класс определяет описание разделов жесткого диска, используемых при дефрагментации жесткого диска. Он поддерживает следующие свойства, доступные только для чтения.

- `Access`, тип: `uint16` — определяет тип доступа к разделу диска. Если значение данного свойства равно `0`, то тип доступа неизвестен. Если значение свойства равно `1`, то доступ разрешен только для чтения. Если значение равно `2`, то доступ разрешен только для записи. Если же значение свойства равно `3`, то доступ разрешен как для чтения, так и для записи.
- `Automount`, тип: `boolean` — значение определяет, поддерживает ли данный раздел диска автоматическое монтирование для операций чтения/записи.
- `Availability`, тип: `uint16` — значение данного свойства определяет состояние устройства. Например, если значение равно `10`, то устройство находится

в состоянии деградации. Если же значение свойства равно от 13 до 15, то устройство находится в одном из режимов энергосбережения.

- BlockSize, тип: uint64 — определяет размер одного блока диска (в байтах).
- BootVolume, тип: boolean — указывает, является ли этот раздел диска загрузочным (то есть он содержит системные файлы операционной системы).
- Capacity, тип: uint64 — определяет размер раздела диска в байтах.
- Caption, тип: string — содержит короткое, не более 64 символов, описание раздела диска.
- Compressed, тип: boolean — определяет, сжат ли данный раздел диска.
- ConfigManagerErrorCode, тип: uint32 — указывает состояние данного раздела по отношению к конфигурационному менеджеру. Например, если значение данного свойства равно 0, то раздел корректно работает. Если значение равно 2, то операционная система не может загрузить драйвер данного устройства. Если значение свойства равно 4, то файлы драйвера для данного устройства повреждены или работают некорректно. Если же значение данного свойства равно 17, то устройству необходим тип ресурса, не известный операционной системе.
- ConfigManagerUserConfig, тип: boolean — определяет, может ли устройство использовать пользовательские настройки.
- CreationClassName, тип: string — указывает название класса, используемого для создания.
- Description, тип: string — содержит описание раздела.
- DeviceID, тип: string — является ключевым. Оно содержит уникальный идентификатор раздела.
- DirtyBitSet, тип: boolean — определяет, помечен ли данный раздел грязным. Раздел помечается грязным в том случае, если операционная система не могла записать или считать с него нужные данные (то есть имеются подозрения на физические или логические ошибки в структуре раздела, и требуется выполнить проверку раздела). Если бит установлен, то перед выполнением таких операций, как дефрагментация или конвертирование, необходимо проверить диск на ошибочные или сбойные секторы.
- DriveType, тип: uint32 — указывает тип диска, которому принадлежит данный раздел. Например, значение 5 данного свойства говорит о том, что устройство является компакт-диском. А значение 4 говорит о том, что раздел является сетевым. Значение же 3 говорит о том, что раздел является частью локального диска.
- ErrorCleared, тип: boolean — свойство определяет, были ли исправлена последняя ошибка в работе устройства, описанная значением свойства LastErrorCode.
- ErrorDescription, тип: string — содержит описание возникшей в работе устройства ошибки. Код ошибки находится в свойстве LastErrorCode.
- ErrorMethodology, тип: string — также содержит описание найденной ошибки и возможного способа ее исправления.

- `FileSystem`, тип: `string` — определяет файловую систему, с помощью которой отформатирован данный раздел.
- `FreeSpace`, тип: `uint64` — указывает количество свободного на разделе места в байтах.
- `InstallDate`, тип: `datetime` — определяет дату установки данного устройства или его драйверов.
- `Label`, тип: `string` — содержит метку раздела (размер метки может быть не более 32 символов).
- `LastErrorCode`, тип: `uint32` — хранит код последней ошибки, возникшей в работе устройства.
- `MaximumFileNameLength`, тип: `uint32` — определяет максимальную длину имени файла (без расширения), поддерживаемую данным разделом.
- `Name`, тип: `string` — указывает имя раздела, если, конечно, оно у него есть.
- `NumberOfBlocks`, тип: `uint64` — определяет общее количество блоков, из которых состоит данный раздел.
- `PageFilePresent`, тип: `boolean` — указывает, находится ли на данном разделе файл подкачки операционной системы.
- `PNPDeviceID`, тип: `string` — определяет идентификатор устройства Plug and Play.
- `PowerManagementCapabilities`, тип: массив элементов `uint16` — указывает возможности данного раздела использовать энергосберегающий режим.
- `PowerManagementSupported`, тип: `boolean` — свойство определяет, может ли вообще данное устройство использовать возможности управления питанием.
- `Purpose`, тип: `string` — описывает медиа-возможности устройства.
- `QuotasEnabled`, тип: `boolean` — определяет, включено ли использование квот на данном устройстве.
- `QuotasIncomplete`, тип: `boolean` — указывает, используются ли квоты в данный момент на данном устройстве.
- `QuotasRebuilding`, тип: `boolean` — если значение данного свойства равно `true`, то компонент использования квот в данный момент настраивается.
- `SerialNumber`, тип: `uint32` — определяет серийный номер устройства.
- `Status`, тип: `string` — указывает описание текущего статуса объекта. Например, данное свойство может содержать одно из представленных ниже значений: `OK`, `Error`, `Starting`, `Stopping`, `Degraded` или `Pred Fail`.
- `StatusInfo`, тип: `uint16` — определяет код статуса устройства. Например, если значение свойства равно `3`, то устройство включено, а если значение равно `4`, то отключено.
- `SupportsDiskQuotas`, тип: `boolean` — указывает, поддерживает ли устройство использование квот.

- SupportsFileBasedCompression, тип: boolean — определяет, поддерживает ли раздел стандартные способы компрессии файлов.
- SystemCreationClassName, тип: string — содержит системное имя класса-создателя.
- SystemName, тип: string — хранит системное имя.
- SystemVolume, тип: boolean — определяет, содержит ли данный раздел файлы, необходимые для запуска операционной системы.

Класс также содержит несколько свойств, доступных как для чтения, так и для записи:

- DriveLetter, тип: string — определяет букву диска;
- IndexingEnabled, тип: boolean — указывает, разрешено ли индексирование данного раздела.

Данный класс также поддерживает несколько методов, позволяющих работать с активацией продукта.

- AddMountPoint — используется для добавления точки монтирования каталога к данному разделу.

  Входящий параметр: строковый параметр, определяющий путь к каталогу.

  Возвращаемые параметры: нет.
- Chkdsk — проверяет данный раздел на повреждения и ошибочные секторы.

  Входящие параметры.

  - Определяет, будут ли исправляться найденные ошибки. Имеет тип boolean. По умолчанию значение данного параметра равно false.
  - Указывает, будет ли выполняться строгая проверка индекса. Нестрогая проверка индекса ускоряет процесс проверки раздела. Имеет тип boolean. По умолчанию значение данного параметра равно true.
  - Определяет, будет ли выполняться пропуск проверки циклов внутри структуры папок. Это ускоряет процесс проверки. Имеет тип boolean. По умолчанию значение данного параметра равно true.
  - Указывает, будет ли насильно выполняться отключение раздела перед его проверкой. После этого все текущие дескрипторы для этого тома станут недействительны. Имеет тип boolean. По умолчанию значение данного параметра равно false.
  - Определяет, будут ли исправляться поврежденные секторы. Имеет тип boolean. По умолчанию значение данного параметра равно false.
  - Указывает, будет ли проверка раздела выполнена при следующей перезагрузке компьютера. Если значение переменной равно false, то проверка будет выполнена немедленно. Имеет тип boolean. По умолчанию значение данного параметра равно false.

  Возвращаемые параметры: нет.

- `Defrag` — выполняет дефрагментацию диска.

  Входящий параметр: определяет, будет ли выполнена дефрагментация диска даже при нехватке свободного места. Имеет тип `boolean`. По умолчанию значение данного параметра равно `false`.

  Возвращаемый параметр: указатель на класс `Win32_DefragAnalysis`.

- `Dismount` — выполняет размонтирование раздела.

  Входящие параметры.

  - Определяет, будет ли насильно выполняться размонтирование. Имеет тип `boolean`. По умолчанию значение данного параметра равно `false`.
  - Определяет, является ли размонтирование постоянным. Имеет тип `boolean`. По умолчанию его значение равно `false`.

  Возвращаемые параметры: нет.

- `ExcludeFromAutoChk` — позволяет исключить выполнение проверки, назначенной с помощью метода `Chkdsk` на следующую перезагрузку компьютера, на некоторых разделах диска.

  Входящие параметры: массив строковых параметров, определяющих разделы диска, проверку которых выполнять не нужно.

  Возвращаемые параметры: нет.

- `Format` — выполняет форматирование раздела.

  Входящие параметры.

  - Строковый параметр, определяющий новую файловую систему. По умолчанию значение данного параметра равно `NTFS`.
  - Определяет, будет ли выполнено быстрое форматирование. Имеет тип `boolean`. По умолчанию значение данного параметра равно `false`.
  - Определяет новый размер кластера. Имеет тип `uint32`. По умолчанию значение данного параметра равно `0`.
  - Строковый параметр, определяющий новую метку раздела. По умолчанию значение данного параметра равно пустой строке.
  - Определяет, будет ли выполняться компрессия раздела. Имеет тип `boolean`. По умолчанию значение данного параметра равно `false`.
  - Определяет версию. Имеет тип `uint32`. По умолчанию значение данного параметра равно `0`.

  Возвращаемые параметры: нет.

- `Mount` — выполняет монтирование файловой системы раздела.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

- `Reset` — выполняет сброс состояния логического устройства. Если возвращает значение `0`, то метод успешно выполнен.

  Входящие параметры: нет.

  Возвращаемые параметры: нет.

- `ScheduleAutoChk` — назначает выполнение проверки разделов диска на следующую перезагрузку компьютера.

  Входящие параметры: массив значений строкового типа, определяющих разделы диска.

  Возвращаемые параметры: нет.

- `SetPowerState` — устанавливает новый режим энергосбережения.

  Входящие параметры.

  - Определяет новое состояние энергосбережения. Например, если значение переменной равно `1`, то режим энергосбережения отключен. Если значение равно `2`, то используется низкий режим энергосбережения. Если же значение переменной равной `3`, то устанавливается режим сна. Имеет тип `uint16`.
  - Определяет время перехода в новое энергосберегающее состояние. Имеет тип `datetime`.

  Возвращаемые параметры: нет.

Класс Win32_DefragAnalysis

Содержит результат выполнения метода `Defrag` класса `Win32_Volume` пространства имен `\\root\cimv2`. Он поддерживает следующие свойства, доступные только для чтения.

- `AverageFileSize`, тип: `uint64` — содержит средний размер файлов.
- `AverageFragmentsPerFile`, тип: `real64` — хранит среднее количество фрагментированных файлов.
- `ClusterSize`, тип: `uint64` — определяет размер кластера файловой системы.
- `ExcessFolderFragments`, тип: `uint64` — указывает общее количество фрагментов папок.
- `FilePercentFragmentation`, тип: `uint32` — определяет процент фрагментированных файлов.
- `FragmentedFolders`, тип: `uint64` — указывает общее количество фрагментированных папок.
- `FreeSpace`, тип: `uint64` — определяет количество свободного места в разделе.
- `FreeSpacePercent`, тип: `uint32` — указывает процент свободного места в разделе.
- `FreeSpacePercentFragmentation`, тип: `uint32` — определяет процент фрагментированного свободного места в разделе.
- `MFTPercentInUse`, тип: `uint32` — указывает процент используемой таблицы MFT.
- `MFTRecordCount`, тип: `uint64` — определяет количество записей в таблице MFT.
- `PageFileSize`, тип: `uint64` — указывает размер файла подкачки в разделе.

- TotalExcessFragments, тип: uint64 — общее количество фрагментов файлов в разделе.
- TotalFiles, тип: uint64 — общее количество файлов в разделе.
- TotalFolders, тип: uint64 — общее количество папок в разделе.
- TotalFragmentedFiles, тип: uint64 — общее количество фрагментированных файлов в разделе.
- TotalMFTFragments, тип: uint64 — общее количество фрагментов таблицы MFT.
- TotalMFTSize, тип: uint64 — общий размер таблицы MFT в разделе.
- TotalPageFileFragments, тип: uint64 — общее количество фрагментов файла подкачки.
- TotalPercentFragmentation, тип: uint32 — общий процент фрагментации раздела.
- UsedSpace, тип: uint64 — определяет процент текущего использования раздела.
- VolumeName, тип: string — содержит название раздела (букву или CLSID-номер).
- VolumeSize, тип: uint64 — определяет общий размер раздела.

Класс Win32_VolumeUserQuota

Данный класс содержит описание квоты для определенного пользователя.

- Account, тип: указатель на объект Win32_Account — является ключевым. Определяет учетную запись пользователя.
- DiskSpaceUsed, тип: uint64 — указывает используемый данным пользователем размер диска (в байтах).
- Status, тип: uint64 — определяет текущий статус работы квоты диска. Например, если значение равно 0, то квота работает нормально. Если значение свойства равно 1, то пользователю было выдано предупреждение. Если же значение равно 2, то пользователь превысил квоту.
- Volume, тип: указатель на объект Win32_Volume — является ключевым. Определяет раздел диска.

Данный класс также содержит несколько свойств, доступных как для чтения, так и для записи.

- Limit, тип: uint64 — указывает предел места в разделе диска для пользователя.
- WarningLimit, тип: uint64 — определяет предел места на диске, при превышении которого пользователю будет выдано предупреждение.

Сжатие и архивация

Как и предыдущие версии, Windows Vista поддерживает автоматический механизм сжатия данных, расположенных на отдельном разделе диска в отдельной папке, или сжатие отдельного файла.

Процесс компрессии и декомпрессии

Процесс сжатия и декомпрессии данных происходит совершенно прозрачно, поэтому сторонние программы его даже не замечают. Сжатие каталога или файла операционной системы состоит из нескольких этапов.

1. Сжимаемый файл разбивается на единицы сжатия. Каждая единица сжатия состоит из 16 кластеров, содержащих данные сжимаемого файла.
2. Каждая единица сжатия анализируется операционной системой на возможность сжатия. Если в процессе анализа определяется, что единицу сжатия можно сжать хотя бы на один кластер, то начинается процесс компрессии единицы сжатия. В противном случае единица сжатия не сжимается.
3. Сжатый файл помещается в смежных областях диска.

Процесс же декомпрессии происходит в обратном порядке. Результат декомпрессии помещается в кэш, что существенно повышает скорость последующих операций доступа к файлу.

Используем оболочку

Сжатие

Проще всего сжать объект операционной системы с помощью его окна Свойства.

Чтобы сжать целый раздел диска, нужно отобразить окно Свойства и на вкладке Общие установить флажок Сжимать диск для экономии места. После этого отобразится окно Подтверждение изменения атрибутов, которое позволяет определить, будет сжато все содержимое раздела или только сам раздел. Если вы сожмете только сам раздел, то его текущее содержимое сжато не будет. Однако, если вы добавите в корень раздела папку или файл, он автоматически будет сжат (по умолчанию сжатые папки и файлы выделяются синим цветом).

Чтобы сжать отдельную папку, нужно отобразить окно Свойства, на его вкладке Общие нажать кнопку Другие и в появившемся окне Дополнительные атрибуты установить флажок Сжимать содержимое для экономии места на диске. Если сжимаемая папка содержит другие папки или файлы, то также отобразится окно Подтверждение изменения атрибутов, содержащее те же возможности, что и при сжатии разделов диска. Новые данные, помещаемые в сжатую папку, автоматически сжимаются.

Процесс сжатия отдельного файла полностью аналогичен сжатию папки. Лишь на последнем этапе никогда не отобразится окно Подтверждение изменения атрибутов.

ПРИМЕЧАНИЕ

Как папка, так и файл не могут быть одновременно сжаты и зашифрованы. Поэтому, как только вы установите флажок Сжимать содержимое для экономии места на диске, сразу же будет снят флажок Шифровать содержимое для защиты данных.

Если же вам нужно отменить сжатие файлов, папок или разделов, то достаточно снять флажок сжатия данных. После этого также может отобразиться окно Подтверждение

изменения атрибутов, с помощью которого можно указать, будет снят флажок шифрования только для раздела или папки или полностью для всего содержимого раздела или папки.

Архивация

Кроме стандартного способа сжатия объектов, операционная система Windows Vista поддерживает архивацию папок и файлов с помощью алгоритма ZIP. Чтобы заархивировать файл или папку, достаточно в ее контекстном меню выбрать команду Отправить ▸ Сжатая ZIP-папка. После этого будет создан новый файл с расширением ZIP.

ПРИМЕЧАНИЕ

Таким же способом можно архивировать сразу несколько файлов и каталогов, выделив их все.

Если же вам нужно разархивировать созданный ранее ZIP-файл, достаточно в его контекстном меню выбрать команду Извлечь все. После этого отобразится мастер Распаковка сжатых ZIP-папок, с помощью которого можно указать каталог, в который будет помещена разархивированная копия файла или папки.

Используем программы командной строки

Сжатие файлов, папок и разделов диска

Для сжатия файлов, папок или разделов можно также использовать программу командной строки `compact.exe`. Ее основной синтаксис довольно прост, а параметры в операционной системе Windows Vista совершенно не изменились. Чтобы выполнить сжатие, нужно воспользоваться параметром `/C`, а если нужно отменить сжатие, то пригодится параметр `/U`:

- `compact.exe /C|/U /S:<раздел>` — позволяет сжать раздел или отменить его сжатие;
- `compact.exe /C|/U /S:<путь к каталогу>` — дает возможность сжать каталог или отменить его сжатие;
- `compact.exe /C|/U /S:<путь к каталогу> <имя файла или шаблон>` — позволяет сжать файл или файлы, удовлетворяющие шаблону и расположенные в соответствующем каталоге, или отменить его сжатие.

При использовании программы `compact.exe` также часто приходится применять параметр `/I`. Если вы не используете его, то при возникновении ошибки в сжатии файла (например, к нему запрещен доступ) работа программы `compact.exe` будет прекращена. Это никак не влияет на сжатие файлов, однако при сжатии папок или каталогов может привести к неполному сжатию. В этом случае нужно использовать параметр `/I`, благодаря которому программа будет работать даже после возникновения ошибки, просто пропуская тот файл, который вызвал ее.

Создание CAB-файлов

Данная программа является оболочкой, вызывающей программу командной строки `makecab.exe`. Поэтому можно использовать как программу `diantz.exe`, так и программу `makecab.exe`.

Создание CAB-файлов также является своеобразным способом сжатия. Они представляют собой разновидности архивов. Более того, операционная система Windows Vista обрабатывает CAB-файлы точно так же, как и ZIP-файлы, которые мы создавали ранее с помощью оболочки (для их обработки используется один и тот же идентификатор `CompressedFolder`).

Основной синтаксис программы `makecab.exe` следующий: `makecab /L <раздел, в который будет скопирован уже заархивированный файл> <путь и имя архивируемого файла> <имя создаваемого CAB-файла>`.

Разархивирование CAB-файлов

Если же вам нужно выполнить разархивирование созданного ранее CAB-файла, то придется воспользоваться либо оболочкой, либо отдельной программой командной строки `expand.exe`. Она поддерживает следующие возможности:

- `expand -D <путь к CAB-файлу и его имя>` — отображает список файлов, заархивированных в данном CAB-файле;
- `expand <путь к CAB-файлу и его имя, либо путь к каталогу, содержащему CAB-файлы и шаблон, по которому можно выбрать требуемые CAB-файлы> -F:<название файла или шаблон, по которому нужно определить, какие из CAB-файлов будут распакованы> <каталог, в который будет распаковано содержимое CAB-файла>` — распаковывает определенные CAB-файлы или часть их содержимого.

Разреженные файлы

Разреженные файлы представляют собой еще один способ сжатия. Если файл, помеченный как разреженный, хранит нулевые данные, операционная система не выделяет на жестком диске места для этих данных. Таким образом, экономится место на диске. Как только нулевые данные файла заменяются значащими данными, для них выделяется место.

Чтобы создать разреженный файл, достаточно воспользоваться командой `fsutil sparse setflag <путь к файлу, который нужно сделать разреженным, и его имя>`. Кроме того, с помощью команды `fsutil sparse queryflag <путь к файлу и его имя>` можно определить, является ли данный файл разреженным.

Обнулить данные в файле можно с помощью команды `fsutil file setzerodata offset=<смещение от начала файла в байтах> length=<размер обнуляемых данных в байтах> <путь к файлу и его имя>`.

Запись дисков

Запись содержимого на перезаписываемый (DVD-RW или CD-RW) или записываемый (DVD-R или CD-R) диск с помощью Windows Vista довольно проста.

Использование возможностей автозапуска

Легче всего начать запись с помещения пустого диска в привод. После того как операционная система распознает диск, она отобразит окно автозапуска, содержащее следующие возможности.

- Записать DVD с данными — запускает программу Проигрыватель Windows Media для выполнения записи данных, доступ к которым можно получить с помощью библиотеки музыкального проигрывателя, на диск.

  Программа Проигрыватель Windows Media откроется уже на вкладке Запись, поэтому вам будет достаточно только выбрать из библиотеки проигрывателя файлы, которые нужно записать на диск, и поместить их в список записи, который расположен в правой части программы. После того как вы это сделаете, достаточно нажать кнопку Начать запись, чтобы начать процесс записи.

- Записать файлы на диск — позволяет записать любые данные на диск с помощью Проводника операционной системы. После выбора данной команды перед вами откроется каталог, который содержит данные, уже записанные (для перезаписываемых дисков) или только готовые к записи.

  Чтобы добавить данные, которые будут записаны на диск, достаточно поместить их в открывшуюся папку. После того как вы добавите в каталог все данные, которые хотите записать на диск (добавляемые вами данные будут скопированы в один из подразделов каталога `%userprofile%\AppData\Local\Microsoft\Windows\Burn`, чтобы изменить это, достаточно воспользоваться параметром строкового типа `StagingPath`, расположенным в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\StagingInfo\{CLSID-номер DVD-RW привода}`), достаточно нажать кнопку Записать на диск, расположенную на панели инструментов. После этого начнется процесс записи.

- Записать видео-DVD — запускает программу DVD-студия Windows для создания на основе ваших видеоданных DVD, воспроизводимого не только на компьютерах, но и на стандартных бытовых проигрывателях DVD.

  При этом способе создания DVD вам будет необходимо знание программы DVD-студия Windows, работа с которой была описана в разд. 4.2.

После того как вы выберете один из описанных выше элементов окна автозапуска, перед вами отобразится окно Записать диск. С его помощью можно указать название создаваемого вами диска, а также формат диска (после того как вы щелкнете кнопкой мыши на ссылке Показать параметры форматирования). С помощью операционной системы Windows Vista можно создать диски следующих форматов файловой системы UDF.

ПРИМЕЧАНИЕ

Файловая система UDF пришла на смену CDFS и позволяет записывать данные на компакт-диски и DVD. Она поддерживает длинные имена файлов, символы Unicode и разреженные файлы.

Файловая система UDF определяется драйвером udfs.sys, расположенным в каталоге %systemroot%\system32\drivers.

- Живая файловая система — создает диски в формате Windows XP. Такие диски не будут читаться с помощью операционных систем ниже Windows XP и бытовых проигрывателей DVD, однако с ними вы сможете обращаться как с флэш-памятью — быстро и легко перезаписывать их содержимое.

  Обратите внимание на ссылку Сменить версию под данным положением переключателя. С ее помощью можно отобразить окно, позволяющее изменить версию формата Живая файловая система, которая будет использоваться для записи диска. Возможны следующие версии.

  - 1.50 — диски данной версии будут считываться операционными системами Windows 2000, Windows XP и Windows 2003 (естественно, и Windows Vista).
  - 2.00 — диски будут считываться операционными системами Windows XP и Windows 2003.
  - 2.01 — версия используется по умолчанию. Диски данной версии будут считываться операционными системами Windows XP и Windows 2003.
  - 2.50 — диски будут считываться только Windows Vista.

  Если значение параметра REG_DWORD-типа IsImapiDataBurnSupported, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\Drives\{CLSID-номер привода DVD}, равно 0, то этот способ записи будет единственным.

- Mastered — создает диски нового формата, которые можно прочитать с помощью любой операционной системы и многих бытовых проигрывателей. Дописать данные к содержимому таких дисков нельзя.

Выбор нужных параметров форматирования и закрытие данного окна приведет к выполнению того действия, которое вы выбрали с помощью окна автозапуска (описанного выше). А вот после того как вы сформируете список данных, которые нужно записать на диск, и начнете процесс записи, перед вами отобразится еще одно окно. С его помощью можно еще раз указать название диска (переопределить), а также скорость, с которой будет выполняться запись диска, и, если вы записываете аудиоданные, является диск аудиодиском или диском с данными.

Команда Проводник

Начать процесс записи можно после помещения DVD в привод и выбора команды Проводник контекстного меню значка диска. После этого отобразится знакомое

вам окно выбора формата диска (окно Записать диск). А после того как вы отформатируете диск, откроется каталог, который содержит данные, уже записанные (для перезаписываемых дисков) или только готовые к записи. Иначе говоря, данный способ эквивалентен выбору элемента Записать файлы на диск окна автозапуска.

Команда Форматировать

И еще одним способом начала процесса записи является выбор команды Форматировать контекстного меню значка диска. После этого отобразится окно Форматирование, позволяющее отформатировать диск с помощью одной из версий формата Живая файловая система.

Команда rundll32.exe

Начать запись на диск можно и с помощью команды `rundll32.exe shell32.dll, PrepareDiscForBurnRunDll <буква, определяющая привод DVD>`. После ввода данной команды отобразится окно выбора формата записываемого диска (если в соответствующем приводе находится пустой диск).

Настройка механизма записи

Чтобы настроить некоторые параметры записи на пустой диск с помощью стандартного механизма операционной системы Windows Vista, достаточно отобразить окно Свойства привода DVD, с помощью которого вы и будете записывать диски, и перейти на вкладку Запись. Она отображается только в том случае, если параметр `REG_DWORD`-типа `Active`, расположенный в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\StagingInfo\{CLSID-номер привода DVD}`, равен `1`. В противном случае запись дисков с помощью соответствующего привода невозможна.

Вкладка Запись содержит следующие возможности.

- Раскрывающийся список приводов в области Запись на диск с рабочего стола — благодаря ему можно указать привод (если у вас их несколько), с помощью которого по умолчанию выполняется процесс записи данных. Именно на него будут передаваться данные, если конкретный привод не был выбран.

  Данный список изменяет значение параметра строкового типа `CD Recorder Drive`, расположенного в ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning`.

- Раскрывающийся список разделов жесткого диска в области Запись на диск с рабочего стола — с его помощью можно указать раздел жесткого диска, который будет использоваться в процессе записи данных на чистый диск. Именно на этом диске будут храниться временные файлы, создаваемые в процессе записи (в каталоге Windows Burn Temp Files раздела диска), поэтому необходимо, чтобы соответствующий раздел имел достаточно свободного пространства.

  По умолчанию используется раздел, с которого запускается операционная система.

Путь к каталогу, в котором будут храниться временные файлы записи, определяется в параметре строкового типа ImageStashLocation, расположенном в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning.

- Флажок Автоматически извлекать диск после записи — если он снят, то после выполнения процесса записи привод не будет открываться. По умолчанию данный флажок установлен.

  Установка флажка изменяет значение параметра строкового типа Auto Eject, расположенного в ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning.

- Кнопка Общие параметры — с ее помощью отображается дополнительное окно, которое содержит единственный флажок Автоматически закрывать текущий сеанс UDF при извлечении диска. Он определяет, будет ли автоматически закрываться записываемая сессия при завершении записи. Закрытие сессии занимает около 200 Мбайт свободного места на записываемом диске, однако в некоторых случаях это необходимая мера, повышающая читаемость записанных на диске данных с помощью бытовых проигрывателей DVD.

  Флажок изменяет значение параметра REG_DWORD-типа UdfsCloseSessionOnEject, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem.

7.7. Работа с принтерами

Как правило, у неподготовленного пользователя не возникает никаких вопросов при установке только что купленного принтера или сканера — большинство принтеров и сканеров подключаются к компьютеру с помощью порта USB, а устройства, подключаемые к данному порту, определяются и устанавливаются операционной системой автоматически. Однако в дальнейшей настройке и работе с данными устройствами могут возникнуть затруднения.

Настройка работы принтера

Сведения обо всех принтерах, которые установлены в операционной системе, содержатся в папке Принтеры. Доступ к ней можно получить с помощью одноименного значка папки Панель управления.

Папка Принтеры содержит как список принтеров, подключенных вами непосредственно к компьютеру, так и список сетевых принтеров. Кроме того, в данной папке присутствует три стандартных значка: Fax, Microsoft Office Document Image Writer и Microsoft XPS Document Writer.

Сетевой принтер представляет собой принтер, подключенный к другому компьютеру, и тем не менее, с его помощью вы можете распечатывать документы. Чтобы сетевой принтер мог корректно работать на вашем компьютере, нужно выполнить

его установку (установку его драйверов). Как правило, эта операция происходит автоматически при обнаружении нового принтера в сети. Однако если этого не произошло, то для установки сетевого принтера можно воспользоваться мастером Установка принтера. Данный мастер отображается при выборе команды Установить принтер из контекстного меню папки Принтеры.

ПРИМЕЧАНИЕ

Мастер Установка принтера можно отобразить и с помощью команды rundll32.exe shell32.dll, SHHelpShortcuts_RunDLL AddPrinter.

Кроме того, вы можете запустить мастер Установка принтера для создания принтера на удаленном компьютере. Для этого нужно воспользоваться командой rundll32 printui.dll,PrintUIEntry /il /c\\<имя компьютера>.

Сразу же на первом шаге мастер предлагает вам выбрать, какой именно принтер нужно установить.

- Можно установить локальный принтер, подключенный к LPT-порту компьютера (как было сказано выше, принтеры, подключенные к USB, устанавливаются автоматически).
- Можно установить сетевой принтер, а также принтеры, подключенные с помощью Bluetooth или WiFi. Именно этот вариант вам нужно выбрать, если вы хотите установить сетевой принтер.

После того как вы выберете установку сетевого принтера, операционная система начнет поиск всех принтеров, которые присутствуют в сети. Если в результате поиска принтера он не был найден, хотя вы точно знаете, что принтер подключен, настроен и работает, можно воспользоваться ссылкой Нужный принтер отсутствует в списке, чтобы ввести путь к принтеру вручную.

После того как вы найдете нужный сетевой принтер, мастер предложит ввести его имя и определить, будет ли он использоваться по умолчанию. После нажатия кнопки Готово сетевой принтер будет установлен и готов к работе.

Настройки сервера принтеров

Сервер принтеров содержит глобальные настройки, которые применяются всеми принтерами операционной системы. Чтобы отобразить окно свойств сервера принтеров, достаточно в контекстном меню папки Принтеры выбрать команду Свойства сервера.

ПРИМЕЧАНИЕ

Отобразить это окно можно и с помощью команды rundll32.exe printui.dll, PrintUIEntry /s. При этом в данной команде можно указать параметр вида /tX, где вместо X указывается номер вкладки окна, которая должна быть открыта.

В данной команде можно также использовать параметр /c\\<имя компьютера>, чтобы отобразить окно свойств сервера принтеров удаленного компьютера.

Окно Свойства: Сервер печати содержит следующие вкладки.

- Формы — содержит список форм, которые могут обрабатывать принтеры данного сервера печати.

  Форма — это размер страницы по вертикали и горизонтали (а также размеры отступов на этой странице), на которой могут печатать принтеры операционной системы.

  Как правило, сервер печати поддерживает очень много форм (а не только известные многим формы A1–A4), однако, если вы не находите нужную вам форму, можно создать собственную. Для этого достаточно установить флажок Создать новую форму, после чего указать размеры новой страницы и размеры отступов на ней.

- Порты — включает список портов компьютера и принтеры, которые подключены к данным портам. С помощью кнопок Добавить порт и Удалить порт вы можете удалить или добавить новый порт.

  Именно с помощью кнопки Добавить порт данной вкладки можно установить новый порт TCP/IP, который можно использовать для подключения к принтеру через Интернет. После нажатия этой кнопки отобразится список типов портов, которые можно установить (по умолчанию можно установить локальный порт, порт TCP/IP и порт Microsoft Document Imaging Writer Monitor, однако с помощью кнопки Новый тип портов можно установить дополнительные типы портов).

ПРИМЕЧАНИЕ

Вызвать окно установки нового типа порта можно и с помощью команды rundll32.exe NTPRINT.dll, PSetupInstallMonitor.

Репозитарий CIM систем семейства Windows содержит класс Win32_TCPIPPrinterPort (хранится в пространстве имен \root\cimv2), экземпляры которого описывают созданные TCP/IP порты.

Данный класс имеет следующие свойства: ByteCount (определяет, будет ли компьютер подсчитывать размер документа перед каждой передачей на печать), HostAddress (указывает IP-адрес сервера печати), Name (ключевое свойство, определяющее имя TCP/IP порта), Protocol (указывает способ подключения к принтеру: Raw (печать непосредственно на принтере), Lpr (печать на принтере или на сервере печати)), SNMPEnabled (определяет, поддерживает ли принтер протокол SNMP).

Если вы выберете установку порта TCP/IP, то запустится Мастер добавления стандартного порта TCP/IP принтера. Данный мастер предложит вам ввести IP-адрес компьютера, к которому подключен принтер, после чего попытается получить доступ к принтерам этого компьютера. Если мастер не сможет автоматически найти принтеры по введенному вами IP-адресу, он предложит вам самостоятельно настроить параметры принтера, введя название используемого сервера печати.

ПРИМЕЧАНИЕ

Этот мастер можно отобразить и с помощью команды rundll32.exe TCPMonUI.dll, LocalAddPortUI.

- Драйверы — отображает список установленных драйверов локальных и сетевых принтеров. С помощью кнопок Добавить и Удалить данной вкладки можно установить новый драйвер или удалить ненужные. Можно также просмотреть список файлов, входящих в драйвер. Для этого нужно выбрать драйвер и нажать кнопку Свойства.

  Список установленных в операционной системе драйверов и файлы, входящие в их состав, содержатся в подразделах ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\PackageInstallation\<тип процессора>`.

ПРИМЕЧАНИЕ

Получить сведения о драйверах принтеров, установленных в операционной системе, можно и с помощью класса Win32_PrinterDriver, принадлежащего пространству имен \root\cimv2. Экземпляры данного класса описывают параметры установленных драйверов и поддерживают следующие свойства: ConfigFile (определяет название файла конфигурации драйвера), DriverPath (указывает путь к драйверу), FilePath (определяет путь к INF-файлу драйвера), InstallDate (указывает дату установки драйвера), MonitorName (определяет имя монитора для драйвера), Name (ключевое свойство, определяющее имя драйвера), Started (указывает, работает ли служба печати), StartMode (определяет режим запуска драйвера).

Кроме того, данный класс поддерживает следующие методы: AddPrinterDriver (позволяет установить новый драйвер принтера), StartService (запустить драйвер принтера), StopService (остановить драйвер).

- Дополнительные параметры — позволяет настроить дополнительные параметры работы сервера печати. К ним относятся следующие указания.
  - Путь к папке, используемой как пул печати. Данный путь хранится в параметре строкового типа `DefaultSpoolDirectory`, расположенном в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers`.
  - Будут ли заноситься в журнал такие события, как ошибки, предупреждения или информация о работе пула печати.
  - Будет ли издаваться звуковой сигнал при ошибке во время печати удаленного документа. Флажок с этим указанием изменяет значение параметра `REG_DWORD`-типа `BeepEnabled`, расположенного в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print`.
  - Будут ли отображаться уведомления о работе локальных и сетевых принтеров.

Настройки принтера

После того как вы установили принтер, вам, возможно, придется настроить параметры его работы. Для этого применяется окно Свойства, отобразить которое можно с помощью одноименной команды контекстного меню значка принтера.

Окно Свойства состоит из следующих вкладок.

- Общие — отображает общую информацию о принтере. Обратите также внимание на кнопку Настройка печати, расположенную на данной вкладке. С ее помощью можно отобразить окно настройки принтера.

  Как правило, окно настройки принтера, отображаемое с помощью кнопки Настройка печати, зависит от производителя вашего принтера (именно он создает данное окно), поэтому и возможности настройки принтера с помощью данного окна различаются. Именно по этой причине мы не будем рассматривать содержимое данного окна.

  Окна же настройки стандартных принтеров одинаковы.

  Для значка Fax с его помощью можно определить используемый по умолчанию размер бумаги, разрешение, а также ориентацию бумаги.

  Для значка Microsoft Office Document Image Writer с его помощью можно также определить размер используемой по умолчанию бумаги и ее ориентацию. Но, кроме того, с помощью данного окна можно указать путь к каталогу, в который будут помещаться напечатанные с помощью этого принтера файлы, а также выходной формат печатаемых файлов (MDI или TIFF определенного качества). Эти настройки заносятся в параметры ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Office\<номер версии>\MODI\MDI writer`.

  Для значка Microsoft XPS Document Writer с его помощью можно определить ориентацию, а также указать, будут ли XPS-документы автоматически открываться в программе XPS Viewer. Кроме того, обратите внимание на кнопку Настройка печати окна настройки принтера. С ее помощью можно изменить размер используемой бумаги, указать, будет ли включено чересстрочное построение изображения, а также формат выходного файла (TIFF или PNG).

- Доступ — позволяет установить общий доступ к локальному принтеру. Иными словами, после установки общего доступа другие пользователи сети смогут установить ваш принтер как сетевой.

  Чтобы сделать принтер общим, достаточно установить флажок Общий доступ к данному принтеру и ввести имя общего принтера.

  Кроме того, обратите внимание на кнопку Дополнительные драйверы. С ее помощью можно указать, драйверы для каких типов процессора можно будет установить пользователям, устанавливающим ваш принтер как сетевой. Например, если в окне, отображаемом при нажатии данной кнопки, указано использование только драйверов для процессоров x86, то пользователи, имеющие 64-битные процессоры (x64 или Itanium), не смогут установить ваш принтер как сетевой.

- Порты — отображает список портов, к которым подключен данный принтер. Кроме того, с помощью флажков данной вкладки можно включить поддержку пула принтеров для данного принтера, а также поддержку двунаправленного доступа к принтеру.

- Дополнительно — позволяет настроить дополнительные параметры работы принтера. Вкладка содержит следующие возможности.
  - Благодаря переключателю, который можно установить в положения Доступен всегда или Доступен с, можно указать время, в течение которого пользователи могут выполнять печать с помощью данного принтера.
  - Используя поле Приоритет, можно указать приоритет печати страниц на данном принтере. Работа с приоритетами печати будет описана ниже.
  - Благодаря кнопке Обработчик печати вы можете определить имя диспетчера очереди печати, обслуживающего задания.
  - С помощью кнопки Страница-разделитель можно указать путь к файлу, содержимое которого будет распечатываться после того, как принтер обработал следующее задание печати (это может быть необходимо для того, чтобы отделить задания одного пользователя от другого, если на принтере могут печатать сразу несколько пользователей).

  На вкладке также присутствуют следующие флажки.
  - Задерживать документы с неподходящими параметрами.
  - Первыми печатать документы из очереди — если флажок установлен, то задания принтером будут выполняться, начиная с начала очереди печати.
  - Сохранять документы после печати — если он установлен, то уже выполненные задания не будут удаляться из очереди печати. Это дает возможность повторно печатать документы, не помещая их заново в очередь.
  - Включить дополнительные возможности печати.
- Управление цветом — содержит кнопку Управление цветом, с помощью которой можно отобразить одноименное окно. Оно позволяет изменить цветовую схему, используемую при печати на принтере.

  После отображения окна на его вкладке Общие в списке Устройство нужно выбрать ваш принтер, после чего установить флажок Использовать мои параметры для этого устройства. Это приведет к активированию кнопки Добавить, с помощью которой как раз и выполняется выбор цветовой схемы принтера.

ПРИМЕЧАНИЕ

Доступ к окну Управление цветом может быть ограничен с помощью групповой политики файла WindowsColorSystem.admx, расположенного в подразделе Конфигурация пользователя ▸ Административные шаблоны ▸ Компоненты Windows ▸ Цветовая система Windows Color System.

Данная политика изменяет значение параметра REG_DWORD-типа ProhibitInstallUninstall, расположенного в ветви Software\Policies\Microsoft\Windows\WindowsColorSystem корневого раздела HKEY_CURRENT_USER или HKEY_LOCAL_MACHINE. Установка значения данного параметра равным 1 запрещает пользователям устанавливать или удалять цветовые схемы.

- Безопасность — позволяет изменить разрешения доступа к принтеру, которые присвоены пользователям компьютера. С помощью данной вкладки можно определить, разрешено ли пользователям выполнять печать с помощью данного принтера, изменять настройки принтера и документа. Благодаря этой вкладке можно также установить аудит доступа к принтерам.

Доступ ко всем настройкам определенного принтера можно получить с помощью экземпляров класса `Win32_Printer`, принадлежащего пространству имен `\root\cimv2`. Данный класс поддерживает следующие свойства.

- `AveragePagesPerMinute` — определяет среднее количество страниц в минуту, которое способен печатать данный принтер.
- `CurrentPaperType` — указывает тип бумаги, который в данный момент использует принтер.
- `Default` — определяет, используется ли данный принтер по умолчанию.
- `DefaultCopies` — указывает количество печатаемых по умолчанию копий документа.
- `DeviceID` — ключевое свойство, определяющее идентификатор принтера.
- `Direct` — если значение данного свойства равно `true`, то задания направляются непосредственно на принтер, а не устанавливаются в очередь.
- `DoCompleteFirst` — если значение свойства равно `true`, то принтер выполняет задания, начиная с начала очереди печати.
- `DriverName` — определяет имя драйвера для данного принтера.
- `EnableBIDI` — если значение данного свойства равно `true`, то принтер может печатать в обоих направлениях.
- `Hidden` — указывает, скрыт ли принтер от пользователей сети.
- `MaxCopies` — определяет максимально возможное количество копий документа, которые может распечатать принтер.
- `MaxSizeSupported` — указывает максимальный размер документа (в килобайтах), который может принять на распечатку принтер.
- `Network` — определяет, является ли данный принтер сетевым.
- `PortName` — указывает порт, к которому подключен принтер.
- `Priority` — определяет приоритет принтера.
- `SeparatorFile` — указывает имя файла, используемого при генерации страницы-разделителя.
- `Shared` — определяет, является ли принтер общим.
- `StartTime` — указывает время, начиная с которого принтеру разрешено выполнять печать.
- `UntilTime` — определяет время, начиная с которого принтеру запрещено выполнять печать.

Кроме того, данный класс поддерживает методы, позволяющие выполнять следующие действия.

- `AddPrinterConnection` — добавить сетевой принтер.
- `CancelAllJobs` — удалить все задания из очереди печати.
- `Pause` — приостановить работу принтера.
- `PrintTestPage` — распечатать тестовую страницу.
- `RenamePrinter` — переименовать принтер.
- `Resume` — возобновить работу принтера.
- `SetDefaultPrinter` — установить данный принтер как принтер по умолчанию.

Групповые политики

Возможности работы с принтерами можно ограничить с помощью групповых политик, описанных в файле `Printing.admx` и расположенных в подразделе Конфигурация пользователя ▸ Административные шаблоны ▸ Панель управления ▸ Принтеры.

Данные политики изменяют значения `REG_DWORD`-типа, расположенные в ветви `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`.

- Запретить добавление принтеров — изменяет значение параметра `NoAddPrinter`. Если он равен `1`, то использование мастера Установка принтера будет запрещено.
- Запретить удаление принтеров — политика меняет значение параметра `NoDeletePrinter`. Если этот параметр равен `1`, то удаление принтеров будет запрещено.

Работа с принтером

Теперь поговорим о вопросах печати на принтере и работе с ним.

Создание нескольких копий принтеров с разными приоритетами доступа

Иногда возникает такая ситуация, когда нужно определить приоритет доступа к принтеру определенных пользователей. Например, когда на одном и том же принтере печатают свои документы члены директората фирмы и обычные пользователи. В этом случае, естественно, документы, переданные на печать директоратом, должны печататься в первую очередь.

В такой ситуации нужно воспользоваться полем приоритета доступа к принтеру. Для этого нужно установить две копии одного и того же принтера. Первая копия устанавливается автоматически, а вторую нужно установить вручную, воспользовавшись мастером Установка принтера. Для этого в данном мастере нужно указать установку локального принтера. В списке портов мастера выбрать элемент USB001

(Порт виртуального принтера для USB), после чего установить драйверы нового принтера (либо выбрать из списка, так как они точно есть на локальном компьютере, ведь вы их уже устанавливали, либо вставить диск с драйверами). В самом конце нужно ввести имя нового принтера и определить параметры общего доступа к принтеру.

Теперь необходимо настроить права доступа к двум копиям принтера (с помощью вкладки Безопасность окна Свойства принтеров). Например, к первой копии могут иметь доступ только работники фирмы (или все пользователи), а ко второй копии принтера — только члены директората.

И последний шаг — настройка приоритета. Чтобы задания от членов директората всегда обрабатывались принтером первыми, нужно в поле Приоритет, расположенном на вкладке Дополнительно окна Свойства принтера, который будет использоваться директоратом, ввести значение 1. А в поле Приоритет принтера, который будет использоваться обычными пользователями, нужно ввести значение 10.

Печать с помощью принтера Microsoft Office Document Image Writer

Принтер Microsoft Office Document Image Writer является стандартным принтером операционной системы Windows Vista и предназначен для создания файла изображения формата TIFF или MDI на основе содержимого текстовых файлов. Печать на данном принтере не вызывает никаких затруднений.

Например, чтобы распечатать документ с помощью Microsoft Word, достаточно воспользоваться командой Печать меню Файл данной программы. После этого в поле имя нужно выбрать принтер Microsoft Office Document Image Writer, установить другие параметры печати и нажать кнопку OK. Это приведет к отображению окна Сохранить как, с помощью которого можно указать имя создаваемого файла изображения и путь к нему. После этого будет создано изображение, содержащее либо одну страницу текстового файла, либо все (в зависимости от настроек печати).

Печать с помощью принтера Microsoft XPS Document Writer

Принтер Microsoft XPS Document Writer является стандартным принтером операционной системы Windows Vista и предназначен для создания файла изображения в XPS-формате на основе содержимого текстовых файлов.

Печать на данном принтере аналогична печати на принтере Microsoft Office Document Image Writer, однако в результате будет создан файл изображения, имеющий XPS-формат.

Формат XPS-файлов основан на XML и новой модели программирования WinFX. Благодаря этому будущие программы, основанные на WinFX, смогут работать с форматом XPS.

XPS-файлы относятся к фиксированным файлам, то есть к файлам, которые не поддерживают изменения содержимого. Это одновременно является и плюсом XPS-файлов, и их минусом: с одной стороны, гарантируется, что визуальное отображение документа всегда будет одинаковым, а с другой стороны, XPS-документы

нельзя переформатировать, например, для того, чтобы корректно отобразить на маленьких экранах КПК.

При печати XPS-документов задания передаются на принтер по новому пути печати, который обходит слой GDI (основные недостатки данного слоя в том, что он не поддерживает градиенты, прозрачность и улучшенные цвета). Это позволяет повысить скорость печати, а также качество результата печати, доведя его до уровня печати PDF.

XPS-документы могут храниться в специальном контейнере, который предназначен для хранения одного или нескольких XPS-документов и ресурсов, необходимых им. Контейнер не только объединяет несколько документов, но и сжимает их, что позволяет сократить скорость передачи XPS-документов через Интернет.

Файлы с расширением XPS открываются с помощью браузера Internet Explorer 7.0 (рис. 7.5).

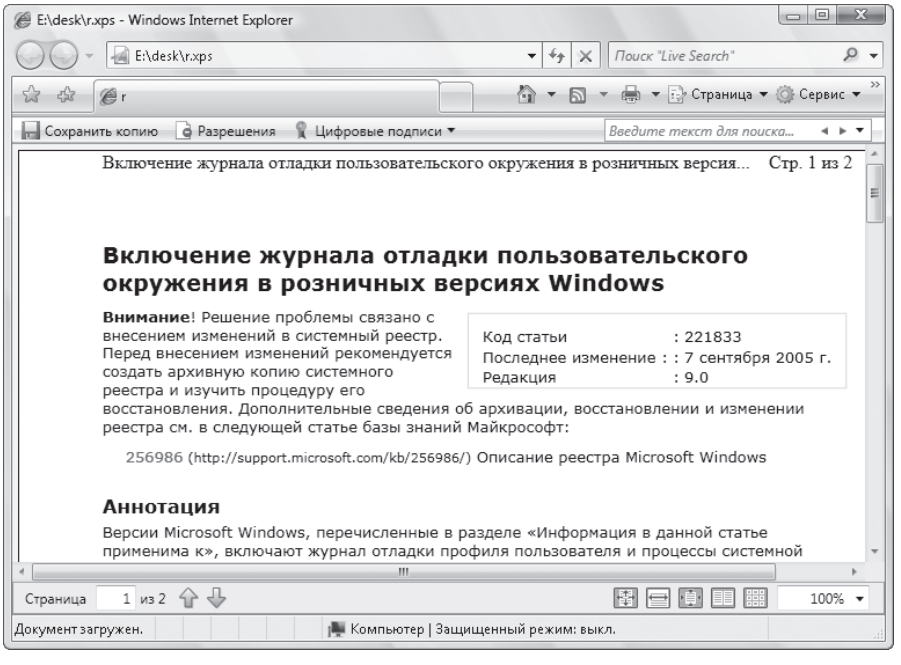


Рис. 7.5. Работа с XPS-файлами

Обратите внимание на кнопки Сохранить копию, Разрешения и Цифровые подписи браузера Internet Explorer.

- Сохранить копию — полезна при работе с XPS-файлами через Интернет. С ее помощью можно сохранить копию XPS-файла на вашем компьютере.
- Разрешения — позволяет указать пользователей, которые могут получить доступ к данному XPS-файлу на основе сетевой учетной записи пользователя или учетной записи .NET Passport пользователя.

- Цифровые подписи — дает возможность подписать данный XPS-файл своим сертификатом (если, конечно, он у вас есть).

ПРИМЕЧАНИЕ

В дальнейшем предполагается разработка возможности подписи XPS-документов с помощью DRM.

Печать с помощью обычного принтера

Печать с помощью обычного принтера выполняется так же, как и с использованием стандартных принтеров операционной системы Windows Vista. Только, естественно, результатом печати будет не файл, а напечатанное на бумаге изображение.

Еще одним отличием работы с данным видом принтеров является то, что задания печати, создаваемые для обычных принтеров, сначала заносятся в очередь печати (окно очереди печати автоматически отображается при выполнении печати). Очередь печати представляет собой набор заданий от пользователей, которые ждут выполнения на принтере. С помощью программы очереди печати вы можете изменять приоритет заданий, удалять задания из очереди либо просматривать сами задания (какие файлы распечатываются).

ПРИМЕЧАНИЕ

Открыть очередь печати принтера можно с помощью команды rundll32.exe printui.dll, PrintUIEntry /n "имя принтера" /o.

В данном разделе мы не будем рассматривать печать с помощью команды Печать меню Файл различных программ — это не должно вызывать затруднений. Вместо этого мы рассмотрим примеры печати и работы с принтерами с помощью различных программ командной строки.

ПРИМЕЧАНИЕ

Получить доступ к содержимому очереди печати можно также с помощью класса Win32_PrintJob репозитария CIM. Класс принадлежит пространству имен \root\cimv2 и определяет экземпляры, хранящие сведения о заданиях, находящихся в очереди печати. Он поддерживает следующие свойства: DataType (определяет формат данных данного задания на печать), Document (указывает название печатаемого документа), HostPrintQueue (определяет имя компьютера, пославшего задание на печать), Name (ключевое свойство, определяющее название данного задания), Priority (указывает приоритет задания), Size (определяет размер документа, переданного на печать), StartTime (указывает время начала выполнения данного задания), TotalPages (определяет количество страниц задания), UntilTime (указывает время, после которого данное задание будет недействительным).

Класс также поддерживает методы Pause и Resume, позволяющие приостанавливать работу задания.

Печать с помощью команд rundll32.exe

Вы можете выполнить печать документа не только с помощью оболочки или программ командной строки, но и с помощью команд `rundll32.exe`:

- `rundll32.exe mshtml, PrintHTML "путь к печатаемому файлу"` — распечатать документ;
- `rundll32.exe shimgvw.dll, ImageView_PrintTo /pt "имя файла изображения" %2 %3 %4` — распечатать изображение.

Отдельно стоит сказать о командах `rundll32.exe`, поддерживаемых библиотекой `printui.dll`. Команды данной библиотеки имеют следующий вид: `rundll32.exe printui.dll, PrintUIEntry <параметры>`. Этих команд много, и их полное описание можно просмотреть с помощью команды `printui.exe /?`.

Печать с помощью программ и сценариев командной строки

Операционная система Windows Vista содержит несколько программ и сценариев командной строки, которые позволяют выполнять распечатывание документов или настройку очереди печати. Рассмотрим некоторые из этих программ и сценариев.

Основной программой для работы с принтерами из командной строки является программа `print.exe`. Использовать эту программу очень просто: `print /D:<название принтера> <путь к файлу, который нужно распечатать>`.

Специально для администраторов Windows Vista содержит набор сценариев, предназначенных для управления работой принтеров. Все эти сценарии находятся в каталоге `%systemroot%\System32\Printing_Admin_Scripts\<название языковой версии сценариев>`.

Prncnfg.vbs. Сценарий предназначен для отображения сведений о настройках принтера. С его помощью можно просматривать настройки принтеров как локального, так и удаленного компьютера. Чтобы просмотреть сведения о настройках принтеров удаленного компьютера, нужно указать дополнительные параметры `-s <имя компьютера> -u <имя пользователя> -w <пароль>`. Сценарий поддерживает следующие возможности.

- `Prncnfg.vbs -g -p <имя принтера>` — отображает следующие сведения о принтере: имя общей папки принтера, имя драйвера принтера, порт, к которому подключен принтер, тип данных для принтера, его приоритет по умолчанию и т. д.
- `Prncnfg.vbs -t -p <имя принтера> <параметры настройки принтера>` — позволяет настроить параметры работы принтера. Возможны следующие параметры настройки для данной команды:
  - `-r <имя порта>` — задает порт, к которому подключен принтер;
  - `-h <общее имя принтера>` — указывает сетевое имя принтера;

- `-f <путь к файлу-разделителю>` — задает путь к файлу, содержимое которого будет разделителем между двумя заданиями на печать;
- `-y <тип данных>` — указывает тип данных, которые могут быть обработаны принтером;
- `-o <приоритет>` — задает приоритет отправки задания на печать;
- `-i <приоритет по умолчанию>` — указывает приоритет по умолчанию для каждого задания на печать;
- `+|-shared` — если установить символ +, то принтер будет считаться общим ресурсом;
- `+|-direct` — если установить символ +, то задания на принтер будут передаваться напрямую, без помещения в очередь заданий;
- `+|-published` — если установить символ +, то принтер будет опубликован в службе Active Directory;
- `+|-keepprintedjobs` — если установить символ +, то задания после печати не будут удаляться из очереди;
- `+|-enablebidi` — если установить символ +, то принтер будет отправлять диспетчеру очереди печати информацию о своем статусе.

- `Prncnfg.vbs -x -p <имя принтера> -z <новое имя принтера>` — изменяет имя принтера.

Prndrvr.vbs. Данный сценарий позволяет устанавливать, удалять или настраивать работу драйверов принтера. С его помощью также можно работать с драйверами принтеров как локального, так и удаленного компьютера. Чтобы работать с драйверами принтеров удаленного компьютера, нужно указать дополнительные параметры `-s <имя компьютера> -u <имя пользователя> -w <пароль>`. Сценарий поддерживает следующие возможности.

- `Prndrvr.vbs -l` — отображает список всех драйверов принтеров, установленных в операционной системе.
- `Prndrvr.vbs -x` — удаляет все драйверы принтеров, которые не используются ни одним из принтеров.
- `Prndrvr.vbs -a -m <путь к драйверу> -v <версия драйвера> -e <драйвер для какого типа процессора>` — устанавливает драйвер определенной версии для определенного типа процессора. В качестве типа процессора можно указывать следующие значения: `Windows NT x86`, `Windows x64` и `Windows IA64`.
- `Prndrvr.vbs -d -m <путь к драйверу> -v <версия драйвера> -e <драйвер для какого типа процессора>` — удаляет драйвер определенной версии для определенного типа процессора.

Prnjobs.vbs. С помощью данного сценария можно приостанавливать печать задания, находящегося в очереди, или выполнять задание на печать. Как и предыдущие

сценарии, он позволяет воспользоваться параметрами -s <имя компьютера> -u <имя пользователя> -w <пароль> для указания компьютера, очередью заданий которого нужно управлять. Сценарий поддерживает следующие возможности.

- Prnjobs -l -p <имя принтера> — отображает список всех заданий на печать, находящихся в очереди соответствующего принтера.
- Prnjobs -z -p <имя принтера> -j <идентификационный номер задания> — приостанавливает обработку задания, находящегося в очереди на печать, номер которого указан в параметре -j.
- Prnjobs -m -p <имя принтера> -j <идентификационный номер задания> — возобновляет обработку задания, находящегося в очереди на печать, номер которого указан в параметре -j.
- Prnjobs -x -p <имя принтера> -j <идентификационный номер задания> — отменяет задание, находящееся в очереди на печать, номер которого указан в параметре -j.

Prnmngr.vbs. Сценарий реализует следующие возможности (также можно воспользоваться параметрами -s <имя компьютера> -u <имя пользователя> -w <пароль> для управления принтерами удаленного компьютера).

- Prnmngr.vbs -l — отображает список всех принтеров локального компьютера и их настройки.
- Prnmngr.vbs -x — удаляет все принтеры, подключенные к компьютеру. Вместо параметра -x может использоваться -xc (удаляет все сетевые принтеры) или -xo (удаляет все локальные принтеры).
- Prnmngr.vbs -g — отображает название принтера по умолчанию.
- Prnmngr.vbs -t -p <имя принтера> — устанавливает новый принтер по умолчанию.

Prnport.vbs. С помощью данного сценария можно создавать и настраивать подключения к удаленному принтеру по порту протокола TCP/IP. Как и предыдущие сценарии, он позволяет воспользоваться параметрами -s <имя компьютера> -u <имя пользователя> -w <пароль> для работы с сетевыми портами TCP/IP принтеров удаленного компьютера. Сценарий поддерживает следующие возможности.

- Prnport.vbs -l — отображает список всех созданных портов TCP/IP.
- Prnport.vbs -a -r <имя порта> -h <IP-адрес удаленного компьютера> -o <тип порта: RAW или LPR> -n <номер порта TCP/IP> — добавляет новый TCP/IP-порт принтера.
- Prnport.vbs -d -r <имя порта> — удаляет TCP/IP-порт принтера.
- Prnport.vbs -g -r <имя порта> — отображает настройки TCP/IP-порта принтера.

Prnqctl.vbs. Данный сценарий реализует следующие возможности (также можно воспользоваться параметрами `-s <имя компьютера> -u <имя пользователя> -w <пароль>` для управления принтерами удаленного компьютера).

- `Prnqctl.vbs -z -p <имя принтера>` — приостанавливает печать на указанном принтере.
- `Prnqctl.vbs -m -p <имя принтера>` — возобновляет печать на указанном принтере.
- `Prnqctl.vbs -x -p <имя принтера>` — отменяет все задания на указанном принтере.
- `Prnqctl.vbs -e -p <имя принтера>` — распечатать пробную страницу на указанном принтере.

Pubprn.vbs. С помощью данного сценария можно выполнить публикацию принтера в Active Directory.

7.8. Другие вопросы администрирования

И напоследок вкратце рассмотрим другие задачи, которые могут возникнуть перед администратором, а также способы их решения и стандартные программы, которые могут понадобиться для этого.

Работа с цифровыми подписями файлов

Каждый драйвер, стандартная библиотека или программа операционной системы должны иметь соответствующую цифровую подпись, удостоверяющую то, что файл был создан соответствующей компанией и она гарантирует корректность работы файла и его абсолютную безопасность.

ПРИМЕЧАНИЕ

Информация о неподписанных драйверах, загружаемых в память, заносится в журнал подраздела Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ CodeIntegrity.

Следовательно, если файлы имеют цифровую подпись, то должны существовать стандартные программы для работы с этими цифровыми подписями. И это действительно так.

Проверка подписи файла

Расположение: `%systemroot%\system32\sigverif.exe`.

Первой программой, которую мы рассмотрим, будет программа для проверки цифровых подписей основных драйверов и библиотек, установленных в операционной системе.

Основное окно программы состоит всего из трех кнопок: Начать, Закрыть и Дополнительно.

С помощью кнопки Начать можно начать сканирование цифровых подписей файлов.

Кнопка Закрыть закрывает программу `sigverif.exe`.

А с помощью кнопки Дополнительно можно отобразить окно Дополнительные параметры проверки подписи файла. Оно содержит настройки файла журнала, в который будет записываться информация о цифровых подписях файлов. Если более конкретно, то в файл журнала будет заноситься следующая информация: количество просканированных файлов, количество подписанных и количество неподписанных файлов, названия файлов, дата их изменения, версия, каталог, в котором содержится цифровая подпись, корпорация, которая выдала цифровую подпись. Обратите внимание на кнопку Просмотр журнала данного окна. После проведения сканирования с помощью данной кнопки можно открыть файл журнала сканирования.

Механизм SFC

Как и предыдущие версии операционной системы, Windows Vista поддерживает возможности SFC, с помощью которых можно проверить все системные файлы операционной системы на корректность.

Для выполнения этой операции предназначена программа командной строки `sfc.exe`. Она поддерживает следующие возможности.

- `sfc.exe /VERIFYONLY|/VERIFYFILE=<путь к файлу>` — выполняет полную проверку системных файлов (либо только проверку одного файла, указанного параметром `/VERIFYFILE`). Если обнаружится, что системный файл был подменен, восстановление стандартного системного файла не выполнять.
- `sfc.exe /SCANNOW|/SCANFILE=<путь к файлу>` — выполняет полную проверку системных файлов (либо только проверку одного файла, указанного параметром `/SCANFILE`). Если обнаружится, что системный файл был подменен, выполнить восстановление на основе стандартного системного файла.

Сведения о том, какие результаты дала проверка с помощью программы `sfc.exe`, заносятся в файл журнала `CBS.log`, расположенный в каталоге `%systemroot%\Logs\CBS`.

Просмотр сведений о работе программ

Казалось бы, такая задача, как просмотр сведений о работе запущенных в данный момент программ, не должна вызывать вопросов. Главным помощником в этом является окно Диспетчер задач, вызвать которое можно с помощью комбинации клавиш Esc+Shift+Ctrl. Дополнительным же помощником могут быть счетчики производительности, рассмотренные нами в гл. 5.

Диспетчер задач

Расположение: `%systemroot%\system32\taskmgr.exe`.

Возможности и интерфейс программы Диспетчер задач практически не изменились. Однако теперь окно Диспетчер задач состоит из шести вкладок (добавилась одна).

- Приложения — отображает список запущенных в данный момент программ, которые имеют собственное окно. С помощью кнопок этой вкладки вы можете завершить выбранную программу, переключиться на нее, а также запустить новую программу.
- Процессы — выводится список процессов, которые в данный момент запущены. По умолчанию отображаются такие сведения о процессах, как имя образа, имя пользователя, с правами которого процесс запущен, процент загрузки процессора данным процессом. Однако с помощью команды Вид ▸ Выбрать столбцы можно отобразить сведения о многих дополнительных параметрах работы процесса.

  Обратите также внимание на контекстное меню любого процесса. С его помощью можно как завершить процесс или дерево процессов (все процессы, связанные узами родительский-дочерний), так и создать дамп памяти, используемой при работе процесса, изменить приоритет работы процесса, начать его отладку и т. д.

  Но главное, если вы используете механизм UAC, то не сможете завершить работу многих системных процессов. В этом случае можно воспользоваться новой командой контекстного меню любого системного процесса, чтобы загрузить программу Диспетчер задач от имени учетной записи Администратор.
- Службы — вкладка является нововведением операционной системы Windows Vista. Она содержит список всех служб операционной системы и отображает, запущены ли они в данный момент. Кроме того, для каждой службы отображается ее подраздел реестра (в поле Имя), описание, а также группа, к которой она относится.

  Обратите также внимание на контекстное меню служб. Оно состоит всего из трех элементов, два из которых позволяют запустить или остановить службу. Последний же элемент позволяет перейти к процессу вкладки Процессы, в контексте которого служба выполняется.
- Быстродействие — отображает стандартные сведения об использовании файла подкачки, оперативной памяти и загруженности процессора. Эта вкладка совершенно не изменилась.
- Сеть — показывает сведения о загруженности сетевых адаптеров, установленных на компьютере.
- Пользователи — отображает сведения о запущенных в данный момент в операционной системе сеансах пользователей. Также с помощью кнопок данной вкладки вы можете отключить конкретный сеанс, послать сообщение пользователю или завершить сеанс.

Обратите также внимание на команду Новая задача (Выполнить) меню Файл. Как и раньше, с ее помощью можно запустить новую программу.

Программы командой строки

Управлять запущенными процессами и просматривать сведения об их работе можно и с помощью стандартных программ командой строки `taskkill.exe` и `tasklist.exe`. Они не являются нововведением операционной системы Windows Vista, поэтому мы рассмотрим их только поверхностно.

Просмотр сведений о процессах с помощью программы tasklist.exe

С помощью данной программы можно просмотреть сведения о работе не только процессов локального компьютера, но и удаленного. Для этого нужно использовать параметры `\S <компьютер> \U <пользователь> \P <пароль>`. При описании примеров использования данной программы эти три параметра будут опускаться, хотя их можно использовать всегда.

- `Tasklist` — отображает список запущенных процессов, их PID, номер и имя сессии, а также количество занятой ими оперативной памяти.
- `Tasklist /V` — показывает расширенную информацию о процессах, в которую входят все данные, получаемые с помощью команды `tasklist`, а также дополнительные данные: имя пользователя, с правами которого запущен процесс, время работы программы, а также заголовок окна программы (если программа имеет основное окно).
- `Tasklist /SVC` — отображает список запущенных процессов, их PID, а также названия служб, которые запущены в контексте данных процессов.
- `Tasklist /M` — выводит список запущенных процессов, их PID, а также библиотеки, которые запущены или используются конкретным процессом.

Завершение процессов с помощью программы taskkill.exe

Благодаря этой программе можно завершить работу определенного процесса или дерева процессов. При этом вы можете завершить работу процесса как локального компьютера, так и удаленного. Для этого нужно использовать параметры `\S <компьютер> \U <пользователь> \P <пароль>`. При описании примеров использования данной программы эти три параметра будут опускаться, хотя их можно использовать всегда. Следующие команды завершают:

- `Taskkill /PID <PID процесса>` — процесс, имеющий соответствующий PID.
- `Taskkill /IM <имя процесса>` — процесс, имеющий соответствующее имя.
- `Taskkill /IM <имя процесса>|/PID <PID процесса> /T` — не только соответствующий процесс, но и все процессы, созданные им.

Запуск программы с помощью программы start.exe

С помощью командной строки можно запускать программы и выполнять команды. Для этого предназначена программа `start.exe`. К сожалению, с ее помощью

нельзя запускать программы на удаленном компьютере. Следующие команды запускают программу:

- `Start \D <каталог>` — `cmd.exe` и в строке приветствия отображает указанный каталог;
- `Start \D <каталог> <программа>` — расположенную в указанном каталоге;
- `Start \LOW | /NORMAL | /HIGH | /REALTIME | /ABOVENORMAL | /BELOWNORMAL \D <каталог> <программа>` — расположенную в указанном каталоге с приоритетом, соответственно, низким, средним, высоким, приоритетом реального времени, приоритетом выше среднего и приоритетом ниже среднего.

Настройка режимов энергопотребления

В операционной системе Windows Vista существенно преобразовался способ изменения режима энергопотребления. Теперь для этого используется мастер Электропитание, который можно отобразить с помощью одноименного значка папки Панель управления.

Мастер Электропитание

Основное окно мастера позволяет выбрать одну из предопределенных схем энергопотребления.

- Сбалансированный — используется по умолчанию и представляет собой что-то среднее между максимальной производительностью и минимальным энергопотреблением. При этом устанавливаются следующие основные параметры энергопотребления:
  - монитор отключается после 20 минут бездействия (при работе от батареи после пяти минут бездействия);
  - жесткий диск отключается после 20 минут бездействия (при работе от батареи — после десяти минут бездействия);
  - компьютер переходит в режим сна после часа бездействия (при работе от батареи — после 15 минут бездействия);
  - адаптер беспроводной сети работает в режиме максимальной производительности;
  - шина PCI-Express работает в сбалансированном режиме.
- Экономия энергии — настраивает компьютер на минимальное энергопотребление и, соответственно, на минимальную производительность. При этом устанавливаются следующие основные параметры энергопотребления:
  - монитор отключается после 20 минут бездействия (при работе от батареи — после 3 минут бездействия);
  - жесткий диск отключается после 20 минут бездействия (при работе от батареи — после 5 минут бездействия);
  - компьютер переходит в режим сна после часа бездействия (при работе от батареи — после 15 минут бездействия);

- адаптер беспроводной сети работает в режиме максимальной производительности;
- шина PCI-Express работает в режиме минимального энергопотребления.

- Высокая производительность — настраивает компьютер на максимальную производительность и, соответственно, максимальное энергопотребление. При этом устанавливаются следующие основные параметры энергопотребления:
  - монитор отключается после 20 минут бездействия;
  - жесткий диск отключается после 20 минут бездействия;
  - компьютер никогда не переходит в режим сна;
  - адаптер беспроводной сети работает в режиме максимальной производительности;
  - шина PCI-Express работает в максимальном режиме.

Основное окно мастера также содержит следующие интересные ссылки.

- Запрос пароля при пробуждении — отображает окно Системные параметры мастера Электропитание. С его помощью можно определить, будет ли выполняться автоматическая блокировка текущего сеанса работы пользователя при выходе из спящего режима (по умолчанию блокировка выполняется для всех стандартных режимов энергопотребления). Благодаря этому окну можно также определить действие, которое будет выполняться при нажатии кнопки выключения системного блока компьютера или ноутбука. По умолчанию выполняется выключение компьютера, однако вы можете изменить его на переход в спящий режим (Hibernate mode) или режим сна (Sleep mode).
- Укажите действие кнопок питания — с помощью данной ссылки также отображается окно Системные параметры мастера Электропитание.
- Создать план электропитания — позволяет создать свою собственную схему энергопотребления на основе одной из трех стандартных. При создании новой схемы нужно выбрать одну из стандартных схем, новое имя, а также время бездействия, через которое будет отключаться монитор или компьютер будет переходить в спящий режим.
- Укажите, когда следует отключать дисплей — отображает окно Изменить параметры плана мастера Электропитание. С его помощью можно изменить основные параметры работы схемы энергопотребления: время бездействия компьютера, после истечения которого будет отключаться монитор или компьютер будет переходить в спящий режим. Кроме того, с помощью ссылки Изменить дополнительные параметры питания можно отобразить окно Электропитание (рис. 7.6), позволяющее изменить остальные параметры работы схемы энергопотребления, которых намного больше, чем в предыдущих версиях операционных систем Windows.
- Настройки перехода в спящий режим — с помощью данной ссылки также отображается окно Изменить параметры плана мастера Электропитание.
- Изменение параметров плана — с помощью данной ссылки также отображается окно Изменить параметры плана мастера Электропитание.

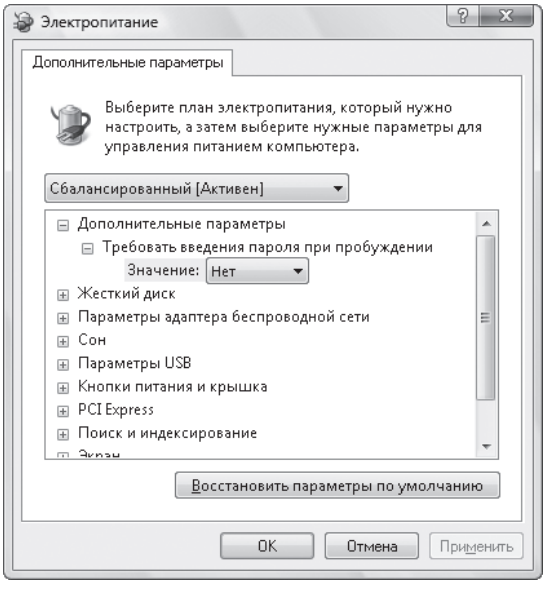


Рис. 7.6. Дополнительные настройки энергопотребления

Программа powercfg.exe

Для настройки энергопотребления компьютера можно также использовать программу командной строки `powercfg.exe`. Она поддерживает много возможностей, некоторые из них мы рассмотрим.

Просмотр сведений о схемах энергопотребления

С помощью первого набора настроек, которые мы рассмотрим, можно просмотреть сведения о режимах энергопотребления, используемых в операционной системе.

- `powercfg.exe -l` — отображает список зарегистрированных в операционной системе схем энергопотребления и их GUID-номера. Напротив схемы энергопотребления, используемой в данный момент, выводится звездочка.

  Каждая схема энергопотребления является дочерним подразделом ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes`. Название подраздела схемы и является ее GUID-номером. Активная же в данный момент схема содержится в параметре строкового типа `ActivePowerScheme`, расположенном в данной ветви реестра.

- `powercfg.exe -q <GUID-номер схемы энергопотребления>` — показывает сведения о работе определенной схемы энергопотребления. GUID-номер схемы можно узнать с помощью команды `powercfg.exe -l`. Если GUID-номер схемы не указывать, то будут отображены сведения о работе активной в данный момент схемы энергопотребления.

  После выполнения данной команды перед вами отобразится список всех настроек энергопотребления, которые можно изменить, их текущее значение, а также минимальное и максимальное значения.

Можно также воспользоваться разновидностью данной команды `powercfg.exe -q <GUID-номер схемы энергопотребления> <GUID-номер подкатегории>`, чтобы просмотреть значение определенной настройки данной схемы энергопотребления.

ПРИМЕЧАНИЕ

Параметр -q программы powercfg.exe отображает не все значения настроек схемы энергопотребления. Чтобы просмотреть полный список настроек схемы энергопотребления, нужно воспользоваться недокументированной командой powercfg.exe -qh.

- `powercfg.exe -GETSECURITYDESCRIPTOR <GUID-номер схемы энергопотребления>` — отображает идентификатор безопасности данной схемы энергопотребления.

  Идентификатор безопасности схемы энергопотребления содержится в параметре строкового типа, названном в честь GUID-номера схемы энергопотребления и расположенном в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\SecurityDescriptors`. Если данный параметр отсутствует в реестре, то используется идентификатор безопасности по умолчанию, хранящийся в параметре строкового типа `Default` данной ветви реестра.

- `powercfg.exe -GETACTIVESCHEME` — показывает активную в данный момент схему энергопотребления.
- `powercfg.exe -aliases` — отображает список всех GUID-номеров, назначенных настройкам и подкатегориям схем энергопотребления.

Изменение сведений о схемах энергопотребления

Следующий набор настроек позволяет изменить параметры работы схем энергопотребления.

- `powercfg.exe -changename <GUID-номер схемы энергопотребления> <новое название схемы> <новое описание схемы>` — изменяет название и описание схемы энергопотребления.

  Название схемы энергопотребления содержится в параметре строкового типа `FriendlyName`, расположенном в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes\<GUID-номер схемы энергопотребления>`.

  Описание схемы энергопотребления содержится в параметре строкового типа `Description`, расположенном в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes\<GUID-номер схемы энергопотребления>`.

- `powercfg.exe -SETSECURITYDESCRIPTOR <GUID-номер схемы энергопотребления> <строка SDDL>` — устанавливает новый идентификатор безопасности для данной схемы энергопотребления.

- `powercfg.exe -S <GUID-номер схемы энергопотребления>` — изменяет активную схему энергопотребления.
- `powercfg.exe -D <GUID-номер схемы энергопотребления>` — удаляет соответствующую схему энергопотребления.
- `powercfg.exe -DELETESETTING <GUID-номер подкатегории> <GUID-номер настройки>` — удаляет значение указанной настройки, хранящейся в подкатегории активной в данный момент схемы энергопотребления.
- `powercfg.exe -DUPLICATESCHEME <GUID-номер схемы энергопотребления>` — создает новую схему энергопотребления на основе указанной.
- `powercfg.exe -X <константа настройки> <новое значение>` — позволяет изменить значения параметров работы текущей схемы энергопотребления. Данная команда поддерживает следующие константы настроек.
  - `-monitor-timeout-ac` — определяет интервал простоя компьютера в минутах, по истечении которого монитор будет отключаться (при работе от сети).

    Данная константа изменяет значение параметра `REG_DWORD`-типа `ACSettingIndex` (хранится в секундах), расположенного в ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes\381b4222-f694-41f0-9685-ff5bb260df2e\7516b95f-f776-4464-8c53-06167f40cc99\3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e` (вы, наверное, догадались, что три последних подраздела данной ветви реестра — это GUID-номер схемы энергопотребления, GUID-номер подкатегории и GUID-номер настройки).
  - `-monitor-timeout-dc` — определяет интервал простоя компьютера в минутах, по истечении которого монитор будет отключаться (при работе от батареи).

    Данная константа изменяет значение параметра `REG_DWORD`-типа `DCSettingIndex` (хранится в секундах), расположенного в той же ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes\381b4222-f694-41f0-9685-ff5bb260df2e\7516b95f-f776-4464-8c53-06167f40cc99\3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e`.

    Остальные константы, описанные далее, изменяют такие же параметры реестра, но хранящиеся в других подразделах ветви `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes\<GUID-номер схемы энергопотребления>\<GUID-номер подкатегории>`, поэтому их мы рассматривать не будем.
  - `-disk-timeout-ac` — указывает интервал простоя компьютера в минутах, по истечении которого жесткий диск будет отключаться (при работе от сети).
  - `-disk-timeout-dc` — определяет интервал простоя компьютера в минутах, по истечении которого жесткий диск будет отключаться (при работе от батареи).

- `-standby-timeout-ac` — указывает интервал простоя компьютера в минутах, по истечении которого компьютер будет переходить в состояние сна (при работе от сети).
- `-standby-timeout-dc` — определяет интервал простоя компьютера в минутах, по истечении которого компьютер будет переходить в состояние сна (при работе от батареи).
- `-hibernate-timeout-ac` — указывает интервал простоя компьютера в минутах, по истечении которого компьютер будет переходить в спящий режим (при работе от сети).
- `-hibernate-timeout-dc` — определяет интервал простоя компьютера в минутах, по истечении которого компьютер будет переходить в спящий режим (при работе от батареи).

Настройка режимов работы компьютера: спящий режим и режим сна

Программа `powercfg.exe` поддерживает набор команд, позволяющих управлять работой компьютера в состояниях Hibernate (спящий режим) и Sleep (режим сна).

ПРИМЕЧАНИЕ

Раз уж мы заговорили о режимах энергопотребления, то также следует упомянуть о новом режиме снижения энергопотребления, присутствующем в операционной системе Windows Vista, — режиме сна (Sleep mode). В этом режиме операционная система заносит все содержимое оперативной памяти на жесткий диск (как при переходе в спящий режим (Hibernate mode)), но после этого электропитание еще некоторое время подается на оперативную память (в спящем режиме (Hibernate mode) после занесения содержимого оперативной памяти на диск компьютер сразу же выключается).

Информация о событиях, которые замедляют скорость входа и выхода из спящего режима, заносится в журнал подраздела Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Diagnosis-Performance. Все записи данного типа имеют категорию (Task Category) Standby Performance Monitor.

Программу можно использовать в виде команды `powercfg.exe -a`, которая отображает сведения о том, поддерживает ли ваш компьютер состояния сна уровней S1, S2 и S3.

Стандарт ACPI, который на данный момент уже поддерживается всеми производителями оборудования и используется в операционной системе Windows Vista, определяет шесть состояний, в которых может находиться операционная система и устройства компьютера. Это состояния от S0 до S5.

- S0 — компьютер работает в своем стандартном режиме (обычная работа компьютера), при котором питание подается на каждый компонент компьютера. Данное состояние, как правило, аналогично состоянию D0 для устройств.
- S1 — компьютер находится в состоянии сна. Данное состояние, как правило, аналогично состоянию D2 для устройств.
- S2 — компьютер находится в состоянии сна. Данное состояние, как правило, аналогично состоянию D2 для устройств.

- S3 — компьютер находится в глубоком состоянии сна. В этом состоянии процессор отключен. Данное состояние, как правило, аналогично состоянию D2 для устройств.
- S4 — компьютер находится в спящем режиме (Hibernate mode). Содержимое оперативной памяти помещено на жесткий диск (в файл `hiberfil.sys`, расположенный в корневом каталоге системного раздела), а компьютер полностью отключен. Это состояние ничем не отличается от состояния S5. Лишь в момент включения компьютера `ntldr` проверяет, содержит ли файл `hiberfil.sys` данные оперативной памяти. И если содержит, то эти данные помещаются обратно в оперативную память, и возобновляется работа операционной системы с того момента, на котором произошел переход в спящий режим. Данное состояние, как правило, аналогично состоянию D3 для устройств.
- S5 — компьютер полностью отключен. Для его включения нужно нажать кнопку электропитания. Данное состояние, как правило, аналогично состоянию D3 для устройств.

Итак, состояния уровней S0–S5 определяются ACPI. Состояния же уровней D0–D3 определяются производителями устройств. При этом производители устройства сами решают, какое состояние устройства (DX) будет соответствовать состоянию ACPI (SX). Такое соответствие называется сопоставлением энергосбережения.

Вы можете просмотреть сопоставление энергосбережения для определенного устройства с помощью консоли `devmgmt.msc`. Для этого нужно отобразить окно Свойства для конкретного устройства, отображаемого в данной оснастке, и перейти на вкладку Сведения данного окна. После этого в раскрывающемся списке Свойство выбрать элемент Сведения о питании (рис. 7.7). Это приведет к отображению в поле Значение такой информации, как сопоставление энергосбережения (Сопоставления энергосбережения), а также состояние, в котором в данный момент находится устройство (Текущее состояние электропитания).

- `powercfg.exe -DEVICEQUERY <константа состояния флагов>` — отображает список устройств компьютера, которые поддерживают те или иные состояния флагов, указанные в константе. Можно использовать следующие константы, отображающие список устройств, которые:
  - `wake_from_S1_supported` — могут пробуждать компьютер от состояния сна S1;
  - `wake_from_S2_supported` — могут пробуждать компьютер от состояния сна S2;
  - `wake_from_S3_supported` — могут пробуждать компьютер от состояния сна S3;
  - `wake_from_any` — могут пробуждать компьютер из любого состояния сна;
  - `S1_supported` — поддерживают состояние S1;
  - `S2_supported` — поддерживают состояние S2;
  - `S3_supported` — поддерживают состояние S3;

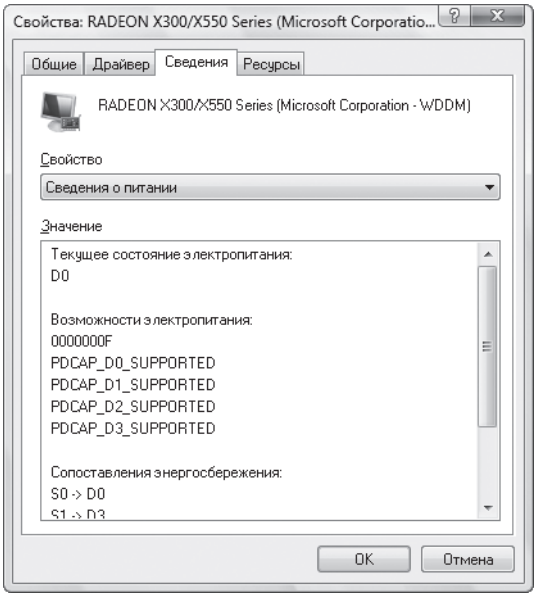


Рис. 7.7. Отображение сопоставления состояний SX и DX

- `S4_supported` — поддерживают состояние S4 (спящий режим);
- `wake_programmable` — поддерживают возможность пользовательской настройки вывода компьютера из спящего режима любого уровня;
- `wake_armed` — в данный момент настроены на вывод компьютера из состояния спящего режима любого уровня;
- `all_devices` — отображает список всех устройств компьютера;
- `all_devices_verbose` — список всех устройств компьютера, а также настройки каждого устройства (имя драйвера, имя производителя, номер шины, поддерживаемые уровни спящего режима и многое другое).

- `powercfg.exe -DEVICEENABLEWAKE|-DEVICEDISABLEWAKE <название устройства>` — разрешает (или запрещает) указанному устройству пробуждать компьютер от спящего режима. Имя устройства можно попробовать узнать с помощью параметра `-DEVICEQUERY` данной программы.

ПРИМЕЧАНИЕ

Разрешить (или запретить) устройству выводить компьютер из состояния сна можно и с помощью оболочки операционной системы. Для этого нужно воспользоваться окном Свойства устройства (отображается с помощью консоли devmgmt.msc). Если устройство поддерживает возможность вывода компьютера из состояния сна, то в окне Свойства будет присутствовать вкладка Управление электропитанием, которая будет содержать флажок Разрешить устройству выводить компьютер из ждущего режима

Вкладка Управление электропитанием для некоторых устройств (например, для USB Root HUB) может также содержать флажок Разрешить отключение этого устройства

для экономии энергии. С его помощью можно определить, разрешено ли операционной системе отключать питание устройства (если оно не используется определенное время) для уменьшения энергопотребления.

- `powercfg.exe /lastwake` — выводит информацию о последнем переходе в спящий режим.
- `powercfg.exe -H ON|OFF` — позволяет разрешить или запретить возможность перехода в спящий режим.

Другие возможности программы

С помощью следующей команды можно изменить дополнительные настройки энергопотребления.

`powercfg.exe -export|-import <путь к файлу и его имя> <GUID-номер схемы энергопотребления>` — экспортирует (импортирует) настройки конкретной схемы энергопотребления в файл (из файла в реестр).

Недокументированные возможности программы

Данная программа поддерживает несколько команд, которые не описаны в справке, отображаемой после ввода команды `powercfg.exe /?`. Эти команды в некотором случае могут быть полезны, поэтому рассмотрим их.

- `powercfg.exe -restoredefaultschemes` — удаляет все созданные пользователем схемы энергопотребления и восстанавливает настройки трех стандартных схем энергопотребления операционной системы Windows Vista (или тех схем, которыми были заменены стандартные схемы энергопотребления с помощью команды `powercfg.exe -replacedefaultschemes`).

  Настройки схем энергопотребления, используемых по умолчанию, содержатся в подразделах ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\User\Default\PowerSchemes`.
- `powercfg.exe -restoreindividualdefaultscheme <GUID-номер схемы энергопотребления>` — удаляет указанную в команде схему энергопотребления и заменяет ее используемой операционной системой по умолчанию.
- `powercfg.exe -replacedefaultschemes` — заменяет настройки схем энергопотребления, применяемых операционной системой по умолчанию, текущими настройками. После выполнения данной команды схемами по умолчанию станут схемы с настройками, указанными в данный момент.
- `powercfg.exe -SetPowerValueMax <GUID-номер подкатегории> <GUID-номер настройки> <новое максимальное значение настройки>` — изменяет максимальное значение, которое можно установить для данной настройки.

  Команда изменяет значение, хранящееся в параметре `REG_DWORD`-типа `ValueMax`, расположенном в ветви системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings\<GUID-номер схемы энергопотребления>\<GUID-номер подкатегории>`.

- `powercfg.exe -SetPowerValueMin <GUID-номер подкатегории> <GUID-номер настройки> <новое минимальное значение настройки>` — изменяет минимальное значение, которое можно установить для данной настройки.

  Данная команда изменяет значение, хранящееся в параметре `REG_DWORD`-типа `ValueMin`, расположенном в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings\<GUID-номер схемы энергопотребления>\<GUID-номер подкатегории>`.

- `powercfg.exe -SetPowerValueIncrement <GUID-номер подкатегории> <GUID-номер настройки> <новое значение шага>` — изменяет шаг, с которым можно увеличивать значение данной настройки.

  Команда изменяет значение, хранящееся в параметре `REG_DWORD`-типа `ValueIncrement`, расположенном в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings\<GUID-номер схемы энергопотребления>\<GUID-номер подкатегории>`.

- `powercfg.exe -SavePoliciesToDefaultUser` — сохраняет настройки для пользователя по умолчанию. Эта команда может выполняться только системной учетной записью.

Групповые политики

Настроить параметры энергопотребления можно и с помощью групповых политик, описанных в файле `Power.admx` и расположенных в разделе **Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Управление электропитанием** и его дочерних подразделах.

Политики данного подраздела изменяют значения параметров `REG_DWORD`-типа `ACSettingIndex` (настройки при питании от сети) и `DCSettingIndex` (настройки при питании от батареи), расположенных в подразделах `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings`. В зависимости от подраздела, в котором они находятся, определяется и выполняемое ими действие. Например, они могут находиться в следующих подразделах.

- `6738E2C4-E8A5-4A42-B16A-E040E769756E` — параметры этого подраздела определяют интервал бездействия жесткого диска (в секундах), по истечении которого он будет отключен.
- `3C0BC021-C8A8-4E07-A973-6B14CBCB2B7E` — его параметры указывают интервал бездействия компьютера (в секундах), по истечении которого монитор будет отключен.
- `5CA83367-6E45-459F-A27B-476B1D01C936` — параметры этого подраздела определяют действие, которое будет выполняться при закрытии крышки ноутбука. Например, если значение параметра равно `3`, то компьютер выключится. Если значение параметра равно `2`, то компьютер перейдет в спящий режим. А если значение параметра равно `1`, то произойдет переход в режим сна. Также значения параметров этого подраздела могут быть равными `0`. В этом случае никаких действий не произойдет.

- 96996BC0-AD50-47EC-923B-6F41874DD9EB — его параметры указывают действие, которое будет выполняться при нажатии пользователем кнопки перехода в режим сна. Например, если значение параметра равно 3, то компьютер выключится. Если значение параметра равно 2, то произойдет переход в спящий режим. А если значение параметра равно 1, то компьютер перейдет в режим сна. Также значения параметров этого подраздела могут быть равными 0. В этом случае никаких действий не произойдет.
- A7066653-8D6C-40A8-910E-A1F54B84C7E5 — параметры этого подраздела определяют действие, которое будет выполняться при нажатии пользователем кнопки выключения, расположенной в меню Пуск. Например, если значение параметра равно 2, то компьютер выключится. Если значение параметра равно 1, то произойдет переход в спящий режим. А если значение параметра равно 0, то компьютер перейдет в режим сна.
- 7648EFA3-DD9C-4E3E-B566-50F929386280 — его параметры указывают действие, которое будет выполняться при нажатии пользователем кнопки выключения компьютера, расположенной на системном блоке. Например, если значение параметра равно 3, то компьютер выключится. Если значение параметра равно 2, то компьютер перейдет в спящий режим. А если значение параметра равно 1, то произойдет переход в режим сна. Также значения параметров этого подраздела могут быть равными 0. В этом случае никаких действий не произойдет.
- 29F6C1DB-86DA-48C5-9FDB-F2B67B1F44DA — параметры этого подраздела определяют интервал бездействия компьютера (в секундах), по истечении которого операционная система перейдет в режим сна.
- 9D7815A6-7EE4-497E-8888-515A05F02364 — параметры указывают интервал бездействия компьютера (в секундах), по истечении которого операционная система перейдет в спящий режим.
- 90959D22-D6A1-49B9-AF93-BCE885AD335B — его параметры определяют, будет ли выключено адаптивное время ожидания выключения монитора.
- 0e796bdb-100d-47d6-a2d5-f7d2daa51f51 — параметры этого подраздела указывают, будет ли операционная система требовать ввода пароля при выходе из спящего режима.
- abfc2519-3608-4c2a-94ea-171b0ed546ab — его параметры определяют, будут ли разрешены режимы сна S1–S3 при простое компьютера.
- B7A27025-E569-46c2-A504-2B96CAD225A1 — параметры этого подраздела указывают, будет ли операционная система разрешать различным программам препятствовать переходу в режим сна.
- 94ac6d29-73ce-41a6-809f-6363ba21b47e — его параметры определяют, будет использоваться режим сна или ждущий режим.
- 9A66D8D7-4FF7-4EF9-B5A2-5A326CA2A469 — параметр этого подраздела (в нем может находиться только параметр DCSettingIndex) определяет уровень заряда батареи, при котором будет выдаваться сигнал почти полной разрядки батареи.

- `8183ba9a-e910-48da-8769-14ae6dc1170a` — его параметр (в нем может находиться только параметр `DCSettingIndex`) указывает уровень заряда батареи, при котором будет выдаваться сигнал низкого заряда батареи.
- `bcded951-187b-4d05-bccc-f7e51960c258` — параметр этого подраздела (в нем может находиться только параметр `DCSettingIndex`) определяет, будет ли выдаваться уведомление при низком заряде батареи.
- `637EA02F-BBCB-4015-8E2C-A1C7B9C0B546` — его параметр (в нем может находиться только параметр `DCSettingIndex`) указывает действие, которое будет выполняться при почти полной разрядке батареи. Например, если значение параметра равно `3`, то компьютер выключится. Если значение параметра равно `2`, то произойдет переход в спящий режим. А если значение параметра равно `1`, то компьютер перейдет в режим сна. Также значения параметров этого подраздела могут равняться `0`. В этом случае никаких действий не произойдет.
- `d8742dcb-3e6a-4b3c-b3fe-374623cdcf06` — параметр этого подраздела (в нем может находиться только параметр `DCSettingIndex`) определяет действие, которое будет выполняться при низком заряде батареи. Например, если значение параметра равно `3`, то компьютер выключится. Если значение параметра равно `2`, то компьютер перейдет в спящий режим. А если значение параметра равно `1`, то произойдет переход в режим сна. Также значения параметров этого подраздела могут равняться `0`. В этом случае никаких действий не произойдет.

Мастер Родительский контроль

Нововведением операционной системы Windows Vista является мастер Родительский контроль, с помощью которого вы можете ограничить возможности любой пользовательской учетной записи, не имеющей прав администратора. Отобразить данный мастер можно с помощью одноименного значка папки Панель управления.

ПРИМЕЧАНИЕ

Если ваш компьютер подключен к домену Active Directory, то по умолчанию значок Родительский контроль не будет отображаться в папке Панель управления. Чтобы его отобразить, нужно воспользоваться групповой политикой Сделать компонент "Родительский контроль" панели управления видимым в домене, расположенной в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Родительский контроль и описанной в файле ParentalControls.admx.

Данная политика устанавливает значение параметра REG_DWORD-типа WPCEnableOnDomain, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ParentalControls, равным 1.

Информация от компонента Родительский контроль заносится в журнал подраздела Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ ParentalControls.

Основное окно мастера содержит список учетных записей, доступных на компьютере (как пользовательских, так и административных, хотя повторю, что администт-

ративные учетные записи ограничивать нельзя). Вы можете как выбрать учетную запись, которую нужно ограничить, из списка, так и создать новую учетную запись. Для этого применяется ссылка Создать новую учетную запись. После ее выбора мастер предложит вам указать имя новой учетной записи, после чего нужно нажать кнопку Создать учетную запись. Это приведет к созданию новой учетной записи пользовательского типа, не ограниченной паролем, к настройкам родительского контроля для которой вы сразу же и перейдете (рис. 7.8).

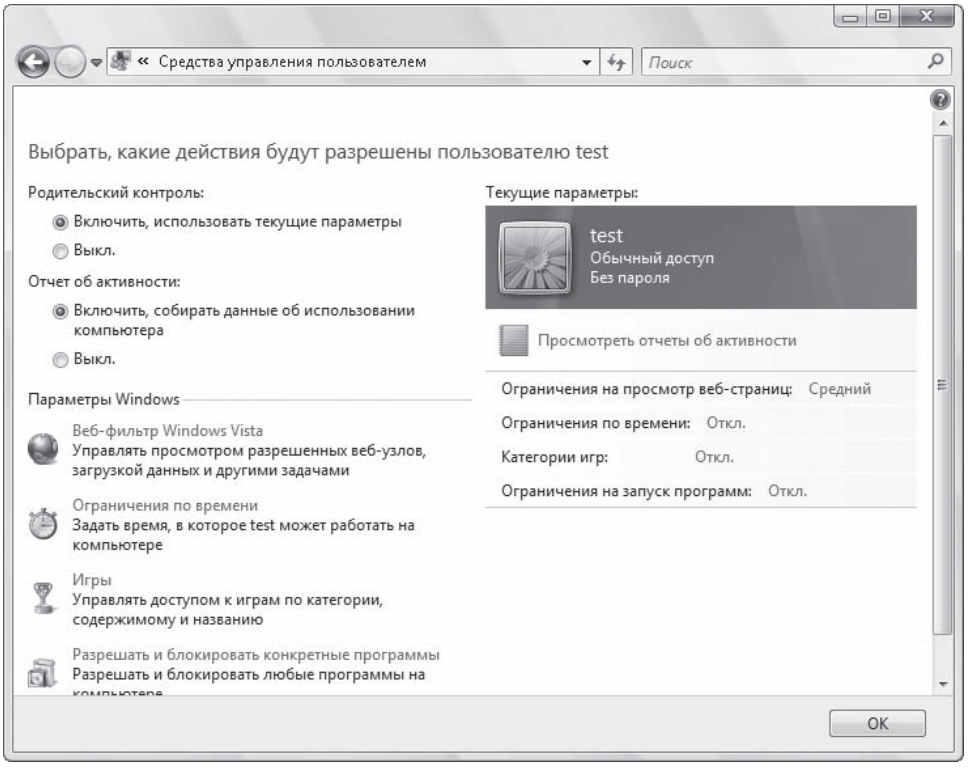


Рис. 7.8. Настройки родительского контроля

Окно настроек родительского контроля содержит два основных переключателя.

- Родительский контроль — позволяет включить или отключить функции родительского контроля для данной учетной записи пользователя. По умолчанию функции родительского контроля отключены (переключатель установлен в положение Выкл.).
- Отчет об активности — если функции родительского контроля включены, то с помощью данного переключателя можно определить, будут ли сохраняться действия данного пользователя в файле. Если данный переключатель установить в положение Включить, собирать данные об использовании компьютера, то вы сможете просмотреть сведения о работе пользователя с помощью значка Отчет об активности данного мастера.

Диалоговое окно настроек родительского контроля также содержит следующие значки и ссылки.

- Веб-фильтр Windows Vista — позволяет перейти в окно Ограничения на просмотр веб-страниц, с помощью которого можно наложить ограничения на сайты, разрешенные для просмотра данному пользователю, а также определить, разрешено ли ему загружать файлы из Интернета. Вы можете как выбрать определенный уровень безопасности (с помощью переключателя Выберите уровень ограничений для веб-узлов), так и самостоятельно указать блокируемое содержимое веб-страниц (алкоголь, порнография, курение, чаты, почтовые службы, оружие, насилие и т. д.). Кроме того, с помощью ссылки Изменить список разрешенных и запрещенных веб-узлов можно вручную указать список URL-адресов веб-сайтов, доступ к которым запрещен или разрешен пользователю. После выбора настроек нужно нажать кнопку OK.
- Ограничение по времени — разрешает указать дни и время, когда данному пользователю можно входить в систему. Для этого вы переходите в окно Ограничение по времени, содержащее таблицу дней (строки) и часов (столбцы). По умолчанию пользователю разрешено входить в любое время. Чтобы указать время, когда доступ пользователю запрещен, нужно провести указателем мыши с нажатой левой кнопкой мыши по соответствующим ячейкам таблицы. После выбора настроек нужно нажать кнопку OK.
- Игры — позволяет указать игровой рейтинг, на основе которого будет определяться, разрешено ли данному пользователю играть в соответствующую игру. По умолчанию используется рейтинг Для старшего возраста, однако вы можете изменить рейтинг, щелкнув кнопкой мыши на ссылке Задать категории для игр окна Средства управления играми. В операционной системе Windows Vista классификация рейтингов производится на основе возраста играющего. Например, рейтинг Для старшего возраста предназначен для лиц, не достигших 18 лет (это самый старший рейтинг из имеющихся в операционной системе Windows Vista), рейтинг Для всех предназначен для лиц, не достигших 6 лет, а рейтинг Для детей предназначен для лиц, не достигших трех лет. Кроме того, в окне выбора рейтинга вы также можете определить направления игр, доступ к которым пользователю запрещен. Для этого нужно воспользоваться флажками поля Блокировать эти типы содержимого.
- Разрешать и блокировать конкретные программы — благодаря этому значку вы можете указать список программ, которые можно запускать пользователю. По умолчанию ему можно запускать любые программы.
- Просмотреть отчеты об активности — отображает сведения о работе данного пользователя за последние семь дней (по умолчанию). После выбора данного значка вы перейдете в окно Средство просмотра действий пользователя. Оно содержит два поля. Левое поле отображает дерево рапортов. В правом же поле можно просмотреть содержимое этих рапортов. Кроме того, с помощью кнопки Создать отчет панели инструментов окна вы можете создать HTML-файл, содержащий сведения о работе пользователя.

  Обратите также внимание на ссылку Параметры семейной безопасности, отображаемую на левой панели основного окна мастера Родительский контроль. После

ее выбора отобразится окно Параметры семейной безопасности, позволяющее указать количество дней, информация за которые будет отображаться в окне Средство просмотра действий пользователя.

Работа с WMI

Для работы с компонентом Родительский контроль можно использовать новые классы репозитария управления CIM. Они находятся в пространстве имен `\\.\root\cimv2\Applications\WindowsParentalControls`.

Класс WpcRating

Класс поддерживает следующие свойства.

- `ID`, тип: `string` — является ключевым. Оно определяет CLSID-номер родительского рейтинга.
- `LongName`, тип: `string` — определяет длинное имя родительского рейтинга.
- `SystemID`, тип: `string` — является ключевым. Оно определяет CLSID-номер системного рейтинга, которому принадлежит данный рейтинг.
- `ShortName`, тип: `string` — указывает короткое имя родительского рейтинга.
- `Description`, тип: `string` — содержит описание данного рейтинга.
- `IsDeprecated`, тип: `string` — если значение данного свойства равно `true`, то рейтинг является осуждающим. По умолчанию значение данного свойства равно `false`.
- `UpdatedRating`, тип: `string` — определяет адрес, используемый для обновления рейтинга.
- `Level`, тип: `uint32` — указывает относительный индексный уровень данного рейтинга.
- `MinAge`, тип: `uint32` — определяет минимальный возраст рейтинга. По умолчанию значение данного свойства равно `0`.
- `IconPath`, тип: `string` — содержит путь к изображению для системного рейтинга.
- `IconResourceID`, тип: `string` — хранит идентификатор ресурса изображения для системного рейтинга.
- `IconType`, тип: `string` — содержит тип расширения изображения для системного рейтинга.

Класс WpcRatingsDescriptor

Класс содержит следующие свойства.

- `ID`, тип: `string` — определяет идентификатор дескриптора.
- `SystemID`, тип: `string` — является ключевым. Оно содержит CLSID-номер, представляющий дескриптор, определяющий системный рейтинг.
- `Name`, тип: `string` — хранит имя дескриптора.
- `Description`, тип: `string` — содержит описание дескриптора.

- `IsDeprecated`, тип: `string` — если значение данного свойства равно `true`, то дескриптор является осуждающим. По умолчанию значение свойства равно `false`.
- `UpdatedDescriptor`, тип: `string` — определяет адрес, используемый для обновления дескриптора.
- `IconPath`, тип: `string` — содержит путь к изображению для системного рейтинга.
- `IconResourceID`, тип: `string` — хранит идентификатор ресурса изображения для системного рейтинга.
- `IconType`, тип: `string` — содержит тип изображения для системного рейтинга.

Класс WpcRatingsSystem

Класс поддерживает следующие свойства.

- `ID`, тип: `string` — является ключевым. Оно содержит CLSID-номер, идентифицирующий системный рейтинг.
- `Type`, тип: `uint32` — определяет тип системного рейтинга.
- `LongName`, тип: `string` — указывает длинное имя системного рейтинга.
- `ShortName`, тип: `string` — определяет короткое имя системного рейтинга.
- `Description`, тип: `string` — содержит описание данного системного рейтинга.
- `WebAddress`, тип: `string` — указывает адрес системного рейтинга.
- `LogoPath`, тип: `string` — хранит путь к изображению данного системного рейтинга.
- `LogoResourceID`, тип: `string` — содержит идентификатор ресурса изображения для данного системного рейтинга.
- `LogoResourceType`, тип: `string` — хранит тип файла ресурса для данного системного рейтинга.
- `Version`, тип: `string` — определяет версию рейтинга.

Класс WpcSystemSettings

Значения свойств данного класса доступны как для чтения, так и для записи.

- `CurrentGamesRatingSystem`, тип: `string` — содержит CLSID-номер текущего игрового системного рейтинга.
- `HTTPExemptionList`, тип: массив строковых значений — хранит фильтр освобожденных HTTP-адресов.
- `URLExemptionList`, тип: массив строковых значений — содержит фильтр освобожденных URL-адресов.
- `LogViewReminderInterval`, тип: `uint32` — определяет количество дней до возникновения напоминания проверки файлов журналов.

- UMIEnabled, тип: boolean — указывает, включен ли пользовательский мониторинг.
- LastLogView, тип: datetime — определяет дату последней проверки файлов журналов.
- FilterID, тип: string — указывает CLSID-номер текущего веб-фильтра.
- FilterName, тип: string — определяет имя текущего веб-фильтра.

Данный класс также поддерживает следующие методы.

- AddUser — создает настройки для новой учетной записи пользователя.

  Входящий параметр: строковый параметр, определяющий SID пользователя.

  Возвращаемые параметры: нет.
- RemoveUser — удаляет настройки для учетной записи пользователя.

  Входящий параметр: строковый параметр, определяющий SID пользователя.

  Возвращаемые параметры: нет.

Класс WpcUserSettings

Класс содержит следующие свойства.

- SID, тип: string — является ключевым, доступно только для чтения. Определяет SID учетной записи пользователя, для которого предназначены настройки, описанные экземпляром данного класса.
- WpcEnabled, тип: boolean — указывает, включен ли родительский контроль для данного пользователя.
- LoggingRequired, тип: boolean — определяет, включена ли запись файла журнала для данного пользователя.
- HourlyRestrictions, тип: boolean — указывает, установлен ли вход по определенным часам для данного пользователя.
- OverrideRequests, тип: boolean — определяет, включены ли доминирующие запросы для данного пользователя.
- LogonHours, тип: массив из семи значений типа uint32 — указывает часы, в которые данный пользователь может входить в систему.
- AppRestrictions, тип: boolean — определяет, запрещен ли пользователю запуск приложений.

Класс WpcExtension

Класс поддерживает следующие свойства.

- ID, тип: string — является ключевым, доступно только для чтения. Содержит идентификатор расширения.
- Silo, тип: uint32 — свойство является ключевым, доступно только для чтения. Содержит идентификатор Silo для данного расширения. Данное свойство может принимать значения от 0 до 6.

- `ImagePath`, тип: `string` — указывает путь к изображению для данного расширения.
- `Path`, тип: `string` — определяет путь к исполняемому файлу расширения.
- `Name`, тип: `string` — содержит имя расширения.
- `SubTitle`, тип: `string` — хранит подзаголовок для расширения.

Класс WpcGameOverride

Класс содержит следующие свойства.

- `AppID`, тип: `string` — является ключевым. Содержит идентификатор приложения (игры).
- `SID`, тип: `string` — свойство является ключевым. Содержит SID учетной записи.
- `Allowed`, тип: `uint32` — доступно как для чтения, так и для записи. Оно определяет, разрешено или запрещено данное приложение. Свойство может принимать значения от `0` до `2`.

Класс WpcAppOverride

Значения свойств данного класса поддерживают только чтения.

- `RuleID`, тип: `string` — свойство является ключевым. Содержит идентификатор правила.
- `SID`, тип: `string` — является ключевым. Хранит SID учетной записи.
- `Path`, тип: `string` — содержит путь к доминирующему приложению.

Класс WpcGamesSettings

Класс поддерживает следующие свойства.

- `SID`, тип: `string` — является ключевым, доступно только для чтения. Содержит SID учетной записи.
- `Blocked`, тип: `boolean` — определяет, разрешена или запрещена данная игра.
- `SystemID`, тип: `string` — свойство является ключевым, доступно только для чтения. Определяет CLSID-номер системного рейтинга, используемого для данных настроек.
- `AllowUnrated`, тип: `boolean` — указывает, разрешен ли запуск программы без определения рейтинга.
- `MaxAllowed`, тип: `string` — определяет идентификатор максимального рейтинга, доступного для данной системы.
- `DeniedDescriptors`, тип: массив значений строкового типа — содержит коллекцию запрещенных дескрипторов.

Класс WpcURLOverride

Класс поддерживает следующие свойства.

- `URL`, тип: `string` — является ключевым. Определяет URL-адрес, доступ к которому запрещен или разрешен для определенной учетной записи пользователя.

- SID, тип: string — свойство является ключевым. Содержит SID учетной записи.
- Allowed, тип: uint32 — значение данного свойства доступно как для чтения, так и для записи. Указывает, разрешено или запрещено данное приложение. Данное свойство может принимать значения от 0 до 2.

Класс WpcWebSettings

Класс содержит следующие свойства.

- SID, тип: string — является ключевым, доступно только для чтения. Хранит SID учетной записи.
- FilterOn, тип: boolean — определяет, включен ли фильтр для данного пользователя.
- FilterLevel, тип: uint32 — указывает уровень фильтра. Данное свойство может принимать значения от 0 до 5.
- FileDownloadsBlocked, тип: boolean — определяет, запрещено ли пользователю загружать файлы.
- BlockUnrated, тип: boolean — указывает, может ли пользователь получить доступ ко всем сайтам, которые не содержатся в назначенном для него рейтинге.
- BlockedCategoryList, тип: массив значений типа uint32 — содержит список заблокированных категорий.

Класс WpcClamper

Класс содержит метод LockDownGameInstance, который блокирует исключение, определенное соответствующим экземпляром данного класса.

Входящий параметр: строковый параметр, определяющий идентификатор исключения.

Возвращаемые параметры: нет.

Работа с автономными файлами

В операционной системе Windows Vista, как и в предыдущих версиях, присутствует возможность работы с автономными файлами. Автономные файлы — это сетевые файлы, доступ к которым можно получить даже в том случае, если удаленный компьютер, на котором они находятся, сейчас недоступен. В этом случае вы получаете доступ к копии файла, которая находится на вашем компьютере, а при получении доступа к удаленному компьютеру копия файла синхронизируется с оригиналом.

ПРИМЕЧАНИЕ

Информация о работе с автономными файлами заносится в журнал подраздела Applications and Services Logs ▸ Microsoft ▸ Windows ▸ OfflineFiles.

Если работа с автономными файлами разрешена, то для создания автономного файла или каталога нужно в контекстном меню файла или каталога удаленного

компьютера выбрать команду Сделать доступными автономно. После этого отобразится окно, выполняющее синхронизацию выбранного файла или каталога. Сведения о результате синхронизации можно просмотреть в мастере Центр синхронизации, который мы рассмотрим далее.

Окно Автономные файлы

Если раньше получить доступ к настройкам автономных файлов можно было с помощью вкладки окна Свойства папки, то теперь она не существует. Для доступа к настройкам автономных файлов нужно использовать значок Автономные файлы папки Панель управления. После выбора данного значка отобразится окно Автономные файлы, содержащее следующие вкладки.

ПРИМЕЧАНИЕ

Окно Автономные файлы можно также отобразить, введя команду rundll32.exe cscui.dll, CSCOptions_RunDLL.

- Общие — позволяет включить или отключить механизм автономных файлов, а также открыть мастер Центр синхронизации или каталог Папка автономных файлов (хранит список ваших автономных файлов, а также автономных файлов других компьютеров).
- Использование диска — отображает количество места на диске, которое может занимать каталог автономных файлов (а также временных файлов), а также используемое в данный момент количество места на диске. Кроме того, с помощью данной вкладки вы можете изменить размер места на диске, доступный автономным файлам (по умолчанию 12% от общего объема диска), а также удалить временные файлы.
- Шифрование — позволяет зашифровать или расшифровать автономные файлы. Чтобы зашифровать файлы, достаточно нажать кнопку Зашифровать. Если же нужно расшифровать файлы, то необходимо воспользоваться кнопкой Расшифровать.
- Сеть — дает возможность определить, будет ли выполняться автоматическая проверка медленного соединения, а также интервал проверки в минутах.

Мастер Центр синхронизации

Мастер Центр синхронизации можно отобразить с помощью одноименного значка папки Панель управления.

С помощью мастера Центр синхронизации можно просмотреть сведения о прошедших процессах синхронизации автономных файлов, а также выполнить новый процесс синхронизации (с помощью кнопки Синхронизировать все) или остановить проходящий в данный момент (кнопка Остановить все).

Основное окно мастера содержит следующие значки.

- Настройка синхронизации (аналогичен ссылке Настройка новой связи синхронизации) — устанавливает новую синхронизацию.

- Результаты синхронизации (аналогичен ссылке Просмотр результатов синхронизации) — отображает результаты прошедших в данный сеанс работы пользователя процессов синхронизации.
- Конфликты (аналогичен ссылке Просмотр конфликтов синхронизации) — выводит список конфликтов, произошедших в данный сеанс работы пользователя процессов синхронизации.

Кроме того, в поле Папки основного окна мастера Центр синхронизации отображается список каталогов, которые можно синхронизировать. Если автономные файлы включены, то в этом поле отображается папка Автономные файлы. С помощью контекстного меню данной папки можно выполнить синхронизацию автономных файлов или назначить ее на определенное время. Если же вы откроете данную папку, то сможете просмотреть список автономных файлов, а также отключить их.

Классы WMI

Напоследок стоит заметить, что теперь доступ к автономным файлам и их настройкам можно получить с помощью инструментария управления Windows (WMI). Для этого в пространство имен `\\root\cimv2` были добавлены новые классы, наиболее интересные свойства и методы которых описаны ниже.

Класс Win32_OfflineFilesFileSysInfo

Данный класс содержит сведения об автономных файлах, имеющихся на локальном компьютере. Он поддерживает следующие свойства, доступные только для чтения, которые возвращают:

- `LocalAttributes`, тип: `uint32` — атрибуты копии локального автономного файла;
- `LocalChangeTime`, тип: `datetime` — время последнего изменения локальной копии автономного файла;
- `LocalCreationTime`, тип: `datetime` — время создания локальной копии автономного файла;
- `LocalLastAccessTime`, тип: `datetime` — время последнего доступа к локальной копии автономного файла;
- `LocalLastWriteTime`, тип: `datetime` — время последнего изменения локальной копии автономного файла;
- `LocalSize`, тип: `sint64` — размер (в байтах) локальной копии автономного файла;
- `OriginalAttributes`, тип: `uint32` — атрибуты автономного файла-оригинала;
- `OriginalChangeTime`, тип: `datetime` — время последнего изменения автономного файла-оригинала;
- `OriginalCreationTime`, тип: `datetime` — время создания автономного файла-оригинала;
- `OriginalLastAccessTime`, тип: `datetime` — время последнего доступа к автономному файлу-оригиналу;

- `OriginalLastWriteTime`, тип: `datetime` — время последнего изменения автономного файла-оригинала;
- `OriginalSize`, тип: `sint64` — размер автономного файла-оригинала в байтах;
- `RemoteAttributes`, тип: `uint32` — атрибуты копии удаленного автономного файла;
- `RemoteChangeTime`, тип: `datetime` — время последнего изменения удаленной копии автономного файла;
- `RemoteCreationTime`, тип: `datetime` — время создания удаленной копии автономного файла;
- `RemoteLastAccessTime`, тип: `datetime` — время последнего доступа к удаленной копии автономного файла;
- `RemoteLastWriteTime`, тип: `datetime` — время последнего изменения удаленной копии автономного файла;
- `RemoteSize`, тип: `sint64` — размер (в байтах) удаленной копии автономного файла.

Класс Win32_OfflineFilesPinInfo

Содержит сведения о принадлежности автономного файла определенным объектам. Он поддерживает следующие свойства, доступные только для чтения.

- `Pinned`, тип: `boolean` — указывает принадлежность данного автономного файла.
- `PinnedForComputer`, тип: `uint32` — определяет, принадлежит ли данный автономный файл всем пользователям компьютера. Возможными значениями данного свойства являются: принадлежит, не принадлежит, состояние унаследовано.
- `PinnedForFolderRedirection`, тип: `uint32` — указывает, можно ли пользователю применять компонент перенаправления папки операционной системы для данного автономного файла. Возможными значениями данного свойства являются: принадлежит, не принадлежит, состояние унаследовано.
- `PinnedForUser`, тип: `uint32` — определяет, принадлежит ли данный автономный файл текущему пользователю. Возможными значениями данного свойства являются: принадлежит, не принадлежит, состояние унаследовано.
- `PinnedForUserByPolicy`, тип: `uint32` — указывает, принадлежит ли данный автономный файл текущему пользователю на основе состояния групповой политики. Возможными значениями данного свойства являются: принадлежит, не принадлежит, состояние унаследовано.

Класс Win32_OfflineFilesChangeInfo

Содержит описание возможностей изменения локальной копии автономного файла. Он поддерживает следующие свойства, доступные только для чтения, которые указывают:

- `CreatedOffline`, тип: `boolean` — разрешено ли создавать автономный файл, если сетевой доступ к оригинальной копии автономного файла отсутствует;

- `DeletedOffline`, тип: `boolean` — разрешено ли удалять автономный файл, если сетевой доступ к оригинальной копии автономного файла отсутствует;
- `Dirty`, тип: `boolean` — была ли изменена копия автономного файла, пока доступ к ее оригиналу отсутствовал;
- `ModifiedAttributes`, тип: `boolean` — разрешено ли изменять автономный файл, если сетевой доступ к оригинальной копии автономного файла отсутствует;
- `ModifiedData`, тип: `boolean` — было ли изменено содержимое копии автономного файла, пока доступ к ее оригиналу отсутствовал;
- `ModifiedTime`, тип: `boolean` — была ли изменена временная метка копии автономного файла, пока доступ к ее оригиналу отсутствовал.

Класс Win32_OfflineFilesConnectionInfo

Содержит сведения о состоянии сетевого подключения для данного автономного файла. Он поддерживает следующие свойства, доступные только для чтения, которые определяют текущее состояние.

- `ConnectState`, тип: `uint32` — сетевого подключения к оригиналу данного автономного файла; возможны следующие значения данного свойства: неизвестно, сетевое подключение отсутствует и работа ведется с копией файла, сетевое подключение установлено и работа ведется с оригиналом автономного файла.
- `OfflineReason`, тип: `uint32` — доступа к автономным файлам; возможны следующие значения данного свойства: неизвестно, значение свойства не применимо, работа в автономном режиме, работа по медленному соединению, сетевое подключение отсутствует, необходима синхронизация, элемент приостановлен.

Класс Win32_OfflineFilesSuspendInfo

Класс содержит сведения о приостановленной синхронизации элемента. Он поддерживает следующие свойства, доступные только для чтения.

- `Suspended`, тип: `boolean` — определяет, приостановлена ли синхронизация элемента в данный момент.
- `SuspendedRoot`, тип: `boolean` — указывает, приостановлено ли дерево элементов.

Класс Win32_OfflineFilesProgress

Содержит сведения о текущем состоянии синхронизации автономного файла. Класс поддерживает следующие свойства, доступные только для чтения.

- `CallbackReason`, тип: `uint32` — определяет, поддерживает ли автономный файл обратный вызов. Возможные значения: `Progress` и `SyncConflictResolution`.
- `ProgressReason`, тип: `uint32` — указывает текущее состояние связи с оригиналом автономного файла. Возможные значения данного свойства: начало, окончание, элемент начала, элемент окончания.
- `Result`, тип: `uint32` — определяет код результата операции синхронизации.

Этот класс также поддерживает одно свойство, доступное как для чтения, так и для записи. Это свойство `Abort`, имеющее тип `boolean`, которое позволяет остановить операцию синхронизации данного автономного файла.

Класс Win32_OfflineFilesSimpleProgress

Класс содержит сведения о текущем состоянии синхронизации автономного файла. Он поддерживает следующие свойства, доступные только для чтения.

- `CallbackReason`, тип: `uint32` — указывает, поддерживает ли автономный файл обратный вызов. Возможные значения: `Progress` и `SyncConflictResolution`.
- `ProgressReason`, тип: `uint32` — определяет текущее состояние связи с оригиналом автономного файла. Возможные значения данного свойства: начало, окончание, элемент начала, элемент окончания.
- `Result`, тип: `uint32` — указывает код результата операции синхронизации.

Класс также поддерживает два свойства, доступных как для чтения, так и для записи. Это свойство `Abort`, имеющее тип `boolean`, которое позволяет остановить операцию синхронизации данного автономного файла. И свойство `Retry`, имеющее тип `uint32`, которое позволяет повторить операцию синхронизации данного автономного файла, если предыдущая синхронизация была неудачной.

Класс Win32_OfflineFilesItem

Класс определяет состояние элемента. Он поддерживает следующие свойства, доступные только для чтения.

- `ChangeInfo`, тип: указатель на объект `Win32_OfflineChangeInfo` — возвращает указатель на информацию элемента.
- `ConnectionInfo`, тип: указатель на объект `Win32_OfflineConnectionInfo` — хранит информацию о соединении элемента.
- `FileSysInfo`, тип: указатель на объект `Win32_OfflineFilesFileSysInfo` — содержит информацию об элементе.
- `ItemName`, тип: `string` — хранит имя автономного файла без пути к нему.
- `ItemPath`, тип: `string` — является ключевым. Оно содержит путь к элементу.
- `ItemType`, тип: `uint32` — определяет тип элемента. Возможны следующие типы: файл, каталог, общий ресурс, сервер.
- `ParentItemPath`, тип: `string` — возвращает путь к родительскому элементу. Если значение данного свойства равно `NULL`, то элемент является сервером.
- `PinInfo`, тип: указатель на объект `Win32_OfflineFilesPinInfo` — определяет информацию о синхронизации.
- `SuspendInfo`, тип: указатель на объект `Win32_OfflineSuspendInfo` — указывает информацию о приостановке элемента.

Класс Win32_OfflineFilesCache

Данный класс определяет настройки работы автономных файлов. Он содержит следующие свойства, доступные только для чтения.

- `Active`, тип: `boolean` — указывает, разрешены ли автономные файлы.
- `Enabled`, тип: `boolean` — определяет, разрешены ли автономные файлы.
- `Location`, тип: `string` — указывает путь к каталогу, содержащему автономные файлы.

Класс также поддерживает следующие методы, позволяющие изменить параметры работы автономных файлов.

- `DeleteItems` — удаляет один или несколько элементов из кэша автономного файла.

  Входящие параметры:

  - массив путей к файлам, имеющий тип `string`;
  - флаги, имеющие тип `uint32`.

  Возвращаемые параметры: нет.
- `Enable` — включает или отключает использование автономных файлов.

  Входящий параметр: флаг нового состояния механизма автономных файлов.

  Возвращаемый параметр: имеет тип `boolean` и определяет, необходима ли перезагрузка.
- `Encrypt` — включает или отключает возможность шифрования кэша автономных файлов.

  Входящие параметры:

  - флаг, определяющий, включено или нет шифрование, имеет тип `boolean`;
  - флаги команды, имеют тип `uint32`.

  Возвращаемые параметры: нет.
- `Pin` — определяет, что элемент доступен в автономном режиме.

  Входящие параметры:

  - массив путей к файлам, имеющий тип `string`;
  - флаги команды, имеют тип `uint32`;
  - `Deep` — имеет тип `boolean`.

  Возвращаемые параметры: нет.
- `RenameItem` — изменяет путь к кэшу автономных файлов.

  Входящие параметры:

  - строковый параметр, определяющий оригинальный путь;
  - строковый параметр, определяющий новый путь;

- параметр типа `boolean`, определяющий, будет ли происходить дублирование информации.

Возвращаемые параметры: нет.

- `SuspendRoot` — приостанавливает или нет путь к дереву каталогов кэша автономных файлов.

  Входящие параметры:

  - строковый параметр, определяющий путь к каталогу;
  - параметр типа `boolean`, определяющий, будет ли приостановлено использование данного пути.

  Возвращаемые параметры: нет.

- `Synchronize` — выполняет синхронизацию одного или нескольких файлов.

  Входящие параметры:

  - массив путей к файлам, которые нужно синхронизировать, имеющий тип `string`;
  - флаги команды, имеют тип `uint32`.

  Возвращаемые параметры: нет.

- `Unpin` — отменяет доступ к файлам в автономном режиме.

  Входящие параметры:

  - массив путей к файлам, имеющий тип `string`;
  - флаги команды, имеют тип `uint32`;
  - `Deep` — имеет тип `boolean`.

  Возвращаемые параметры: нет.

Групповые политики

Работу данного мастера можно ограничить с помощью групповых политик файла `OfflineFiles.admx`, расположенных в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Сеть ▸ Автономные файлы.

Данные политики изменяют значения следующих параметров `REG_DWORD`-типа, расположенных в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache`.

- `EncryptCache` — если значение данного параметра равно `1`, то будет выполняться шифрование кэша автономных файлов локального компьютера.
- `CacheQuotaLimit` — значение этого параметра определяет объем свободного пространства в мегабайтах, который будет использоваться для хранения автономных файлов. По умолчанию для хранения автономных файлов используется 25 % от объема диска.
- `CacheQuotaLimitUnpinned` — его значение определяет объем свободного пространства в мегабайтах, который будет использоваться для хранения авто-

матически кэшируемых файлов. По умолчанию для их хранения используется все свободное пространство раздела диска.

- `Enabled` — если значение данного параметра равно `0`, то использование автономных файлов будет запрещено.
- `NoMakeAvailableOffline` — при установке значения этого параметра равным `1` команда Сделать доступными автономно не будет отображаться в контекстном меню сетевых папок и файлов. Параметр можно также создавать в ветви реестра корневого раздела `HKEY_CURRENT_USER`.
- `EconomicalAdminPinning` — если значение данного параметра равно `1`, то при входе пользователя в систему будет выполняться синхронизация только файлов и папок, назначенных для синхронизации администратором и еще недоступных в автономном режиме. Синхронизация файлов и папок, назначенных администратором и уже доступных в автономном режиме, будет выполняться позже. Список всех автономных файлов, назначенных для синхронизации администратором, хранится в виде параметров строкового типа ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache\AssignedOfflineFolders`.
- `SlowLinkEnabled` — при установке значения этого параметра равным `1` будет включен режим обнаружения медленных подключений. При этом список компьютеров, для которых будет применяться этот режим, хранится в параметрах строкового типа ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetCache\SlowLinkParams`. Имя параметра данной ветви реестра определяет название компьютера. Значение же определяет параметры, по которым можно обнаружить, что на текущий момент используется медленное подключение. При обнаружении медленного режима все запросы к удаленным файлам будут перенаправляться в кэш автономных файлов компьютера.

Тестирование производительности

В операционной системе Windows Vista появилась новая возможность, позволяющая тестировать компоненты компьютера на производительность. Для этого можно использовать как специальное окно, так и новую программу командной строки.

Окно Счетчики и средства производительности

Чтобы протестировать производительность всех компонентов компьютера, можно воспользоваться окном Счетчики и средства производительности, которое вызывается с помощью одноименного значка папки Панель управления.

Основное окно состоит из поля, отображающего значения предыдущих тестов производительности компонентов компьютера. Это поле содержит такие элементы, как Процессор, Память (RAM), Графика, Графика для игр, Основной жесткий диск. Напротив каждого из этих элементов отображается соответствующий результат тестов.

Чтобы начать тестирование, нужно нажать кнопку Обновить оценку. После этого начнется процесс тестирования, информация о проведении которого будет отображаться в специальном окне Индекс производительности Windows. После окончания тестирования перед вами отобразится рейтинг конфигурации вашего компьютера. Если же вам нужно просмотреть детальную информацию о тестировании компьютера, то воспользуйтесь оснасткой `eventvwr.msc`. Проще всего это сделать с помощью ссылки Просмотр сведений о производительности в журнале событий, отображаемой в мастере Дополнительные инструменты (данный мастер отображается после выбора ссылки Дополнительные инструменты панели ссылок мастера Счетчики и средства производительности).

С помощью групповых политик файла `PerfCenterCPL.admx`, расположенных в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Панель управления производительностью, можно настроить ограничения доступа к данному мастеру.

Данные политики изменяют значения параметров `REG_DWORD`-типа, расположенных в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Control Panel\Performance Control Panel`.

- Отключение доступа к разделу решения проблем производительности — изменяет значение параметра `SolutionsEnabled`. Если его значение равно `0`, то в мастере Дополнительные инструменты (отображается после выбора одноименной ссылки на панели ссылок) не будет отображаться содержимое поля Вопросы производительности.
- Отключение доступа к основному разделу панели управления производительностью — политика изменяет значение параметра `PerfCplEnabled`. Если значение данного параметра равно `0`, то доступ к мастеру Счетчики и средства производительности будет запрещен.
- Отключение доступа к разделу ПВТ и фирменной символики корпорации Майкрософт — изменяет значение параметра `UpsellEnabled`. Если значение параметра равно `0`, то в мастере не будут отображаться ссылки Microsoft.

Средство оценки системы Windows

Расположение: `%systemroot%\system32\winsat.exe`.

Протестировать ваш компьютер на производительность можно с помощью программы командной строки `WinSAT.exe`. Чтобы просмотреть описание возможностей данной программы, введите команду `winsat /?`.

Перед тем как описывать основные возможности программы, следует упомянуть, что результаты всех тестов, проведенных с ее помощью, заносятся в журнал Operational оснастки Просмотр событий (как и результаты проведения теста с помощью рассмотренного выше мастера Счетчики и средства производительности). Данный журнал расположен в разделе Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Diagnostics-Performance оснастки.

С помощью программы `WinSAT.exe` можно выполнить следующие действия.

Просмотр сведений о компонентах компьютера

Для просмотра сведений о компонентах компьютера используется такая команда, как `WinSAT.exe -v`.

С ее помощью можно узнать следующие сведения о компьютере: версию операционной системы, название процессора и его частоту, количество процессоров, ядер, ядер в каждом процессоре, размер кэша L1 и L2. Можно также узнать описание видеокарты, поддерживает ли она пиксельные шейдеры 2.0 и драйвер LDDM, объем памяти видеокарты, используемое разрешение экрана, а также объем оперативной памяти.

Этой командой можно воспользоваться и при проведении тестов производительности. В этом случае будут отображены дополнительные сведения о тестируемом компоненте и настройках, используемых при тестировании.

Проверка производительности оперативной памяти

Основной командой для проверки производительности оперативной памяти является команда `WinSAT.exe mem`. После ее запуска в течение двух секунд будет выполняться проверка производительности оперативной памяти, после чего будет отображен результат проверки — количество мегабайт в секунду, которые успела обработать оперативная память за это время.

Команда проверки производительности оперативной памяти поддерживает множество дополнительных параметров, но на страницах данной книги о них не будет рассказано.

Проверка производительности Direct3D

Основной командой для проверки производительности Direct3D является команда `WinSAT.exe dwm`. После ее запуска в течение десяти секунд будет выполняться проверка производительности видеокарты в режиме Direct3D, после чего будет отображен результат проверки — количество кадров в секунду (frames per seconds), выводимых видеокартой, а также пропускная способность памяти видеокарт.

Команда проверки производительности Direct3D поддерживает множество дополнительных параметров, но на страницах данной книги о них не будет рассказано.

Проверка производительности при кодировании видео

Можно также выполнить проверку производительности компьютера на основе теста кодирования видео. Для этого предназначена команда `WinSAT.exe media -input <тестовый файл, который нужно кодировать> -encode <профиль кодировки>`.

Вместе с программой Средство оценки системы Windows поставляется два тестовых файла: `winsat.wmv` (имеет размер 4,42 Мбайт) и `winsatencode.wmv` (имеет

размер 3,98 Мбайт). Оба расположены в каталоге `%systemroot%\performance\winsat`.

Профиль кодировки также расположен в каталоге `%systemroot%\performance\winsat`. Он называется `winsat.prx` и, по сути, представляет собой обычный текстовый файл, в котором указано расширение, битрейт и другие параметры кодирования файла. Поэтому, в определенных пределах, вы можете создавать свои собственные профили на основе поставляемого по умолчанию.

Например, для проверки производительности компьютера можно воспользоваться следующей командой кодирования: `WinSAT.exe media -input c:\windows\performance\winsat\winsatencode.wmv -encode c:\windows\performance\winsat\winsat.prx`. Заметьте, что для работы программы нужно обязательно указать пути к файлам, а не только их имена.

Команда проверки производительности при кодировании видео поддерживает несколько дополнительных параметров, но на страницах данной книги о них не будет рассказано.

Проверка производительности компьютера на основе заставки

Проверить производительность компьютера можно и на основе заставки, используемой при установке операционной системы Windows Vista. Для этого достаточно воспользоваться командой `WinSAT.exe aurora`, после чего запустится заставка, отображаемая при установке операционной системы.

Команда проверки производительности на основе заставки поддерживает несколько дополнительных параметров, но на страницах данной книги о них не будет рассказано.

Проверка возможностей видеокарты

Еще одним тестом программы, который проверяет возможности видеокарты, является тест на основе создания 3D-объектов. Самой простой командой его запуска является команда `WinSAT.exe d3d -time <количество секунд проверки>`. После запуска данной команды на белом фоне экрана будут передвигаться серые объекты.

Команда проверки возможностей видеокарты поддерживает множество дополнительных параметров, но на страницах данной книги о них не будет рассказано.

Проверка производительности процессора

Проверку производительности процессора можно выполнить на основе двух тестов: теста шифрования файла и теста компрессии файла.

Для выполнения теста шифрования файла используется команда `WinSAT.exe cpu -encryption2`. Для выполнения теста компрессии файла предназначена команда `WinSAT.exe cpu -compression2`.

Проверка производительности процессора выполняется в течение девяти секунд, после чего будет отображен результат проверки — количество мегабайт в секунду, которые за это время удалось обработать.

Команда проверки производительности процессора поддерживает несколько дополнительных параметров, но на страницах данной книги о них не будет рассказано.

Проверка производительности жесткого диска

Существует четыре параметра работы жесткого диска, производительность которых можно проверить. Соответственно, изменяются и параметры, которые нужно указать в команде.

Общий формат команды для проверки производительности жесткого диска следующий: `WinSAT.exe disk <параметры> -n <номер жесткого диска>`.

Значение параметра `-n` указывает номер физического диска, который нужно протестировать. Диски нумеруются, начиная с нуля.

Набор параметров, указываемых в команде, определяет параметр работы жесткого диска, который нужно протестировать. Итак, можно протестировать следующие параметры работы жесткого диска.

- Время последовательного чтения данных жестким диском. Для этого нужно указать параметры `-seq -read`.
- Время произвольного чтения данных жестким диском. Для этого нужно указать параметры `-ran -read`.
- Время последовательной записи данных жестким диском. Для этого нужно указать параметры `-seq -write`.
- Время произвольной записи данных жестким диском. Для этого нужно указать параметры `-ran -write`.

Например, чтобы проверить первый жесткий диск на время произвольного чтения данных, нужно воспользоваться командой `WinSAT.exe disk -ran -read -n 0`.

Команда проверки производительности жесткого диска поддерживает множество дополнительных параметров, но на страницах данной книги о них не будет рассказано.

Общая проверка производительности компьютера

Если же вы хотите проверить все компоненты компьютера, то можно воспользоваться одной из описанных ниже команд.

Итак, достаточно воспользоваться командой `winsat.exe formal`, после чего начнется выполнение всех тестов, описанных выше. Результатом проведения данных тестов будет общая таблица производительности вашего компьютера, отображающая результаты следующих тестов:

- производительность процессора на основе теста компрессии файла;
- производительность процессора на основе теста шифрования файла;
- производительность оперативной памяти;
- производительность Direct3D9 Alpha Blend;
- производительность Direct3D9 Texture Load;

- производительность Direct3D9 ALU;
- производительность жесткого диска;
- производительность кодирования видео;
- производительность декодирования видео;
- общее время выполнения всех тестов.

Если же нужно выполнить только тестирование видеоподсистемы, то можно воспользоваться командой `winsat.exe graphicsformal`. Результатом выполнения данной команды будет таблица, отображающая следующие результаты:

- производительность видеокарты;
- пропускную способность памяти видеокарты;
- производительность Direct3D9 Alpha Blend;
- производительность Direct3D9 Texture Load;
- производительность Direct3D9 ALU;
- общее время выполнения всех тестов.

Можно также провести комплексное тестирование, тестирование возможностей видеокарты в котором будет выполнено на основе заставки, отображаемой при установке операционной системы. Для этого применяется команда `winsat.exe moobe`. Однако применение данной команды возможно только в том случае, если значение параметра `REG_DWORD`-типа `MOOBE`, расположенного в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinSAT`, равно `0`.

Отображаемые после работы данной команды результаты аналогичны получаемым с помощью команды `winsat.exe formal`.

Работа с WMI

В операционной системе Windows Vista появился новый класс инструментария управления Windows, предназначенный для работы с компонентом тестирования производительности. Данный класс содержит информацию о производительности компьютера, полученную в последнем тесте. Он называется `Win32_WinSAT` и находится в пространстве имен `\\.\root\cimv2`.

Класс `Win32_WinSAT` включает в себя следующие свойства, доступные только для чтения.

- `CombinedGraphicsMetric`, тип: `real32` — определяет значение производительности, полученное при комбинированном тестировании графики.
- `CombinedGraphicsScore`, тип: `real32` — указывает общую оценку, полученную при комбинированном тестировании графики.
- `CPUMetric`, тип: `real32` — определяет значение производительности, полученное при тестировании процессора.

- `CPUScore`, тип: `real32` — указывает общую оценку, полученную при тестировании процессора.
- `D3DMetric`, тип: `real32` — определяет значение производительности, полученное при тестировании возможностей Direct3D.
- `D3DScore`, тип: `real32` — указывает общую оценку, полученную при тестировании возможностей Direct3D.
- `DiskMetric`, тип: `real32` — определяет значение производительности, полученное при тестировании скорости обращения к жесткому диску.
- `DiskScore`, тип: `real32` — указывает общую оценку, полученную при тестировании скорости обращения к жесткому диску.
- `GraphicsMetric`, тип: `real32` — определяет значение производительности, полученное при тестировании графической подсистемы компьютера.
- `GraphicsScore`, тип: `real32` — указывает общую оценку, полученную при тестировании графической подсистемы компьютера.
- `MemoryMetric`, тип: `real32` — определяет значение производительности, полученное при тестировании оперативной памяти.
- `MemoryScore`, тип: `real32` — указывает общую оценку, полученную при тестировании оперативной памяти.
- `TimeTaken`, тип: `string` — свойство является ключевым. Оно содержит описание даты последнего тестирования компонентов компьютера. По умолчанию значение свойства равно `MostRecentAssessment`.
- `WinSATAssessmentState`, тип: `uint32` — значение определяет, было ли вообще когда-нибудь проведено тестирование производительности компьютера.
- `WinSPRLevel`, тип: `uint16` — содержит общую оценку производительности компьютера. Именно эта оценка отображается в поле Оценка окна Система (которое вызывается с помощью комбинации клавиш Windows+Pause Break).

Центр обеспечения безопасности

Мастер Центр обеспечения безопасности операционной системы Windows Vista практически не изменился по сравнению с предыдущими версиями Windows. Как и раньше, с его помощью вы можете включить или отключить такие компоненты операционной системы, как Брандмауэр, Автоматическое обновление, Защита от вирусов, Другие параметры безопасности.

ПРИМЕЧАНИЕ

Если ваш компьютер подключен к домену Active Directory, то по умолчанию компонент Центр обеспечения безопасности будет отключен. Если вы хотите его включить, то нужно воспользоваться групповой политикой Включить "Центр обеспечения безопасности" (только для компьютеров в домене), расположенной в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Центр обеспечения безопасности и описанной в файле Securitycenter.admx.

Данная политика устанавливает значение параметра REG_DWORD-типа SecurityCenterInDomain, расположенного в ветви реестра HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Security Center, равным 1.

Особенностью компонента Центр обеспечения безопасности операционной системы Windows Vista является то, что его значок всегда отображается в области уведомления. Однако с помощью окон операционной системы можно отключить отображение уведомлений о работе компонента Центр обеспечения безопасности (например, если вы отключили автоматическое обновление, то по умолчанию при каждом входе в систему отображается уведомление о том, что это очень опасно) или полностью скрыть его значок из области уведомлений.

Чтобы отключить подобные уведомления, нужно воспользоваться ссылкой Изменение способа предупреждения центром безопасности панели ссылок мастера Центр обеспечения безопасности. После ее выбора перед вами отобразится окно Центр обеспечения безопасности Windows, содержащее три кнопки.

- Да, уведомлять и отображать значок (рекомендуется) — отображать уведомления о работе компонента операционной системы Центр обеспечения безопасности.
- Не уведомлять, но отображать значок — не отображать уведомления о работе компонента операционной системы Центр обеспечения безопасности, но отображать его значок в области уведомления.
- Не уведомлять и не отображать этот значок (не рекомендуется) — не отображать уведомления о работе компонента операционной системы Центр обеспечения безопасности, а также не отображать его значок в области уведомления.

Обратите также внимание на параметры REG_DWORD-типа ветви системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center\Svc.

- AntiSpywareOverride — если установить значение данного параметра равным 1, то компоненту Центр обеспечения безопасности будет запрещено выполнять мониторинг состояния стандартного malware-продукта.
- AntiVirusOverride — при установке значения этого параметра равным 1 компоненту Центр обеспечения безопасности будет запрещено выполнять мониторинг состояния стандартной антивирусной программы.
- FirewallOverride — если установить значение данного параметра равным 1, то компоненту Центр обеспечения безопасности будет запрещено выполнять мониторинг состояния стандартного брандмауэра Windows Vista.

Центр обновления Windows

Обратите также внимание на ссылку Центр обновления Windows мастера Центр обеспечения безопасности. С ее помощью можно отобразить одноименный мастер (также его можно отобразить с помощью значка Центр обновления Windows папки Панель управления). Данный мастер позволяет управлять обновлением Windows Vista, а также просматривать историю обновлений. Он содержит следующие ссылки.

ПРИМЕЧАНИЕ

Информация о работе службы обновлений заносится в журнал подраздела Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ WindowsUpdateClient.

- Проверка обновлений — содержит кнопку, с помощью которой можно проверить новые обновления для операционной системы и программ на сайте Microsoft. С помощью данной ссылки можно также просмотреть дату последней проверки обновления и дату последней установки обновления.
- Изменить параметры — позволяет включить или отключить автоматическое обновление, а также определить время автоматического обновления и указать, будет выполняться загрузка найденного обновления и его установка или просто загрузка без установки.
- Просмотр журнала обновлений — разрешает просмотреть историю загруженных обновлений.
- Восстановить скрытые обновления — отображает список скрытых обновлений, а также позволяет их заново установить.
- Обновления: вопросы и ответы — с помощью данной ссылки можно отобразить мастер Windows Ultimate, содержащий справку по новому компоненту операционной системы Windows Ultimate Extras. Данный компонент позволяет загрузить дополнительные службы, программы и советы по работе с Windows Vista Ultimate (компонент Windows Ultimate Extras доступен только для этой операционной системы). Также с помощью мастера Windows Ultimate можно выполнить поиск новых программ и служб. Для этого нужно воспользоваться ссылкой Загрузка программ, служб и специального содержимого с веб-узла Windows Ultimate Extras.
- Установленные обновления. Отображает список установленных обновлений мастера Программы и компоненты.

Работу с компонентом Центр обновления Windows операционной системы можно настроить с помощью групповых политик, расположенных в подразделе Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Центр обновления Windows и описанных в файле `WindowsUpdate.admx`.

Настройки Центра обновления Windows можно изменить с помощью параметров `REG_DWORD`-типа, расположенных в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate`.

- `WUServer` — имеет строковый тип, содержит имя сервера, к которому служба обновления должна обращаться при поиске новых обновлений.
- `WUStatusServer` — параметр строкового типа. Он содержит имя сервера, используемого для хранения статистики обновлений.
- `TargetGroupEnabled` — если значение данного параметра равно `1`, то возможность указания целевого имени группы будет использоваться службой обновления Windows.

- `TargetGroup` — имеет строковый тип, позволяет определить целевое имя группы. Данное имя будет использоваться для поиска новых обновлений на сервере сети и определения того, нужно ли данному компьютеру устанавливать эти обновления.

Остальные же настройки Центра обновления Windows можно изменить с помощью параметров `REG_DWORD`-типа, расположенных в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU`.

- `IncludeRecommendedUpdates` — если значение данного параметра равно `1`, то служба обновления Windows будет загружать с сайта как все важные, так и рекомендуемые обновления.
- `UseWUServer` — при установке значения этого параметра равным `1` служба обновления Windows для поиска новых обновлений будет обращаться на указанный в параметре `WUServer` сервер. Кроме того, служба обновлений будет определять адрес сервера, используемого для хранения статистической информации о выполнении обновлений, на основе значения параметра `WUStatusServer`.
- `RescheduleWaitTimeEnabled` — если значение данного параметра равно `1`, то стандартный интервал ожидания перед выполнением пропущенных обновлений будет изменен с помощью значения параметра `RescheduleWaitTime`. Этот параметр используется лишь в том случае, если значение параметра `AUOptions` равно `4`.
- `RescheduleWaitTime` — значение данного параметра определяет интервал (в минутах) ожидания, по истечении которого служба обновления начнет выполнение ранее пропущенных запланированных обновлений. Значение данного параметра используется только в том случае, если параметр `RescheduleWaitTimeEnabled` равен `1`. По умолчанию пропущенное запланированное обновление будет выполняться через минуту после запуска компьютера.
- `RebootRelaunchTimeoutEnabled` — если значение данного параметра равно `1`, то стандартный интервал ожидания перед выводом повторного приглашения на перезагрузку (для установки запланированного обновления) будет изменен с помощью значения параметра `RebootRelaunchTimeout`. Он используется лишь в том случае, если значение параметра `AUOptions` равно `4`.
- `RebootRelaunchTimeout` — значение этого параметра определяет интервал (в минутах) ожидания, по истечении которого будет отображено повторное приглашение на перезагрузку компьютера. Значение данного параметра используется только в том случае, если параметр `RebootRelaunchTimeoutEnabled` равен `1`. По умолчанию используется интервал ожидания в 10 минут.
- `RebootWarningTimeoutEnabled` — если значение данного параметра равно `1`, то стандартный интервал ожидания перед выводом первого приглашения на перезагрузку (для установки запланированного обновления) будет изменен с помощью значения параметра `RebootWarningTimeout`. Данный параметр используется лишь в том случае, если значение параметра `AUOptions` равно `4`.

- RebootWarningTimeout — значение данного параметра определяет интервал (в минутах) ожидания, по истечении которого будет отображено первое приглашение на перезагрузку компьютера. Значение используется только в том случае, если параметр RebootWarningTimeoutEnabled равен 1. По умолчанию используется интервал ожидания в 5 минут.
- NoAutoRebootWithLoggedOnUsers — если значение данного параметра равно 1, то вместо выполнения автоматической перезагрузки после запланированной установки обновления пользователю будет выведен запрос с предложением перезагрузки.
- AUPowerManagement — при установке значения этого параметра равным 1 будет разрешено пробуждение компьютера из состояния сна (если необходимо установить новое обновление).
- NoAUShutdownOption — если значение данного параметра равно 1, то в окне Завершение работы Windows после загрузки нового обновления не будет отображаться команда Установить обновления и завершить работу. Параметр также доступен в корневом разделе HKEY_CURRENT_USER.
- NoAUAsDefaultShutdownOption — при установке значения этого параметра равным 1 команда Установить обновления и завершить работу, отображаемая в окне Завершение работы Windows после загрузки нового обновления, не будет устанавливаться как действие по умолчанию. Параметр также доступен в корневом разделе HKEY_CURRENT_USER.
- AUOptions — если значение данного параметра равно 2, то операционная система будет уведомлять пользователя перед загрузкой и перед установкой обновлений (в области уведомлений будет появляться сообщение о том, что обновления готовы к загрузке или установке). Если значение данного параметра равно 3, то операционная система будет уведомлять пользователя только при установке уже загруженных обновлений. Если же значение равно 4, то загрузка и установка обновлений будут выполняться согласно установленному расписанию без уведомления пользователя. Расписание обновлений определяется в параметрах ScheduledInstallDay и ScheduledInstallTime.
- NoAutoUpdate — при установке значения этого параметра равным 1 будет запрещена возможность автоматического обновления.
- ScheduledInstallDay — значение данного параметра определяет день, на который будет назначен поиск новых обновлений.
- ScheduledInstallTime — значение определяет час, на который будет назначен поиск новых обновлений.
- DetectionFrequencyEnabled — если значение данного параметра равно 1, то стандартная частота поиска новых обновлений будет заменена значением, указанным в параметре DetectionFrequency. При этом частота поиска обновлений будет изменена только в том случае, если значение параметра UseWUServer равно 1.
- DetectionFrequency — значение определяет частоту (в часах), с которой служба обновления будет выполнять поиск новых обновлений. По умолчанию используется интервал в 22 часа.

- `ElevateNonAdmins` — если значение данного параметра равно `1`, то уведомления об установке обновлений будут отображаться не только администраторам компьютера, но и обычным пользователям.
- `AutoInstallMinorUpdates` — при установке значения этого параметра равным `1` обновления, не требующие перезагрузки компьютера после своей установки, будут устанавливаться сразу после загрузки.

Работа с WMI

В операционной системе Windows Vista появилось новое пространство имен репозитария CIM, содержащее классы, позволяющие просматривать содержимое компонента Центр обновления Windows. Данное пространство имен называется `\\.\root\SecurityCenter`. Оно поддерживает следующие классы.

Класс AntiVirusProduct

Данный класс описывает установленный в операционной системе антивирусный пакет. Его свойства доступны как для чтения, так и для записи.

- `companyName`, тип: `string` — определяет название компании, которая создала данный антивирусный пакет.
- `displayName`, тип: `string` — указывает название программы.
- `instanceGuid`, тип: `string` — является ключевым. Оно определяет CLSID-номер установленного продукта.
- `onAccessScanningEnabled`, тип: `boolean` — указывает, разрешен ли процесс сканирования компьютера.
- `pathToSignedProductExe`, тип: `string` — содержит путь к программе.
- `productUptoDate`, тип: `boolean` — содержит дату программы.
- `versionNumber`, тип: `string` — определяет версию антивирусного пакета.

Класс FirewallProduct

Данный класс описывает установленный в операционной системе брандмауэр. Его свойства доступны как для чтения, так и для записи.

- `companyName`, тип: `string` — определяет название компании, которая выпустила данный брандмауэр.
- `displayName`, тип: `string` — указывает название брандмауэра.
- `instanceGuid`, тип: `string` — является ключевым. Оно определяет CLSID-номер установленного продукта.
- `enabled`, тип: `boolean` — указывает, работает ли брандмауэр в данный момент.
- `onAccessScanningEnabled`, тип: `boolean` — определяет, разрешен ли процесс сканирования компьютера.
- `pathToSignedProductExe`, тип: `string` — содержит путь к программе.
- `versionNumber`, тип: `string` — определяет версию брандмауэра.

Класс AntiSpywareProduct

Данный класс описывает установленный в операционной системе продукт, предназначенный для поиска шпионских программ и модулей. Например, к такому продукту относится стандартная программа Защитник Windows операционной системы Windows Vista. Свойства данного класса доступны как для чтения, так и для записи.

- `CompanyName`, тип: `string` — определяет название компании, которая создала данный продукт.
- `DisplayName`, тип: `string` — указывает название продукта.
- `InstanceGuid`, тип: `string` — является ключевым. Оно определяет CLSID-номер установленного продукта.
- `pathToSignedProductExe`, тип: `string` — содержит путь к программе.
- `productEnabled`, тип: `Boolean` — определяет, работает ли продукт в данный момент.
- `productUptoDate`, тип: `Boolean` — содержит дату программы.
- `versionNumber`, тип: `string` — указывает версию продукта.

Механизм совместимости

Немаловажным условием комфортной работы пользователей в новой операционной системе Windows Vista является возможность запуска программ, написанных для предыдущих версий операционных систем семейства Windows.

Действительно, нет ничего хуже, чем ошибка при попытке установки или запуска жизненно необходимой вам программы, которая раньше отлично работала на предыдущих версиях Windows. Иногда такая ошибка может поставить последнюю точку в вопросе выбора операционной системы, в которой будет работать пользователь. И, конечно, не в пользу новой операционной системы Windows Vista.

Однако, если вы все-таки столкнулись с ситуацией, когда какая-то программа не хочет работать в новой операционной системе, не стоит сразу отчаиваться. Операционная система Windows Vista, как и предыдущие версии операционной системы Windows, содержит в своей стандартной поставке компонент, с помощью которого можно для конкретной программы эмулировать условия запуска под операционной системой Windows любой версии, более старой, чем Windows Vista.

Для этого можно воспользоваться как минимум двумя способами.

Первым и самым быстрым способом является использование вкладки Совместимость окна Свойства. Данная вкладка есть во всех окнах Свойства, принадлежащих исполняемым файлам или ярлыкам на них. Ее изображение представлено на рис. 7.9.

Вкладка Совместимость содержит следующие области.

- Режим совместимости — именно с помощью флажка данной области можно активировать режим совместимости для конкретной программы. После этого

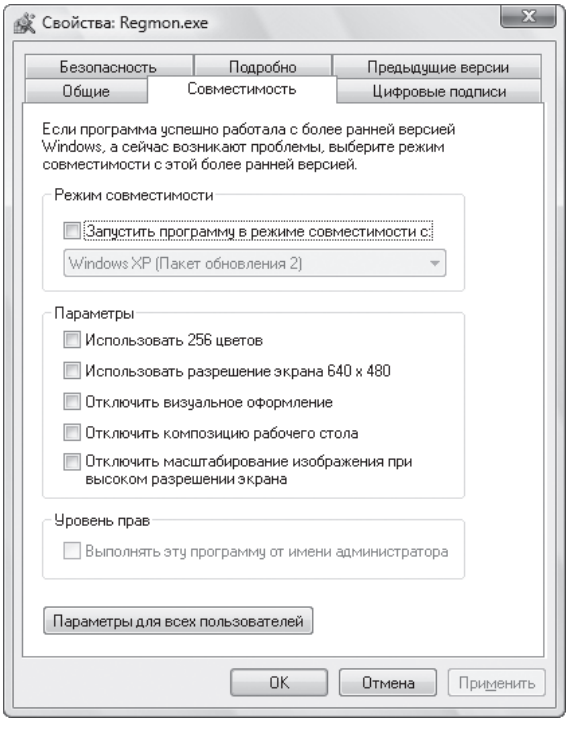


Рис. 7.9. Вкладка Совместимость

в раскрывающемся списке нужно выбрать операционную систему, которую будет эмулировать Windows Vista. Можно выбрать такие операционные системы, как Windows 95, Windows 98, Windows NT 4.0, Windows 2000, Windows XP SP2 и Windows 2003 Server.

- Параметры — позволяет указать дополнительные параметры запуска программы в совместимом режиме. К ним относятся возможность запуска программы с использованием разрешения экрана 640 × 480, запуск в 256-цветном режиме, запуск с отключенными визуальными темами или с отключенными настройками DPI.
- Уровень прав — с помощью флажка данной области можно указать, что программа для данного пользователя должна запускаться с правами администратора.

Кнопка Параметры для всех пользователей позволяет отобразить вкладку Совместимость, с помощью которой можно настроить параметры запуска программы в режиме совместимости для всех пользователей, а не только для одного.

Вторым же способом запуска программы в режиме совместимости является использование Мастера совместимости программ. Чтобы запустить данный мастер, нужно воспользоваться программой Справка и поддержка, доступ к которой можно получить либо с помощью меню Пуск, либо нажав клавишу F1. Проще всего после запуска программы Справка и поддержка в ее строке поиска ввести `Compatibility`

Wizard. Результатом поиска будет ссылка Запуск мастера совместимости, после выбора которой будет запущен мастер совместимости программ.

Основное окно мастера совместимости программ представлено на рис. 7.10.

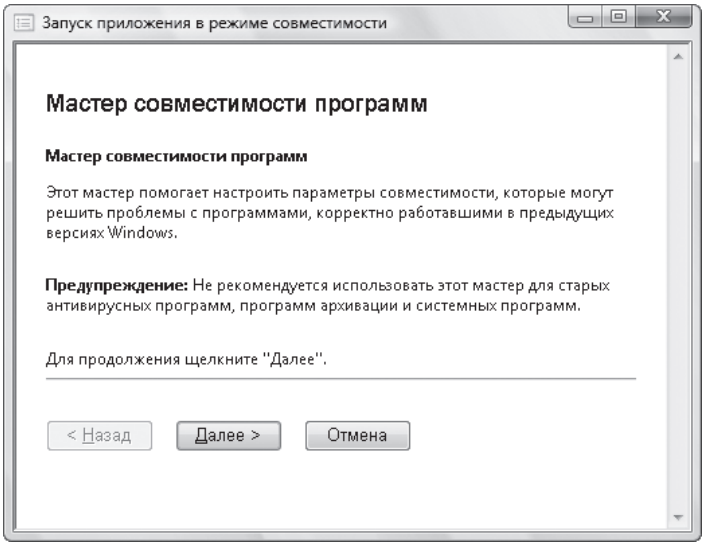


Рис. 7.10. Первый шаг мастера совместимости программ

Как и с помощью первого способа установки параметров совместимости программ, с помощью мастера совместимости можно настроить запуск в режиме совместимости не только программ, расположенных на жестком диске, но и программ, расположенных на компакт-диске или DVD. Для этого нужно выбрать соответствующее положение переключателя Каким образом открыть программу, для которой требуется настроить параметры совместимости?.

- Выбрать из списка программ — позволяет выбрать программу из списка программ, найденных на жестком диске. Поиск программ выполняется при каждом запуске мастера совместимости и может занять продолжительное время.
- Использовать программу на компакт-диске — дает возможность выбрать программы, расположенные на компакт-диске или DVD. После установки переключателя в это положение мастер попросит вас вставить диск в привод (если он еще не вставлен), а после этого вы перейдете к шагу выбора параметров совместимости мастера.
- Найти программу вручную — позволяет ввести путь к программе вручную.

После того как вы выберете программу, которую нужно запустить в режиме совместимости, мастер попросит вас указать все те настройки, которые мы рассматривали при описании вкладки Совместимость. Сначала будет предложено выбрать операционную систему, которую нужно эмулировать, потом дополнительные настройки совместимости, а потом определить, будет ли программа запускаться

с правами администратора. После этого будет выполнена попытка запуска программы, однако окно мастера закрыто не будет. На последнем шаге мастера вы должны будете ответить на вопросы, работает ли программа корректно и хотите ли вы отослать сведения о работе программы в совместимом режиме корпорации Microsoft.

Хранение сведений о запуске программы в совместимом режиме в реестре

Но как же операционная система определяет, какую программу нужно запускать в совместимом режиме, а какую в обычном? Как часто бывает, для этого используются сведения, хранящиеся в реестре. Сведения обо всех программах, запускаемых в совместимом режиме, хранятся в параметрах строкового типа (каждый параметр описывает сведения о запуске одной программы) ветви реестра `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers` (или ветви корневого раздела `HKEY_LOCAL_MACHINE`, в этом случает программы запускаются в совместимом режиме для всех пользователей). Название параметра данной ветви реестра соответствует пути к программе и ее названию. Значение же параметра состоит из слов, разделенных между собой пробелами. Первое слово определяет операционную систему, которую нужно эмулировать (соответственно, `WIN95`, `WIN98`, `NT4SP5`, `WIN2000`, `WINXPSP2` или `WINSRV03SP1`), а остальные — дополнительные параметры запуска в совместимом режиме (соответственно, слова `256COLOR`, `640X480`, `DISABLETHEMES`, `DISABLEDWM` и `HIGHDPIAWARE`).

В реестре также содержатся сведения о программах, которые не могут работать в новой операционной системе. Если вы попытаетесь установить такую программу, то отобразится окно, сообщающее о том, что данная версия программы несовместима с операционной системой Windows Vista. Данное окно запускается с помощью программы `pcaui.exe`, ссылка на которую содержится в параметре `REG_EXPAND_SZ`-типа `ApphelpUIExe`, расположенном в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags`.

Групповые политики

Механизм совместимости программ, реализованный в операционной системе Windows Vista, как и многие другие компоненты данной операционной системы, можно настроить с помощью групповых политик. Для этого применяется подраздел групповых политик Конфигурация компьютера ▸ Административные шаблоны ▸ Компоненты Windows ▸ Совместимость приложений. Все политики данного подраздела изменяют параметры, расположенные в ветви реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AppCompat` и имеющие тип `REG_DWORD`.

- `VDMDisallowed` — если значение данного параметра равно `1`, то запуск 16-разрядных программ подсистемы MS-DOS (файл `ntvdm.exe`) будет запрещен. Этот параметр доступен и в корневом разделе `HKEY_CURRENT_USER`.
- `DisablePropPage` — при установке значения этого параметра равным `1` не будет отображаться вкладка Совместимость окна Свойства исполняемых файлов и ярлыков на них.

- `DisableEngine` — если значение данного параметра равно `1`, то механизм проверки несовместимых с Windows Vista приложений (при запуске приложений) использоваться не будет.
- `DisableWizard` — при установке значения этого параметра равным `1` будет запрещено отображение мастера совместимости программ.
- `DisablePCA` — если значение данного параметра равно `1`, то помощник по совместимости программ будет отключен. Этот помощник следит за запускаемыми программами и в случае обнаружения неполадок извещает о них пользователя. Параметр доступен и в корневом разделе `HKEY_CURRENT_USER`.

ПРИМЕЧАНИЕ

Информация об обнаруженных ассистентом Помощник по совместимости несовместимых с операционной системой Windows Vista программах заносится в журнал подраздела Журналы приложений и служб ▸ Microsoft ▸ Windows ▸ Program-Compatibility-Assistant.

Групповые политики операционной системы Windows Vista также содержат отдельные политики для настройки поведения ассистента Помощник по совместимости программ. Они находятся в подразделе групповых политик Конфигурация компьютера ▸ Административные шаблоны ▸ Система ▸ Диагностика ▸ Диагностика совместимости приложений. Все политики данного подраздела изменяют параметры, расположенные в подразделах ветви `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WDI` и имеющие тип `REG_DWORD`.

- Уведомлять о блокированных драйверах — политика определяет, будет ли ассистент в случае обнаружения невозможности установки драйвера отображать уведомление с предложением найти корректный драйвер на сайте Microsoft. Если данная политика запрещена, то уведомление с предложением поиска другого драйвера отображаться не будет.

  Запрещение данной политики присваивает параметру `EnabledScenarioExecutionLevel`, расположенному в подразделе `{affc81e2-612a-4f70-6fb2-916ff5c7e3f8}`, значение `1`. Также создается параметр `ScenarioExecutionEnabled`, значение которого равно `1`.

- Обнаружение сбоев приложений, вызванных устаревшими библиотеками DLL или COM-объектами Windows — указывает, будет ли ассистент следить за установкой приложений и запуском ими устаревших DLL- или COM-объектов. Если данная политика включена, то ассистент при обнаружении попытки обращения к устаревшим объектам, из-за которого и происходит сбой установки, отображает окно с отображением сведений об устаревшем объекте и предложением посетить сайт Microsoft для поиска решений возникшей проблемы.

  Установка данной политики присваивает параметру `EnabledScenarioExecutionLevel`, расположенному в подразделе `{659F08FB-2FAB-42a7-BD4F-566CFA528769}`, значение `1` или `2`. Значение `1` устанавливается, если в раскрывающемся списке Режим запуска сценария политики выбрать Только диагностика

и обнаружение. Значение 2 присваивается при выборе Обнаружение, диагностика и решение.

Также создается параметр ScenarioExecutionEnabled, значение которого равно 1.

- Обнаружение сбоев установки приложений — политика определяет, будет ли ассистент перед началом установки приложения проверять его совместимость с операционной системой Windows Vista с помощью эвристики. Если после проверки ассистент предполагает, что приложение не сможет инсталлироваться, то он запускает установку приложения в режиме совместимости с Windows XP. Чтобы запретить ассистенту выполнение проверки методом эвристики, нужно запретить использование этой политики.

  Запрещение данной политики присваивает параметру EnabledScenarioExecutionLevel, расположенному в подразделе {acfd1ca6-18b6-4ccf-9c07-580cdb6eded4}, значение 1. Также создается параметр ScenarioExecutionEnabled, значение которого равно 1.

- Обнаружение средств установки приложений, требующих прав администратора — указывает, будет ли ассистент перед началом установки приложения проверять, необходимы ли при этом права администратора.

  Установка данной политики присваивает параметру EnabledScenarioExecutionLevel, расположенному в подразделе {D113E4AA-2D07-41b1-8D9B-C065194A791D}, значение 1 или 2. Значение 1 устанавливается, если в раскрывающемся списке политики выбрать Только диагностика и обнаружение. Значение 2 присваивается при выборе Обнаружение, диагностика и решение.

  Также создается параметр ScenarioExecutionEnabled, значение которого равно 1.

- Обнаружение приложений, не способных запустить средства установки при включенном контроле учетных записей пользователей (UAC) — политика определяет, будет ли ассистент перед началом установки приложения проверять, может ли выполняться установка приложения при работе механизма UAC.

  Установка данной политики присваивает параметру EnabledScenarioExecutionLevel, расположенному в подразделе {081D3213-48AA-4533-9284-D98F01BDC8E6}, значение 1 или 2. Значение 1 устанавливается, если в раскрывающемся списке политики выбрать Только диагностика и обнаружение. Значение 2 присваивается при выборе Обнаружение, диагностика и решение.

  Также создается параметр ScenarioExecutionEnabled, значение которого равно 1.

На этом мы закончим рассмотрение вопросов администрирования операционной системы Windows Vista.