Альтер В. Е., Матвеев М. Д., Апанасевич Н. Р. и др.

Хакинг Windows 8

ПРАКТИЧЕСКОЕ РУКОВОДСТВО

(КНИГА + CD + ВИРТУАЛЬНЫЙ CD)

Наука и Техника
Санкт-Петербург
2014

Альтер В. Е., Матвеев М. Д., Апанасевич Н. Р. и др.

ХАКИНГ WINDOWS 8. ПРАКТИЧЕСКОЕ РУКОВОДСТВО. КНИГА + CD + ВИРТУАЛЬНЫЙ CD. — СПб.: Наука и Техника, 2014. — 304 с.: ил (+ CD).

Серия “Самоучитель“

Хакинг — это доступ к базовым механизмам, скрытым настройкам системы и их использование. Цель данных действий может быть как положительная (улучшить, оптимизировать, задать нужное поведение), так и отрицательная (сломать, навредить и т.д.). Авторы данной книги не несут ответственности за вредоносное использование описываемых в книге приемов.

В этой книге вы найдете: хакинг интерфейса Windows 8, хакинг рабочей среды Windows 8, хакинг системных настроек, настройку нужного поведения системы, использование реестра для редактирования системных настроек Windows 8, хакинг механизмов безопасности Windows 8, хакинг подключения к Интернету и браузера Internet Explorer, удаленное управление компьютером с Windows 8 через Интернет.

Книга написана простым и доступным языком с пояснением всех необходимых понятий. Книга предназначена “продвинутым“ пользователям компьютеров, а также всем, кто хочет ими стать. К книге прилагается загрузочный CD-реаниматор, который позволит восстановить систему после сбоев, а также виртуальный CD (скачивается с сайта издательства) с программами, упоминаемыми и используемыми в книге, а также некоторыми другими.

Обратите внимание, что применимость многих настроек и приемов, рассмотренных в книге, зависит от версии Windows 8. В максимальном количестве они применимы в версии Windows 8 Профессиональная и Windows 8 Корпоративная. Все торговые марки, упоминаемые в книге, являются собственностью их правообладателей.

Контактные телефоны издательства:
(812) 412 70 25, (812) 412 70 26, (044) 516 38 66

Официальный сайт: www.nit.com.ru

Содержание

Принятые соглашения

Обратите внимание, что по тексту упоминается кнопка Пуск. В разных версиях Windows 8 дела с кнопкой Пуск обстоят по-разному. Кроме того, кнопка Пуск в Windows 8 может быть реализована с помощью доп. программ. Поэтому упоминание кнопки Пуск воспринимайте в своем контексте, и если ее у вас нет, то пропускайте все, что с ней связано.

Обратите также внимание, что многие настройки, приемы и хаки в книге реализованы через механизм групповых политик и использование редактора групповых политик. Данные инструменты присутствуют не во всех версиях Windows 8. Гарантировано они присутствуют в версии Windows 8 Профессиональная и Windows 8 Корпоративная.

Глава 1.

Консоль управления ММС

Доступ к средствам «тонкой» настройки операционной системы Windows 8, можно получить через *Консоль управления MMC*. Консоль управления MMC группирует все средства администрирования, используемые для управления сетями, компьютерами, службами и другими системными компонентами. Именно здесь сосредоточены все основные инструменты и возможности, которые мы будем использовать для хакинга Windows 8

Оснастка является основным компонентом консоли и предоставляет доступ к определенным средствам администрирования. Например, получить доступ к локальным групповым политикам можно при помощи оснастки *Редактор объектов групповой политики*. При этом работа с оснасткой возможна только из консоли управления, запуск оснастки без запуска консоли не представляется возможным. Вы можете создавать свои собственные оснастки консоли управления, как на базе уже существующей оснастки, так и полностью самостоятельно.

1.1. Основные приемы работы в Консоли управления MMC

В то время как Консоль управления MMC доступна любому пользователю системы, многие оснастки могут быть запущены только под учетной записью администратора. В частности, интересующая нас оснастка Редактор объектов групповой политики не может быть запущена пользователем с непривилегированной учетной записью операционной системы. Если вы создаете оснастку консоли управления самостоятельно, вы можете выбрать для нее необходимый уровень режима доступа.

Для того чтобы запустить Консоль управления MMC:

1. Нажмите сочетание клавиш **Windows+R**. Откроется диалоговое окно **Выполнить** (Run).
2. В поле ввода **Открыть** (Open) введите «mmc».
3. Нажмите кнопку **ОК**, чтобы подтвердить запуск программы. Откроется окно пустой Консоли управления MMC.

Запустить Консоль управления MMC можно иначе:

1. Нажмите клавишу **Windows** для вызова меню «Пуск».
2. В поле ввода **Найти программы и файлы** (Search programs and files) введите «mmc».
3. Нажмите клавишу **Enter**.

Рабочее окно Консоли Управления MMC

Рассмотрим рабочее окно программы Консоль управления MMC (рис. 1.1).

В самой верхней части экрана программы располагается строка меню, в ней вы можете увидеть пункты:

Рис. 1.1. Рабочее окно программы Консоль управления MMC

- **Файл** (File). Здесь находятся команды создания, открытия и сохранения консоли, загрузки и удаления оснасток. Также здесь вы найдете команду **Параметры** (Options), отвечающие за основные настройки программы.
- **Действие** (Action). Здесь находятся команды, позволяющие создавать правила, осуществлять фильтрацию в дереве консоли, экспортировать список и некоторые другие действия. Состав может заметно отличаться от оснастки к оснастке.

- **Вид** (View) включает команды, позволяющие настроить интерфейс программы.
- **Избранное** (Favorites) предоставляет доступ к избранному.
- **Окно** (Window). Команды данной группы определяют расположение окон программы, позволяют создавать новые окна консоли и осуществлять переключения между ними.
- **Справка** (Help) предоставляет доступ к справочной системе программы, а также общей информации о Консоли управления MMC и текущим открытым оснасткам.

Также в верхней части экрана вы можете увидеть панель инструментов. Содержание панели инструментов может существенно изменяться в зависимости от открытой в текущий момент оснастки. Тем не менее, шесть кнопок остаются неизменными для любой оснастки:

- Кнопки  и  позволяют перейти на один шаг среди совершенных действий назад и вперед соответственно. Первая кнопка отменит последнее, совершенное в Консоли управления действие, вторая кнопка позволит принять отмененное изменение снова. Подобные функции являются стандартными для программ операционных систем семейства Windows, их применение не должно вызвать у вас проблем.
- Кнопка  отвечает за отображение области **Дерево консоли** (Console tree), находящейся в левой части экрана программы.
- Кнопка  отвечает за отображение области **Действия** (Actions), находящейся в правой части экрана программы. Большинство пользователей Консоли Управления MMC считают область **Действия** (Actions) бесполезной. Отключение отображения этой области для многих является первым действием при начале работы с программой. Для удобства кнопка вынесена на панель инструментов.
- Нажатие кнопки  вызовет справочную систему программы, в которой вы можете получить необходимую информацию о Консоли Управления MMC и приемах работы в программе.
- Кнопка  позволяет быстро экспортировать список в текстовый файл.

После того, как некоторая оснастка будет открыта, на панели управления станут доступны еще несколько кнопок. Например, кнопка  предназна-

чена для более удобной навигации по дереву консоли, она позволяет быстро подняться на один уровень дерева вверх.

В левой части экрана программы Консоль управления MMC располагается область **Дерево консоли** (Console tree). Она содержит различные средства администрирования, такие как правила, политики. Эти средства администрирования в Консоли управления сгруппированы по папкам и отображены в формате дерева, что довольно удобно; в дальнейшем условимся называть различные средства администрирования элементами. Работа с деревом консоли подобна работе с Проводником Windows, только вместо привычных файлов здесь находятся некоторые элементы консоли. Например, для оснастки Редактор объектов групповой политики это будут политики и их параметры.

В центральной части экрана программы располагается **Область сведений** (Taskpad). По умолчанию она занимает основную долю экрана программы. В ней отображаются развернутые сведения о средствах администрирования, для каждой оснастки эти сведения будут индивидуальны. Например, для оснастки Редактор объектов групповой политики в этой области отображаются имена параметров и политик, их текущие состояния, пользовательские комментарии и некоторые другие сведения.

Область **Действия** (Actions) в правой части экрана предоставляет быстрый доступ к некоторым дополнительным действиям, специфичным для данной оснастки. Содержание данной области совпадает с пунктом меню **Действия** (Actions) панели инструментов. Большинство пользователей предпочитают скрывать эту область, чтобы предоставить больше пространства для других областей.

Добавление и удаление оснасток

Пустая Консоль управления MMC не имеет никакого практического применения, для того, чтобы начать работу, необходимо добавить оснастку. Вы можете создать собственную оснастку, а можете загрузить ранее созданную. В рамках этой книги мы будем пользоваться только стандартными оснастками консоли управления, такими как Редактор объектов групповой политики или Сертификаты.

Чтобы добавить или удалить оснастку консоли управления:

1. Выберите команду меню **Файл ⇒ Добавить или удалить оснастку (File ⇒ Add/Remove Snap-In).** Появится диалоговое окно **Добавление и удаление оснасток (Add or Remove Snap-Ins)** (рис. 1.2). Данное диалоговое окно можно вызвать также одновременным нажатием клавиш **Ctrl+M.**

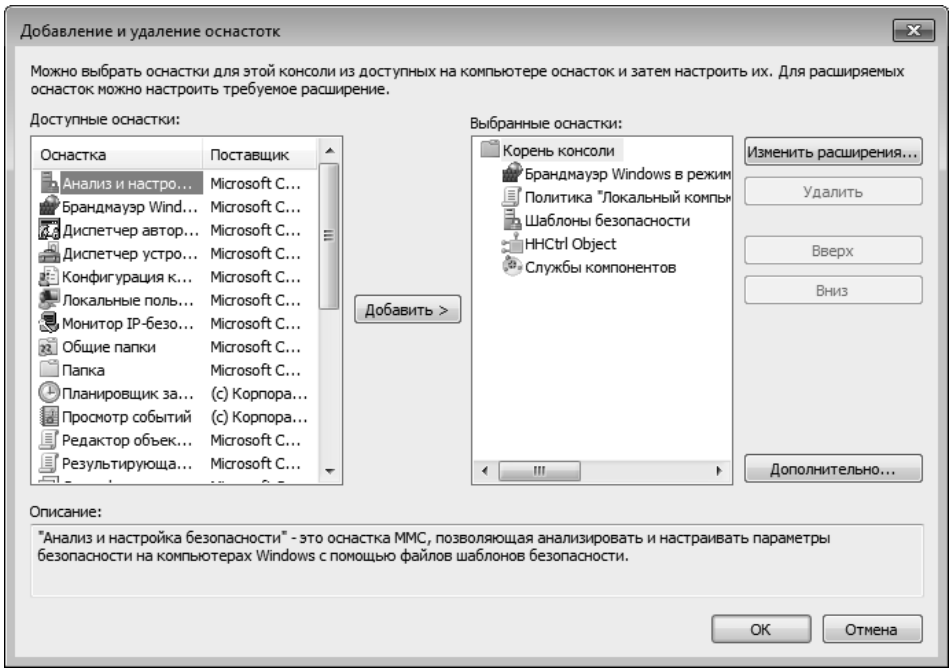


Рис. 1.2. *Диалоговое окно* Добавление и удаление оснасток

2. В списке **Доступные оснастки** (Available snap-ins) в левой части появившегося диалогового окна найдите интересующую вас оснастку. Получить краткую информацию по каждой оснастке можно в текстовом поле в нижней части диалогового окна. Для некоторых оснасток описание может отсутствовать.

3. Нажмите кнопку **Добавить** (Add). Выбранная оснастка добавится в список **Выбранные оснастки** (Selected snap-ins), который находится в левой части диалогового окна. Для некоторых оснасток предварительно необходимо выбрать объект администрирования в серии диалоговых окон. Например, для оснастки Редактор объектов групповой политики необходимо указать объект применения групповых политик.

4. Если вы хотите удалить оснастку, выделите ее мышью в списке **Выбранные оснастки** (Selected snap-ins) и нажмите кнопку **Удалить** (Remove).

5. Если вы хотите открыть несколько оснасток одновременно, перед вами встанет проблема последовательности их расположения в Консоли управления MMC. Для изменения порядка расположения

оснасток в окне Консоли управления MMC воспользуйтесь кнопками **Вверх** (Move Up) и **Вниз** (Move Down) диалогового окна **Добавление и удаление оснасток** (Add or Remove Snap-Ins).

6. Для завершения добавления или удаления оснасток щелкните **ОК**.

Подобным образом в одном окне консоли вы можете открыть несколько оснасток, настроить их под свой вкус. После чего вам, возможно, захочется сохранить все настройки консоли — в противном случае вам придется перед каждым началом работы с консолью производить все действия заново.

Сохранение файла консоли управления

После того, как вы определенным образом настроили Консоль управления MMC, загрузили необходимые оснастки, вы можете сохранить вашу консоль управления. Файл консоли управления имеет расширение .msc. Этот файл вы можете, например, сохранить на рабочий стол для быстрого запуска или передать коллеге.

Для того чтобы сохранить файл консоли управления:

1. Выберите команду меню **Файл ⇒ Параметры (File ⇒ Options).** Откроется диалоговое окно **Параметры (Options).**
2. На вкладке **Консоль** (Console) появившегося диалогового окна в поле ввода в верхней части экрана наберите имя файла консоли.
3. Нажмите кнопку **Сменить значок** (Change Icon). Откроется диалоговое окно **Смена значка** (Change Icon).
4. Выберите понравившееся изображение из предложенных в списке **Текущий значок** (Current Icon) или загрузите собственное. Для этого нажмите кнопку **Обзор** (Browse).
5. Подтвердите выбор нажатием кнопки **ОК**.

В диалоговом окне **Параметры** (Options) в раскрывающемся списке **Режим консоли** (Console mode) выберите:

- **Авторский** (Author mode), если хотите предоставить пользователю файла полный доступ к Консоли управления MMC. При помощи данного файла пользователь сможет добавлять и удалять оснастки, просматривать все участки дерева, создавать новые окна, а также создавать виды панели задач и задачи.
- **Пользовательский — полный доступ** (User mode — full access), если необходимо ограничить пользователя лишь в возможности изменения свойств консоли, а также добавления и удаления оснасток. В

остальном пользователь имеет полный доступ к дереву консоли.

- **Пользовательский — огр. доступ, много окон** (User mode — limited access, multiple window). Данный режим ограничит доступ пользователей к участкам дерева, невидимым в окне консоли. То есть пользователь получит доступ только к участкам дерева, которые были раскрыты к моменту сохранения файла консоли. При этом в данном режиме сохраняются все ограничения, которые были установлены для режима **Пользовательский — полный доступ** (User mode — full access).
- **Пользовательский — огр. доступ, одно окно** (User mode — limited access, single window). Этот режим ко всем ограничениям предыдущего прибавляет еще возможность работы только в одном окне. Пользователь при этом не имеет доступа к элементам управления, разрешающим работу со множественными окнами.

Если режимом консоли вы выбрали не **Авторский** (Author mode), то флажки **Не сохранять изменения для этой консоли** (Do not save changes to this console) и **Разрешить пользователю настраивать вид консоли** (Allow the user to customize views) станут активными. Установка первого флажка запретит пользователям вносить изменения в консоль, что немаловажно с точки зрения безопасности. Второй флажок разрешит пользователям доступ к диалоговому окну **Настройка вида** (Customize View), позволяющему настроить интерфейс программы.

6. Нажмите кнопку **ОК**, чтобы подтвердить изменение параметров.
7. Выберите команду меню **Файл ⇒ Сохранить как (File ⇒ Save As). Откроется диалоговое окно Сохранить как (Save As).**
8. В появившемся диалоговом окне определите пункт сохранения файла консоли, подтвердите сохранение нажатием кнопки **Сохранить** (Save).

Полученным файлом можете пользоваться как вы, так и другие пользователи. Грамотно настроенный файл консоли позволит сэкономить вам немало времени. При предоставлении прав другим лицам пользуйтесь правилом «наименьших привилегий»: оставляйте пользователям только необходимый минимум возможностей, это сделает систему более безопасной.

Работа с «Избранным»

Как правило, все оснастки консоли управления содержат огромное множе-

ство элементов. Так, например, оснастка Редактор объектов групповой политики содержит сотни узлов и тысячи параметров политик. Когда администратору системы при постоянной работе приходится каждый раз искать одни и те же параметры политик для редактирования, это занимает немало времени. В данной ситуации будет полезна функция создания и использования «Избранного»: она позволяет отсеять от огромного множества элементов наиболее интересные, вы можете сгруппировать их по папкам и всегда иметь к ним быстрый доступ.

Для того чтобы добавить элемент в «Избранное»:

1. Выделите интересующий вас элемент в дереве консоли при помощи мыши.
2. Выберите команду меню **Избранное ⇒ Добавить в избранное (Favorites ⇒ Add to Favorites)**. Откроется диалоговое окно **Добавление в папку «Избранное» (Add to Favorites).**
3. В поле ввода **Имя** (Name) введите название, которое будет отображаться вместо того имени элемента, которое отображается в дереве консоли — зачастую имена элементов довольно громоздкие, вы же можете заменить их удобными и короткими на свой вкус.
4. Возможно, со временем ваш список «Избранного» приобретет довольно большие размеры. Чтобы в нем не потеряться, можно разбить его на смысловые узлы, иными словами, создать папки для «Избранного». Для этого нажмите кнопку **Создать папку** (New Folder). В появившемся диалоговом окне введите название для узла и нажмите кнопку **ОК**.

Теперь в панели инструментов программы Консоль управления MMC при выборе пункта **Избранное** (Favorites) вы увидите ваш список элементов, разбитый на узлы в соответствии с вашим планом. Выбрать любой из них вы можете простым щелчком мыши.

Если в свое время вы пренебрегли созданием удобной структуры для ваших «Избранных» элементов или просто решите изменить состав списка, то в любой момент вы можете все привести в порядок. Для этого:

1. Выберите команду меню **Избранное ⇒ Упорядочить избранное (Favorites ⇒ Organize Favorites).** Откроется диалоговое окно **Упорядочить избранное (Organize Favorites)** (рис. 1.3).
2. В центральной части окна вы увидите список «Избранных» элементов, оформленный в виде дерева. Выберите в дереве интересующий элемент или папку.

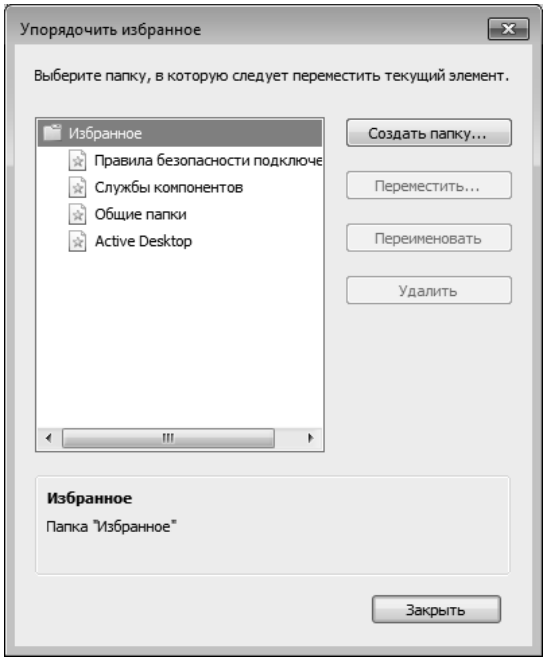


Рис. 1.3. *Диалоговое окно* Упорядочить избранное

3. Если вы хотите:

   - Переместить элемент или папку в другое место, то нажмите кнопку **Переместить** (Move to Folder). Откроется диалоговое окно **Папка для избранного** (Select Favorites Folder), в центральной части которого находится древовидный список «Избранного». Выберите папку, в которую необходимо перенести исходный элемент или папку, и нажмите кнопку **ОК**.
   - Переименовать элемент или папку, то нажмите кнопку **Переименовать** (Rename). Введите новое имя, затем нажмите клавишу **Enter**.
   - Удалить элемент или папку, то нажмите кнопку **Удалить** (Delete). Будьте внимательны: программа удалит выделенный объект без предупреждения. Если вы удаляете папку, то автоматически будет удалено все ее содержимое: другие папки и элементы. При этом вы также не получите от программы никакого предупреждения.
   - Создать новую папку, то нажмите кнопку **Создать папку** (Create Folder). В появившемся диалоговом окне укажите имя объ-

екта и нажмите кнопку **ОК**. Новая папка будет создана внутри объекта, который был выделен до нажатия кнопки. В случае ошибки, вы всегда можете исправить расположение элемента или папки при помощи кнопки **Переместить** (Move to Folder).

4. Когда вы закончите работу по настройке структуры «Избранного», нажмите кнопку **Закрыть** (Close).

Правильно составленный и структурированный список «Избранного» может сэкономить вам большое количество времени. Впрочем, если помимо элементов «Избранного» вы не используете прочих элементов оснастки даже изредка, имеет смысл создания новой оснастки только на основе элементов «Избранного». Данный ход отнимет у вас не так много времени, но позволит сделать работу еще удобнее.

1.2. Обзор стандартных оснасток

В Консоли управления MMC вы имеете возможность работать с огромным количеством стандартных оснасток, модифицировать их и создавать свои собственные. Практически все стандартные оснастки могут быть запущены более быстрым путем — напрямую через командную строку операционной системы, минуя запуск пользователем Консоли управления MMC.

Хотя в этой книге мы будем использовать в основном об оснастке Редактор объектов групповой политики, бегло рассмотрим некоторые другие стандартные оснастки. В Консоли управления MMC вы можете добавить следующие стандартные оснастки:

- **Анализ и настройка безопасности** (Security Configuration and Analysis). Оснастка позволяет настраивать параметры безопасности на компьютерах под управлением операционной системы Windows с помощью файлов шаблонов безопасности, а также производить анализ безопасности операционной системы.
- **Брандмауэр Windows с дополнительной безопасностью на локальном компьютере** (Windows Firewall with Advanced Security). Данная оснастка позволяет производить настройку встроенного в операционную систему Windows брандмауэра. Также вы можете работать с этой оснасткой через консоль wf.msc или запустив ее через Панель управления Windows.
- **Диспетчер авторизации** (Authorization Manager). Диспетчер авторизации позволяет задавать ролевые разрешения для приложений, использующих диспетчер авторизации. Приложения диспетчера ав-

торизации хранят политику авторизации в виде хранилищ авторизации, сохраненных в Active Directory или файлах XML. Политика вызывается диспетчером авторизации во время выполнения приложения. Также вы можете работать с этой оснасткой через консоль azman.msc.

- **Диспетчер устройств** (Device Manager). Диспетчер устройств предоставляет доступ к списку установленного на компьютере оборудования и соответствующих этому оборудованию драйверов. Здесь пользователь может совершить полноценную настройку оборудования. Также вы можете работать с этой оснасткой через консоль devmgmt.msc.
- **Конфигурация клиента защиты доступа к сети** (NAP Client Configuration). Оснастка позволяет настроить параметры конфигурации клиента защиты доступа к сети, а также осуществлять дальнейшее их управление. Вообще, речь идет о параметрах работы компонента NAP, суть работы которого заключается в блокировании доступа к системе компьютеров, не удовлетворяющих определенным вами требованиям. Также вы можете работать с этой оснасткой через консоль napclcfg.msc.
- **Локальные пользователи и группы** (Local Users and Groups). Оснастка позволяет добавлять, удалять и редактировать содержимое учетных записей и групп учетных записей пользователей операционной системы. Также вы можете работать с этой оснасткой через консоль lusrmgr.msc.
- **Монитор IP-безопасности** (IP-security Monitor). Оснастка используется для наблюдения за состоянием IP-безопасности и политикой IPsec, применяемой на текущем и других компьютерах. Данная информация может оказаться полезной при устранения неполадок в IPsec, а также при тестировании создаваемых политик.
- **Общие папки** (Shared Folders). Оснастка позволяет просматривать списки общих папок компьютера, созданных сетевых сессий, а также открытых по сети файлов. При помощи этой оснастки пользователь может создавать, редактировать и удалять различные параметры общих папок. Также вы можете работать с этой оснасткой через консоль fsmgmt.msc.
- **Папка** (Folder). Данная стандартная оснастка, по сути, не является самостоятельной: она служит скорее для упорядочивания готовой консоли. Все, что она делает, — осуществляет добавление пустой папки к дереву консоли.

- **Планировщик заданий** (Task Scheduler). Оснастка предоставляет доступ к списку автоматически запускаемых задач операционной системы. Здесь же вы можете добавлять различные типы задач или импортировать их из сторонних источников, просматривать журналы заданий, создавать различные простые и сложные структуры задач и многое другое. Также вы можете работать с этой оснасткой через консоль taskschd.msc.
- **Просмотр событий** (Event Viewer). Используя эту оснастку, вы получите удобный инструмент просмотра журнала событий операционной системы. В этих журналах содержится множество сведений о работе компонентов операционной системы, а также различных сторонних программ. Журналы событий — мощнейший инструмент в руках умелого системного администратора. Вы также можете работать с этой оснасткой через консоль eventvwr.msc.
- **Редактор объектов групповой политики** (Group Policy Object Editor). Именно об этой оснастке будет идти речь в основной части книги. Оснастка предоставляет доступ к работе групповых политик операционной системы. Также вы можете работать с этой оснасткой через консоль gpedit.msc.
- **Результирующая политика** (Resultant Set of Policy). Данная оснастка несколько упрощает процесс настройки групповых политик, действующих на конкретного пользователя. Оснастка используется как для уже применяемой политики, так и для определения, какая политика будет применена к пользователю компьютера. Также вы можете работать с этой оснасткой через консоль rsop.msc.
- **Сертификаты** (Certificates). Данная оснастка позволяет управлять пользовательскими сертификатами, сертификатами локального или удаленного компьютера, сертификатами удаленной или локальной службы. Консоль с этой оснасткой также может быть запущена через командную строку операционной системы — ее имя certmgr.msc.
- **Системный монитор** (Performance Monitor). Монитор производительности позволяет просматривать данные о производительности системы, такие как аппаратные сведения и системные ресурсы, используемые операционной системой, службами и работающими приложениями. Данные могут быть получены либо в режиме реального времени, либо в файле журнала. Также вы можете работать с этой оснасткой для остановки различных процессов, запуска и остановки системных служб, просмотра цепочки ожидания потока и идентификации файлов, ответственных за блокировку процессов, анализа вза-

имоблокировки процессов. Работа с оснасткой возможна через консоль perfmon.exe.

- **Службы** (Services). Оснастка позволяет запускать, останавливать и производить настройку служб операционной системы. Также вы можете работать с этой оснасткой через консоль services.msc или запустив ее через Панель управления Windows.
- **Службы компонентов** (Component Services). Оснастка позволяет получить доступ к ActiveX-объектам как локального, так и удаленного компьютера. Главным образом оснастка полезна для работы с настройками приложений COM+. Приложения COM+ представляют собой набор компонентов COM, взаимодействующих друг с другом и выполняющих управление очередями или реализующих возможность настройки параметров безопасности на основе ролей. Также вы можете работать с этой оснасткой через консоль comexp.msc.
- **Ссылка на веб-ресурс** (Link to Web Address). Данная стандартная оснастка, по сути, не является самостоятельной: при ее помощи вы можете добавить узел дерева консоли, в области сведений которого будет отображаться определенная пользователем веб-страница.
- **Управление TPM** (TPM Management). С помощью данной оснастки пользователь может управлять работой доверенного платформенного модуля TPM, который позволяет хранить конфиденциальные данные пользователя, параметры конфигурации компьютера и операционной системы. Также вы можете работать с этой оснасткой через консоль tpm.msc.
- **Управление компьютером** (Computer Management). Оснастка предоставляет множество средств управления операционной системой. Вы можете управлять настройками служебных программ, запоминающих устройств, служб и приложений из одной оснастки. В числе служебных программ числятся такие приложения, как Планировщик заданий, Просмотр событий, Общие папки, Локальные пользователи и группы, Производительность, Диспетчер устройств. Настройки многих из этих приложений доступны через отдельные специализированные оснастки. Также вы можете работать с оснасткой **Управление компьютером** (Computer Management) через консоль CompMgmtLauncher.exe.
- **Управление дисками** (Disk Management). Оснастка предоставляет широкие возможности по работе с разделами жестких дисков компьютера: вы можете форматировать разделы, работать с виртуальными дисками, изменять буквы дисков, создавать зеркальные образы

разделов и выполнять многие другие действия. Работа с этой оснасткой возможна также через консоль diskmgmt.msc.

- **Управление печатью** (Print Management). Оснастка представляет собой удобное средство управления работой серверов печати локального или удаленного компьютера, а также развернутыми принтерами. Также вы можете работать с этой оснасткой через консоль printmanagement.msc.
- **Управление политикой IP-безопасности** (IP-security Policy Management). Оснастка предоставляет средства для работы с политиками IPSec, ответственными за безопасное соединение с другими компьютерами. Также вы можете работать с этой оснасткой через консоль secpol.msc.
- **Управляющий элемент WMI** (WMI Control). Оснастка предназначена для настройки параметров работы службы Инструментарий управления Windows (WMI) на локальном или удаленном компьютере. Также вы можете работать с этой оснасткой через консоль wmimgmt.msc.
- **Шаблоны безопасности** (Security Templates). Оснастка помогает при работе с шаблонами безопасности Windows: создание, изменение, настройка шаблонов безопасности и многие другие возможности.
- **Элементы управления ActiveX** (ActiveX Control). Данная стандартная оснастка, по сути, не является самостоятельной: при ее помощи вы можете добавить узел дерева консоли, в области сведений которого будет содержаться Active-X элемент.

Консоль управления MMC предоставляет пользователю большое количество стандартных оснасток. Причем некоторые из оснасток частично или полностью перекрывают друг друга — то есть включают в себя функционал другой оснастки. Оснастка Редактор объектов групповой политики в этом плане сильно отличилась: освоив навыки работы в ней, запомнив расположение важных узлов, вы сможете полностью отказаться от использования большинства других оснасток, даже если вам приходится реализовывать сложнейшие административные задачи на компьютере.

1.3. Способы открытия редактора объектов групповой политики

В рамках данной книги осуществлять хакинг Windows 8 мы будем главным образом через редактирование так называемых групповых политик — фун-

даментальных настроек и правил работы системы.

Обратите внимание, что работа с групповыми политиками возможно только в версии Windows 8 Профессиональная или Windows 8 Корпоративная. Существует несколько способов открытия редактора для работы с объектами групповой политики. Скорее всего, вы будете пользоваться каким-то одним способом, однако для решения определенных задач могут потребоваться другие. Поэтому рассмотрим несколько путей открытия Редактора объектов групповой политики.

> **Примечание**. Редактор объектов групповой политики может быть запущен только под учетной записью администратора системы.

Первый способ вы могли бы предугадать на основании сведений, полученных из предыдущей главы книги — необходимо всего лишь добавить оснастку Редактор объектов групповой политики в Консоли управления MMC:

1. Откройте программу Консоль управления MMC.
2. Выберите команду меню **Файл ⇒ Добавить или удавить оснастку (File ⇒ Add/Remove Snap-In).** Появится диалоговое окно **Добавление и удаление оснасток (Add or Remove Snap-Ins).** Данное диалоговое окно можно вызвать также одновременным нажатием клавиш **Ctrl+M.**
3. В списке **Доступные оснастки** (Available snap-ins) в левой части появившегося диалогового окна найдите оснастку **Редактор объектов групповой политики** (Group Policy Object Editor).
4. В списке в левой части появившегося диалогового окна найдите пункт **Редактор объектов групповой политики** (Group Policy Object Editor). Нажмите кнопку **Добавить** (Add) или дважды щелкните мышью по этому пункту. Откроется диалоговое окно **Выбор объекта групповой политики** (Select Group Policy Object).
5. В появившемся диалоговом окне нажмите кнопку **Обзор** (Browse). Откроется диалоговое окно **Поиск объекта групповой политики** (Browse for a Group Policy Object).
6. Откройте вкладку **Пользователи** (Users) диалогового окна **Поиск объекта групповой политики** (Browse for a Group Policy Object) (рис. 1.4). На этой вкладке находится список доступных учетных записей операционной системы. Вы можете заметить, что кроме непосредственных учетных записей в списке есть еще два пункта: **Админи-**

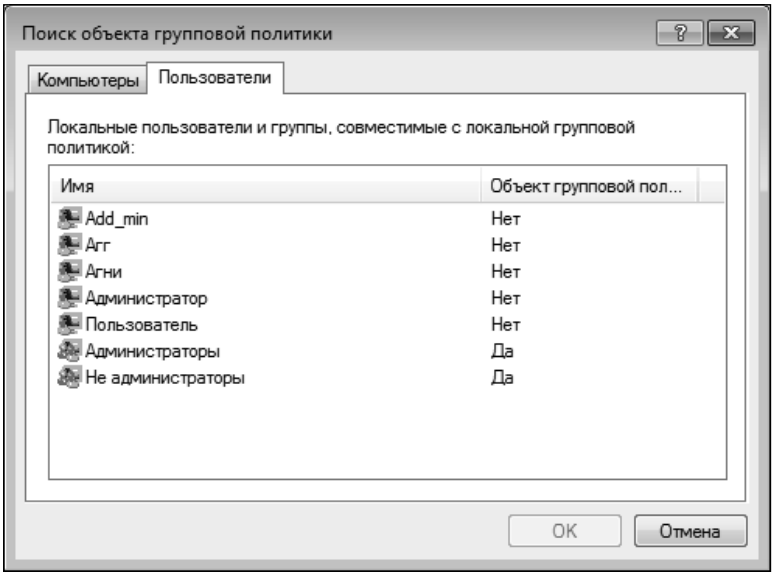


Рис. 1.4. *Диалоговое окно* Поиск объекта групповой политики

страторы (Administrators) и **Не администраторы** (Non-Administrators). Первый пункт определяет применение групповой политики ко всем учетным записям администраторов системы, второй — ко всем учетным записям системы без администраторских привилегий.

7. Щелчком мыши выделите необходимый объект применения групповой политики. Нажмите кнопку **ОК**.

8. В диалоговом окне **Выбор объекта групповой политики** (Select Group Policy Object) нажмите кнопку **Готово** (Finish).

9. В диалоговом окне **Добавление и удаление оснасток** (Add or Remove Snap-Ins) нажмите кнопку **ОК**. В Консоли управления MMC откроется оснастка **Редактор объектов групповой политики** (Group Policy Object Editor).

Довольно долгий путь, особенно если вы обращаетесь к данной оснастке постоянно. Поэтому для ускорения доступа вы можете сохранить файл консоли — тогда доступ к уже настроенному Редактору объектов групповой политики можно будет получить в два щелчка мыши.

В несколько урезанном варианте Редактор объектов групповой политики может быть запущен, минуя открытие Консоли управления MMC. Однако в этом случае вы сможете работать только с локальными групповыми политиками. Впрочем, в данной книге в основном рассматривается работа именно с локальными групповыми политиками, поэтому для работы данной версии редактора будет достаточно.

Для запуска Редактора локальной групповой политики:

1. Нажмите сочетание клавиш **Windows+R**. Откроется диалоговое окно **Выполнить** (Run).
2. В поле ввода **Открыть** (Open) введите «gpedit.msc».
3. Нажмите кнопку **ОК**, чтобы подтвердить запуск программы. Откроется окно **Редактор локальной групповой политики** (Local Group Policy Editor) (рис. 1.5).

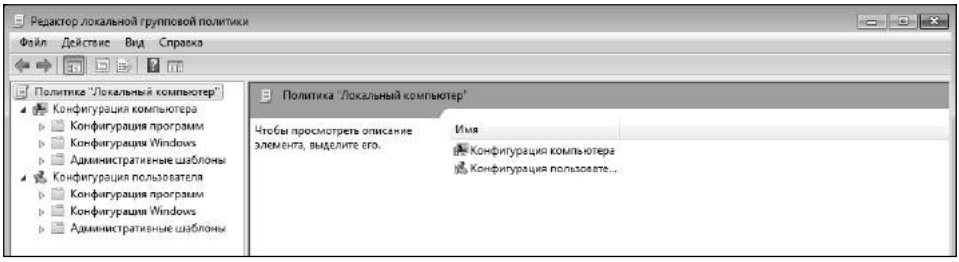


Рис. 1.5. ***Окно оснастки Редактор локальной групповой политики***

Интерфейс программы Редактора локальной групповой политики практически полностью совпадает с интерфейсом соответствующей оснастки.

Существует еще несколько способов открытия Редактора объектов групповой политики, применимых для реализации политик к специфичным объектам, таким как сайт, домен или подразделение. Эта задача реализуется с использованием Active Directory. Ввиду редкого применения, данный способ рассмотрен в книге не будет.

При рассмотрении политик и их параметров мы в основном будем пользоваться Редактором локальной групповой политики, поэтому все примеры ориентированы на использование именно этой оснастки.

1.4. Начало работы в Редакторе локальной групповой политики

Как вы можете заметить, интерфейс Редактора локальной групповой политики практически идентичен интерфейсу оснастки Консоли управления MMC. В левой части окна, в области **Дерево консоли** (Console tree) размещен список всех доступных узлов оснастки групповых политик операционной системы: политик и их параметров. В правой части окна отображаются доступные для редактирования политики и параметры политик выбранного узла. По умолчанию область **Действия** (Actions) скрыта, но вы всегда мо-

жете включить ее отображение. При работе с групповыми политиками применение ей найти непросто, она лишь будет занимать ценное пространство окна программы, поэтому для большинства пользователей возможность включить ее отображение не представит интереса.

Для настройки параметра необходимой политики необходимо найти его в огромном дереве групповых политик Windows, затем дважды щелкнуть по нему мышью. Появится диалоговое окно настройки параметра групповой политики. Вид отображаемого диалогового окна может отличаться для различных политик. Все диалоговые окна настройки параметров политик узла **Административные шаблоны** (Administrative Templates) выглядят единообразно, для других же узлов их вид значительно отличается от параметра к параметру.

Зачастую найти необходимую политику или ее параметр оказывается не так-то просто, поэтому в книге будут рассмотрены способы фильтрации политик для ускорения процесса поисков. Для начала рассмотрим способы ускоренного передвижения по окну консоли — вы можете сэкономить немало времени, выполняя некоторые действия при помощи клавиатуры. Вот некоторые из них:

- Клавиша **Tab** позволяет быстро переключаться между областями активного окна консоли. При этом переключение областей осуществляется по замкнутому кругу. Использование сочетания клавиш **Shift**+**Tab** позволяет осуществлять переключение в обратном направлении.
- Клавиша — на цифровой клавиатуре позволяет осуществить свертывание содержимого выбранного узла дерева консоли. Клавиша **+** цифровой клавиатуры, наоборот, производит развертывание содержимого выбранного узла.
- Клавиша ***** на цифровой клавиатуре позволяет осуществить полное развертывание содержимого всех узлов дерева консоли, расположенных под выбранным узлом. Данная возможность полезна, когда вы производите поиск необходимой политики, постепенно закрывая ненужные, уже просмотренные, узлы дерева.
- При помощи клавиш с изображением стрелок удобно перемещаться по дереву консоли: клавиши ↑ и ↓ позволяют перемещать выделение узла в вертикальной плоскости, клавиши ← и → позволяют сворачивать и развертывать содержимое узла. Если использовать клавиши ← и → на пустом узле, их действие идентично нажатию клавиш ↑ и ↓ соответственно.

- Клавиша **Page Up** перемещает выделение на самый верхний видимый элемент области. Клавиша **Page Down** соответственно перемещает выделение на самый нижний видимый элемент области. Клавиши **Home** и **End** позволяют быстро выбрать первый или последний элемент области.
- Сочетание клавиш **Alt**+← установит выделение на предыдущий выделенный объект, после чего станет возможно применение сочетания клавиш **Alt**+→ — установление выделения на следующий выделенный объект.

Все перечисленные выше приемы использования клавиатуры при работе с оснасткой Редактор локальной групповой политики могут быть использованы с любой другой оснасткой Консоли управления MMC. В конечном счете использование клавиатуры может сэкономить значительное количество времени: попробуйте на практике сами.

При первом просмотре дерева консоли вы можете заметить два основных узла: **Конфигурация компьютера** (Computer Configuration) и **Конфигурация пользователя** (User Configuration). Политики первого узла применяются к компьютеру независимо от пользователя, работающего в данный момент с системой.

Политики второго узла применяются к пользователю независимо от компьютера, с которого был осуществлен вход в систему. На деле достаточно усвоить: политики узла **Конфигурация пользователя** (User Configuration) применяются к конкретному пользователю, в то время как политики узла **Конфигурация компьютера** (Computer Configuration) применяются ко всем пользователям операционной системы одновременно. Вы можете заметить, что основная масса политик обоих узлов совпадает, однако сходство это не абсолютное: некоторые политики существуют для применения только на пользователя или только на компьютер.

Все используемые вами политики применяются каждый раз при загрузке операционной системы, внесении изменений в оснастке, а также обновляются каждые полтора-два часа в фоновом режиме.

В каждом из основных узлов оснастки находится по три дочерних: **Конфигурация Windows** (Windows Settings), **Конфигурация программ** (Software Settings), **Административные шаблоны** (Administrative Templates). Данные узлы будут подробно рассмотрены в книге, но для начала приведем их краткую характеристику.

В узле **Конфигурация Windows** (Windows Settings) содержатся средства настройки учетной записи и безопасности компьютера. В составе данного

узла вы можете увидеть пять дочерних:

- **Политика разрешения имен** (Name Resolution Policy). Этот узел может быть найден только в составе основного узла **Конфигурация компьютера** (Computer Configuration), в основном узле **Конфигурация пользователя** (User Configuration) он отсутствует. Узел **Политика разрешения имен** (Name Resolution Policy) позволяет управлять расширением таблицы политик разрешения имен, содержащей параметры конфигурации для безопасности DNS.
- **Сценарии** (Scripts). Настройка сценариев автозапуска и завершения работы операционной системы. Операционная система Windows предоставляет широкие возможности работы со сценариями: вы можете использовать сценарии ActiveX, пакетные файлы и сценарии PowerShell.
- **Развернутые принтеры** (Deployed Printers). Политики данного узла помогают настроить совместное использование принтеров.
- **Параметры безопасности** (Security Settings). Политики узла предназначены для обеспечения безопасности системы.
- **QoS на основе политики** (Policy-based QoS). Политики данного узла определяют настройки проводных сетей: приоритеты трафика, управление скоростью передачи данных и другие.
- **Настройки Internet Explorer** (Internet Explorer Maintenance). Управление различными параметрами стандартного браузера операционной системы Windows, а также некоторыми настройками сетей. Данный узел доступен только в основном узле **Конфигурация пользователя** (User Configuration).

Узел **Административные шаблоны** (Administrative Templates) является самым большим: в нем содержатся тысячи параметров приложений и компонентов операционной системы. Политики данного узла основываются на записях Реестра Windows: каждому параметру политики узла **Административные шаблоны** (Administrative Templates) соответствует определенный параметр системного реестра Windows. Однако работа с Реестром Windows трудна и неудобна, в то время как работа с оснасткой Редактор объектов групповой политики проста и позволяет решить поставленные задачи в кратчайшие сроки.

Глава 2.

Хакинг интерфейса Windows 8

Прежде чем читать данную главу обязательно ознакомьтесь с принятыми соглашениями, обозначенными на стр. 10. Использование локальных политик для настройки пользовательского окружения в операционной системе Windows 8 открывает широкие возможности как перед системным администратором, так и перед простым пользователем операционной системы. В этой главе мы с вами познакомимся с основными параметрами, помогающими настроить интерфейс операционной системы — панель задач, пространство рабочего стола и мини-приложения.

2.1. Управление параметрами панели задач Windows

Данная часть главы будет достаточно объемной, так как использование групповых политик для настройки панели задач предлагает очень большое количество различных параметров. Первое, с чем мы познакомимся в данной части главы, — запрет на изменение любых параметров панели задач.

Блокировка перемещения панели задач

Если вам требуется заблокировать перемещение панели задач по сторонам рабочего стола, вы можете переместить ее в нужное положение, после чего заблокировать эту возможность. Для этого нужно активировать соответствующую политику:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач (**User Configuration ⇒ Administrative Templates ⇒ Taskbar**)**.
2. Дважды щелкните мышью по параметру **Запретить перемещение панели задач в другое положение на экране** (Prevent users moving taskbar to another screen dock location). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled). Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).

4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Следующий параметр запрещает изменение размера и перемещение панели задач, но при этом автоматическое скрытие и другие возможности панели задач можно по-прежнему настраивать:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Menu and Taskbar).
2. Дважды щелкните мышью по параметру **Закрепить панель задач** (Lock the Taskbar). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

> **Примечание.** Если этот параметр включен, то панель быстрого запуска и все остальные панели инструментов на панели задач пользователя также закрепляются. Пользователь не может изменять положение панели инструментов, а также скрывать и отображать ее с помощью контекстного меню панели задач.

После этого, при попытке изменения положения панели задач при помощи контекстного меню, пользователь увидит, что в контекстном меню, вызываемом при щелчке правой кнопки мыши по панели задач, пункт **Закрепить панель задач** (Lock the Taskbar) не только активирован, но и недоступен для редактирования.

Сокрытие панелей инструментов в панели задач

Редактор групповых политик также позволяет полностью скрыть все дополнительные панели инструментов на панели задач. Активируется это другим параметром групповых политик:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Не отображать панели инструментов в панели задач** (Do not display any custom toolbars in the taskbar). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).

4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После активации данного параметра из контекстного меню, вызываемого щелчком правой кнопки мыши по панели задач, исчезнет пункт **Панели** (Toolbars), а после перезагрузки операционной системы с панели задач будут скрыты все дополнительные панели инструментов.

Сокрытие значков в области уведомлений

Помимо запрета отображения часов в области уведомлений, с помощью редактора групповых политик в операционных системах Windows 8 и Windows Server 2008/2012 можно также скрыть большинство прочих значков.

> **Примечание**. Обратите внимание на то, что изменения отображения значков в области уведомления вступят в силу лишь после перезагрузки операционной системы.

Начнем со значка регулятора громкости:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Скрыть значок регулятора громкости** (Remove the volume control icon). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Для того, чтобы скрыть индикатор батареи, нужно изменить другой параметр:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Скрыть индикатор батареи** (Remove the battery meter). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Если вы хотите скрыть индикатор сети, выполните следующие шаги:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Скрыть значок сети** (Remove Network icon from Start Menu). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Если же вы хотите скрыть всю область уведомлений панели задач, активируйте параметр **Скрыть область уведомлений** (Hide the notification area):

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Скрыть область уведомлений** (Hide the notification area). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Аналогичным образом можно скрыть значок, отвечающий за программу центра поддержки пользователей Windows:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Удалить значок центра поддержки** (Remove Action Center icon). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Если вы хотите запретить отображение вновь добавленных значков в области уведомления и при этом разрешить пользователям настраивать и скрывать их, активируйте следующий параметр:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Отключение автоматического отображение значков уведомлений в панели задач** (Turn off automatic promotion of notification icons to the taskbar). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Удаление часов из области уведомлений

В том случае, если вы хотите скрыть часы в области уведомлений, вам нужно будет внести следующие изменения в редакторе групповых политик:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Удалить часы из системной области уведомлений** (Remove Clock from the system notifications area). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После этого для удаления часов из области уведомления необходимо перезагрузить компьютер. Вновь загрузив операционную систему Windows 8, вы уже не увидите часы на привычном месте.

Запрет скрытия значков

Для экономии места на панели задач разработчики семейства операционных систем Windows предусмотрели возможность частичного скрытия значков из области уведомлений. Если вы как системный администратор хотите запретить пользователям скрывать значки, можно сделать это с помощью редактора групповых политик:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative

Templates ⇒ Taskbar).

2. Дважды щелкните мышью по параметру **Отключить очистку области уведомлений** (Turn off notification area cleanup). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Теперь осталось только перезагрузить компьютер для того, чтобы увидеть эффект изменения настройки. Теперь все значки без исключения будут отображаться на панели задач.

Запрет группировки элементов на панели задач

По умолчанию в операционных системах Windows, начиная с версий Windows XP Professional и Windows Server 2003, на панели задач предусмотрена группировка схожих элементов панели задач. Если вы хотите заблокировать эту функцию, активируйте следующий параметр:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Запретить группировку элементов панели задач** (Prevent grouping of taskbar items). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После активации данного параметра схожие элементы на панели задач не будут группироваться друг с другом.

Запрет закрепления Ярлыков в списках переходов

В операционной системе Windows 8 появилось дополнительное подспорье при работе с уже открывавшимися папками, веб-сайтами и файлами. К каждому ярлыку программы предусмотрен список переходов, отображающий последние посещенные (а также закрепленные пользователем) каталоги и документы, открывавшиеся в этой программе.

Если вы хотите запретить пользователям закрепление элементов в списках

переходов на панели задач, это можно легко сделать при помощи редактора групповых политик:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Запретить закрепление элементов в списках переходов** (Do not allow pinning items in Jump Lists). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После активации данного параметра пользователи не смогут закреплять файлы, папки, веб-сайты и прочие элементы в списках переходов панели задач. Кроме того, пользователи не смогут удалить закрепленные ранее элементы.

Запрет отображения и отслеживания элементов в списках переходов удаленных расположений

На панели задач отображаются списки переходов из программ. Они дают возможность более оперативно открыть определенное расположение или файл. Если вы хотите, чтобы в этих списках фигурировали только локальные файлы, а файлы, расположенные на других компьютерах, игнорировались, активируйте соответствующий параметр с помощью редактора групповых политик:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Не отображать и не отслеживать элементы в списках переходов из удаленных расположений** (Do not display or track items in Jump Lists from remote locations). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После активации данного параметра из списков переходов исчезнут все удаленные файлы, за исключением тех, которые пользователь самостоятельно закрепил в списках переходов.

Отключение всплывающих уведомлений

Если вы хотите избавить себя или других пользователей от всплывающих в области панели задач уведомлений, вы можете легко сделать это с помощью редактора групповых политик:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Отключить всплывающие напоминания** (Turn off all balloon notifications). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После этого операционная система перестанет уведомлять вас о различных событиях за счет использования всплывающих уведомлений.

Однако если вы хотите отключить только всплывающие уведомления, вызываемые компонентами операционной системы (а не сторонними программами), вы можете изменить другой параметр в редакторе групповых политик:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Отключить всплывающие уведомления объявлений компонентов** (Turn off feature advertisement balloon notifications). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

При изменении этого параметра все всплывающие уведомления, кроме уведомлений компонентов операционной системы, будут отображаться.

Запрет управления панелями инструментов

Панель задач предлагает пользователю значительное расширение возможностей за счет использования дополнительных панелей инструментов. По умолчанию в операционной системе Windows 8 включена только одна дополнительная панель — языковая, с помощью которой можно изменять языки ввода.

Пользователь может с легкостью добавить новые панели инструментов с помощью контекстного меню, вызываемого щелчком правой кнопки мыши по панели задач.

Однако, в том случае, если требуется запретить добавление и удаление панелей инструментов, это можно сделать с помощью соответствующей политики:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Запретить добавление и удаление панелей инструментов** (Prevent users from adding or removing toolbars). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После включения данного параметра содержимое пункта **Панели** (Toolbars) контекстного меню, вызываемого щелчком правой кнопки мыши по панели задач, невозможно будет изменить.

Если вы не хотите устанавливать запрет на добавление и удаление дополнительных панелей, а лишь планируете заблокировать настройку данных элементов пользовательского интерфейса — активируйте другой параметр в редакторе групповых политик:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Рабочий стол** (User Configuration ⇒ Administrative Templates ⇒ Desktop).
2. Дважды щелкните мышью по параметру **Запретить настройку панелей инструментов рабочего стола** (Prevent users from setting toolbars). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).

4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Схожие функции выполняет политика **Запретить добавление, перетаскивание и закрытие панелей инструментов панели задач** (Prevent users from adding, setting or closing toolbars).

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Рабочий стол** (User Configuration ⇒ Administrative Templates ⇒ Desktop).
2. Дважды щелкните мышью по параметру **Запретить добавление, перетаскивание и закрытие панелей инструментов панели задач** (Prevent users from adding, setting or closing toolbars). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После этого любое изменение свойств и настроек панелей будет заблокировано.

Запрет на вызов контекстного меню панели задач

Если же вы не хотите ограничивать пользовательские настройки панели задач частично, а запретить всякое изменение настроек этих элементов, вы можете просто запретить запуск контекстного меню, появляющегося при щелчке правой кнопки мыши по панели задач и кнопке **Пуск** (Start). Для этого достаточно выполнить четыре простых шага:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Запретить доступ к контекстному меню для панели задач** (Remove access to the context menus for the taskbar). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После этого, при попытке вызова контекстного меню ничего происходить не будет. При этом контекстное меню для задач и ярлыков будет продолжать работать.

Запрет закрепления программ в панели задач

В новой панели задач, появившейся в операционной системе Windows 8, появилась возможность прикрепить приложения к панели задач. Это решение позволяет убить одним выстрелом сразу двух зайцев: совместить панель быстрого запуска с панелью задач.

Экономия места и удобная работа с приложениями в одном флаконе. Однако если вы хотите отключить возможность добавления пользователями новых прикрепленных приложений, можно использовать для этого соответствующий параметр групповых политик:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar)
2. Дважды щелкните мышью по параметру **Запретить закрепление программ в панели задач** (Do not allow pinning programs to the Taskbar). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После включения данного параметра пункт **Закрепить программу в панели задач** (Do not allow pinning programs to the Taskbar) пропадет из контекстного меню, вызываемого щелчком правой кнопки мыши по приложению в панели задач. При этом возможность откреплять ранее прикрепленные к панели задач приложения сохраняется.

Так же с помощью редактора групповых политик в операционной системе Windows 8 (Windows Server 2008) можно с помощью изменения одного из параметров удалить все закрепленные в панели задач программы:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Удалить закрепленные программы из панели задач** (Remove pinned programs from the Taskbar). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Если вы включите оба параметра, при следующем входе в систему пользо-

ватель увидит пустую панель задач и не сможет разместить на ней ярлыки приложений.

Запрет изменения размера панели задач

С помощью изменения параметров групповых политик можно также запретить изменение размера панели задач. Делается это очень просто:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Запретить изменение размера панели задач** (Prevent users from resizing the taskbar) Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После активации данного параметра пользователь не сможет изменить размер панели задач.

Запрет перемещения панелей инструментов

Точно так же, с помощью изменения параметров групповых политик, можно запретить перемещение панелей инструментов пользователем операционной системы Windows. Для активации данного ограничения необходимо изменить соответствующий параметр:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar)
2. Дважды щелкните мышью по параметру **Запретить перемещение панелей инструментов** (Prevent users from rearranging toolbars). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Теперь при попытке изменения размеров или перемещения дополнительных панелей инструментов, несмотря на соответствующие изменения указателя мыши, размер и положение панелей инструментов изменяться не будет.

Блокировка всех параметров панели задач

Блокировка всех параметров панели задач запрещает пользователю вносить какие-либо изменения в настройки панели задач. Чтобы активировать данный параметр, нужно:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Блокировать все параметры панели задач** (Lock all taskbar settings). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После этого при попытке редактирования свойств панели задач в диалоговом окне с настройками не будут отображаться вкладки **Панели задач** (Taskbar) и **Панели инструментов** (Toolbars) (рис 2.1).

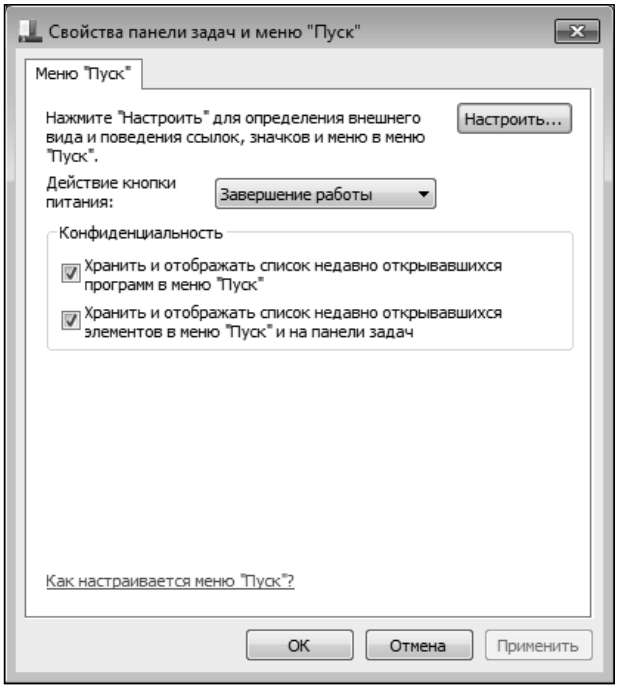


Рис 2.1. ***Диалоговое окно*** **Свойства панели задач и меню «Пуск»** ***при запрете изменения настроек панели задач***

Запрет изменения параметров панели задач

Если вы хотите полностью запретить изменение любых параметров панели задач, вы можете воспользоваться следующим параметром:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Запретить изменение параметров панели задач и меню «Пуск»** (Prevent changes to Taskbar and Start Menu Settings). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После этого будет запрещен вызов диалогового окна с настройками данных элементов с помощью щелчка правой кнопки мыши по кнопке **Пуск** (Start) или панели задач.

Изменение параметров поиска в окне Проводник

Вероятно, вы заметили, что по умолчанию в поле с результатами поиска отображается еще ссылка **Ознакомиться с другими результатами поиска** (See more results). Эта ссылка открывает окно программы Проводник, который отображает все найденные файлы, папки, ярлыки и документы, подходящие под данный поисковый запрос. В том случае, если вы хотите удалить эту ссылку, вам нужно воспользоваться соответствующим параметром в редакторе групповых политик:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar)
2. Дважды щелкните мышью по параметру **Удалить ссылку «Ознакомиться с другими результатами» или «Поиск везде»** (Remove See More Results/ Search Everywhere Link). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).

4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После этого вы не увидите ссылки, открывающей проводник Windows в результатах поиска.

Запрет поиска файлов и соединений

Если вы хотите запретить отображение файлов и папок в результатах поиска, вам нужно изменить следующий параметр:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Запретить поиск файлов** (Do not search files). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После активации данного параметра при вводе запросов в поле ввода **Найти программы и файлы** (Search programs and files) в результатах не будут отображаться папки и файлы.

Если же вы хотите, чтобы в результатах поиска не отображались соединения, измените другой параметр:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Запретить поиск соединений** (Do not search communications). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После активации данного параметра при вводе запросов в поле ввода **Найти программы и файлы** (Search programs and files) в результатах поиска не будут отображены соединения, созданные в операционной системе.

Запрет поиска программ и элементов панели управления

Если вы хотите запретить пользователям компьютера с операционной системой Windows 8 видеть в результатах поиска программы и элементы панели управления, активируйте следующую политику:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Запретить поиск программ и элементов панели управления** (Do not search programs and Control Panel items). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После активации данного параметра при вводе запросов в поле ввода **Найти программы и файлы** (Search programs and files) в результатах не будут отображаться ярлыки программ и компонентов панели управления.

Настройка поиска файлов для пустых ярлыков

В семействе операционных систем Windows, начиная с версии Windows 2000, при отсутствии файла, на который ссылает ярлык (файл с расширением .lnk), операционная система самостоятельно пытается найти путь к конечному файлу сначала в папках, сопоставленных с данным ярлыком, а затем и на всем жестком диске. Если вы хотите отключить функцию поиска на всем диске, активируйте следующий параметр:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Не использовать сопоставление ярлыков оболочки на основе поиска** (Do not use search-based method when resolving shell shortcuts). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После активации данного параметра, если ярлык будет ссылаться на отсутствующий объект, операционная система выдаст сообщение о том, что конечный файл не найдет, и не предпримет попыток к его поиску.

> **Примечание**. Данный метод поиска файлов работает только в файловой системе NTFS.

Если же вы, напротив, хотите, чтобы операционная система Windows сразу начинала искать потерянные файлы на диске, минуя поиск по сопоставленным с ярлыком каталогам, активируйте другой параметр:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Не использовать метод на основе отслеживания для сопоставления ярлыков** (Do not use tracing-based method when resolving shell shortcuts). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Удаление и блокировка команд Завершение работы, Сон и Гибернация

Запрет завершения работы, перевода компьютера в режим сна или гибернации позволяет установить запрет на выполнение данных команд для всех программ. Таким образом, при запрете использования данных команд никаким образом нельзя завершить работу операционной системы или перевести ее в спящий или ждущий режим.

Чтобы активировать данную политику, необходимо:

1. Перейти в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкнуть мышью по параметру **Удаление команд «Завершение работы», «Перезагрузка», «Сон» и «Гибернация»** (move and prevent access to the Shut Down, Sleep, And Hibernate commands). Откроется одноименное окно для редактирования данной политики.

3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

При попытке выключения компьютера каим-либо из вышеперечисленных способов система выдаст диалоговое окно с предупреждением о невозможности выполнения данной команды.

Запуск команды «Выполнить» в отдельной области памяти

В операционной системе Windows 8 предусмотрена возможность запуска файла в отдельном (выделенном) 16-разрядном режиме виртуализации системы DOS, что позволяет обеспечить более корректную работу 16-разрядных приложений.

Если вы используете 16-разрядные приложения в своей работе, вы можете активировать возможность их запуска в области выделенной памяти:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель задач** (User Configuration ⇒ Administrative Templates ⇒ Taskbar).
2. Дважды щелкните мышью по параметру **Добавить флажок «Запустить в отдельной области памяти» в окно команды «Выполнить»** (Add «Run in Separate Memory Space» check box to Run dialog box). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После этого, при открытии диалогового окна **Выполнить** (Run), вы сможете увидеть флажок **Запустить в отдельной области памяти** (Run in Separate Memory Space) в нижней части диалогового окна.

2.2. Хакинг рабочего стола

Теперь перейдем ко второй части главы, которая будет посвящена настройкам рабочего стола при помощи редактора групповых политик.

Запрет сворачивания окна Aero Shake

Многие пользователи операционной системы Windows 8 положительно отнеслись к новой графической системе Aero, появившейся в операционной системе Windows Vista. Операционная версия Windows 8 добавила в графическую систему Aero ряд новшеств, одним из которых можно назвать функцию Aero Shake. Ее суть проста: для того, чтобы оставить на рабочем столе только активное окно, достаточно установить указатель мыши на заголовок нужного окна, а затем, зажав и не отпуская левую кнопку мыши, потрясти окно. Кому-то функция Aero Shake пришлась по нраву, а кому-то мешает работать. Для второй группы пользователей разработчики операционной системы Windows 8 предусмотрели отключение функции Aero Shake при помощи редактора групповых политик. Сделать это можно следующим образом:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Рабочий стол** (User Configuration ⇒ Administrative Templates ⇒ Desktop).
2. Дважды щелкните мышью по параметру **Отключить сворачивание окна Aero Shake жестом мышью** (Turn off Aero Shake window minimizing mouse gesture). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
5. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После изменения параметра ни случайно, ни намеренно, жестом свернуть окна не удастся.

Запрет на сохранение настроек

Ну и наконец, мы хотим рассказать о достаточно удобном и практичном параметре редактора групповых политик. Этот параметр называется **Не сохранять параметры при выходе** (Don't save settings at exit).

Если этот параметр включен, пользователь имеет рад ограничений по изменению рабочего стола своего сеанса. Если говорить точнее, пользователь может изменять все параметры рабочего стола, однако после перезагрузки большая часть настроек вернется к установкам, заданным администратором. Безусловно, эти настройки не коснутся ярлыков на рабочем столе, но по-

ложение и размер панели, расположение и размер окон и другие настройки вернутся в состояние по умолчанию. Рассмотрим, как можно активировать данный параметр:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Рабочий стол** (User Configuration ⇒ Administrative Templates ⇒ Desktop).
2. Дважды щелкните мышью по параметру **Не сохранять параметры при выходе** (Don't save settings at exit). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После следующей перезагрузки параметр станет активным.

Ограничение доступа к свойствам элементов рабочего стола

В операционных системах семейства Windows ярлыки основных элементов не только позволяют запускать нужные функции, но и изменять ряд параметров для каждого из элементов. Для того чтобы сделать это, нужно щелкнуть правой кнопкой мыши по нужному ярлыку и в появившемся контекстном меню выбрать пункт свойства.

Для определенного ряда системных ярлыков, таких как **Корзина** (Recycle Bin) и **Компьютер** (Computer), изменение свойств ярлыка несет за собой ряд серьезных корректив системных параметров. Администратор может с легкостью запретить вызов данного пункта меню, активировав соответствующую политику в редакторе групповых политик. Безусловно, это лишь заблокирует один, наиболее простой, путь к изменению свойств системных элементов, однако этого вполне достаточно для создания должного уровня безопасности работы за компьютером, если при этом использовать другие элементы групповых политик.

Вызов окна **Свойства** (Properties) для значка **Компьютер** (Computer) позволит пользователю получить доступ к основным настройкам операционной системы. Однако без должного багажа знаний пользователь запросто может изменить настройки операционной системы не лучшим для полноценной работы образом.

Именно поэтому ограничение доступа к параметру свойства для значка

Компьютер (Computer) позволит быть уверенным в отсутствии временных издержек при работе с компьютером. Заблокировать пункт **Свойства** контекстного меню для значка **Компьютер** очень просто:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Рабочий стол** (User Configuration ⇒ Administrative Templates ⇒ Desktop).
2. Дважды щелкните мышью по параметру **Удалить пункт «Свойства» из контекстного меню значка «Компьютер»** (Remove Properties from the Computer icon context menu). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Ограничение изменения настроек элемента **Корзина** (Recycle Bin), расположенного на рабочем столе, обеспечивает сохранность файлов пользователя, так как при удалении файлов и папок операционная система запрашивает подтверждение на данное действие, а затем перемещает файл в папку **Корзина** (Recycle Bin). Изменив свойства значка **Корзина** (Recycle Bin), можно отменить эти условия, обеспечивающие безопасность данных пользователя. Запретив доступ к свойствам элемента **Корзина** (Recycle Bin), можно уберечь пользователя операционной системы от возможных неприятных последствий.

Рассмотрим, как скрыть пункт **Свойства** (Properties) в контекстном меню для элемента **Корзина** (Recycle Bin).

Чтобы отключить пункт **Свойства** (Properties) контекстного меню значка **Корзина** (Recycle Bin), нужно:

1. Перейти в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Рабочий стол** (User Configuration ⇒ Administrative Templates ⇒ Desktop).
2. Дважды щелкнуть мышью по параметру **Удалить пункт «Свойства» из контекстного меню компонента «Корзина»** (Remove Properties from the Recycle Bin icon context menu). Откроется одноименное окно для редактирования данной политики.
3. Установить переключатель в положение **Включить** (Enabled).
4. Нажать кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После этого при щелчке правой кнопки мыши по значку **Корзина** (Recycle Bin) пункт свойства не перестанет отображаться, однако при попытке вызова диалогового окна со свойствами элемента **Корзина** (Recycle Bin) пользователь операционной системы увидит диалоговое окно, предупреждающее об ограничении доступа.

Удаление системных значков с рабочего стола

Указанный в предыдущей части главы способ блокировки изменения настроек для ряда системных значков позволяет ограничить способы изменения системных параметров. Однако можно также ограничить доступ к определенным элементам операционной системы еще более радикальными методами. К одному из таких методов относится удаление ярлыков и системных значков с рабочего стола. К тому же, помимо соображений безопасности и ограничения доступа, может быть ряд других причин, которые потребуют удалить ярлыки с рабочего стола. Сюда можно отнести даже желание отображения только фонового изображения на рабочем столе.

Если ярлыки, которые на рабочий стол автоматически добавляют программы после установки и пользователи вручную, удалить достаточно просто, то с сокрытием системных значков у пользователей нередко возникает ряд вопросов.

С помощью редактора групповых политик можно в несколько щелчков мыши скрыть один или несколько ненужных ярлыков с рабочего стола. Перечислим все возможные варианты.

Скрытие значков с рабочего стола начнем с ярлыка браузера Internet Explorer:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Рабочий стол** (User Configuration ⇒ Administrative Templates ⇒ Desktop).
2. Дважды щелкните мышью по параметру **Скрыть значок Internet Explorer с рабочего стола** (Hide Internet Explorer icon on the desktop). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

А теперь скроем значок **Компьютер** (Computer):

1. Перейдите в узел **Конфигурация пользователя ⇒ Административ-**

ные шаблоны ⇒ Рабочий стол (User Configuration ⇒ Administrative Templates ⇒ Desktop).

2. Дважды щелкните мышью по параметру **Удалить значок «Компьютер» с рабочего стола** (Remove Computer icon on the desktop). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После этого можно удалить значок **Сеть** (Network), который предоставляет доступ к сетевым ресурсам:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Рабочий стол** (User Configuration ⇒ Administrative Templates ⇒ Desktop).
2. Дважды щелкните мышью по параметру **Скрыть значок «Сеть» на рабочем столе** (Hide Network locations on desktop). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Если другие ярлыки еще можно было удалить при помощи пункта **Персонализация** (Personalization) контекстного меню, то для значка **Корзина** (Recycle Bin) не существует аналогичного пути сокрытия с рабочего стола. Чтобы удалить значок **Корзина** (Recycle Bin) с помощью групповых политик, нужно:

1. Перейти в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Рабочий стол** (User Configuration ⇒ Administrative Templates ⇒ Desktop).
2. Дважды щелкнуть мышью по параметру **Удалить значок Корзина с рабочего стола** (Remove Recycle Bin icon from desktop). Откроется одноименное окно для редактирования данной политики.
3. Установить переключатель в положение **Включить** (Enabled).
4. Нажать кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После перезагрузки вы не увидите ярлыки, которые скрыли при помощи групповых политик. Однако если вы не хотите удалять ярлыки по одному,

вы можете воспользоваться параметром, который заблокирует отображение всех ярлыков на рабочем столе:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Рабочий стол** (User Configuration ⇒ Administrative Templates ⇒ Desktop).
2. Дважды щелкните мышью по параметру **Скрыть и отключить все элементы рабочего стола** (Hide and Disable all items on the desktop). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После этого на рабочем столе не останется ни одного элемента. Однако все описанные выше операции по сокрытию ярлыков и значков с рабочего стола никак не отражаются на работоспособности самих программ, запущенные другим способом, программы будут работать без каких-либо ограничений.

Перемещение пользовательских папок

Операционные системы Windows, начиная с версии Windows 2000, хранят пользовательские данные в специализированных папках, которые предлагают упрощенный доступ к файлам различного типа. При желании пользователь может с легкостью изменить месторасположение файлов, изменив путь к папке в диалоговом окне со свойствами той или иной пользовательской папки.

Если вы хотите запретить пользователям операционной системы Windows хранить файлы в каталоге, отличном от установленного по умолчанию, вы можете активировать параметр групповой политики, запрещающий перемещение пользовательских папок:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Рабочий стол** (User Configuration ⇒ Administrative Templates ⇒ Desktop).
2. Дважды щелкните мышью по параметру **Запретить пользователям вручную перенаправлять папки пользователей** (Prohibit User from manually redirecting Profile Folders). Откроется одноименное окно для редактирования данной политики.

3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

Теперь после вызова вкладки **Расположение** (Location) диалогового окна **Свойства** (Properties) для папок пользователя вы не увидите управляющих элементов (рис. 2.3) для изменения пути к папке.

Изменение параметров изображений рабочего стола

С помощью редактора групповых политик можно с легкостью привести к единому оформлению фоновые изображения на рабочих столах пользователей операционных систем Windows 8 и Windows Server 2008. Кроме того, существует возможность для ограничения загружаемых на рабочий стол изображений по определенным критериям.

Для того чтобы установить на рабочий стол изображение, а также запретить его смену пользователями самостоятельно, нужно изменить настройки параметра **Фоновые рисунки рабочего стола** (Desktop Wallpaper):

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Рабочий стол ⇒ Active Directory** (User Configuration ⇒ Administrative Templates ⇒ Desktop ⇒ Active Directory).
2. Дважды щелкните мышью по параметру **Фоновые рисунки рабочего стола** (Desktop Wallpaper). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled) и в поле ввода **Имя фонового рисунка** (Wallpaper Name) укажите путь к фоновому изображению с расширением .bmp или .jpg, которое вы хотите разместить на рабочем столе.

Можно ввести локальный путь, такой как C:\Windows\web\wallpaper\home.jpg, или UNC-путь, такой как \\Server\Share\Corp.jpg. Если при входе в систему указанный файл недоступен, то никакой фоновый рисунок не отображается.

4. Укажите параметры отображения рисунка, выбрав из рас-

крывающегося списка **Стиль фонового рисунка** (Wallpaper style) подходящий вариант.

5. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После этого изображение рабочего стола для всех пользователей изменится на указанное в настройках политики.


Windows 8

Глава 3.

Реестр Windows 8

3.1. Что такое реестр. Редактор реестра

Знакомство с реестром

Реестр (англ. registry) — это база данных, в которой хранится информация обо всех настройках и параметрах работы Windows 8, а также конфигурация всех установленных в системе приложений.

В реестре хранятся данные, которые необходимы для правильного функционирования Windows. К ним относятся профили всех пользователей, сведения об установленном программном обеспечении и типах документов, которые могут быть созданы каждой программой, информация о свойствах папок и значках приложений, а также об установленном оборудовании и используемых портах.

С помощью реестра вы можете делать с системой все что угодно — менять всевозможные настройки и параметры, причем даже те, которые невозможно изменить при помощи стандартных средств Windows 8 и ее диалоговых окон.

Однако прежде чем мы приступим к изучению реестра, вы должны ясно себе усвоить, что работать с ним следует предельно осторожно и обдуманно. Изменение некоторых параметров может привести к нарушению работы Windows 8 или даже выходу ее из строя.

Хранится реестр в виде множества двоичных файлов. Поэтому нельзя открыть файл реестра (например, в текстовом редакторе) и отредактировать его по своему усмотрению. Для работы с реестром необходимо использовать специальные программы. Они собирают все файлы реестра воедино и отображают их содержимое в виде единой иерархической структуры.

Стандартной программой, предназначенной для работы с Windows 8 и входящей в ее состав, является программа regedit.exe. Располагается эта программа непосредственно в каталоге, в который была установлена

операционная система (попасть в реестр Windows 8 можно, нажав сочетание Win+ R и в появившемся окне введя regedit) Многие думают, что regedit и есть сам реестр. Однако это заблуждение.

Окно запущенного редактора реестра выглядит так, как показано на рис. 3.1. При этом в левой части окна в виде иерархического дерева показывается структура реестра, а в правой части — содержимое выделенного раздела.

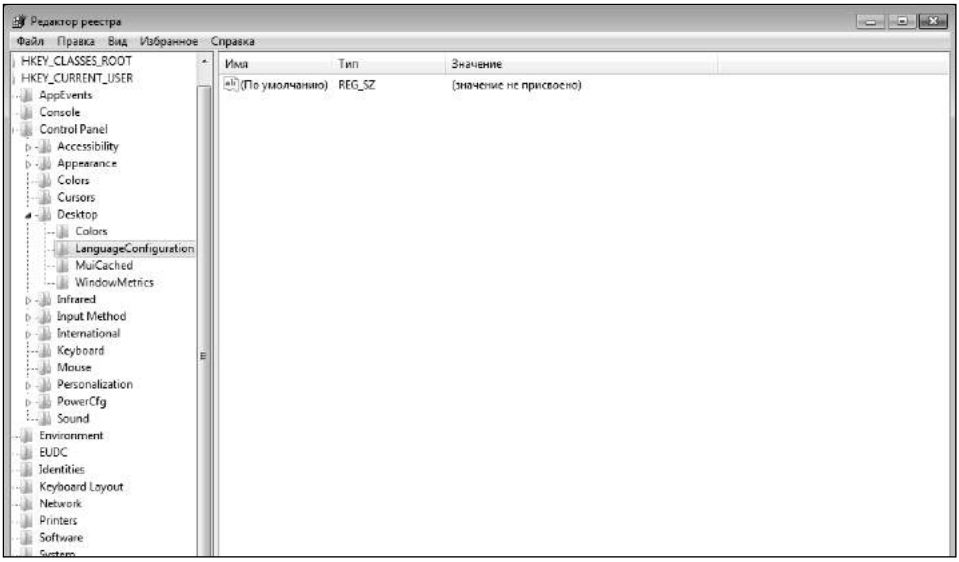


Рис. 3.1. Редактор реестра RegEdit

В русскоязычной технической литературе принято ветви реестра называть ключами (от англ. key). При этом каждый ключ реестра может содержать в себе другие вложенные ключи, а также параметры (англ. value). Именно параметры представляют собой полезное содержимое реестра. А ключи служат лишь для группирования сходных по смыслу и значению ключей. В общем ключи и параметры — это как папки и файлы. Принцип один и тот же.

Примечание.

В официальной документации Microsoft применяется несколько другая терминология. В ней вместо термина «ключ» используется термин «раздел».

Чтобы отобразить содержимое какого-либо ключа, необходимо щелкнуть по его названию в левой части редактора реестра. При этом в правой части откроется список содержащихся в нем параметров. Если

ключ содержит вложенные ключи, то рядом с ним стоит значок + (плюс). Щелкнув мышкой по этому значку, можно раскрыть список вложенных ключей.

Как вносить изменения в реестр и создавать новые ключи

Редактирование реестра предполагает выполнение следующих действий:

- поиск нужного ключа или параметра;
- добавление ключа или параметра;
- изменение значения параметра;
- удаление ключа или параметра;
- переименование ключа или параметра.

Чтобы изменить значение какого-либо параметра, необходимо найти его и отобразить в правой части редактора реестра. Далее выполните по параметру двойной щелчок мышкой, и вы перейдете в режим его редактирования. При этом появится диалоговое окно, в котором вы сможете указать новое значение для параметра (рис. 3.2).

Чтобы создать новый ключ или параметр, вам нужно перейти в тот ключ, внутри которого вы хотите создать это. Далее в строке меню выберите **Правка → Создать**, а затем — что именно вы хотите создать

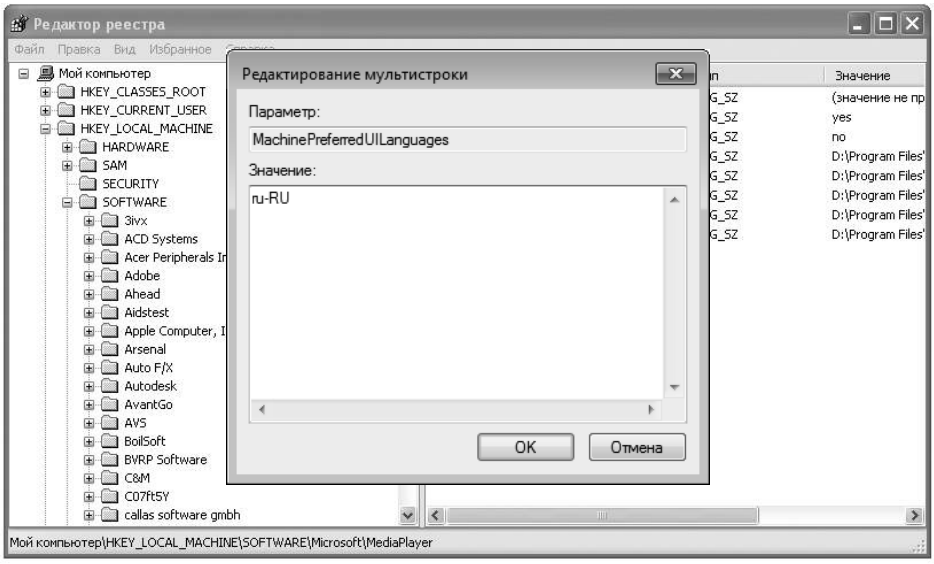


Рис. 3.2. Ввод нового значения для параметра реестра

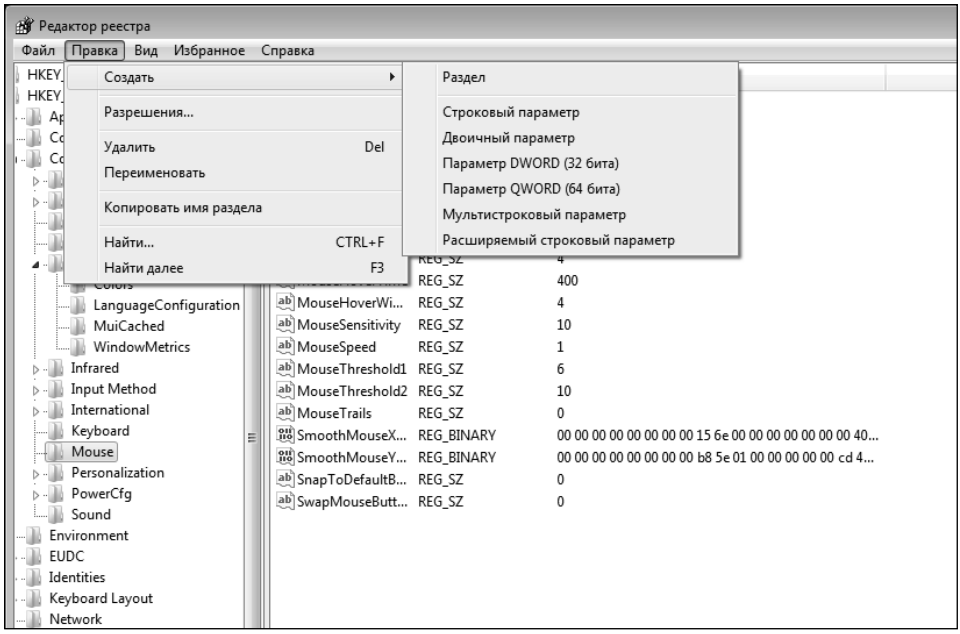


Рис. 3.3. Создание нового параметра

(рис. 3.3). После этого вам будет предложено ввести имя созданного элемента реестра. Если вы таким образом создали ключ, то, чтобы задать для него значение, по нему опять же необходимо дважды щелкнуть мышкой.

Например, чтобы создать новый ключ `TestSubkey` внутри ключа `HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft`, проделайте следующее:

1. Перейдите в ключ `HKEY_LOCAL_MACHINE`.
2. Перейдите в ключ `SOFTWARE`.
3. Перейдите в ключ `Microsoft`.
4. Выберите в меню **Правка → Создать**, а затем — **Раздел**.
5. Введите `TestSubkey` и нажмите клавишу «Enter».

В реестре вы можете переименовать любой параметр или ПОЧТИ любой ключ реестра. Делается это так же, как и переименовывание обычных файлов. Для того, чтобы перейти в режим задания нового имени, выполните любое из следующих действий:

- щелчком мыши выделите ключ или параметр и в строке меню выберите **Правка → Переименовать**;

- щелчком мыши выделите ключ или параметр реестра и нажмите на кнопку «F2».

Чтобы удалить какой-либо ключ или параметр реестра, необходимо выделить его, а затем либо в строке меню выбрать **Правка → Удалить**, либо просто нажать на клавишу «Delete» («Del»).

Чтобы найти какой-либо ключ или раздел, можно воспользоваться встроенным инструментом поиска в редакторе реестра. Для этого вам нужно в строке меню выбрать **Правка → Найти**. После этого на экране появится диалоговое окно Поиск, в котором вы сможете указать название, которое вам нужно найти. Чуть ниже, с помощью флажков, вы можете указать, среди каких элементов реестра (ключи (разделы) и/или параметры) должен производиться поиск.

Кстати, с помощью инструмента поиска очень удобно искать ключи и параметры, относящиеся к какой-либо из установленных в системе программ. Эти ключи и параметры могут быть разбросаны по всему реестру, и вручную найти их может быть не так-то просто.

Как обозначаются параметры и ключи реестра

Запись «ключ `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft`» на практике означает, что вам нужно:

1. Сначала перейти в ключ `HKEY_LOCAL_MACHINE`.
2. Затем из ключа `HKEY_LOCAL_MACHINE` перейти во вложенный в него ключ `SOFTWARE`.
3. А затем из ключа `SOFTWARE` перейти во вложенный в него ключ `Microsoft`.

Аналогичным образом осуществляется и переход в другие ключи. При этом запись типа `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft` является краткой записью перехода, или его еще называют путем.

3.2. Устройство реестра

Структура реестра

Весь реестр Windows 8 делится на 5 основных ветвей — пять стандартных ключей (или разделов), в которые входят все остальные. Эти

ключи называются стандартными ключами. Именно они формируют базовую структуру реестра. Ключи эти таковы:

- **HKEY_CURRENT_USER** — данный ключ является корневым для данных конфигурации пользователя, вошедшего в систему в настоящий момент. Здесь хранятся папки пользователя, цвета экрана и параметры панели управления. Эти сведения сопоставлены с профилем пользователя. Кроме того, в этом разделе могут храниться параметры, используемые различными прикладными программами. Например, программа воспроизведения звуковых файлов может записать в этот раздел список наиболее часто прослушиваемых композиций. Вместо полного имени ключа иногда используется аббревиатура HKCU.

  Наиболее полезным в этом ключе является подключ Software, так как именно в нем можно обнаружить ключи, посвященные каждому из установленных в системе приложений. Обычно такие ключи группируются по производителю.

- **HKEY_USERS** — данный ключ содержит все профили пользователей компьютера. При этом по своей сути раздел HKEY_CURRENT_USER является подключом ключа HKEY_USERS. Просто ключ HKEY_CURRENT_USER был вынесен в число стандартных ключей в целях удобства. В ключе HKEY_USERS ключ HKEY_CURRENT_USER обозначается как длинная строка цифр и букв типа: S-1-5-24-1365425787-34253468867-2342436-700. Кстати, эта абракадабра на самом деле является идентификатором безопасности (SID), под которым работает текущий пользователь (то есть вы). Вместо полного имени ключа HKEY_USERS иногда используется аббревиатура HKU.

- **HKEY_LOCAL_MACHINE** — этот ключ содержит параметры аппаратной конфигурации (устройств компьютера), относящиеся к данному компьютеру. Содержимое данного ключа является абсолютно одинаковым для всех пользователей системы. Вместо полного имени раздела иногда используется аббревиатура HKLM.

- **HKEY_CLASSES_ROOT** — этот ключ по сути является подразделом HKEY_LOCAL_MACHINE\Software. Хранящиеся здесь сведения отвечают за запуск необходимых программ при открытии файлов с различными расширениями. Вместо полного имени раздела иногда используется аббревиатура HKCR. Начиная с Windows 2000, эти сведения хранятся как в HKEY_LOCAL_MACHINE, так и в HKEY_CURRENT_USER. Ключ HKEY_LOCAL_MACHINE\Software\Classes содержит параметры по умолчанию, которые относятся ко всем пользователям локального компьютера. Параметры, содержащиеся в ключе HKEY_CURRENT_USER\Software\Classes, переопределяют принятые по умолчанию и относятся только к текущему

пользователю. Ключ HKEY_CLASSES_ROOT включает в себя данные из обоих источников. Кроме того, ключ HKEY_CLASSES_ROOT предоставляет объединенные данные программам, написанным под ранние версии Windows. Изменения настроек текущего пользователя выполняются в разделе HKEY_CURRENT_USER\Software\Classes. Модификация параметров по умолчанию должна производиться в ключе HKEY_LOCAL_MACHINE\Software\Classes. Данные из разделов, добавленных в HKEY_CLASSES_ROOT, будут сохранены системой в ключе HKEY_LOCAL_MACHINE\Software\Classes. Если изменяется параметр в одном из подключей ключа HKEY_CLASSES_ROOT и такой подключ уже существует в HKEY_CURRENT_USER\Software\Classes, то для хранения информации будет использован ключ HKEY_CURRENT_USER\Software\Classes, а не HKEY_LOCAL_MACHINE\ Software\Classes.

- **HKEY_CURRENT_CONFIG** — данный ключ содержит сведения о профиле оборудования, используемом локальным компьютером при запуске системы.

Типы параметров реестра

Все параметры, используемые в реестре, имеют определенный тип, в соответствии с которым они принимают определенные значения, определенным образом хранятся, обрабатываются и т.д. Всего в Windows 8 предусмотрено 7 типов, к которым принадлежат все параметры реестра.

Каждый тип, как правило, имеет два имени. Все они перечислены в приведенной ниже табл. 3.1.

3.3. Резервное копирование и восстановление реестра

Поскольку реестр не хранится в отдельном файле, то и создавать его резервную копию нельзя. Однако нельзя это сделать, так сказать, впрямую. Но если постараться, то можно сделать резервные копии любых выбранных разделов реестра путем создания «заплаток» к нему.

О том, как эти самые «заплатки» делаются и как их можно использовать, мы поговорим в следующем разделе данной главы.

3.4. Создание и использование «заплаток» реестра

Что такое заплатка реестра и для чего она может использоваться

Заплатка реестра (registry patch) представляет собой простой текстовый файл с расширением .reg, в котором хранится один или несколько ключей или параметров реестра. Заплатки реестра еще иногда так и называют REG-файлами. Стоит выполнить двойной щелчок мыши по такому файлу, как его содержимое автоматически будет добавлено внутрь реестра. Таким образом, помимо всего прочего, механизм заплаток можно эффективно использовать для создания резервных копий

Типы параметров реестра — Таблица 3.1

Имя 1	Имя 2	Описание
Двоичный параметр	REG_BINARY	Двоичные (или их еще называют бинарные) параметры представляют собой набор символов, хранящих в двоичном виде и доступных для редактирования только в шестнадцатеричном формате
Параметр DWORD	REG_DWORD	Параметр такого типа имеет числовое значение. Довольно часто используются значения 0 и 1. При этом 0 означает «нет», а «1» — да. REG_DWORD_BIG_ENDIAN (самый младший байт хранится в памяти в последнем числе). При изменении значения параметра с таким типом, вы можете выбрать систему счисления, в которой он должен отображаться: десятичную или шестнадцатеричную. По умолчанию используется шестнадцатеричная система счисления, но при использовании чисел от 0 до 9 система счисления не имеет никакого значения
Расширяемая строка данных	REG_EXPAND_SZ	Строка данных переменной длины. Этот тип данных включает имена специальных переменных, обрабатываемых при использовании данной программой или службой. Когда программа или служба читает такую строку из реестра, то операционная система автоматически подставляет вместо имени специальной переменной текущее значение этой переменной
Многострочный параметр	REG_MULTI_SZ	Многострочный текст, представляющий собой несколько строк, объединенных воедино. Этот тип, как правило, имеют списки и другие записи в формате, удобном для чтения. Записи разделяются пробелами, запятыми или другими символами

Имя 1	Имя 2	Описание
Строковый параметр	REG_SZ	Текстовая строка фиксированной длины. Содержит обычный текст, который можно прочитать
Двоичный параметр	REG_RESOURCE_LIST	Последовательность вложенных массивов. Служит для хранения списка ресурсов, которые используются драйвером устройства или управляемым им физическим устройством. Обнаруженные данные система сохраняет в разделе \ResourceMap. В окне редактора реестра эти данные отображаются в виде двоичного параметра в шестнадцатеричном формате
Двоичный параметр	REG_RESOURCE_REQUIREMENTS_LIST	Последовательность вложенных массивов. Служит для хранения списка драйверов аппаратных ресурсов, которые могут быть использованы определенным драйвером устройства или управляемым им физическим устройством. Часть этого списка система записывает в раздел \ResourceMap. Данные определяются системой. В окне редактора реестра они отображаются в виде двоичного параметра в шестнадцатеричном формате
Двоичный параметр	REG_FULL_RESOURCE_DESCRIPTOR	Последовательность вложенных массивов. Служит для хранения списка ресурсов, которые используются физическим устройством. Обнаруженные данные система сохраняет в разделе \HardwareDescription. В окне редактора реестра эти данные отображаются в виде двоичного параметра в шестнадцатеричном формате
Отсутствует	REG_NONE	Не имеющие определенного типа данные. Такие данные записываются в реестр системой или приложением. В окне редактора реестра отображаются в виде двоичного параметра в шестнадцатеричном формате
Ссылка	REG_LINK	Символическая ссылка в формате Юникод
Параметр QWORD	REG_QWORD	Данные, представленные в виде 64-разрядного целого. Такие данные отображаются в окне редактора реестра в виде двоичного параметра.

некоторых отдельных частей реестра, а также для переноса их с одного компьютера на другой.

Иметь резервные копии фрагментов реестра иногда бывает очень полезно, так как зачастую программы в ходе своей работы изменяют реестр без вашего ведома и без вашего разрешения. А это может, в свою очередь, приводить к сбоям и конфликтам в работе системы.

Однако вы можете заранее создать заплатку соответствующих разделов реестра (связанных с программой), а в случае возникновения конфликтных ситуаций — активировать ее. В результате все произошедшие из-

менения аннулируются и раздел реестра примет свой первоначальный вид.

Заплатки можно и даже рекомендуется использовать в случаях, когда вы собираетесь поэкспериментировать с реестром. При этом следует сохранить в виде заплаток «подопытные» ключи и параметры реестра.

Создание заплаток реестра

Создание заплатки реестра производится следующим образом:

1. Откройте редактор реестра. Для этого можно нажать **Win + R**, затем ввести в поле команду regedit и нажать «Enter».
2. Выделите ключ (раздел), который вы хотите сохранить в виде заплатки. Вы можете выбрать абсолютно любой ключ. Даже один из стандартных. Однако я рекомендую сохранять в виде заплаток не все подряд, а только то, что действительно необходимо. В противном случае у вас получится слишком большой REG-файл, с которым будет неудобно работать.
3. В строке меню редактора реестра выберите **Файл → Экспорт**.
4. В появившемся диалоговом окне (рис. 3.4) введите имя файла и нажмите на кнопку OK. В результате выбранные вами ветви реестра будут сохранены в файле заплатки.

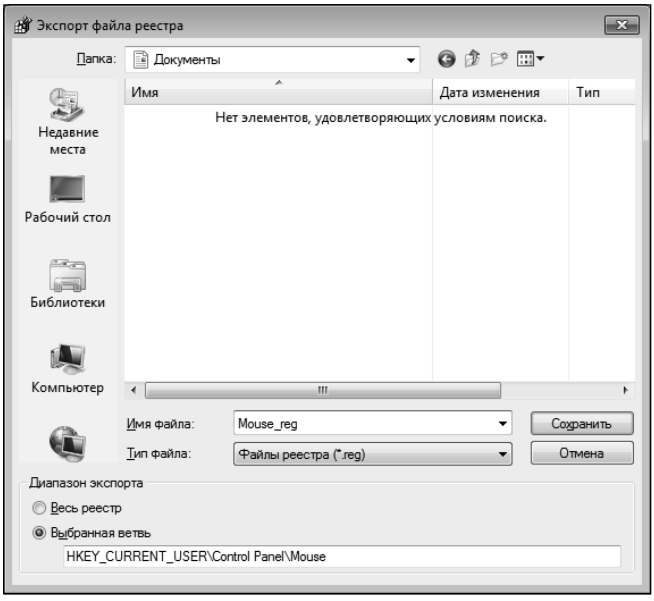


Рис. 3.4. Окно "Экспорт файла реестра"

5. Убедитесь, что файл заплатки был создан, а также в том, что этот файл имеет расширение .reg.

Редактирование заплаток реестра

Как уже говорилось, заплатка по своей сути представляет обычный текстовый файл (см. листинг 3.1). Соответственно, и редактировать его можно как обычный текстовый файл. Для этого вы должны открыть файл заплатки в текстовом редакторе.

Кстати говоря, в процессе редактирования заплатки в текстовом редакторе Word вы сможете воспользоваться всеми возможностями этого редактора и тем самым существенно автоматизировать и упростить редактирование заплатки. В частности, вы можете воспользоваться инструментом поиска/замены, чтобы найти какие-либо параметры и автоматически заменить их на другие.

Это может быть особенно полезно, если параметр встречается очень часто, а вам нужно гарантированно не пропустить ни одного его упоминания. Если бы вы правили вручную, то вам бы пришлось по нескольку раз прокручивать текст заплатки, чтобы удостовериться, а не пропустили ли вы где-нибудь этот параметр. Автоматическое же поиск/замена позволяет чуть ли не мгновенно гарантированно найти упоминания требуемого параметра и в случае необходимости заменить его на другой.

Теперь давайте поподробнее остановимся на содержимом заплатки, а точнее, на том формате, в котором в ней содержатся данные из реестра (см. листинг 3.1).

Листинг 22.1. Пример заплатки

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MediaPlayer]
"IEInstall"="no"
"Installation Directory"="D:\\Program Files\\Windows Media Player"
"Installation DirectoryLFN"="D:\\Program Files\\Windows Media Play-
er"
"BlockUninstall"="yes"
"SkinsDir"="D:\\Program Files\\Windows Media Player\\Skins"
"VisualizationsDir"="D:\\Program Files\\Windows Media
Player\\Visualizations"
"MP2.SaveDir"="D:\\Program Files\\Windows Media Player"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MediaPlayer\8.0]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MediaPlayer\8.0\Registration]
"UDBVersion"="8.0.0.4477"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MediaPlayer\9.0]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MediaPlayer\9.0\Registration]
"UDBVersion"="9.00.00.2980"
"UDBRev"="0"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MediaPlayer\Control]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MediaPlayer\Control\Advanced
Options]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MediaPlayer\Control\Advanced
Options\Streaming Media (Windows Media)]
@="Streaming Media (Windows Media)"
"Page1"="{91643D00-4AFA-11d1-A520-000000000000}"
```

В первой строке файла-заплатки содержится фраза `Windows Registry Editor Version 5.00`, которая, собственно, и сигнализирует системе, что данный файл является заплаткой реестра. Эта строка является необходимой, чтобы система могла правильно воспринять содержимое reg-файла и обработать его должным образом. Поэтому ни в коем случае нельзя стирать эту строку из файла.

Вслед за первой строкой идет перечисление ключей реестра, а также параметров и их значений. При этом имена ключей заключены в квадратные скобки. После имени ключа идет перечисление содержащихся в нем параметров. Каждая строка с параметрами начинается с имени параметра, затем идет знак равенства, а затем указывается значение параметра. Причем имя параметра и его значение всегда заключаются в кавычки:

```
[Ключ 1]
"Параметр 1"="Значение 1"
"Параметр 2"="Значение 2"
"Параметр 3"="Значение 3"

[Ключ 2]
"Параметр 1"="Значение 1"
```

Параметр с именем @ соответствует параметру по умолчанию (default) для данного раздела. Пример такого параметра можно наблюдать в предпоследней строке листинга 3.1.

Напоследок напомню, что редактирование заплатки никаким образом не повлияет на работу системы, пока вы не импортируете ее в реестр. А перед этим не забудьте сохранить измененную заплатку.

Ранее мы рассмотрели, как в REG-файле указываются строковые параметры. Но если в ключе встречаются двоичные или другие парамеры, то они записываются следующим образом:

- **“параметр”=dword:znachenie** — для DWORD параметра (Внимание! dword надо набирать маленькими буквами).
- **“параметр”=hex:XX,XX,...** — для двоичного параметра (Внимание! hex надо набирать маленькими буквами). Здесь XX, XX, XX — двоичные значения.

Применение “заплаток” к реестру

Имеющуюся заплатку вы можете в любой момент применить к реестру и импортировать содержащиеся в ней данные в реестр. Сделать это можно любым из следующих способов:

- Дважды щелкнуть мышкой по файлу с заплаткой, и она будет импортирована в реестр. При этом редактор реестра совсем не обязательно должен быть загружен. После двойного щелчка по REG-файлу система спросит вас, а действительно ли вы хотите добавить информацию из выбранного вами файла в реестр (рис. 3.5). Вам останется лишь ответить утвердительно, нажав на кнопку **Да**, и данные из выбранной «заплатки» будут успешно перенесены в реестр.

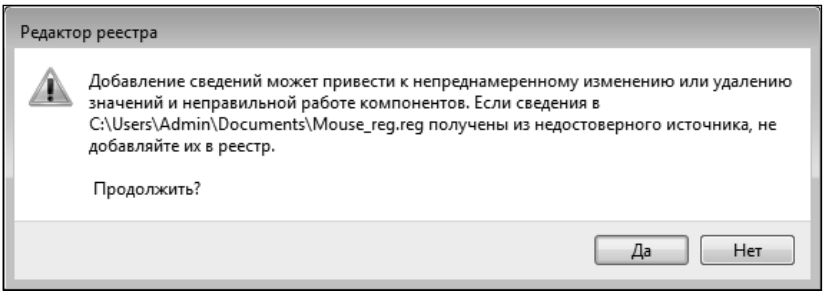


Рис. 3.5. Запрос подтверждения

- При запущенном редакторе реестра RegEdit можно в его строке меню выбрать **Файл → Импорт**, а затем указать, какой именно REG-файл вы хотите добавить в реестр.

- Добавить заплатку в реестр можно и из командной строки. Для этого вам нужно перейти в режим командной строки, а затем с помощью команды **cd** перейти в папку, в которой хранится файл заплатки. Далее, если файл заплатки, к примеру, называется `zaplatka.reg`, вам следует применить команду:

```
regedit /s zaplatka.reg
```

Напоследок хочу лишь еще раз предостеречь вас от необдуманного применения заплаток и редактирования реестра. Будьте осторожны.

Автоматическое удаление данных из реестра

С помощью механизма «заплаток» можно реализовать быстрое удаление каких-либо данных (ключей, параметров) из реестра. Для этого вы можете создать «заплатку» и потом подредактировать ее.

Чтобы ключ был удален из реестра, необходимо в REG-файле поставить знак «-» (минус) перед именем ключа:

```
-[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MediaPlayer\9.0]
```

При удалении ключа из реестра вместе с ним будут удалены и все параметры, содержащиеся в нем. Если же в удаляемом ключе содержатся вложенные ключи, то сработает механизм безопасности Windows, который предотвращает удаление ключей, если в них содержатся вложенные ключи. Чтобы удалить такой ключ, нужно предварительно удалить все вложенные в него ключи.

Если вы хотите удалить не ключ целиком, а только какой-либо параметр из него (или параметры), то в этом случае вы должны для этого параметра после знака равенства поставить значок «-» (минус):

```
"UDBRev"=-
```

Объединение нескольких заплаток

В одну заплатку можно экспортировать ключи только из одной ветки реестра. Однако если вам нужно получить REG-файл, содержащий параметры из разных ветвей реестра, то вы можете сначала сделать несколько отдельных REG-файлов (по одному на каждую ветку), а затем их объединить. Просто скопируйте их содержимое в один текстовый REG-файл и все.

3.5. Как отслеживать изменения в реестре

Очень часто не мешало бы знать, к каким изменениям в реестре приводит та или иная настройка системы, установка и использование той или иной программы. Например, если вы устанавливаете пробную trial-версию программы, действующую, скажем, в течение 15 дней, а потом вырубающуюся, то сведения об изменениях в реестре очень бы пригодились, чтобы по истечении 15 дней немножко подправить реестр так, чтобы система считала, что вы опять только что установили эту программу и снова разрешила бы вам ею пользоваться.

Простой и надежный способ

Идея проста и заключается она в том, чтобы сделать снимок (копию содержимого) ДО произведения каких-либо действий (настроек, установки программы) и ПОСЛЕ этих действий, а потом сравнить. Различия в снимках как раз и будут искомыми изменениями. Сделать это можно следующим образом:

1. Перво-наперво убедитесь, что в системе не работает никакая из программ и не запущены лишние приложения. Дело в том, что эти программы могут вносить изменения в реестр в процессе свой работы, что сведет весь эксперимент «на нет».
2. Откройте редактор реестра RegEdit, перейдите в стандартный основной ключ HKEY_USERS и сделайте его копию в виде заплатки (можно и все остальные стандартные ключи таким образом экспортировать). Если вы создавали несколько REG-файлов и нескольких основных ключей, то соберите их в один REG-файл. Можно сделать и копию всего реестра. Только для этого нужно в строке меню выбрать **Файл → Экспорт**, а потом в появившемся окне **Экспорт файла реестра** (рис. 3.4), помимо имени нового файла, установить переключатель Весь реестр.
3. Произведите необходимы действия.
4. Сразу после действий, ничего больше не трогая, снова сделайте «снимок» стандартного основного ключа HKEY_USERS (или всего реестра).
5. Сравните REG-файлы, сделанные до и после выполнения заданных действий. Сделать это можно либо с помощью текстового редактора (в частности, в редакторе Word такая возможность имеется), либо с помощью команды fc, которая работает из командной строки и позволяет в Windows 8 сравнить содержимое двух произвольных файлов. Для того, чтобы воспользоваться этой командой, необхо-

димо перейти в режим командной строки, затем в окне командной строки перейти в папку с REG-файлами и ввести команду:

```
fc /u snimok1.reg snimok2.reg > otchet.txt
```

где:

- `snimok1.reg` — это REG-файл, сделанный до проведения действий;
- `snimok2.reg` — REG-файл, сделанный после проведения действий;
- `otchet.txt` — текстовый файл, в который будет помещен отчет об имеющихся различиях в REG-файлах.

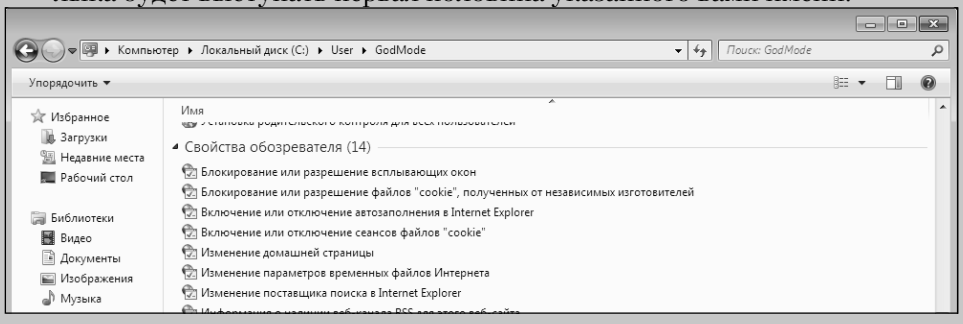
Как включить "режим бога" в Windows 8

В операционной системе Windows 8 в «режиме бога» (см. рис. внизу) пользователю предоставляется возможность получить доступ ко всем инструментам настройки операционной системы в одном месте. Теперь не нужно тратить время на поиски необходимого инструмента! Приятной особенностью использования «режима бога» является приятный и понятный графический интерфейс; все инструменты управления системой объединены в группы, что облегчает их поиск.

«Режим бога» является недокументированной возможностью операционной системы Windows 8 и не имеет поддержки для пользователей от компании Microsoft.

Чтобы получить возможности использования «режима бога», необходимо создать специальный ярлык доступа:

1. Откройте в системе папку, в которой хотите создать ярлык доступа к «режиму бога».
2. Создайте новую папку. Имя папки будет состоять из двух частей. Первая часть задается пользователем, эта часть задает имя ярлыка доступа к «режиму бога». Вторая часть постоянна — это глобальный идентификатор, он указывает системе, что данную папку необходимо преобразовать в ярлык доступа к «режиму бога».
3. Наберите первую половину имени новой папки: в роли первой половины может выступать любое разрешенное имя операционной системы Windows 8. Длина имени произвольна.
4. В роли второй половины имени новой папки введите следующий текст: **.{ED7BA470-8E54-465E-825C-99712043E01C}.** Ввод фигурных скобок и точки, разделяющей первую и вторую части имени папки, обязателен. Будьте внимательны: папка будет преобразована к ярлыку доступа к «режиму бога» только в случае абсолютного соответствия набранных символов.
5. Когда закончите набор имени папки, подтвердите имя нажатием клавиши Enter. Папка будет преобразована в ярлык доступа к «режиму бога». Значок ярлыка примет вид значка Панели управления. В роли имени ярлыка будет выступать первая половина указанного вами имени.



Глава 4.

Хакинг Панели управления

Если компьютер используется несколькими пользователями, то имеет смысл защитить компьютер от их пронырливых рук. В этой главе вы узнаете, как сделать так, чтобы пользователь либо не смог воспользоваться панелью управления, либо смог, но ее определенными элементами, о том, как ограничить функциональность некоторых элементов, как ограничить доступ к языковым настройкам системы. Кроме того, мы расскажем, как ограничить возможности настройки принтеров, а также установку и удаление программ и компонентов системы в Панели управления.

4.1. Настройка доступа к панели управления и ее элементам

В этом разделе вы узнаете, как ограничить доступ пользователей к элементам в панели управления. При настройке ограничения элемента скрывается значок соответствующего элемента в панели управления, но если пользователь попробует открыть элемент другими возможными способами (не из панели управления), то появится уведомление о том, что администратор отключил возможность использования элемента. Также будет рассматриваться параметр, полностью запрещающий доступ к панели управления.

Сокрытие определенных элементов панели управления

Эта политика удаляет выбранные элементы из окна **Панель управления** (Control Panel), а также запрещает доступ к этим элементам из контекстных меню. У каждого элемента панели управления есть свое каноническое имя. И если эти имена перечислить в рассматриваемом параметре политики, то элементы, чьи имена были указаны, больше не будут отображаться в панели управления, и, как уже говорилось, доступ из контекстного меню также будет заблокирован.

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления** (User configuration ⇒ Administrative Templates ⇒ Control Panel).

2. Дважды щелкните мышью по параметру **Скрыть указанные элементы панели управления** (Hide specified Control Panel items). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
5. В области **Параметры** (Options) нажмите кнопку **Показать** (Show). Появится диалоговое окно **Вывод содержания** (Show Contents).
6. В появившемся диалоговом окне щелкните два раза по пустому полю и введите с клавиатуры каноническое имя элемента, например «Microsoft.Mouse», «Microsoft.System» или «Microsoft.Personalization». Чтобы указать имя следующего элемента, нажмите клавишу **Enter** и введите новое каноническое имя.
7. Нажмите кнопку **ОК**, чтобы закрыть диалоговые окна.

После этого значки указанных элементов не будут отображаться в окне **Панель управления** (Control Panel), а доступ к элементу из контекстного меню приведет к появлению уведомления (рис. 4.1). Если параметр отключен или не задан, то ограничений в отображении элементов и любого доступа к ним установлено не будет. Исключение будет только в том случае, если включен и настроен параметр **Показать только заданные элементы панели управления** (Show only specified Control Panel items).

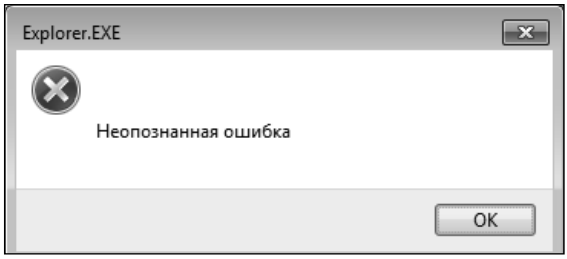


Рис. 4.1. ***Диалоговое окно ошибки доступа к элементу***

Примечание. Элемент «Экран» панели управления нельзя скрыть в контекстном меню рабочего стола с помощью данного параметра. Для скрытия этого элемента и предотвращения изменения пользователями соответствующих параметров используйте параметр **Отключить окно свойств экрана в панели управления** (Disable the Display Control Panel).

Полный список канонических имен элементов перечислен на официальном сайте Microsoft: **go.microsoft.com/fwlink/?LinkId=122973** или в приложении 1 в конце книги.

Отображение только заданных элементов панели управления

Этот параметр удаляет все элементы из окна **Панель управления** (Control Panel), кроме тех элементов, канонические имена которых перечислены в параметре политики. Для того чтобы указать канонические имена элементов:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления** (User configuration ⇒ Administrative Templates ⇒ Control Panel).
2. Дважды щелкните мышью по параметру **Показать только заданные элементы панели управления** (Show only specified Control Panel items). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. В области **Параметры** (Options) нажмите кнопку **Показать** (Show). Появится диалоговое окно **Вывод содержания** (Show Contents).
5. В появившемся диалоговом окне щелкните два раза по пустому полю и введите с клавиатуры каноническое имя элемента. Чтобы указать еще одно, нажмите клавишу **Enter** и введите новое каноническое имя.
6. Нажмите кнопку **ОК**, чтобы закрыть диалоговые окна.

> **Примечание.** Элемент «Экран» панели управления нельзя скрыть в контекстном меню рабочего стола с помощью данного параметра. Для скрытия этого элемента и предотвращения изменения пользователями соответствующих параметров используйте параметр **Отключить окно свойств экрана в панели управления** (Disable the Display Control Panel).

После этого в **Панели управления** (Control Panel) будут отображаться значки только тех элементов, канонические имена которых вы перечислили. Если параметр **Скрыть указанные элементы панели управления** (Hide specified Control Panel items) будет включен, то параметр **Показать только заданные элементы панели управления** (Show only specified Control Panel) будет проигнорирован. Также все элементы, которые не были указаны в параметре политики, будут недоступны не только из окна **Панель управления** (Control Panel), но и с помощью других способов доступа, например контекстного меню.

Если параметр отключен или не настроен, то никаких ограничений в отображении и доступе к элементам панели управления установлено не будет. Исключение будет только в том случае, если включен и настроен параметр **Скрыть указанные элементы панели управления** (Hide specified Control Panel items).

Блокировка настроек экрана

Редактор групповых политик позволяет заблокировать изменение параметров экрана с помощью панели управления. Для этого следует активировать следующий параметр:

1. Перейдите в узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Окно свойств экрана** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Display)/
2. Дважды щелкните мышью по параметру **Отключить окно свойств экрана в панели управления** (Disable the Display Control Panel). Откроется одноименное окно для редактирования данной политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК** в правой нижней части окна для сохранения результатов настройки.

После активации данного параметра в окне **Панель управления (Control Panel) ⇒ Все элементы панели управления (All Control Panel Items)⇒ Экран (Display)** в верхней части будет отображаться сообщение о том, что часть настроек заблокирована системным администратором, а все кнопки, переключатели и поля ввода в окне **Экран (Display)** будут неактивны. При включенном параметре **Отключить окно свойств экрана в панели управления (Disable the Display Control Panel)** пользователи не смогут изменить любые настройки, связанные с экраном, кроме изменения параметров сглаживания шрифтов Clear Type.

Отображение всех элементов панели управления

По умолчанию при открытии окна **Панель управления** (Control Panel) значки элементов отображаются по категориям. При следующем открытии значки элементов будут отображаться так, как выбрал пользователь при последнем открытии окна **Панель управления** (Control Panel). Для того чтобы все значки элементов всегда отображались в окне **Панель управления** (Control Panel), выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления** (User configuration ⇒ Administrative Templates ⇒ Control Panel).
2. Дважды щелкните мышью по параметру **Всегда открывать все элементы панели управления при ее открытии** (Always open All Control Panel

items when opening Control Panel). Откроется диалоговое окно редактирования параметра политики.

3. Установите переключатель в положение **Включить** (Enable).
4. Нажмите кнопку **ОК**.

Теперь если в последний раз использовалось отображение значков по категориям, при следующем открытии окна **Панель управления** (Control Panel) будут отображаться мелкие значки. Если в последний раз было выбрано отображение крупных значков, то оно останется при следующем открытии.

Запрещение доступа к панели управления

Для того чтобы запретить доступ ко всем элементам панели управления, следует выполнить данные шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления** (User configuration ⇒ Administrative Templates ⇒ Control Panel).
2. Дважды щелкните мышью по параметру **Запретить доступ к панели управления** (Prohibit access to the Control Panel). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. Нажмите кнопку **ОК**.

После этого программа Control.exe, которая отвечает за работу панели управления, будет заблокирована, что приведет к невозможности открыть окно **Панель управления** (Control Panel). Также будет удалена кнопка **Панель управления** (Control Panel) из меню **Пуск** (Start) и папка **Панель управления** (Control Panel) из окна проводника Windows. Будут заблокированы любые попытки доступа к элементам из контекстного меню (рис. 4.2).

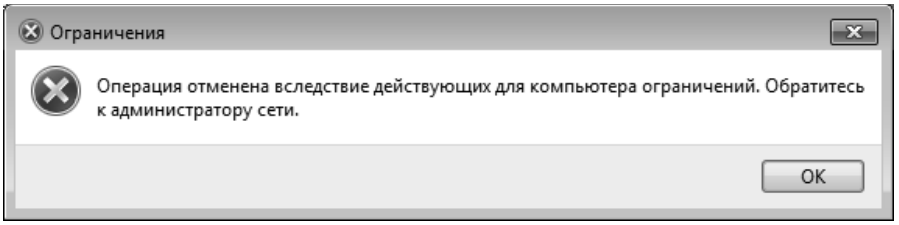


Рис. 4.2. ***Диалоговое окно с уведомлением об ограничении доступа***

Если параметр отключен или не настроен, то доступ к панели управления будет открыт.

4.2. Персонализация

В этом разделе вы узнаете о том, как ограничить доступ к настройкам интерфейса операционной системы Windows.

Запрещение изменения оформления

По умолчанию абсолютно любой пользователь может изменить тему в окне **Персонализация** (Personalization). Вы можете запретить пользователю изменять тему, выполнив следующие шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Персонализация** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Personalization).
2. Дважды щелкните мышью по параметру **Запретить изменение темы** (Prevent changing theme). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
5. Нажмите кнопку **ОК**.

Теперь выбор тем в окне **Персонализация** (Personalization) будет невозможным, однако это не будет мешать пользователю выбрать фон рабочего стола, цвет окна, установить новые звуки интерфейса и изменить заставку. Если параметр отключен или не задан, то ограничения возможности изменения тем установлены не будут.

Аналогичная ситуация и с запретом изменения стилей оформления и кнопок. Для того чтобы запретить вносить изменения пользователями в стили оформления диалоговых окон и кнопок, отображаемых на экране компьютера:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Персонализация** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Personalization).
2. Дважды щелкните мышью по параметру **Запретить изменение стилей оформления окон и кнопок** (Prevent changing visual style for windows and buttons). Откроется диалоговое окно редактирования параметра политики.

3. Установите переключатель в положение **Включить** (Enable).
4. Нажмите кнопку **ОК**.

Теперь изменение стилей оформления будет невозможным. Если параметр отключен или не задан, то любой пользователь сможет изменить стиль оформления окон и кнопок.

Для того чтобы сделать неактивными некоторые кнопки и ссылки в окне **Персонализация** (Personalization), достаточно всего лишь активировать определенные параметры политики.

Чтобы запретить возможность изменения цвета темы Aero, системных цветов и цветовых схем для рабочего стола и окон, включите параметр **Запретить изменение цвета и оформления окон** (Prevent changing windows color and appearance). После этого кнопка **Цвет окна** (Windows Color) в окне **Персонализация** (Personalization) будет недоступна. Если этот параметр отключен или не задан, то возможность изменения цвета оформления окон будет доступной.

Чтобы исключить возможность изменения или добавления фона рабочего стола, включите параметр **Запретить изменение фона рабочего стола** (Prevent changing desktop background). После этого кнопка **Фон рабочего стола** (Desktop Background) в окне **Персонализация** (Personalization) будет недоступна. Если этот параметр отключен или не задан, то любой пользователь компьютера сможет воспользоваться возможностью изменения фона рабочего стола.

Чтобы запретить изменять значки рабочего стола, включите параметр **Изменение значков рабочего стола** (Prevent changing desktop icons). После этого ссылка **Параметры значков рабочего стола** (Change desktop icons), расположенная в левой части окна **Персонализация** (Personalization), будет скрыта. Если параметр отключен или не задан, то пользователи могут свободно изменять вид значков рабочего стола, отображать и скрывать значки. Параметр влияет только на следующие значки: **Компьютер** (Computer), **Файлы пользователя** (User's files), **Сеть** (Network), **Панель управления** (Network) и **Корзина** (Recycle Bin).

Для того чтобы исключить возможность изменения указателей мыши, включите параметр **Запретить изменение указателей мыши** (Prevent changing mouse pointers). После этого ссылка **Изменение указателей мыши** (Change mouse pointers), расположенная в левой части окна **Персонализация** (Personalization), будет скрыта. Если параметр отключен или не задан, то ограничение на использование настроек в окне **Свойства: Мышь** (Mouse Properties) установлено не будет.

Для того чтобы исключить возможность добавления, настройки или изменения заставки на компьютере, включите параметр **Запретить изменение заставки** (Prevent changing screen saver). После этого кнопка **Заставка** (Screen Saver) в окне **Персонализация** (Personalization) будет недоступна. Запуск заставок при этом не запрещается. Если же параметр отключен или не настроен, то ограничений в настройках заставки компьютера установлено не будет.

Чтобы заблокировать возможность добавления, изменения и удаления звуковых схем, включите параметр **Запретить изменение звуков** (Prevent changing sounds). После этого кнопка **Звуки** (Sounds) в окне **Персонализация** (Personalization) будет недоступна. Если параметр отключен или не задан, то запрет в настройках системных звуков не применяется.

Следующий параметр неработоспособен в Windows 8 и позволяет заблокировать возможность изменения цветовой схемы текущей темы рабочего стола. Для этого следует включить параметр **Запретить изменение цветовой темы** (Prevent changing color scheme). Если параметр отключен или не задан, то любой пользователь может изменить цветовую схему темы рабочего стола.

Применение выбранной темы

Этот параметр позволяет установить файл темы, который будет применяться при первом входе пользователя в систему. Для того чтобы включить параметр, выполните следующие шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Персонализация** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Personalization).
2. Дважды щелкните мышью по параметру **Применить указанную тему** (Load a specific theme). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. В области **Параметры** (Options) в поле ввода **Путь к файлу темы** (Path to theme file) укажите полный путь к файлу темы.
5. Нажмите кнопку **ОК**.

После этого при первом входе пользователя в систему вместо стандартной темы Windows 8 будет использована указанная тема. Параметр не запрещает дальнейшее изменение темы пользователем, а также любых других эле-

ментов темы, таких как фон рабочего стола, заставка, цвет окон и системные звуки.

Параметр **Применить конкретный файл стиля оформления или классический стиль** (Force a specific visual style file or force Windows Classic) позволяет применить файл стиля оформления, указанный в параметре. После выбора стиля оформления пользователи, изменяя тему, не смогут применять другие стили оформления. Для того чтобы включить параметр, выполните следующие шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Персонализация** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Personalization).
2. Дважды щелкните мышью по параметру **Применить конкретный файл стиля оформления или классический стиль** (Force a specific visual style file or force Windows Classic). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. В области **Параметры** (Options) в поле ввода **Путь к файлу стиля оформления** (Path to Visual Style) укажите путь к файлу стиля оформления. Файл может быть расположен как на локальном компьютере (aero.msstyles), так и на удаленном сервере. Если файл расположен на удаленном сервере, то указывается UNC-путь в формате \\сервер\общий_ресурс\aero.msstyles. Чтобы выбрать классический стиль Windows — оставьте поле пустым.
5. Нажмите кнопку **ОК**.

После включения параметра пользователи смогут менять темы оформления Windows, но стиль оформления применяться не будет.

Управление параметрами заставки компьютера

Для того чтобы включить или отключить использование заставки компьютера, выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Персонализация** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Personalization).
2. Дважды щелкните мышью по параметру **Включить заставку** (Enable screen saver). Откроется диалоговое окно редактирования параметра политики.

3. Установите переключатель в положение **Включить** (Enabled) для того, чтобы заставки на компьютере использовались, или в положение **Отключить** (Disabled), чтобы заставки были отключены.
4. Нажмите кнопку **ОК**.

Если переключатель был установлен в положение **Включить** (Enabled), то заставки будут использоваться на компьютере так, как и по умолчанию. Если было выбрано положение **Отключить** (Disabled), то заставка использоваться не будет, а настройки в диалоговом окне **Параметры экранной заставки** (Screen Saver Settings) станут неактивными (рис. 4.3).

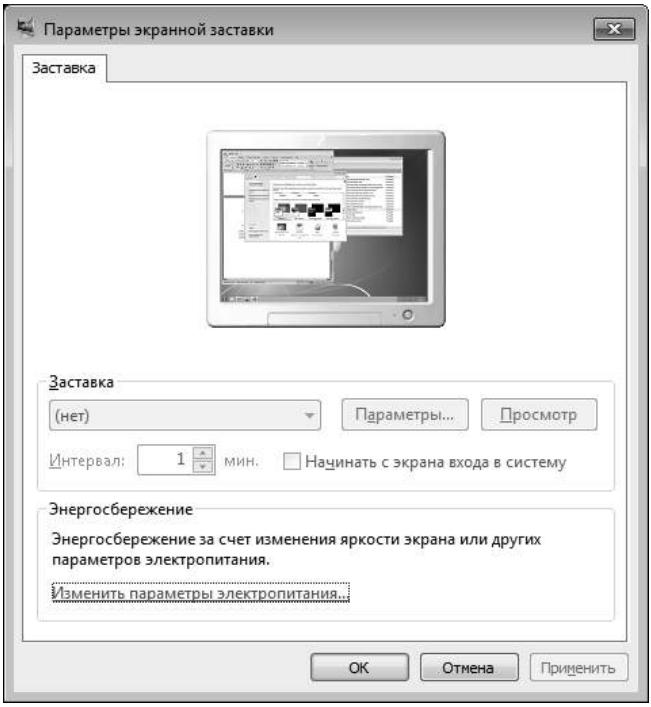


Рис. 4.3. *Диалоговое окно* Параметры экранной заставки

Для того чтобы указать время бездействия пользователя, по истечении которого будет запускаться заставка, выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Персонализация** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Personalization).
2. Дважды щелкните мышью по параметру **Таймаут заставки** (Screen saver timeout). Откроется диалоговое окно редактирования параметра политики.

3. Установите переключатель в положение **Включить** (Enable).
4. В области **Параметры** (Options) в поле ввода со счетчиком **Секунды** (Seconds) укажите количество секунд бездействия.
5. Нажмите кнопку **ОК**.

Если время ожидания рано нулю, заставка не запускается, так же как если отключен параметр **Включить заставку**. Время ожидания можно указывать в интервале от 1 секунды до 86400 секунд (24 часа). По умолчанию используется значение 900 секунд (15 минут). Если параметр не задан, то используется значение по умолчанию. Если параметр отключен, то он не применяется.

Для того чтобы включить парольную защиту заставок на компьютере, выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Персонализация** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Personalization).
2. Дважды щелкните мышью по параметру **Парольная защита заставки** (Password protect the screen saver). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. Нажмите кнопку **ОК**.

После этого все заставки будут защищены паролем. А чтобы пользователи не смогли изменить пароль, флажок **Начинать с экрана входа в систему** (On resume, display logon screen) в диалоговом окне **Параметры экранной заставки** (Screen Saver Settings) будет недоступен. Если же параметр отключен или не задан, то пользователи могут пользоваться возможностью установки парольной защиты заставки без ограничений.

Параметр **Применить указанную заставку** (Force specific screen saver) позволяет запретить изменение заставки рабочего стола и использовать только ту заставку, исполняемый файл которой будет указан в параметре. Для того чтобы включить параметр, выполните следующие шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Персонализация** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Personalization).
2. Дважды щелкните мышью по параметру **Применить указанную заставку** (Force specific screen saver). Откроется диалоговое окно редактирования параметра политики.

3. Установите переключатель в положение **Включить** (Enable).
4. В области **Параметры** (Options) в поле ввода **Имя исполняемого файла заставки** (Screen saver executable name) укажите исполняемый файл заставки. Если файл расположен в каталоге %Systemroot%\System32, то введите название файла и расширение .scr. Если исполняемый файл заставки расположен в другом каталоге, то необходимо ввести полный путь к файлу.
5. Нажмите кнопку **ОК**.

После включения параметра будет использоваться только указанная заставка. Раскрывающийся список выбора заставок станет недоступным, и пользователи не смогут ее изменить. Параметр пропускается в том случае, если указанная заставка не будет установлена на компьютере.

4.3. Управление элементом «Программы и компоненты»

В этом разделе вы узнаете, как ограничить для пользователя возможности использования элемента **Программы и компоненты** (Programs and Features) панели управления.

Сокрытие компоненты Программы и компоненты

Для того чтобы полностью запретить использование компонента **Программы и компоненты** (Programs and Features), выполните следующие шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒Панель управления ⇒ Программы** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Programs).
2. Дважды щелкните мышью по параметру **Скрыть панель управления «Программы»** (Hide the Programs Control Panel). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
5. Нажмите кнопку **ОК**.

Теперь компонентом **Программы и компоненты** (Programs and Features) воспользоваться нельзя. Само окно компонента откроется, но все его воз-

можности будут неактивными, а при попытке открыть диалоговое окно **Компоненты Windows** (Windows Features) появится уведомление о том, что этот компонент отключен системным администратором. Этот параметр имеет наибольший приоритет перед остальными параметрами политики в группе **Программы** (Programs).

Несмотря на полный запрет использования компонента панели управления **Программы и компоненты** (Programs and Features), другие способы установки и удаления программ заблокированы не будут (можно, как и раньше, устанавливать и удалять программы посредством их собственных инсталляторов).

Если параметр отключен или не задан, то панель управления **Программы** (Programs) будет доступна всем пользователям компьютера.

Сокрытие отдельных элементов панели управления

Для того чтобы скрыть отдельный элемент панели управления, связанный с настройкой программ, достаточно просто включить соответствующий элементу параметр политики.

Чтобы отключить страницу **Настройка доступа программ и умолчаний** (Set program access and computer defaults) из компонента панели управления **Программы по умолчанию** (Default Programs), выполните следующие шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒Панель управления ⇒ Программы** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Programs).
2. Дважды щелкните мышью по параметру **Скрытие страницы доступа к программам и параметров по умолчанию** (Hide «Set Program Access and Computer Defaults» page). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. Нажмите кнопку **ОК**.

После этого пользователи не смогут воспользоваться страницей **Настройка доступа программ и умолчаний** (Set program access and computer defaults). Эта страница позволяет назначать программы по умолчанию для выполнения определенных действий (например, использование браузера Internet Explorer как программы по умолчанию для работы с веб-страницами). Если параметр отключен или не задан, то любой пользователь сможет воспользоваться страницей **Настройка доступа программ и умолчаний** (Set program access and computer defaults) для изменения соответствующих настроек.

Следующие параметры включаются аналогично и доступны в группе **Программы** (Programs).

Чтобы скрыть страницу **Программы и компоненты** (Programs and Features), которая содержит список установленных на компьютере программ, включите параметр **Скрыть страницу «Программы и компоненты»** (Hide «Programs and Features» page). После этого список установленных программ отображаться не будет.

Чтобы скрыть страницу **Установленные обновления** (Installed Updates), которая вызывается при переходе по ссылке **Просмотр установленных обновлений** (View installed updates), включите параметр **Скрыть страницу «Установленные обновления»** (Hide «Installed Updates» page). После этого список установленных обновлений, загруженных с сайта Windows Update или с сайтов программ сторонних производителей, отображаться не будет.

Чтобы скрыть окно **Компоненты Windows** (Windows Features), которое отображается при нажатии ссылки **Включение или отключение компонентов Windows** (Turn Windows features on or off), включите параметр **Скрыть «Компоненты Windows»** (Hide «Windows Features»). После этого, при попытке вызвать окно **Компоненты Windows** (Windows Features), появится уведомление о том, что системный администратор отключил компоненты Windows (рис. 4.4).

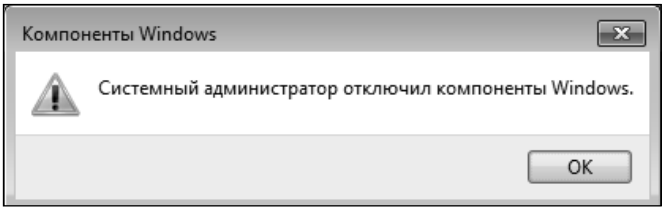


Рис. 4.4. ***Диалоговое окно, уведомляющее о блокировке элемента***

Страница **Получение программ** (Get Programs) отображает список программ, опубликованных системным администратором. Список предназначается для того, чтобы уведомить пользователя об их доступности, рекомендовать программу к использованию или просто упростить ее установку. Для того чтобы скрыть эту страницу, включите параметр **Скрыть страницу «Получение программ»** (Hide «Get Programs» page). После этого пользователи не смогут просматривать программы, опубликованные системным администратором, и использовать страницу **Получение программ** (Hide «Get Programs) для их установки. Однако параметр не запрещает другие способы установки этих программ.

Для того чтобы скрыть страницу **Windows Marketplace**, которая позволя-

ет пользователям приобретать и загружать программы на компьютер, включите параметр **Скрыть «Windows Marketplace»** (Hide «Windows Marketplace»). После этого пользователь не сможет воспользоваться компонентом **Получить новые программы с Windows Marketplace** (Get new programs from Windows Marketplace) панели управления **Программы и компоненты** (Programs and Features). Однако это не помешает пользователю воспользоваться услугами Windows Marketplace другими способами.

4.4. Работа с принтерами

В этом разделе мы расскажем о том, как ограничить возможности установки и удаления принтеров, а также изменить адрес в службе Active Directory, с которого начинается поиск принтеров.

Управление разрешениями на добавление и удаление принтеров

Для того чтобы запретить всевозможные способы установки локальных и сетевых принтеров, а также установки новых принтеров путем перетаскивания значка принтера в папку **Принтеры** (Printers):

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Принтеры** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Printers).
2. Дважды щелкните мышью по параметру **Запретить добавление принтеров** (Prevent addition of printers). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
5. Нажмите кнопку **ОК**.

После этого будет удален значок **Установка принтера** (Add Printer) из папки **Принтеры** (Printers) в панели управления. При попытке перетащить значок принтера в папку **Принтеры** (Printers) появится уведомление о запрете выполнения операции. Тем не менее этот параметр не запрещает установку принтера при помощи мастера установки оборудования и с помощью других программ.

Если параметр отключен или не задан, то пользователи могут установить но-

вый принтер любым способом, в том числе и методом перетаскивания значка принтера в папку **Принтеры** (Printers).

Для того чтобы запретить удаление принтеров командой **Удалить** (Delete) в папке **Printers,** выполните следующие шаги, активируйте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Принтеры** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Printers).
2. Дважды щелкните мышью по параметру **Запретить удаление принтеров** (Prevent deletion of printers). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. Нажмите кнопку **ОК**.

После этого при попытке удалить принтер появится сообщение о том, что выполнение данной операции запрещено. Тем не менее параметр не запрещает использование сторонних программ для удаления принтеров. Если параметр отключен или не задан, то пользователи могут удалить установленный принтер любым способом, в том числе и командой **Удалить** (Delete) в папке **Принтеры** (Printers).

Разрешение обзора сети для поиска принтеров

По умолчанию при установке сетевого принтера без указания его имени мастер установки принтеров выводит весь список общих принтеров в сети и предлагает выбрать из этого списка модель. Для того чтобы страница обзора сетевых принтеров в окне мастера установки принтеров не отображалась, выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Принтеры** (User configuration ⇒ Administrative Templates ⇒ Control Panel ⇒ Printers).
2. Дважды щелкните мышью по параметру **Разрешить обзор сети для поиска принтеров** (Browse the network to find printers). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Отключить** (Disabled).
4. Нажмите кнопку **ОК**.

После этого поиск принтеров в сети будет невозможен, и для установки принтера потребуется ввести его имя вручную. Этот параметр влияет толь-

ко на работу мастера установки принтера, поиск сетевых принтеров и возможность подключения к ним в других программах не блокируется.

4.5. Настройка языковых и региональных стандартов

В этом разделе вы узнаете, как скрыть определенные параметры, связанные с настройкой языка системы, а также как установить ограничения выбора и использования языков Windows.

Скрытие параметров

Для того чтобы из панели управления **Язык и региональные стандарты** (Region and Language Options) скрыть вкладку **Дополнительно** (Administrative), в которую входят интерфейсы для задания системных языковых стандартов и копирования параметров для пользователя по умолчанию, включите параметр **Скрыть параметры управления в панели «Язык и региональные стандарты»** (Hide Regional and Language Options administrative options), расположенный в папке **Язык и региональные стандарты** (Region and Language Options). Для этого активируйте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Язык и региональные стандарты** (User Configuration Administrative ⇒ Templates ⇒ Control Panel ⇒ Regional and Language Options).
2. Дважды щелкните мышью по параметру **Скрыть параметры управления в панели «Язык и региональные стандарты»** (Hide Regional and Language Options administrative options). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
5. Нажмите кнопку **ОК**.

После этого вкладка **Дополнительно** (Administrative) будет скрыта. Если параметр отключен или не задан, то вкладка будет отображаться, однако некоторые включенные параметры могут помешать изменению параметров, расположенных в этой вкладке.

Аналогичным способом скрываются нижеперечисленные параметры.

Чтобы скрыть вкладку **Расположение** (Location) в панели управления **Язык и региональные стандарты** (Region and Language), включите параметр **Скрыть параметр географического положения** (Hide the geographic location option). Вкладка **Расположение** (Location) позволяет указать текущее расположение пользователя, исходя из которого некоторые программы будут предлагать дополнительную местную информацию (например, новости или прогноз погоды). Если параметр отключен или не задан, то вкладка будет отображаться, однако некоторые включенные параметры могут помешать изменению параметров, расположенных в этой вкладке.

Чтобы скрыть кнопку **Установить или удалить язык** (Install/uninstall languages), расположенную во вкладке **Языки и клавиатуры** (Keyboard and Languages) панели управления **Язык и региональные стандарты** (Region and Languages), включите параметр **Скрыть параметры выбора языковой группы** (Hide the select language group options). При нажатии этой кнопки открывается диалоговое окно, в котором можно добавить или удалить языки, которые могут использоваться для отображения текста, распознавания речи и рукописного ввода. Если параметр отключен или не задан, то пользователь может воспользоваться возможностью изменения языка интерфейса операционной системы, установки новых языков и удаления установленных, однако некоторые включенные параметры могут помешать изменению настроек языка интерфейса.

Чтобы скрыть вкладку **Форматы** (Formats) панели управления **Язык и региональные стандарты** (Region and Languages), включите параметр **Скрыть параметры выбора и настройки языкового стандарта** (Hide user locale selection and customization options). Вкладка **Форматы** (Formats) позволяет указать языковой формат, формат краткой и полной даты, кратного и полного времени, первый день недели, а также числовые форматы и форматы денежных единиц. Если параметр отключен или не задан, то вкладка будет отображаться, однако некоторые включенные параметры могут помешать изменению параметров, расположенных в этой вкладке.

Ограничение выбора языка меню и диалоговых окон Windows

Чтобы ограничить пользователей каким-либо одним из языков, отключая меню и элементы управления диалогового окна в панели управления **Язык и региональные стандарты** (Region and Language), настройте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Язык и региональные стандарты** (User

Configuration Administrative ⇒ Templates ⇒ Control Panel ⇒ Regional and Language Options).

2. Дважды щелкните мышью по параметру **Ограничить выбор языка меню и диалогов Windows** (Restrict selection of Windows menus and dialogs language). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. В области **Параметры** (Options) в раскрывающемся списке **Ограничить пользователей следующими языками** (Restrict users to the following language) выберите необходимый язык (например, **Русский** (Russian)).
5. Нажмите кнопку **ОК**.

Если выбранный язык не установлен на целевом компьютере, то автоматически будет использован английский язык.

Если параметр отключен или не задан, то ограничения выбора языка меню и диалогов Windows не будут применяться.

Установка языка интерфейса Windows

Если на компьютере установлено больше одного языка пользовательского интерфейса, то стоит настроить язык по умолчанию для таких компьютеров. Для того чтобы выбрать язык интерфейса по умолчанию, выполните следующие шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Панель управления ⇒ Язык и региональные стандарты** (User Configuration Administrative ⇒ Templates ⇒ Control Panel ⇒ Regional and Language Options).
2. Дважды щелкните мышью по параметру **Ограничить язык интерфейса Windows для указанного пользователя** (Restricts the UI languages Windows should use for the selected user). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enable).
4. В области **Параметры** (Options) в раскрывающемся списке **Ограничить пользователей следующими языками** (Restrict users to the following language) выберите необходимый язык, который вы хотите использовать на этом компьютере.
5. Нажмите кнопку **ОК**.

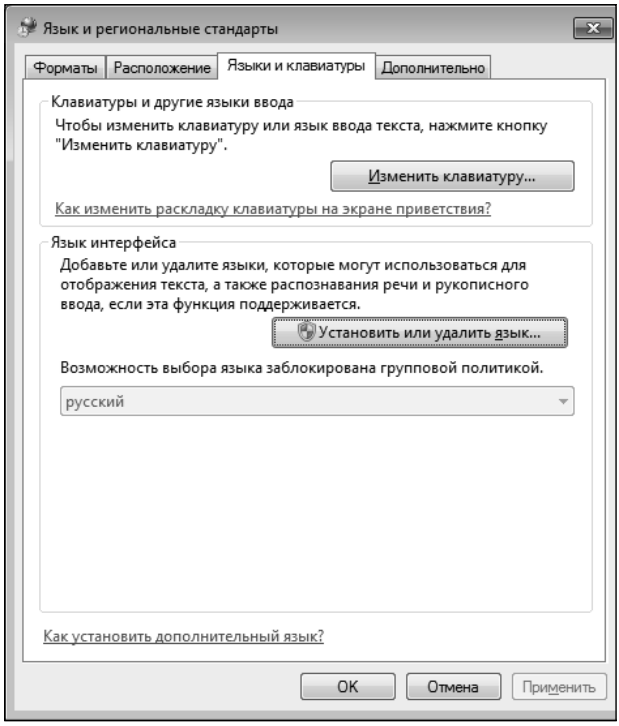


Рис. 4.5. ***Возможность выбора языка заблокирована групповой политикой***

После этого пользовательский интерфейс нельзя будет изменить (рис. 4.5).

Если указанный в параметре язык не установлен на компьютере, то выбор языка по умолчанию определяется пользователем.

Если параметр отключен или не задан, то пользователь может воспользоваться возможностью изменения языка интерфейса операционной системы.

Заключение

Прочитав эту небольшую главу, вы получили все необходимые знания о том, как настроить панель управления в Редакторе локальной групповой политики: теперь вы знаете, как ограничить отображение и функциональность элементов панели управления, заблокировать установку и удаление принтеров, программ и системных компонентов. В следующих главах мы детально разберем различные групповые политики операционных систем Windows 8.


Windows 8

Глава 5.

Хакинг системных элементов Windows 8

В этой главе вы узнаете, как настроить параметры системных элементов в Редакторе локальных групповых политик: запретить запуск определенных программ, запретить использование определенных компонентов системы (например, командной строки или системного реестра), изменить параметры входа в систему и выход из нее, режимы энергопотребления, параметры диагностики системы, обновления системы и функционирования справки Microsoft.

5.1. Базовые настройки системы

Базовые настройки системы располагаются в корне **Административные шаблоны ⇒ Система** и отвечают за основные параметры системы, интерфейса пользователя, размещение установочных файлов Windows, запрета запуска определенных приложений или использования системных компонентов, например системного реестра Windows.

Запрет запуска приложений из справки перечисленных программ

По умолчанию каждый пользователь может запустить приложения из электронной справки. Для того чтобы запретить запуск приложений таким способом, активируйте следующий параметр:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система** (Computer Configuration ⇒ Administrative Templates ⇒ System).
2. Дважды щелкните мышью по параметру **Запретить запуск из справки перечисленных программ** (Restrict these programs from being launched from Help). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в поле ввода **Введите имена исполняемых файлов разделенные запятыми** (Enter executables separated

by commas) введите с клавиатуры названия исполняемых файлов программ (например, calc.exe), запуск которых вы хотите ограничить, разделяя их запятой.

5. Нажмите кнопку **ОК**.

Примечание. Этот параметр задается в группах политик «Конфигурация компьютера» и «Конфигурация пользователя». Если этот параметр задан в обеих группах, то будет ограничен запуск программ, указанных в каждой из них.

Использование альтернативного интерфейса пользователя

По умолчанию интерфейс пользователя создает программа Проводник. Этот интерфейс нам, естественно, более привычен и, возможно, как ни крути, удобнее, чем все остальные. Но, так или иначе, интерфейс проводника Windows можно заменить на другой, используя вместо Explorer.exe другой исполняемый файл. Для того чтобы указать исполняемый файл альтернативного интерфейса, настройте следующую политику:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система** (Computer Configuration ⇒ Administrative Templates ⇒ System).
2. Дважды щелкните мышью по параметру **Настраиваемый интерфейс пользователя** (Custom User Interface). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в поле ввода **Имя файла программы интерфейса** (Interface file name) введите название исполняемого файла программы альтернативного интерфейса системы (по умолчанию используется Explorer.exe).
5. Нажмите кнопку **ОК**.

Для того чтобы задействовать параметр, программа интерфейса должна быть скопирована на общий сетевой ресурс или на системный диск. И только после этого можно указывать название исполняемого файла альтернативного интерфейса.

Если программа интерфейса расположена в папке, не указанной в переменной среды «Path» для системы, следует ввести полный путь к файлу. Вы можете просмотреть значение переменной на своем компьютере в диалоговом окне **Переменные среды** (Environment Variables), вызываемом на вкладке **Дополнительно** (Advanced) окна **Свойства системы** (System Properties).

Запрет использования командной строки

Для того чтобы пользователи не могли запускать окно командной строки, а также запускать пакетные файлы (.cmd и .bat), выполните следующие действия:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система** (Computer Configuration ⇒ Administrative Templates ⇒ System).
2. Дважды щелкните мышью по параметру **Запретить использование командной строки** (Prevent access to the command prompt). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в раскрывающемся списке **Запретить также обработку сценариев в командной строке?** (Disable the command prompt script processing also?) выберите необходимый пункт:
   - **Да** (Yes) — пакетные файлы на компьютере выполняться не будут.
   - **Нет** (No) — пакетные файлы будут выполняться.
5. Нажмите кнопку **ОК**.

Теперь попытки запустить окно командной строки будут заканчиваться неудачей (рис. 5.1).

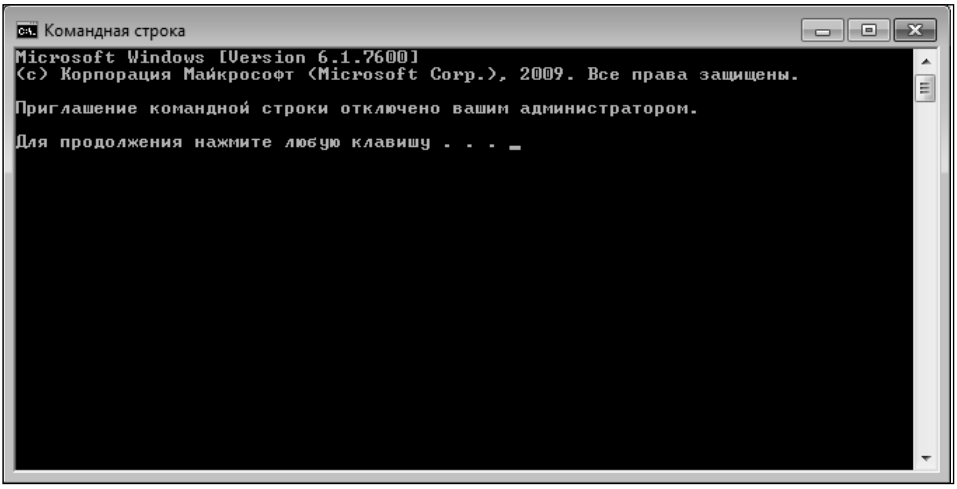


Рис. 5.1. ***Запрет обработки сценариев в окне*** **Командная строка**

Если параметр отключен или не задан, то пользователи смогут использовать функции командной строки, а также запускать пакетные файлы.

Не рекомендуется запрещать выполнение пакетных файлов на компьютере, если на нем используются сценарии входа, выхода, автоматического запуска, завершения работы, а также если используются службы удаленных рабочих столов.

Ограничение доступа к средствам редактирования реестра

Для того чтобы защитить компьютер от несанкционированного доступа пользователя в реестр системы, выполните следующие шаги:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система** (Computer Configuration ⇒ Administrative Templates ⇒ System).
2. Дважды щелкните мышью по параметру **Запретить доступ к средствам редактирования реестра** (Prevent access to registry editing tools). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в раскрывающемся списке **Отключить запуск редактора реестра без предупреждения?** (Disable regedit from running silently?) выберите необходимый пункт:
   - **Да** (Yes) — отключить.
   - **Нет** (No) — не отключать.
5. Нажмите кнопку **ОК**.

Теперь при попытке запуска реестра пользователь будет уведомлен о невозможности использования реестра (рис. 5.2).

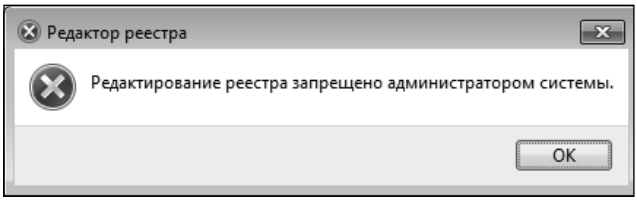


Рис. 5.2. ***Запрет редактирования реестра***

Если параметр отключен или не задан, то пользователи смогут запускать редактор реестра и пользоваться им.

Ограничение запуска приложений Windows

При возникновении необходимости ограничения списка приложений, которые может запустить пользователь, можно воспользоваться следующим параметром:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система** (Computer Configuration ⇒ Administrative Templates ⇒ System).
2. Дважды щелкните мышью по параметру **Не запускать указанные приложения Windows** (Don't run specified Windows applications). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled). Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
4. В области **Параметры** (Options) нажмите кнопку **Показать** (Show). Появится диалоговое окно **Вывод содержания** (List of disallowed applications).
5. В появившемся диалоговом окне щелкните два раза по пустому полю и введите с клавиатуры имя исполняемого файла (например, Notepad.exe) или документа. Чтобы указать еще одно имя файла, нажмите клавишу **Enter** и введите имя.
6. Нажмите кнопку **ОК**, чтобы закрыть диалоговые окна.

Теперь при попытке запустить введенное в список приложение будет появляться уведомление о невозможности запуска (рис. 5.3).

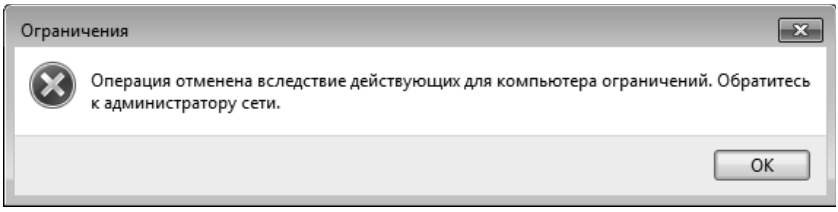


Рис. 5.3. ***Уведомление о невозможности запуска приложения***

Однако если пользователи имеют доступ к командной строке, то это им не помешает запустить приложение из окна командной строки. В этом случае имеет смысл запретить запуск файла CMD.exe.

Если параметр отключен или не задан, то пользователь сможет запускать любые установленные приложения без ограничений. Однако некоторые

включенные и настроенные параметры могут вызвать исключения, например параметр **Выполнять только указанные приложения** (Run only specified Windows applications).

Аналогичным способом настраивается параметр **Выполнять только указанные приложения** (Run only specified Windows applications) с отличием в том, что здесь нужно указать список программ, которые можно будет запускать в системе через Проводник Windows. Аналогично ничто не помешает пользователям воспользоваться командной строкой для запуска приложений.

Если параметр отключен или не задан, то пользователь не будет ограничен списком разрешенных к запуску приложений. Однако некоторые включенные и настроенные параметры могут вызвать исключения, например параметр **Не запускать указанные приложения Windows** (Don't run specified Windows applications).

Запрет автоматического шифрования файлов, перемещаемых в зашифрованные папки

По умолчанию если незашифрованный файл переместить в зашифрованную папку, то этот файл будет автоматически зашифрован после перемещения. Для того чтобы отключить автоматическое зашифровывание файла при перемещении его в зашифрованную папку, выполните следующие действия:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система** (Computer Configuration ⇒ Administrative Templates ⇒ System).
2. Дважды щелкните мышью по параметру **Не выполнять автоматическое шифрование файлов, перемещаемых в зашифрованные папки** (Do not automatically encrypt files moved to encrypted folders). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

После этого, если незашифрованный файл переместить в зашифрованную папку, он не будет автоматически зашифровываться. Однако файлы будут автоматически зашифровываться при перемещении их в другие тома или при создании нового файла.

Управление постоянной временной меткой

Постоянная метка позволяет системе определить время неожиданного от-

ключения, посредством записи на диск текущего времени по расписанию, задаваемое интервалом временной метки. По умолчанию постоянная временная метка обновляется каждые 60 секунд. Для того чтобы изменить это значение, выполните следующие шаги:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система** (Computer Configuration ⇒ Administrative Templates ⇒ System).
2. Дважды щелкните мышью по параметру **Включить постоянную метку** (Enable Persistent Time Stamp). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в поле **Сек** (Seconds) введите с клавиатуры значение от 1 до 86400 секунд — период записи постоянной временной метки. 86400 секунд равно одному дню.
5. Нажмите кнопку **ОК**.

После этого постоянная временная метка будет обновляться в соответствии с новым заданным интервалом. Если параметр отключить, то постоянная временная метка будет отключена, и определение времени отключения станет невозможным.

Отображение сообщений о подробном состоянии системы

По умолчанию система не отображает своего подробного текущего состояния во время выполнения процесса запуска и завершения работы системы. Для того чтобы включить отображение подробного состояния системы, настройте следующую политику:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система** (Computer Configuration ⇒ Administrative Templates ⇒ System).
2. Дважды щелкните мышью по параметру **Подробные или обычные сообщения состояния** (Verbose vs normal status messages). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

После этого во время запуска и завершения работы система будет отображать свое текущее состояние, отражая каждый шаг запуска и завершения работы системы.

Политика не будет соблюдаться в том случае, если включен параметр удаления состояния загрузки/завершения работы системы/входа в систему/выхода из системы.

Изменение локации установочных файлов

По умолчанию в операционной системе Windows установочные файлы пакета обновления располагаются в каталоге, использованном при последней установке пакета обновлений в данной системе. Для того чтобы указать другое размещение для установочных файлов пакета обновления Windows, выполните следующие действия:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система** (Computer Configuration ⇒ Administrative Templates ⇒ System).
2. Дважды щелкните мышью по параметру **Указать размещение установочных файлов пакета обновления Windows** (Specify Windows Service Pack installation file location). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в поле ввода **Путь к установочным файлам пакета обновления Windows** (Windows Service Pack Setup file path) введите путь размещения установочных файлов пакета обновления.
5. Нажмите кнопку **ОК**.

Аналогичным способом настраивается параметр **Указать расположение установочных файлов Windows** (Specify Windows installation file location), который отвечает за указание пути размещения установочных файлов Windows. Путь вводится в поле ввода **Путь к установочным файлам Windows** (Windows Setup file path).

Если параметр отключен или не задан, то путь к установочным файлам Windows будет тот же, что был использован при установке операционной системы.

5.2. Настройка окна Безопасность Windows

Этот раздел содержит настройки параметров узла **Варианты действий после нажатия CTRL+ALT+DEL** (Ctrl+Alt+Del Options). В параметрах этого узла

можно настроить действие системы при использовании сочетания трех клавиш: **Ctrl+Alt+Del,** например блокировку использования диспетчера задач или блокировку компьютера.

Запрет изменения пароля

По умолчанию каждый пользователь может воспользоваться кнопкой **Смена пароля** в окне **Безопасность Windows**, которое вызывается нажатием сочетания клавиш **Ctrl+Alt+Del**. Для того чтобы пользователи не смогли воспользоваться этой кнопкой и сменить свой пароль по собственному желанию, выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Варианты действий после нажатия CTRL+ALT+DEL** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Ctrl+Alt+Del Options).
2. Дважды щелкните мышью по параметру **Запретить изменение пароля** (Remove Change Password). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled). Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
4. Нажмите кнопку **ОК**.

Кнопка смены пароля будет отключена, и пользователи не смогут изменить свой пароль. Однако эта политика не мешает изменить пароль по запросу системы. Система запрашивает пароль по требованию администратора или по истечении срока действия пароля.

Запрет блокировки компьютера

Когда система блокируется, скрывается рабочий стол, что не дает возможности воспользоваться системой. Блокировку может отменить пользователь, который заблокировал систему, или же системный администратор. Чтобы запретить блокировку компьютера:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Варианты действий после нажатия CTRL+ALT+DEL** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Ctrl+Alt+Del Options).
2. Дважды щелкните мышью по параметру **Запретить блокировку**

компьютера (Remove Lock Computer). Откроется диалоговое окно редактирования параметра политики.

3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Если параметр отключен или не задан, то блокировка компьютера будет разрешена.

Удаление Диспетчера задач

Используя эту политику, можно запретить пользователям запускать и использовать Диспетчер задач. Для этого активируйте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Варианты действий после нажатия CTRL+ALT+DEL** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Ctrl+Alt+Del Options).
2. Дважды щелкните мышью по параметру **Удалить диспетчер задач** (Remove Task Manager). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Теперь при попытке вызвать Диспетчер задач пользователь получит уведомление о том, что вызов Диспетчера задач невозможен по причине блокировки данной политикой (рис. 5.4).

Если этот параметр отключен или не настроен, то любой пользователь сможет запустить Диспетчер задач.

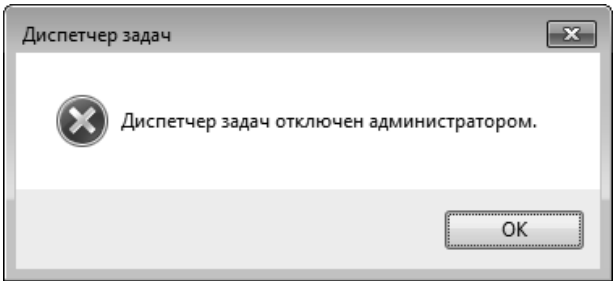


Рис. 5.4. ***Уведомление об отключенном Диспетчере задач***

Запрет завершения сеанса

Для того чтобы отключить или вообще удалить все команды меню и кнопки, которые позволяют пользователю выполнить выход из системы, выполните следующие шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Варианты действий после нажатия CTRL+ALT+DEL** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Ctrl+Alt+Del Options).
2. Дважды щелкните мышью по параметру **Запретить завершение сеанса** (Remove Logoff). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Если параметр отключен или не задан, то команды меню и кнопки выхода из системы будут отображаться и функционировать, как положено.

5.3. Действия при входе в систему

В этом разделе будут рассмотрены параметры узла **Вход в систему** (Logon), отвечающие за параметры действий при входе в систему. Здесь можно настроить, какие приложения система может автоматически запускать при входе в систему, установку домена при входе, отключение звука Windows и несколько других параметров.

Создание списка программ, запускаемых при входе в систему

Вы можете создать пользовательский список дополнительных программ и документов, которые будут автоматически запущены при следующей загрузке системы, однократно. Эти программы добавляются к стандартному списку программ и служб, которые система автоматически запускает при загрузке. Для того чтобы игнорировать список программ, выполняемых однократно, выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Вход в систему** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Logon).
2. Дважды щелкните мышью по параметру **Не обрабатывать список**

однократного запуска программ (Do not process the run once list). Откроется диалоговое окно редактирования параметра политики.

3. Установите переключатель в положение **Включить** (Enabled). Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
4. Нажмите кнопку **ОК**.

Настройки списков программ, выполняемых однократно, хранятся в разделе реестра HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce.

Также можно создать список дополнительных программ и документов, запускаемых системой автоматически на компьютерах под управлением Windows 2000 Professional, Windows XP Professional и Windows Vista. Эти программы добавятся к стандартному списку автоматически запускаемых программ и служб. Для того чтобы проигнорировать этот список программ, активируйте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Вход в систему** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Logon).
2. Дважды щелкните мышью по параметру **Не обрабатывать список запуска старых программ** (Do not process the legacy run list). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Если этот параметр отключен или не задан, то список старых программ будет добавлен к списку программ, запускаемых при входе в систему.

Для того чтобы задать список дополнительных программ и документов, которые Windows автоматически запустит при входе пользователя в систему, настройте следующую политику:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Вход в систему** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Logon).
2. Дважды щелкните мышью по параметру **Выполнять эти программы при входе в систему** (Run these programs at user logon). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).

4. В области **Параметры** (Options) нажмите кнопку **Показать** (Show). Появится диалоговое окно **Вывод содержания** (Show Contents) (рис. 5.6).
5. В появившемся диалоговом окне щелкните два раза по пустому полю и введите с клавиатуры имя исполняемого файла или документа. Чтобы указать следующее имя файла, нажмите клавишу **Enter**. Если файл находится в каталоге, отличном от %Systemroot%, нужно указать полный путь.
6. Нажмите кнопку **ОК**, чтобы закрыть диалоговые окна.

Детальная настройка входа в систему

Чтобы система постоянно использовала классическое окно входа в систему, активируйте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Вход в систему** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Logon).
2. Дважды щелкните мышью по параметру **Всегда классический вход в систему** (Always use classic logon). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

По умолчанию для членов рабочей группы задано упрощенное окно входа. Если компьютер не входит в домен, то параметр срабатывает.

Чтобы отключить звук запуска Windows, а также запретить его настройку в компоненте **Звук** (Sound) панели управления, выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Вход в систему** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Logon).
2. Дважды щелкните мышью по параметру **Отключить звук запуска Windows** (Turn off Windows Startup Sound). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Звук запуска Windows воспроизводится при запуске системы. Он может

быть включен и отключен в компоненте **Звук** (Sound) панели управления. Использование параметра автоматически запрещает пользователям настройку поведения звука запуска Windows, но не запрещает изменение поведения других звуков. Если параметр отключен, то звук запуска Windows будет воспроизводиться при входе любого пользователя в систему. Если параметр не настроен, то любой пользователь может выбрать звуковой файл по желанию в соответствующем компоненте панели управления.

Чтобы игнорировать фон входа в Windows, активируйте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Вход в систему** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Logon).
2. Дважды щелкните мышью по параметру **Всегда использовать настраиваемый фон входа в систему** (Always use custom logon background). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

После этого экран входа в систему всегда будет пытаться загружать настраиваемый фон вместо стандартного входа в Windows. Если параметр отключен или не задан, то будет использоваться стандартный или пользовательский фон экрана входа в систему.

Для того чтобы скрыть кнопку **Смена пользователя** (Change User) в пользовательском интерфейсе входа в систему, меню кнопки **Пуск** (Start) и диспетчере задач, выполните следующие шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Вход в систему** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Logon).
2. Дважды щелкните мышью по параметру **Скрыть точки входа для быстрого переключения пользователей** (Hide entry points for Fast User Swithing). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Если параметр отключен или не задан, то кнопка **Смена пользователя** (Change User) будет отображаться.

5.4. Управление запоминающими устройствами

В этом разделе мы рассмотрим параметры, запрещающие выполнение действий с определенными съемными устройствами, а также другие политики, связанные с работой съемных запоминающих устройств.

Для того чтобы запретить чтение данных с компакт-дисков и DVD-дисков, активируйте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Доступ к съемным запоминающим устройствам** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Removable Storage Access).
2. Дважды щелкните мышью по параметру **Компакт диски и DVD-диски: Запретить чтение** (CD and DVD: Deny read access). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled). Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
4. Нажмите кнопку **ОК**.

Теперь при попытке считать информацию с компакт-диска или DVD-диска будет появляться диалоговое окно, информирующее пользователя о блокировке доступа к запоминающему устройству (рис. 5.5).

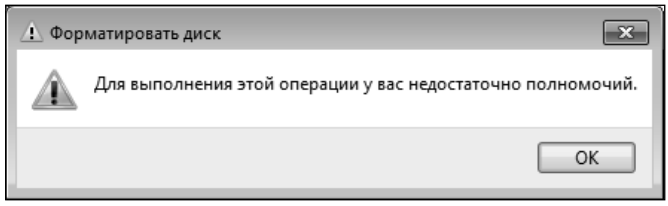


Рис. 5.5. ***Уведомление о блокировке доступа к DVD-диску***

Для того чтобы запретить запись данных на компакт-диски и DVD-диски, включите параметр **Компакт диски и DVD диски: Запретить запись** (CD and DVD: Deny write access):

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Доступ к съемным запоминающим устройствам** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Removable Storage Access).

2. Дважды щелкните мышью по параметру **Компакт-диски и DVD-диски: Запретить запись** (CD and DVD: Deny write access). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Аналогичным образом вы можете запретить чтение и запись данных с (на) накопителей на гибких дисках, активировав параметры **Накопители на гибких дисках: Запретить чтение** (Floppy Drives: Deny read access) и **Накопители на гибких дисках: Запретить запись** (Floppy Drives: Deny write access); съемных дисков (**Съемные диски: Запретить чтение** (Removable Drives: Deny read access) и **Съемные диски: Запретить запись** (Removable Drives: Deny write access)); ленточных накопителей (**Ленточные накопители: Запретить чтение** (Tape Drives: Deny read access) и **Ленточные накопители: Запретить запись** (Tape Drives: Deny write access)) WPD-устройств (Windows Portable Device) (**WPD-устройства: Запретить чтение** (WPD Devices: Deny read access) и **WPD-устройства: Запретить запись** (WPD Devices: Deny write access)).

Для того чтобы запретить чтение данных с нестандартных съемных запоминающих устройств, активируйте параметры **Специальные классы: Запретить чтение** (Custom Classes: Deny read access) и **Специальные классы: Запретить запись** (Custom Classes: Deny write access).

Запрет доступа к любому классу съемных устройств

Для того чтобы запретить любой доступ к любому классу съемных запоминающих устройств, активируйте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Доступ к съемным запоминающим устройствам** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Removable Storage Access).
2. Дважды щелкните мышью по параметру **Съемные запоминающие устройства всех классов: Запретить любой доступ** (All Removable Storage classes: Deny all access). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Данный параметр имеет наиболее высокий приоритет по сравнению с любым другим параметром политики для отдельного съемного запоминающего устройства.

Если параметр отключен или не задан, то запись и чтение данных будет разрешены для запоминающих устройств любого класса.

Для того чтобы установить период времени, после которого система выполнит перезагрузку для принудительного применения изменений в правах доступа к съемным запоминающим устройствам, выполните следующие шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Доступ к съемным запоминающим устройствам** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Removable Storage Access).
2. Дважды щелкните мышью по параметру **Время (в секундах) до принудительной перезагрузки** (Time (in seconds) to force reboot). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в поле **Время** (Time) укажите количество секунд, которое система будет ожидать до принудительной перезагрузки.
5. Нажмите кнопку **ОК**.

Без принудительной перезагрузки права доступа не вступят в действие до перезапуска системы.

Для того чтобы предоставить обычным пользователям прямой доступ к съемным запоминающим устройствам в удаленных сеансах, настройте следующую политику:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Доступ к съемным запоминающим устройствам** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Removable Storage Access).
2. Дважды щелкните мышью по параметру **Все съемные запоминающие устройства: разрешение прямого доступа в удаленных сеансах** (All Removable Storage: Allow direct access in remote sessions). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Если параметр отключен или не настроен, то удаленным пользователям не будет предоставляться прямой доступ к съемным запоминающим устройствам в удаленных сеансах.

5.5. Управление профилями пользователей

В этом разделе мы рассмотрим настройки параметров узла **Профили пользователей** (User Profiles): как определенные папки исключить из перемещаемого профиля, запретим регистрацию временных профилей, укажем путь перемещаемым профилям и некоторые другие параметры.

Изменение синхронизации сетевых папок

По умолчанию при нахождении пользователя в системе сетевые папки остаются в интерактивном режиме. Однако можно настроить синхронизацию определенных сетевых папок при входе или выходе пользователя из системы. Такой вариант способствует разрешению возможных проблем с приложениями, которые некорректно работают с автономными файлами, в то время как пользователь находится в интерактивном режиме. Для того чтобы включить такой тип синхронизации, активируйте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Профили пользователей** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ User Profiles).
2. Дважды щелкните мышью по параметру **Синхронизировать сетевые папки только в момент входа или выхода из системы** (Network directories to sync at Logon/Logoff time only). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в поле ввода введите имена сетевых папок, разделяя их точкой с запятой.
5. Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
6. Нажмите кнопку **ОК**.

Однако не следует использовать параметр для приостановки любых корневых перенаправляемых папок (например, Appdate\Roaming или Документы). Следует приостанавливать подпапки этих родительских папок.

Если параметр отключен или не задан, то сетевые папки будут вести себя так же, как и другие кэшированные данные, обрабатываемые политикой автономных файлов. Если сетевые пути доступны, то останутся в интерактивном режиме при нахождении пользователя в системе.

Исключение папки из перемещаемого профиля

Этот параметр позволяет исключить папки, которые включены в перемещаемый профиль. По умолчанию параметр отключен, и из перемещаемых профилей пользователя исключаются папки Appdata\Local, Appdata\LocalLow, а также все их подпапки (например, History или Temp). Однако вы можете указать имена других папок, которые вы бы не хотели включать в перемещаемый профиль. Для этого настройте следующую политику:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Профили пользователей** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ User Profiles).
2. Дважды щелкните мышью по параметру **Исключить папки из перемещаемого профиля** (Exclude directories in roaming profile). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в поле ввода введите имена тех папок, которые вы не хотите включать в перемещаемый профиль. Имена разделяются точкой с запятой.
5. Нажмите кнопку **ОК**.

Ограничение размера профиля пользователя

По умолчанию система не ограничивает размер профилей. Используя рассматриваемый параметр, можно установить ограничение на размер профилей, как локальных, так и перемещаемых. Для того чтобы настроить ограничение размера профиля, настройте следующую политику:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Профили пользователей** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ User Profiles).
2. Дважды щелкните мышью по параметру **Ограничить размер профиля** (Limit profile size). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options):
    - В поле ввода **Настраиваемое сообщение** (Custom Message) введите сообщение, которое будет отображаться при превышении ограничения размера профиля (рис. 5.6).

- Используйте поле ввода со счетчиком **Максимальный размер профиля (КБ)** (Max Profile Size) для указания максимального размера профиля (указывается в килобайтах).
- Установите флажок **Отображать файлы реестра в списке файлов** (Show registry files in the file list) для того, чтобы включить файлы реестра в список файлов профиля.
- Установите флажок **Уведомлять пользователя, если превышен допустимый размер профиля** (Notify user when profile storage space is exceeded) для того, чтобы система периодически отображала уведомление о превышении ограничения.
- Используйте поле ввода со счетчиком **Напоминать пользователю каждые X минут** (Remind user every X minutes) для указания количества минут, по истечении которых будет отображаться уведомление о превышении ограничения.

5. Нажмите кнопку **ОК**.

Теперь, если размер профиля будет превышен, то пользователь будет уведомлен об этом (рис. 5.6).

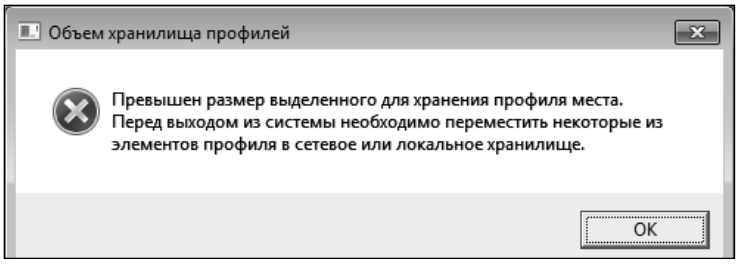


Рис. 5.6. *Диалоговое окно* Объем хранилища профилей

Добавление группы «Администраторы» в перемещаемые профили

По умолчанию полный доступ к своему профилю получает только пользователь, а группа администраторов к файлам доступа не получает. Данный параметр добавляет группу администраторов к общему ресурсу перемещаемого профиля пользователя. После чего этот профиль создается при следующем входе в систему, в указанном администратором месте, администраторы получают полный доступ к папкам пользователя.

Для того чтобы администраторы получили доступ к папкам пользователя:

1. Откройте узел **Конфигурация пользователя ⇒ Администра-**

тивные шаблоны ⇒ Система ⇒ Профили пользователей (User Configuration ⇒ Administrative Templates ⇒ System ⇒ User Profiles).

2. Дважды щелкните мышью по параметру **Добавляет группу безопасности «Администраторы» к перемещаемым профилям пользователя** (Add the Administrators security group to roaming user profiles). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Если параметр включен после создания профиля, он не будет влиять на ранее созданный профиль. Также параметр должен определиться на компьютере пользователя, но не на сервере, так как именно пользовательский компьютер задает разрешение доступа к ресурсам для перемещаемого профиля во время его создания.

По умолчанию администраторы не имеют доступа к файлам, расположенным в папках пользователя, однако имеют возможность стать владельцами этих папок и выдать разрешение на доступ к файлам.

Удаление неиспользуемых профилей

Если за компьютером работает много пользователей и у каждого существует свой профиль, то можно использовать параметр политики, позволяющий автоматически удалить неиспользуемый профиль в случае, если пользователь не использовал компьютер в течение определенного количества дней. Для того чтобы воспользоваться этой функцией, выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Профили пользователей** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ User Profiles).
2. Дважды щелкните мышью по параметру **Удалять при перезагрузке системы профили пользователей по истечении указанного числа дней** (Delete user profiles older than a specified number of days on system restart). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) укажите в счетчике количество дней, по истечении которых профиль считается неиспользуемым.
5. Нажмите кнопку **ОК**.

Одним днем считается 24 часа после получения доступа к конкретному профилю пользователя.

Отключение проверки разрешения на папку

По умолчанию, когда папка перемещаемых профилей пользователя существует и пользователь или группа администраторов не являются ее владельцами, система не копирует файлы в папку или из папки перемещаемых пользователей. Пользователю выводится сообщение об ошибке, а в журнал событий добавляется соответствующая запись. После чего используется кэшированный профиль или выдается временный профиль в случае отсутствия кэшированного.

Для того чтобы отключить проверку разрешения на папку, когда папка существует:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Профили пользователей** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ User Profiles).
2. Дважды щелкните мышью по параметру **Не проверять собственность пользователя перемещаемых папок профиля** (Do not check for user ownership of Roaming Profile Folders). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Удаление кэшированных копий перемещаемых профилей

Перемещаемые профили хранятся на сетевом сервере. И когда пользователи, использующие перемещаемый профиль, выходят из системы, выполняется сохранение этого профиля на локальном жестком диске используемого компьютера. Это делается на случай, если при следующем входе в систему сервер, на котором располагается перемещаемый профиль, будет не доступен. Копия на локальном компьютере используется также в том случае, если для загрузки перемещаемого профиля, расположенного на сервере, требуется длительное время. Если вы не нуждаетесь в локальных копиях профиля, то можете отключить эту функцию.

Для того чтобы отключить сохранение профиля:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Профили пользователей** (User

Configuration ⇒ Administrative Templates ⇒ System ⇒ User Profiles).

2. Дважды щелкните мышью по параметру **Удалять кэшированные копии перемещаемых пользователей** (Delete cached copies of roaming profiles). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Теперь все локальные копии перемещаемых профилей будут удаляться при выходе из системы. Сам перемещаемый профиль будет оставаться только на сетевом сервере.

Если используется медленное подключение, то не рекомендуется включать этот параметр, так как система в таком случае будет требовать наличие локальной копии перемещаемого профиля.

Принудительная выгрузка реестра при выходе из системы

По умолчанию система Windows всегда выгружает реестр пользователя при выходе его из системы, даже в том случае, когда остаются открытые дескрипторы к пользовательским разделам реестра. Используя этот параметр, можно запретить выгрузку реестра пользователя при выходе его из системы. Для этого выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Профили пользователей** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ User Profiles).
2. Дважды щелкните мышью по параметру **Не выполнять принудительной выгрузки реестра пользователя при его выходе из системы** (Do not forcefully unload the users registry at user logoff). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Теперь операционная система не будет принудительно выгружать реестр пользователя при выходе из системы, но будет это делать после закрытия дескрипторов к пользовательским разделам реестра.

Этот параметр используется в случае возникновения проблем совместимости приложений, не рекомендуется включать этот параметр по умолчанию, так как это может привести к проблемам получения пользователями обновленных версий их перемещаемых профилей.

5.6. Языковые стандарты

В этом разделе мы рассмотрим настройку параметров, расположенных в узле **Службы языковых стандартов** (Locale Services): запрет выбора пользовательских языковых стандартов, ограничение языковых стандартов, запрет изменения географического положения и запрет переопределения языкового стандарта.

Запрет выбора пользовательских языковых стандартов

Этот параметр позволяет запретить пользователю выбирать пользовательский языковой стандарт. Однако это ему не запрещает выбрать один из замещающих языковых стандартов, если они установлены. Для того чтобы включить параметр, выполните следующие шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Службы языковых стандартов** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Locale Services).
2. Дважды щелкните мышью по параметру **Запретить выбор пользовательских языковых стандартов** (Disallow selection of Custom Locates). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled). Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
4. Нажмите кнопку **ОК**.

Пользователь будет ограничен набором языковых стандартов, которые поставляются в комплектации операционной системы. Имейте в виду, что параметр не будет влиять на выбор замещающего языкового стандарта. Необходимо настроить права в каталоге %windir%\Globalization таким образом, чтобы пользователи без соответствующих прав доступа не могли устанавливать языковые стандарты.

Ограничение языковых стандартов

Этот параметр позволяет ограничивать выбор пользователя указанным списком языковых стандартов. Если этот список пуст, то пользовательские стандарты будут зафиксированы на текущих значениях. Этот параметр не изменяет существование значений языковых стандартов пользователей, од-

нако когда пользователь попытается изменить языковой стандарт, его выбор будет ограничен языковыми стандартами, указанными в списке параметра. Для того чтобы задать список языковых стандартов, выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Службы языковых стандартов** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Locale Services).
2. Дважды щелкните мышью по параметру **Ограничить пользовательские языковые стандарты** (Restrict user locates). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options), в поле ввода **Пользовательские языковые стандарты** (User Locales) введите список языковых стандартов. Список языковых стандартов задается названиями языков, названия разделяются точкой с запятой. Например, ru-RU означает Русский. Задав в списке «ru-RU;en-US», можно ограничить языковые стандарты пользователя русским (Россия) и английским (США) языками.
5. Нажмите кнопку **ОК**.

Аналогичным образом настраивается параметр **Ограничить системные языковые параметры** (Restrict system locales). В отличие от выше рассматриваемого параметра, этот параметр позволяет ограничивать допустимые системные языковые стандарты, указанные списком. Когда администратор в следующий раз попытается изменить системный языковой стандарт на компьютере, его выбор будет ограничен языковыми стандартами, которые указаны в списке.

Если параметр отключен или не задан, то пользователи смогут выбрать любой языковой стандарт по желанию, кроме случаев, когда активен параметр **Запретить выбор пользовательских языковых стандартов** (Disallow selection of Custom Locates).

Запрет изменения географического положения

Этот параметр позволяет запретить пользователями смену своего географического положения. Если этот параметр включен, пользователи не смогут изменять свое географическое положение. Для того чтобы включить параметр, выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Службы языковых стандартов** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Locale Services).
2. Дважды щелкните мышью по параметру **Запретить изменение географического положения** (Disallow changing of geographic location). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Если параметр отключен или не задан, то пользователи смогут изменять свое географическое положение по желанию.

Запрет переопределения параметров языкового стандарта

Для того чтобы пользователь не мог переопределять свой стандарт, изменяя отдельные параметры, выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Службы языковых стандартов** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Locale Services).
2. Дважды щелкните мышью по параметру **Не позволять пользователю переопределять параметры языкового стандарта** (Disallow user overdrive of locate settings). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Теперь пользователь не сможет настроить языковой стандарт пользовательскими переопределениями. Все изменения пользователем каких-либо параметров будут зафиксированы. Для удаления произведенных пользователем изменений необходимо восстановить параметры по умолчанию, а затем применить этот параметр.

5.7. Установка драйверов

В этом разделе описаны настройки, связанные с установкой драйверов: где искать драйвера устройств и каким пользователям разрешено устанавливать драйвера устройств.

Разрешение на установку драйверов пользователями

В операционных системах не ниже Windows Vista предусмотрена возможность задания списка кодов GUID класса установки устройств, описывающих драйверы устройств, которые могут быть установлены в этой системе членами группы «Пользователи». Эти драйверы должны быть подписаны согласно политике подписывания драйверов Windows или быть подписаны издателями, находящимися в хранилище доверенных издателей.

Для того чтобы перечислить классы установки устройств, настройте следующую политику:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Установка драйвера** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Driver Installation).
2. Дважды щелкните мышью по параметру **Разрешить пользователям, не являющимся администраторами, устанавливать драйвера для этих классов установки устройств** (Allow non-administrator users install this classes devices drivers). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) нажмите кнопку **Показать** (Show). Появится диалоговое окно **Вывод содержания** (Show Contents).
5. В появившемся диалоговом окне щелкните два раза по пустому полю и введите с клавиатуры GUID, представляющий класс установки устройств. Для того чтобы указать еще один глобальный уникальный идентификатор, нажмите клавишу **Enter**.
6. Нажмите кнопку **ОК**.

Если параметр отключен или не задан, то только администраторы смогут устанавливать драйвера устройств.

5.8. Установка устройств

В этом разделе мы рассмотрим параметры, связанные с установкой устройств: установка порядка поиска драйверов устройств, сколько системе будет отведено времени на установку устройств, возможность отключить уведомление об обнаружении нового устройства, настройку удаленного до-

ступа к Plug and Play и некоторые другие параметры.

Порядок поиска драйверов устройств

Для того чтобы указать системе порядок поиска драйверов устройств, выполните следующие шаги:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Установка устройства** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Device Installation).
2. Дважды щелкните мышью по параметру **Задать порядок поиска в исходных расположениях драйверов устройств** (Specify search order for device driver source locations). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Enable) в раскрывающемся списке **Выберите порядок поиска** (Select search order) выберите необходимый параметр:
   - **Искать в Центре обновления Windows в первую очередь** (Search Windows Update First) —поиск драйверов система будет выполнять в первую очередь в Центре обновления Windows.
   - **Искать в Центре обновления Windows в последнюю очередь** (Search Windows Update Last) —поиск драйверов система будет выполнять в последнюю очередь в Центре обновления Windows.
   - **Не искать в Центре обновления Windows** (Do not search Windows Update) — при поиске драйверов система не будет выполнять поиск в Центре обновления Windows.
5. Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
6. Нажмите кнопку **ОК**.

Если параметр отключен или не задан, указать порядок поиска драйвера устройств смогут только администраторы.

Настройка времени ожидания установки устройства

По умолчанию система выделяет на установку устройства 300 секунд (5 ми-

нут) — если за это время устройство не будет установлено, то система прекратит выполнение установки устройства. Для того чтобы изменить время ожидания установки, настройте следующий параметр:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Установка устройства** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Device Installation).
2. Дважды щелкните мышью по параметру **Настроить времени ожидания установки устройства** (Configure device installation time-out). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в поле **Время ожидания установки устройства** (Device Installation Timeout) введите количество секунд, которое система должна ожидать при установке устройства.
5. Нажмите кнопку **ОК**.

Если параметр отключен или не задан, то используется значение параметра по умолчанию, на завершение установки устройства отводится 300 секунд.

Отключение напоминания о новом оборудовании

По умолчанию во время установки драйвера появляется всплывающее уведомление **Найдено новое оборудование**. Для того чтобы отключить уведомление, активируйте следующий параметр:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Установка устройства** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Device Installation).
2. Дважды щелкните мышью по параметру **Отключить всплывающие напоминания «Найдено новое оборудование» во время установки драйвера** (Turn off “Found New Hardware” balloons during device installation). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Теперь во время установки драйвера уведомление об обнаружении нового устройства не будет отображаться.

Запрет отправки отчета об ошибках Windows

По умолчанию при установленном общем драйвере устройства система отправляет отчеты об ошибках Windows. Для того чтобы отключить отправку данных в таких случаях, активируйте следующий параметр:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Установка устройства** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Device Installation).
2. Дважды щелкните мышью по параметру **Не посылать отчет об ошибках Windows, если для устройства установлен общий драйвер** (Do not send a Windows error report when a generic driver is installed on a device). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Теперь при установленном общем драйвере отчет об ошибках Windows не будет отправляться.

Аналогичным способом настраивается параметр **Запретить Windows отправлять отчет об ошибках, если драйвер устройства запрашивает дополнительное программное обеспечение** (Prevent Windows from sending an error report when a device driver requests additional software during installation). По умолчанию система отправляет отчеты об ошибках при установке драйвера устройства, запрашивающего дополнительное программное обеспечение. Для того чтобы отключить отправку отчетов об ошибках в таком случае, достаточно включить параметр.

Если параметр отключен или не задан, то при нахождении ошибок в установке драйвера устройства Windows будет отправлять отчет об ошибках и запрашивать дополнительное программное обеспечение.

Запрет создания точек восстановления

По умолчанию перед установкой нового устройства система автоматически создает контрольную точку восстановления, что позволяет в случае неполадок с устройством откатить систему до того состояния, когда устройство не было установлено. Создание точек восстановления можно отключить:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Установка устройства** (Computer

Configuration ⇒ Administrative Templates ⇒ System ⇒ Device Installation).

2. Дважды щелкните мышью по параметру **Не создавать контрольную точку восстановления системы во время работы устройства, при которой, как правило, требуется создание точки восстановления** (Prevent creation of a system restore point during device activity that would normally prompt creation of a restore point). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Теперь во время установки драйвера точки восстановления системы не будут создаваться.

Настройка удаленного доступа Plug and Play

По умолчанию в операционной системе Windows удаленные подключения к самонастраивающимся устройствам запрещены. Чтобы разрешить удаленный доступ к интерфейсу таких устройств, активируйте следующий параметр:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Установка устройства** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Device Installation).
2. Дважды щелкните мышью по параметру **Разрешить удаленный доступ к устройствам Plug and Play** (Allow remote access to the Plug and Play interface). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

После этого будет разрешено удаленное подключение к самонастраивающимся устройствам.

Запрет получения метаданных устройств

По умолчанию в операционной системе разрешено получение метаданных устройств Windows из Интернета и определяется оно параметром в диалоговом окне **Параметры установки устройств** (Device Installation Settings).

Для того чтобы запретить получение метаданных устройств из Интернета, выполните следующие шаги:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Установка устройства** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Device Installation).
2. Дважды щелкните мышью по параметру **Запретить получение метаданных устройств из Интернета** (Prevent device metadata retrieval from the Internet). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Теперь получение метаданных устройств из Интернета будет невозможным.

Если параметр отключен или не задан, то получение метаданных устройств Windows из Интернета будет зависеть от того, какие настройки указаны в диалоговом окне **Параметры установки устройств** (Devise Installation Setting).

Ограничения на установку устройств

По умолчанию члены группы администраторов подчиняются всем параметрам политики, которые ограничивают установку устройств. Это не позволяет устанавливать и обновлять драйвера любых устройств, какими бы ни были параметры политики. Для того чтобы администраторы могли использовать возможности установки и обновления драйверов для любого устройства, следует выполнить следующие шаги:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Установка устройства ⇒ Ограничение на установку устройств** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Device Installation ⇒ Device Installation Restriction).
2. Дважды щелкните мышью по параметру **Разрешить администраторам заменять политики ограничения установки устройств** (Allow administrators to overdrive Device Installation Restriction policies). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Теперь члены группы **Администраторы** (Administrators) могут воспользоваться мастером добавления оборудования и мастером обновления драйверов для любых устройств.

Аналогично настраивается параметр **Запретить установку съемных устройств** (Prevent installation of removable drivers), который позволяет запретить установку съемных устройств. Параметр **Запретить установку устройств, не описанных другими параметрами политики** (Prevent installation of devices not described by other policy settings) позволяет запретить системе установку и обновление драйверов устройств, не указанных в параметрах политики **Разрешить установку устройств, соответствующих какому-либо из этих кодов устройств** (Allow installation of devices that match any of these device IDs) (об этом параметре мы расскажем ниже).

Если параметр **Запретить установку съемных устройств** (Prevent installation of removable drivers) отключен или не задан, то для съемных устройств драйвера можно устанавливать только для новых устройств, для уже существующих — обновлять. Однако другие параметры политики могут помешать этому.

Для того чтобы указать список кодов глобальных уникальных идентификаторов (GUID) класса установки устройств для драйверов устройств, которые можно установить в системе, выполните следующие действия:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Установка устройства ⇒ Ограничение на установку устройств** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Device Installation ⇒ Device Installation Restriction).
2. Дважды щелкните мышью по параметру **Разрешить установку устройств с использованием драйверов, соответствующих этим классам установки устройств** (Allow installation of devices using driver that match these device setup classes). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) нажмите кнопку **Показать** (Show). Появится диалоговое окно **Вывод содержания** (Show Contents).
5. В появившемся диалоговом окне щелкните два раза по пустому полю и введите с клавиатуры GUID, представляющий класс установки устройств. Для того чтобы указать еще один глобальный уникальный идентификатор, нажмите клавишу **Enter**.
6. Нажмите кнопку **ОК**, чтобы закрыть диалоговые окна.

После этого система может устанавливать и обновлять драйвера тех устройств, чьи GUID класса установки устройств были указаны в списке параметра. Если какой-нибудь другой параметр политики мешает установке устройства, то драйвера не будут устанавливаться и обновляться для него, независимо, в списке GUID его класса установки или нет.

Аналогичным образом настраиваются параметры **Запретить установку устройств с использованием драйверов, соответствующих этим классам установки устройств** (Prevent installation of devices using drivers that match these device setup classes) и **Запретить установку устройств с указанными кодами устройств** (Prevent installation of devices that match any of these device IDs), с той разницей, что в списке, расположенном в диалоговом окне **Вывод содержания** (Show Contents), указываются GUID тех классов установки устройств, для которых необходимо запретить установку и обновление драйверов устройств. Также в этом параметре, в области **Параметры** (Options) можно установить флажок **Также применить для соответствующих устройств, которые уже были установлены** (Also apply to matching devices that are already installed), при установке которого будет возможным запретить обновление уже установленных драйверов.

В случае если была предпринята попытка установки драйверов для тех устройств, установка драйверов для которых была запрещена параметрами политики, появляется сообщение, уведомляющее пользователя о невозможности установки драйвера устройства. Для того чтобы изменить выводимое сообщение на свое собственное, настройте следующую политику:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Установка устройства ⇒ Ограничение на установку устройств** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Device Installation ⇒ Device Installation Restriction).
2. Дважды щелкните мышью по параметру **Отображать специальное сообщение, когда установка запрещена параметром политики** (Display a custom message when installation is prevented by a policy setting). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в поле ввода **Уточняющий текст** (Detail Text) введите текст, который будут видеть пользователи при попытке установить драйвер для устройства, для которого запрещено устанавливать драйвера устройств. Длина текста не должна превышать 128 символов.

5. Нажмите кнопку **ОК**.

Сообщение также появляется при попытке установить устройство, запрещенное к установке параметрами политики. Однако за это сообщение отвечает другой параметр — **Отображать заголовок специального сообщения, когда установка устройств запрещена параметром политики** (Display a custom message title when device installation is prevented by a policy setting). Текст вводится с клавиатуры в поле ввода **Основной текст** (Main Text), которое расположено в области **Параметры** (Options). Текст не должен превышать 63 символов.

Также существует возможность установить время ожидания системы до перезагрузки с целью принудительного изменения в политиках ограничения установки устройств. Для того чтобы установить время, настройте следующую политику:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Установка устройства ⇒ Ограничение на установку устройств** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Device Installation ⇒ Device Installation Restriction).
2. Дважды щелкните мышью по параметру **Время (сек.) до принудительной перезагрузки при необходимости введения параметров политики в действие** (Time (in seconds) to force reboot when required for policy changes to take effect). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в поле **Время ожидания до перезагрузки** (Reboot Timeout) укажите количество секунд, ожидаемых системой до перезагрузки.
5. Нажмите кнопку **ОК**.

Если принудительная перезагрузка не выполняется, то право ограничения установки устройств не вступит в силу до перезапуска системы.

5.9. Параметры связи через Интернет

В этом разделе мы рассмотрим параметры, расположенные в узле **Управление связью через Интернет** (Internet Communications settings). Здесь располагается большое количество настроек, как-либо связанных с использованием Интернета, начиная от отправки отчетов об ошибках Windows и заканчивая отключением рейтинга справочной информации.

Справка и поддержка

По умолчанию пользователи могут выставлять рейтинги для справочной системы. Рейтинг справочной системы предназначен как элемент обратной связи для оценки качества и пользы представленной справочной информации пользователю. Возможно отключение оценки справочной информации. Для того чтобы это сделать, активируйте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Управление связью через Интернет ⇒ Параметры связи через Интернет** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Internet Communication Management ⇒ Internet Communications settings).
2. Дважды щелкните мышью по параметру **Отключение рейтинга справки** (Turn off Help Ratings). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled). Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
4. Нажмите кнопку **ОК**.

Теперь оценка справочной информации будет недоступна.

Также можно запретить пользователю участвовать в программе по улучшению справочной информации, для чего включите параметр **Отключение программы улучшения справки** (Turn off Help Experience Improvement Program).

Пользователи, которые имеют доступ в Интернет, могут просматривать справочную информацию из Интернета, используя центр справки и поддержки Windows. Это позволяет Microsoft информировать пользователя самыми последними вариантами справочной информации. Однако если включить параметр **Отключение «Windows в Интернете»** (Turn off Windows Online), пользователи не смогут получить доступ к обновленной справочной информации.

Пользователи, которые работают с планшетными компьютерами, имеют возможность автоматической отправки отчетов об ошибках распознавания рукописного текста. В случае возникновения проблем с распознаванием текста немедленно создается отчет, который отправляется в корпорацию Microsoft. Корпорация Microsoft, анализируя полученные отчеты, дорабатывает средство распознавания текста и исправляет недоработки. Если включить параметр **Отключить отчеты об ошибках распознавания рукописного тек-**

ста (Turn off handwriting recognition error reporting), то пользователи не смогут воспользоваться средством составления отчетов и естественно в корпорацию Microsoft ничего отправлено не будет.

По умолчанию операционная система собирает анонимную информацию об использовании программного обеспечения и службы Windows Messenger. Полученная информация используется корпорацией Microsoft в целях улучшения продукта и усовершенствования новых версий. Сбор анонимной информации можно отключить, для чего стоит включить параметр **Отключить участие в программе улучшения поддержки пользователей Windows Messenger** (Turn off the Windows Messenger Customer Experience Improvement Program).

Печать по протоколу HTTP

В операционной системе Windows имеется возможность выбора режима печати через Интернет, используя протокол HTTP. Согласно ей, вы можете распечатывать документы на принтерах, расположенных в интрасети или в сети Интернет. Эту возможность можно отключить:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Управление связью через Интернет ⇒ Параметры связи через Интернет** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Internet Communication Management ⇒ Internet Communications settings).
2. Дважды щелкните мышью по параметру **Отключить печать по протоколу HTTP** (Turn off printing over HTTP). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

После чего пользователю будет закрыт доступ печати по протоколу HTTP.

Также имеется возможности отключения загрузки драйверов принтера, работающего по протоколу HTTP, без которых невозможна печать на принтере. Для того чтобы отключить возможность загрузки драйверов, включите параметр **Отключение загрузки драйверов принтера по протоколу HTTP** (Turn off downloading of print drives over HTTP). Включение параметра только запрещает загрузку специальных драйверов, но никак не влияет на распечатку текста на этих принтерах. Также этот запрет не распространяется на установленные локальные драйверы.

Сопоставление файлов

Если в операционной системе Windows попытаться открыть файл с незарегистрированным расширением, то появится диалоговое окно выбора способа сопоставления неизвестного расширения с приложением. На выбор два варианта:

- **Поиск соответствия в Интернете** (Use the Web service to find the correct program) — использование интернет-сервиса сопоставления расширения с приложением.
- **Выбор программы из списка установленных программ** (Select a program from a list of installed programs) — выбор одной из установленных на компьютере программ, в котором откроется текущий файл, а также в котором будут открываться другие файлы того же расширения.

Чтобы это диалоговое окно не появлялось, а сразу открывалось диалоговое окно выбора установленной программы, выполните следующие шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Управление связью через Интернет ⇒ Параметры связи через Интернет** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Internet Communication Management ⇒ Internet Communications settings).
2. Дважды щелкните мышью по параметру **Отключить службу сопоставления файлов Интернета** (Turn off Internet File Association service). Откроется диалоговое окно редактирования параметра политики.

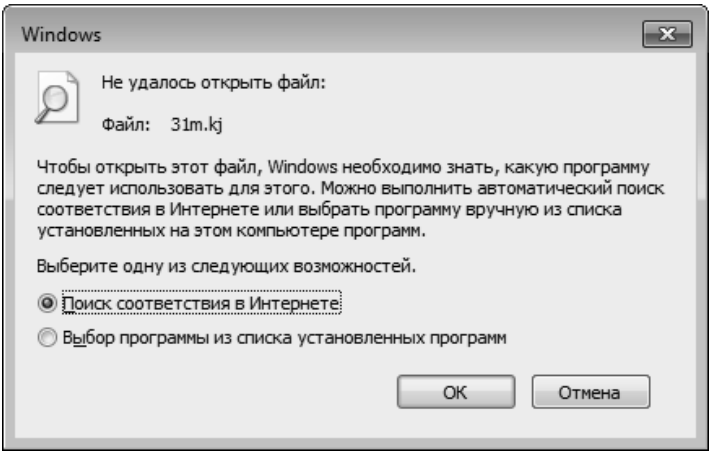


Рис. 5.7. ***Диалоговое окно сопоставления файла***

3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

После чего диалоговое окно выбора способа сопоставления, показанное на рис. 5.7, больше не будет отвлекать вас.

Веб-публикации

Операционная система Windows загружает и обновляет список поставщиков, выполняющих запросы на веб-публикацию и заказы отпечатков. Используя этот список, можно выбрать одну из предоставленных компаний и воспользоваться предоставляемыми ими услугами: хранение информации или распечатка фотографий. Возможно отключение загрузки списка поставщиков. Для этого выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Управление связью через Интернет ⇒ Параметры связи через Интернет** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Internet Communication Management ⇒ Internet Communications settings).
2. Дважды щелкните мышью по параметру **Отключить загрузку из Интернета для мастеров веб-публикаций и заказа отпечатков** (Turn off Internet download for Web publishing and online ordering wizards). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Новые поставщики не будут загружены в список поставщиков, однако это не значит, что загруженные ранее поставщики не будут отображаться.

Для того чтобы полностью отключить возможность заказа отпечатков через Интернет, включите параметр **Отключить заказ отпечатков через Интернет в списке задач для изображений** (Turn off the "Publish to web" picture task). После чего в списке задач для изображений будет скрыта эта возможность. Возможно скрытие пунктов **Опубликовать в вебе**, **Опубликовать эту папку в вебе** и **Опубликовать выделенные объекты в вебе** среди задач для файлов и папок в окне проводника Windows. Для этого активируйте параметр **Отключить веб-публикацию в списке задач для файлов и папок** (Turn off the "Publish to Web" task for files and folders).

Если параметр отключен, то образцы рукописного ввода будут отсылаться в корпорацию Microsoft автоматически, если параметр не задан, то пользователи могут включать и отключать отправку образцов самостоятельно.

Отключение автоматического обновления корневых сертификатов

По умолчанию сертификаты используются для безопасного подключения к сайту или при работе с электронной почтой. Сертификаты может выдать любой издатель, но для получения максимальной гарантии безопасности сертификат должен выдаваться доверенным центром сертификации. В комплектацию операционной системы уже включен список доверенных центров. По умолчанию при получении сертификата, выданного неизвестным центром, выполняется подключение к сайту Центра обновления Windows, для того чтобы проверить наличие издателя в списке доверенных центров сертификации Microsoft. Для того чтобы заблокировать подключение к сайту, активируйте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Управление связью через Интернет ⇒ Параметры связи через Интернет** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Internet Communication Management ⇒ Internet Communications settings).
2. Дважды щелкните мышью по параметру **Выключить автоматическое обновление корневых сертификатов** (Turn off Automatic Root Certificates Update). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Теперь при получении сертификата, выданного неизвестным центром, не будет выполняться подключение к сайту Центра обновления Windows.

Отключение ссылок просмотра событий «Events.asp»

Средство просмотра событий преобразует все http-адреса в активные ссылки, при щелчке мышью по которым запускается веб-браузер. Если событие создано компонентом Microsoft, то в конце текста описания будет располагаться ссылка «Дополнительные сведения», после щелчка по которой в корпорацию Microsoft отправляются данные о событии и пользователю выводится описание причин возникновения события.

Чтобы отключить размещение ссылки «Дополнительные сведения», активируйте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Управление связью через Интернет ⇒ Па-**

раметры связи через Интернет (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Internet Communication Management ⇒ Internet Communications settings).

2. Дважды щелкните мышью по параметру **Отключить ссылки просмотра событий «Events.asp»** (Turn off Event Viewer "Events.asp" links). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Теперь в конце описания не будет появляться сообщение «Дополнительные сведения», а URL-адреса описания будут неактивными.

Запрет обновления справочной системы через Интернет

В Центре справки и поддержки есть динамически обновляемый раздел «Знаете ли Вы?». При активном подключении к Интернету Центр справки и поддержки предоставляет пользователю актуальные на текущий момент сведения об операционной системе Windows и самом компьютере. Если у вас отсутствует подключение к Интернету или вы просто не хотите получать актуальную информацию, то вы можете отключить обновление этого раздела.

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Управление связью через Интернет ⇒ Параметры связи через Интернет** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Internet Communication Management ⇒ Internet Communications settings).
2. Дважды щелкните мышью по параметру **Отключение центра справки и поддержки «Знаете ли вы?»** (Turn off Help and Supports Center "Did you know?"). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled). Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
4. Нажмите кнопку **ОК**.

После активации данной политики справочная система Windows будет работать в автономном режиме и ее содержимое не будет обновляться.

Отключение поиска в базе знаний Microsoft

База знаний Microsoft представляет собой источник справочной информации, технической поддержки и средств диагностики для продуктов корпорации. Пользователи могут выполнять поиск в базе знаний Microsoft прямо в окне приложения Центр справки и поддержки при наличии интернет-соединения. При отсутствии интернет-соединения возможность поиска в базе знаний Microsoft можно отключить. Для того чтобы это сделать, выполните следующие шаги:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Управление связью через Интернет ⇒ Параметры связи через Интернет** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Internet Communication Management ⇒ Internet Communications settings).
2. Дважды щелкните мышью по параметру **Отключить поиск в базе знаний Майкрософт в окне «Центр справки и поддержки»** (Turn off Help and Support Center Microsoft Knowledge Base search). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

После чего поиск будет выполняться в содержимом встроенной справки.

Если параметр отключен или не задан, то поиск в базе знаний Microsoft будет выполняться при условии, что есть доступ в Интернет и поиск в базе знаний не отключен на странице настройки параметров поиска.

Отключение отчетов об ошибках Windows

При возникновении ошибки в работе приложения или системы, их зависания в корпорацию Microsoft отправляется отчет об ошибках. Корпорация использует эти отчеты для улучшения качества программных продуктов. Имеется возможность отключения отправки отчетов и уведомления пользователя об ошибках. Для этого выполните следующие действия:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Управление связью через Интернет ⇒ Параметры связи через Интернет** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Internet Communication Management ⇒ Internet Communications settings).
2. Дважды щелкните мышью по параметру **Отключить отчеты об**

ошибках Windows (Turn off Windows Error Reports). Откроется диалоговое окно редактирования параметра политики.

3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Включенный параметр делает невозможным отправку отчетов об ошибках Windows в корпорацию Microsoft.

Блокировка доступа к возможностям Центра обновления Windows

По умолчанию пользователи получают доступ к Центру обновления Windows, а также получают уведомления и критические обновления через службу автоматического обновления Windows. Если вы не хотите использовать автоматическое обновление системы, то можете отключить его. Для этого активируйте следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Управление связью через Интернет ⇒ Параметры связи через Интернет** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Internet Communication Management ⇒ Internet Communications settings).
2. Дважды щелкните мышью по параметру **Отключить доступ ко всем возможностям Центра обновления Windows** (Turn off access to all Windows Update features). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

После чего будут осуществлены следующие ограничения:

- Заблокирован доступ к сайту Центра обновления Windows.
- Отключена функция автоматического обновления Windows.
- Отключены уведомления о доступности критических обновлений.
- Запрещена автоматическая установка обновлений драйверов.

Если параметр отключен или не задан, то пользователи получат доступ к Центру обновления Windows, будет включено автоматическое обновление системы и драйверов устройств, будет включены уведомления о доступности критических обновлений.

Отключение Помощника по поиску

Когда пользователь ищет информацию на локальном компьютере или в Интернете, «Помощник по поиску» периодически подключается к серверу Microsoft , чтобы загрузить обновления политики конфиденциальности и дополнительных информационных файлов, которые используются для форматирования и отображения результатов. По умолчанию загружаются обновления содержимого для всех случаев, кроме классического поиска. Но обновления можно отключить полностью. Для этого следует активировать следующий параметр:

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Система ⇒ Управление связью через Интернет ⇒ Параметры связи через Интернет** (User Configuration ⇒ Administrative Templates ⇒ System ⇒ Internet Communication Management ⇒ Internet Communications settings).
2. Дважды щелкните мышью по параметру **Отключить обновление информационных файлов «Помощника по поиску»** (Turn off Search Companion content file updates). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

После активации данной политики «Помощник по поиску» не будет загружать обновления содержимого во время выполнения поиска. Однако при поиске в Интернете искомый текст и сведения о поставщике услуг поиска будут отправляться в корпорацию Microsoft.

5.10. Настройка функций диагностики

Здесь мы рассмотрим способы изменения параметров диагностики жестких дисков, сценариев, поврежденных системных файлов и файлов MSI, диагностики совместимости приложений и утечки памяти Windows, а также диагностики службы технической поддержки Windows.

Параметры обработки сценариев

По умолчанию служба DPS удаляет данные сценария после того, как их объем превысит 256 МБ. Для того чтобы изменить максимальный объем сохранения данных сценария службы диагностики, настройте следующую политику:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Troubleshooting and Diagnostics).
2. Дважды щелкните мышью по параметру **Диагностика: настройка сохранения сценария** (Diagnostics: Configure scenario retention). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в поле **Максимальный объем данных сценария** (Scenario data size limit) укажите максимальный размер в мегабайтах.
5. Нажмите кнопку **ОК**.

После этого данные сценариев диагностики будут сохраняться до тех пор, пока не будет достигнут указанный предел. Сам параметр вступит в силу только в том случае, если запущена служба DPS, если же служба DPS отключена, то никаких удалений данных сценария диагностики произведено не будет.

А для того чтобы выбрать уровень выполнения сценария, настройте следующую политику:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Troubleshooting and Diagnostics).
2. Дважды щелкните мышью по параметру **Диагностика: настройка уровня выполнения сценария** (Diagnostics: Configure scenario retention). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в раскрывающемся списке **Уровень выполнения сценария** (Scenario Execution Level) выберите необходимый уровень:
   - **Только обнаружение и диагностика** (Detection and Troubleshooting Only) — служба DPS будет обнаруживать проблемы и пытаться определить их причины. Если причины будут найдены, то они будут записаны в журнал событий, однако никаких действий по устранению проблем выполнено не будет.

- **Обнаружение, диагностика и решение проблем** (Detection, Troubleshooting and Resolution) — служба DPS будет обнаруживать проблемы и пытаться устранить их либо уведомит пользователя о том, что существует решение устранения проблемы.

5. Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
6. Нажмите кнопку **ОК**.

Как и предыдущий параметр, этот параметр вступает в силу только в том случае, если включена служба DPS.

Если параметр отключен, то система не сможет обнаруживать, диагностировать и решать проблемы, обрабатываемые службой DPS. Если параметр не задан, то служба DPS присвоит всем сценариям значение **Обнаружение, диагностика и решение проблем** (Detection, Troubleshooting and Resolution), если не заданы другие параметры для отдельных сценариев.

Параметры восстановления поврежденных файлов

Для того чтобы настроить поведение при восстановлении поврежденных системных файлов, следует настроить следующую политику:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика ⇒ Восстановление поврежденного файла** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Troubleshooting and Diagnostics ⇒ Corrupted file recovery).
2. Дважды щелкните мышью по параметру **Настройка поведения восстановления поврежденного файла** (Configure Corrupted File Recovery Behavior). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в раскрывающемся списке **Уровень выполнения сценария** (Scenario Execution Level) выберите необходимый уровень:

   - **Обычное** (Regular) — обнаружение, устранение неполадок и восстановление поврежденных файлов с автоматическим запуском минимального интерфейса пользователя. Если необходима перезагрузка Windows, то появится соответствующее диалоговое окно. Это поведение является поведением по умолчанию.

- **Только выявление неполадок** (Troubleshooting Only) — обнаружение поврежденных файлов и выявление неполадок с автоматическим запуском без интерфейса пользователя. В данном поведении автоматическое восстановление выполняться не будет, если восстановление возможно, то система запишет в журнал событий необходимые данные.
- **Без уведомления** (Silent) — обнаружение, устранение неполадок и восстановление поврежденных файлов с автоматическим запуском без интерфейса пользователя. При необходимости перезагрузки система запишет об этом в журнал событий.

5. Нажмите кнопку **ОК**.

Примечание. Этот параметр вступит в силу только в том случае, если включена служба политики диагностики DPS. Если служба DPS отключена, то восстановление поврежденных файлов выполняться не будет.

Если параметр отключен, то восстановление поврежденных файлов выполняться не будет, если параметр не задан, то восстановление поврежденных файлов будет выполняться на уровне выполнения сценария **Обычный** (Regular).

Параметры восстановления поврежденного файла MSI

Эта политика позволяет выбрать способ поведения при восстановлении поврежденных установочных файлов MSI. Для управления ею выполните следующие действия:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика ⇒ Восстановление поврежденного файла MSI** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Troubleshooting and Diagnostics ⇒ MSI Corrupted File Recovery).

2. Дважды щелкните мышью по параметру **Настройка поведения восстановления поврежденного файла MSI** (Configure MSI Corrupted File Recovery Behavior). Откроется диалоговое окно редактирования параметра политики.

3. Установите переключатель в положение **Включить** (Enabled).

4. В области **Параметры** (Options) в раскрывающемся списке **Уровень выполнения сценария** (Scenario Execution Level) выберите необходимый уровень:

   - **Запрос устранения** (Prompt for Resolution) — обнаружение, выявление неполадок и восстановление поврежденных приложений MSI. При возникновении необходимости в повторной установке приложения система выведет для пользователя соответствующее диалоговое окно. Это поведение является поведением по умолчанию.

   - **Только выявление неполадок** (Troubleshooting Only) — обнаружение и проверка повреждения файла будут выполнены без пользовательского интерфейса. Попытка восстановления не предпринимается.

   - **Без уведомления** (Silent) — обнаружение, устранение неполадок и уведомление приложения MSI о повторной установке будут выполняться без пользовательского интерфейса. При обнаружении повреждения система зарегистрирует событие и предложит повторно запустить приложение. Используется при работе без монитора и является поведением по умолчанию сервера Windows при восстановлении.

5. Нажмите кнопку **ОК**.

Если параметр отключен, то будет отключено устранение неполадок и поведение при восстановлении для поврежденных файлов. Если параметр не задан, то значение поведения при восстановлении поврежденных файлов будет по умолчанию — **Запрос устранения** (Prompt for Resolution).

Параметры диагностики совместимости приложений

По умолчанию помощник по совместимости программ уведомляет пользователя о блокировке драйвера в случае его несовместимости, а также предлагает найти решение на сайте Microsoft. Чтобы проводилась диагностика драйверов, которые были заблокированы по причине проблем с совместимостью, активируйте следующий параметр:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика ⇒ Диагностика совместимости приложений** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Troubleshooting and Diagnostics ⇒ Application Compatibility Diagnostics).
2. Дважды щелкните мышью по параметру **Уведомлять о блокированных драйверах** (Notify blocked drivers). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled). Нажмите кнопку **ОК**.

Если же параметр отключен, то при блокировке драйвера пользователь не будет уведомлен об этом, и предложение проверить наличие решения на сайте Microsoft не поступит.

> **Примечание.** Чтобы параметр был задействован, необходимо, чтобы была запущена служба политики диагностики (DPS) и служба помощника по совместимости программ.

Бывает, что приложение установки не может запуститься или корректно работать в операционной системе Windows по той причине, что приложение создавалось для другой версии системы, как правило, ниже текущей. По умолчанию помощник совместимости программ обнаруживает сбои в процессе установки приложений. Вы можете управлять данной функцией, включив или отключив обнаружение сбоев установки приложений:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика ⇒ Диагностика совместимости приложений** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Troubleshooting and Diagnostics ⇒ Application Compatibility Diagnostics).
2. Дважды щелкните мышью по параметру **Обнаружение сбоев установки приложений** (Detect application install failures). Откроется диалоговое окно редактирования параметра политики.

3. Установите переключатель в положение **Включить** (Enabled) или **Отключить** (Disabled).
4. Нажмите кнопку **ОК**.

> **Примечание.** Данный параметр не будет иметь значения, если отключен Помощник по совместимости программ. Кроме того, должны быть запущены служба политики диагностики (DPS) и служба помощника по совместимости программ.

При включенном или незаданном параметре помощник совместимости приложений при обнаружении сбоя в процессе установки приложений предложит пользователю перезапустить программу установки в режиме совместимости с операционной системой Microsoft Windows XP.

Вы можете управлять средством обнаружения сбоев приложений, вызванных устаревшими COM-библиотеками:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика ⇒ Диагностика совместимости приложений** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Troubleshooting and Diagnostics ⇒ Application Compatibility Diagnostics).
2. Дважды щелкните мышью по параметру **Обнаруживать сбои приложений, вызванных устаревшими библиотеками** (Detect application failures caused by deprecated COM objects). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в раскрывающемся списке **Уровень выполнения сценария** (Scenario Execution Level) выберите:
   - **Обнаружение, диагностика и решение** (Detection, Troubleshooting and Resolution) — при обнаружении сбоя Помощник по совместимости программ уведомит пользователя о найденном сбое и предложит проверить решения на сайте корпорации Microsoft.
   - **Только обнаружение и диагностика** (Detection and Troubleshooting Only) —Помощником по совместимости программ будут обнаруживаться сбои, однако ничего не будет предпринято по поводу решения сбоев.
5. Нажмите кнопку **ОК**.

После включения параметра Помощник по совместимости программ будет обнаруживать сбои, вызванные в результате создания устаревших COM-объектов.

Аналогичным образом настраиваются остальные параметры в узле **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика ⇒ Диагностика совместимости приложений** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Troubleshooting and Diagnostics ⇒ Application Compatibility Diagnostics).

После включения параметра **Обнаружение сбоев приложений, вызванных устаревшими библиотеками DLL Windows** (Detect application failures caused by deprecated Windows DLLs), Помощник по совместимости программ будет производить диагностику сбоев программ, которые возникают при загрузке библиотек DLL.

После включения параметра **Обнаружение средств установки приложений, требующих прав администратора** (Detect application installers that need to be run as administrator), Помощник по совместимости программ будет обнаруживать сбои программ установки приложений, для которых контролем учетных записей пользователей не было дано разрешения на запуск с правами администратора. При обнаружении сбоя Помощник по совместимости предложит перезапустить программу установки с использованием прав администратора.

После включения параметра **Обнаружение приложений, неспособных запустить средства установки при включенном контроле учетных записей пользователей (UAC)** (Detect applications unable to launch installers under UAC), Помощник по совместимости программ будет обнаруживать сбои программ, которые возникают в результате попыток запуска дочерних процессов, какими являются программы установки (например, программы установки обновлений). При обнаружении подобного сбоя Помощник по совместимости программ включит режим совместимости, который позволяет программе запустить средство установки таким образом, будто оно имеет права администратора.

Все эти параметры будут задействованы только в том случае, если включена служба политики диагностики (DPS) и служба Помощника по совместимости программ.

Параметры диагностики утечки памяти Windows

Для управления диагностикой проблем утечки памяти Windows (если параметр не задан, служба диагностики функционирует):

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика ⇒ Диагностика утечки памяти Windows** (Computer Configuration ⇒ Administrative Templates ⇒

System ⇒ Troubleshooting and Diagnostics ⇒ Windows Memory Leak Diagnosis).

2. Дважды щелкните мышью по параметру **Настройка уровня выполнения сценария** (Configure Scenario Execution Level). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled) или **Отключить** (Disabled). Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
4. Нажмите кнопку **ОК**.

После этого служба политики диагностики DPS сможет диагностировать проблемы, связанные с утечкой памяти. Если этот параметр отключен, то служба DPS не сможет диагностировать эти проблемы. Этот параметр будет задействован лишь в том случае, если запущена служба политики диагностики.

Управление запланированным обслуживанием

Для того чтобы использовать возможность выполнения запланированной диагностики для обнаружения и решения проблем системы, настройте следующую политику:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика ⇒ Запланированное обслуживание** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Troubleshooting and Diagnostics ⇒ Scheduled Maintenance).
2. Дважды щелкните мышью по параметру **Настроить поведение при запланированном обслуживании** (Configure Scheduled Maintenance Behavior). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled). Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
4. В области **Параметры** (Options) в раскрывающемся списке **Уровень выполнения** (Execution Level) выберите необходимый вариант выполнения проверки:
   - **Обычный** (Regular) — система будет периодически выявлять неполадки и уведомлять пользователя при обнаружении проблем. Пользователь сам будет решать проблему.

- **Только выявление неполадок** (Troubleshooting Only) — система будет выявлять неполадки, а также устранять часть найденных неполадок без требования вмешательства пользователя.

5. Нажмите кнопку **ОК**.

Если этот параметр политики не задан, приоритетом будут обладать локальные предпочтения выявления неполадок, настроенные в панели управления. Если никакие локальные предпочтения выявления неполадок не заданы, для обнаружения, выявления неполадок и их устранения по умолчанию включается запланированная диагностика.

Управление механизмом отказоустойчивой кучи

Механизм работы отказоустойчивой кучи заключается в том, что при повреждении выделенной памяти система будет автоматически отмечать процесс, который вызвал ошибку. При повторной ошибке в течение двух часов операционная система применит заплатку совместимости на этот процесс. Вы можете разрешить или запретить работу данного механизма:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика ⇒ Отказоустойчивая куча** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Troubleshooting and Diagnostics ⇒ Fault Tolerant Heap).
2. Дважды щелкните мышью по параметру **Настройка уровня выполнения сценария** (Configure Scenario Execution Level). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

После этого служба политики диагностики (DPS) сможет обнаруживать и пытаться автоматически устранить неполадки, связанные с повреждением кучи. Если параметр не задан, то механизм отказоустойчивой кучи функционирует.

Управление средством диагностики службы технической поддержки

Вы можете разрешить пользователям пользоваться средством диагностики службы технической поддержки Microsoft для сбора данных диагностики и их последующей передачи специалистам службы поддержки с целью решить проблему:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика ⇒ Средство диагностики службы технической поддержки Майкрософт** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Troubleshooting and Diagnostics ⇒ Microsoft Support Diagnostic Tool).
2. Дважды щелкните мышью по параметру **Средство диагностики службы технической поддержки Майкрософт (MSDT): включите интерактивное взаимодействие с поставщиком поддержки** (Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with Support Provider). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

По умолчанию поставщиком поддержки является корпорация Microsoft.

Если параметр политики отключен, то средство диагностики службы технической поддержки Microsoft не сможет выполняться в режиме поддержки, а это значит, что никакие данные не будут ни собираться, ни отправляться.

В некоторых случаях для решения проблем средство диагностики службы технической поддержки Microsoft может запросить у пользователя разрешение на загрузку дополнительных средств диагностики. Это необходимо для полного устранения возникших проблем. Чтобы ограничить загрузку дополнительных средств, выполните следующие действия:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика ⇒ Средство диагностики службы технической поддержки Майкрософт** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Troubleshooting and Diagnostics ⇒ Microsoft Support Diagnostic Tool).
2. Дважды щелкните мышью по параметру **Средство диагностики службы технической поддержки Майкрософт: ограничить загрузку служебных средств** (Microsoft Support Diagnostic Tool: Restrict tool download). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options) в раскрывающемся списке **Загрузка инструментальных средств разрешена** (Tool downloads allowed) выберите вариант ограничения загрузки дополнительных средств:
   - **Локальное и удаленное устранение неполадок** (Local and re-

mote troubleshooting) — средство диагностики службы технической поддержки Microsoft будет запрашивать разрешение на загрузку дополнительных средств.

- **Только удаленное устранение неполадок** (Remote troubleshooting only) — средство диагностики службы технической поддержки Microsoft будет запрашивать у пользователя разрешение на загрузку дополнительных средств для диагностики проблемы только на удаленных компьютерах.

5. Нажмите кнопку **ОК**.

Если параметр политики отключить, то средство диагностики службы технической поддержки Microsoft не сможет загружать дополнительные средства и производить диагностику проблем на удаленных компьютерах.

А для того чтобы пользователи могли использовать средство диагностики службы технической поддержки Microsoft для сбора данных диагностики и их передачи специалистам службы Microsoft, активируйте следующий параметр:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Диагностика ⇒ Средство диагностики службы технической поддержки Майкрософт** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Troubleshooting and Diagnostics ⇒ Microsoft Support Diagnostic Tool).
2. Дважды щелкните мышью по параметру **Средство диагностики службы технической поддержки Майкрософт: настройка режима работы** (Microsoft Support Diagnostic Tool: Configure execution level). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Если параметр политики отключен, то средство диагностики службы технической поддержки Microsoft не сможет собирать данные диагностики. Если же параметр не задан — средство диагностики включено.

5.11. Управление электропитанием

В этом разделе мы рассмотрим параметры, связанные с управлением электропитанием, такими как: запрос пароля при выходе из энергосберегающего режима, выбор схемы управления питанием, настройки уведомлений об энергосбережении (например, низкой зарядке батарей), параметры электро-

питания жесткого диска, действия при нажатии кнопок, отвечающих за питание, и некоторые другие параметры.

Выбор схемы управления питанием

С помощью этого параметра можно указать, какую схему управления питанием необходимо использовать и при этом запретить пользователям изменять ее:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Управление электропитанием** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Power Management).
2. Дважды щелкните мышью по параметру **Выберите текущую схему управления питанием** (Select an Active Power Plan). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options), в раскрывающемся списке **Текущая схема управления питанием** (Active Power Plan), выберите режим управления питанием:
   - **Автоматический** (Automatic) — полная оптимизация управления питанием. При необходимости обеспечивает максимальное быстродействие, при отсутствии активности экономит энергию.
   - **Высокая производительность** (High Performance) — увеличивает производительность и скорость отклика системы. При работе с переносными компьютерами аккумуляторная батарея разряжается наиболее быстро.
   - **Режим экономии энергии** (Power Saver) — экономит энергию за счет снижения быстродействия системы. Схема полезна для пользователей переносных компьютеров, так как позволяет дольше сохранять заряд батареи.
5. Нажмите кнопку **ОК**.

Для того чтобы указать настраиваемую схему управления питанием, используйте параметр **Настраиваемая текущая схема управления питанием** (Specify a Custom Active Power Plan). Здесь выбирается текущая схема управления питанием согласно указанному GUID-идентификатору схемы управления питанием. Загрузить идентификатор GUID настраиваемой схемы управления питанием можно при помощи команды `powercfg`, введенной в командной строке (рис. 5.8).

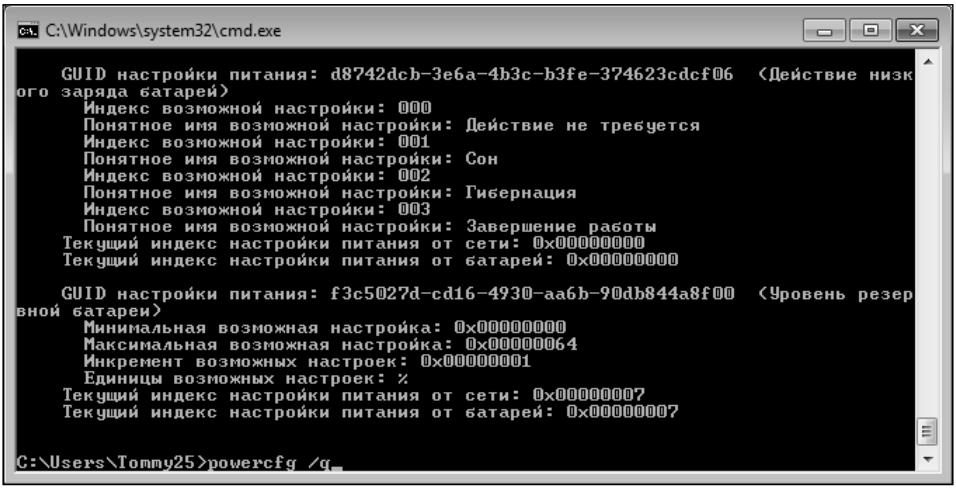


Рис. 5.8. Использование команды powercfg /q

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Управление электропитанием** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Power Management).
2. Дважды щелкните мышью по параметру **Укажите настраиваемую текущую схему управления питанием** (Specify a Custom Active Power Plan). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options), в поле ввода **Настраиваемая схема управления питанием** (Custom Active Power Plan), укажите схему управления питанием в формате идентификатора GUID, например d8742dcb-3e6a-4b3c-b3fe-374623cdcf06).
5. Нажмите кнопку **ОК**.

Управление параметрами жесткого диска

Изменяя параметры жесткого диска в узле управления электропитанием, вы можете выбрать период отсутствия активности, после которого система отключит жесткий диск. Для того чтобы указать период отсутствия активности, выполните следующие действия:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Управление электропитанием ⇒ Параме-**

тры жесткого диска (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Power Management ⇒ Hard Disk Settings).

2. Дважды щелкните мышью по параметру:
   - **Отключить жесткий диск (Питание от сети)** (Turn Off the Hard Disk (Plugged In)) — для настройки компьютера, работающего от электросети (настольный компьютер).
   - **Отключить жесткий диск (Питание от батареи)** (Turn Off the Hard Disk (On Battery)) — для настройки компьютера, работающего от батареи (ноутбуки, TabletPC).
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options), в поле **Отключить жесткий диск** (Turn Off the Hard Disk) укажите период отсутствия активности, после которого жесткий диск будет отключен. Период измеряется в секундах.
5. Нажмите кнопку **ОК**.

Конфигурирование кнопок питания

В этом разделе содержатся настройки действий кнопок и действий при закрытии крышки ноутбука. Настройки политик в этом разделе не отличаются друг от друга, поэтому мы рассмотрим изменение одного параметра, про остальные расскажем вкратце.

Для того чтобы настроить действие системы при нажатии на кнопку отключения питания, выполните следующие шаги:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Управление электропитанием ⇒ Параметры кнопок Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Управление электропитанием** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Button Settings).
2. Дважды щелкните мышью по параметру:
   - **Выберите действие кнопки включения питания (Питание от сети)** (Select the Power Button Action (Plugged In)) — для настройки кнопки включения питания, если компьютер работает в режиме питания от электросети.
   - **Выберите действие кнопки включения питания (Питание от батареи)** (Select the Power Button Action (On Battery)) — для

настройки кнопки включения питания, если компьютер работает от батареи.

3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options), в раскрывающемся списке **Действие кнопки включения питания** (Button Power Action) выберите, какое действие выполнять системе при нажатии пользователем кнопки питания.
5. Нажмите кнопку **ОК**.

Для того чтобы выбрать действие системы при нажатии пользователем кнопки перехода в режим сна, используйте параметр **Выберите действие кнопки перехода в режим сна** (Select the Sleep Button Action).

Для того чтобы выбрать действие системы при закрытии пользователем крышки ноутбука, используйте параметр **Выберите действие при закрытии крышки компьютера** (Select the Lid Switch Action).

В раскрывающемся списке, расположенном в области **Параметры** (Options), могут быть доступны, в зависимости от параметра, следующие пункты:

- **Не предпринимать действий** (Take no action). При выполнении пользователем действия, указанного в параметре, система никак не будет реагировать.
- **Гибернация** (Hibernate). Перевод компьютера в режим энергосбережения.
- **Режим сна** (Sleep). Перевод компьютера в спящий режим.
- **Выключение** (Shut down). Выключение компьютера.

Управление параметрами режимов сна

В этом разделе размещаются параметры различных режимов сна, такие как время ожидания перехода в режим энергосбережения, запрос пароля при выходе из спящего режима, препятствование приложений на переход системы в режим энергосбережения, переход в режим энергосбережения с открытыми сетевыми файлами, а также работу гибридного спящего режима.

Изменение времени ожидания перехода в режимы энергосбережения

Для того чтобы указать период ожидания перехода системы в режим сна, настройте следующую политику:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Управление электропитанием ⇒ Параметры режимов сна** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Power Management ⇒ Sleep Settings).
2. Дважды щелкните мышью по параметру:
   - **Укажите время ожидания перехода в режим сна (Питание от сети)** (Specify the System Sleep Timeout (Plugged In)) — для настройки периода перехода в режим сна, если компьютер работает в режиме питания от электросети.
   - **Укажите время ожидания перехода в режим сна (Питание от батареи)** (Specify the System Sleep Timeout (On Battery) — для настройки периода перехода в режим сна, если компьютер работает от батареи.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options), в поле **Время ожидания перехода системы в режим сна** (System Sleep Timeout) укажите период ожидания перехода системы в режим сна, указывается в секундах.
5. Нажмите кнопку **ОК**.

Если система будет не активна в течение указанного времени, то компьютер перейдет в режим сна. Используйте параметр **Укажите время ожидания для перехода в режим гибернации** (Specify the System Hibernate Timeout) для указания периода бездействия перед тем, как система перейдет в режим гибернации.

Используйте параметр **Укажите время ожидания автоматического перехода в режим сна** (Specify the Unattended Sleep Timeout) для указания периода бездействия перед тем, как Windows автоматически перейдет в спящий режим, если пользователь будет отсутствовать у компьютера. При включении этого параметра нужно ввести значение, указывающее время отсутствия активности в секундах. Если указать 0 секунд, то система не будет автоматически переходить в спящий режим.

Включение режима запроса пароля при выходе из спящего режима

По умолчанию система запрашивает пароль профиля пользователя при выходе из режима сна. Однако запрос пароля можно отключить или, наоборот, включить (если он отключен), что предотвратит посторонний вход в систему. Для включения запроса пароля, отдельно в режимах питания компьюте-

ра от батареи и электросети, настройте следующую политику:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Управление электропитанием ⇒ Параметры режимов сна** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Power Management ⇒ Sleep Settings).
2. Дважды щелкните мышью по параметру:
   - **Требовать пароль при выходе из спящего режима (Питание от сети)** (Require a Password When a Computer Wakes (Plugged In)).
   - **Требовать пароль при выходе из спящего режима (Питание от батареи)** (Require a Password When a Computer Wakes (On Battery)).
3. Установите переключатель в положение **Включить** (Enabled).
4. Нажмите кнопку **ОК**.

Выбор режима сна при простое компьютера

Параметр определяет, может ли система использовать различные режимы при переходе компьютера в режим сна. Если политика **Разрешить различные режимы сна (S1-S3) при простое компьютера** (Allow Standby States (S1-S3) When Sleeping) включена, то система может использовать различные режимы при переходе компьютера в режим сна. Если этот параметр отключен, единственным разрешенным режимом сна является режим гибернации.

Настройки перехода компьютера в спящий режим

Чтобы разрешить приложениям препятствовать переходу системы в режим сна, включите параметр **Разрешить приложениям препятствовать переходу системы в режим сна** (Allow Applications to Prevent Automatic Sleep). Чтобы разрешить приложениям блокировать переход системы в спящий режим, включите параметр **Разрешить приложениям предотвращать автоматический переход в спящий режим** (Allow Applications to Prevent Automatic Sleep).

Некоторые приложения могут блокировать переход системы в режимы энергосбережения, независимо от того, активен ли компьютер или нет. К таким приложениям относится антивирус, который проверяет на данный момент компьютер, запущенная дефрагментация жесткого диска, воспроизводящийся фильм или песня и так далее.

Для того чтобы разрешить или запретить переход в спящий режим с откры-

тыми сетевыми файлами, настройте параметр **Разрешить автоматический переход в спящий режим с открытыми сетевыми файлами** (Allow Automatic Sleep with Open Network Files).

Также доступен параметр **Отключить гибридный спящий режим** (Turn Off Hybrid Sleep), при включении которого система не будет создавать файл спящего режима при переходе в режим сна.

Управление параметрами уведомления

В этом разделе описаны параметры уведомления пользователя о текущем состоянии батареи.

Чтобы указать уровень сигнала батареи, при котором включается сигнал низкого заряда батареи, настройте следующую политику:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Управление электропитанием ⇒ Параметры уведомления** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Power Management ⇒ Notification Settings).
2. Дважды щелкните мышью по параметру **Уровень сигнала низкого разряда батареи** (Low Battery Notification Level). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель в положение **Включить** (Enabled).
4. В области **Параметры** (Options), в поле **Уровень сигнала низкого заряда батареи** (Low Battery Notification Level) введите, на сколько процентов должна быть заряжена батарея, чтобы включился сигнал низкого заряда батареи.
5. Если вы документируете все свои действия в отношении групповых политик, оставьте примечания в поле ввода **Комментарий** (Comments).
6. Нажмите кнопку **ОК**.

Аналогично настраивается уровень сигнала почти полной разрядки батареи (параметр **Уровень сигнала почти полной разрядки батареи** (Critical Battery Notification Level)) и параметр **Уровень сигнала резервной батареи** (Reserve Battery Notification Level), только в этом случае указанный уровень сигнала батареи означает включение сигнала использования резервной батареи.

По желанию, можно отключить уведомление о низком уровне заряда батареи, активировав параметр **Отключить уведомление при низком уровне за-**

ряда батареи (Turn Off Low Battery User Notification). Для установки уровня низкого уровня заряда батареи используйте параметр **Уровень низкого сигнала заряда батареи** (Low Battery Notification Level). Уведомление будет показано только в том случае, если параметр **Действие при низком заряде батареи** (Low Battery Notification Action) имеет значение **Не предпринимать действий** (Take no action).

Кроме этого, можно настроить поведение системы при разряде батареи. Для этого используйте параметры **Действие при почти полной разрядке батареи** (Critical Battery Notification Action) и **Действие при низком заряде батареи** (Low Battery Notification Action). Действие выбирается в раскрывающемся списке области **Параметры** (Options), расположенного в диалоговом окне редактирования параметра политики. На выбор предложено четыре варианта:

- **Не предпринимать действий** (Take no action). При выполнении пользователем действия, указанного в параметре, система никак не будет реагировать.
- **Гибернация** (Hibernate). Перевод компьютера в режим энергосбережения.
- **Режим сна** (Sleep). Перевод компьютера в спящий режим.
- **Выключение** (Shut Down). Выключение компьютера.

Управление параметрами экрана и видео

Вы можете указать уровень яркости экрана при автоматическом снижении яркости операционной системой, как в случае питания компьютера от электросети, так и от батареи:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Управление электропитанием ⇒ Параметры экрана и видео** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Power Management ⇒ Video and Display Settings).
2. Дважды щелкните мышью по параметру:
   - **Указать яркость монитора (Питание от сети)** (Specify the Display Brightness (Plugged In)).
   - **Указать яркость монитора (Питание от батареи)** (Specify the Display Brightness (On Battery)).
3. Установите переключатель в положение **Включить** (Enabled).

4. В области **Параметры** (Options), в поле **Уменьшение яркость монитора** (Display Dim Brightness) введите, на сколько процентов должна быть уменьшена яркость монитора при автоматическом уменьшении яркости монитора системой. Яркость монитора указывается в процентах.
5. Нажмите кнопку **ОК**.

Чтобы указать период бездействия системы, после которого автоматически будет снижена яркость монитора, включите параметр **Уменьшить яркость монитора** (Reduce Display Brightness). В поле **Уменьшить яркость монитора** (Reduce Display Brightness), расположенном в области **Параметры** (Options), укажите количество секунд. Если компьютер будет неактивен в течение этого времени, то яркость монитора будет уменьшена. Аналогично настраивается параметр **Отключить дисплей** (Turn Off the Display), по истечении указанного в котором времени операционная система отключает дисплей.

Вы можете управлять фоновым показом слайдов на рабочем столе, активировав или отключив параметр **Включить фоновый показ слайдов на рабочем столе** (Turn On Desktop Background Slideshow).

Для того чтобы система автоматически настроила параметры, указывающие промежуток отсутствия активности, после которого система отключала бы монитор компьютера, включите параметр **Выключить адаптивное время ожидания выключения дисплея** (Turn Off Adaptive Display Timeout). При включении этой политики система автоматически настроит параметры, основываясь на активности мыши и клавиатуры, для предотвращения выключения дисплея.

Глава 6.

Хакинг подключения к Интернету

Обратите внимание, что описываемые в этой главе параметры отличны от описываемых в главе, посвященной настройке Internet Explorer.

6.1. Компонент локальной групповой политики Настройка Internet Explorer

В настоящее время браузер стал одним из основных инструментов работы на компьютере. Изначально Всемирная паутина, для работы с которой предназначаются программы данного типа, была лишь местом поиска и просмотра текстовой и графической информации. Но благодаря многообразию современных интернет-сервисов современный браузер позволяет решать очень широкий спектр рабочих задач. Некоторые пользователи проводят в нем от 20 до 80 процентов времени работы за компьютером. Поэтому грамотная настройка этого инструмента — важнейшая часть конфигурирования рабочей среды современного пользователя.

Локальные групповые политики предоставляют большой выбор возможностей для настройки браузера, входящего в состав операционной системы Windows — Internet Explorer. Параметры обозревателя Internet Explorer сосредоточены в трех различных местах:

- Компонент **Настройка Internet Explorer** (Internet Explorer Maintenance). Он расположен в ветви **Конфигурация пользователя ⇒ Конфигурация Windows** (User Configuration ⇒ Windows Settings).
- Ветви **Internet Explorer**. Ветви с таким названием присутствуют в двух местах:
    - Одна ветвь **Internet Explorer** расположена в разделе, отвечающем за административные политики компьютера в целом. Чтобы добраться до нее, откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Компоненты Windows** (Computer Configuration ⇒ Administrative Templates ⇒ Windows Components).
    - Вторая ветвь **Internet Explorer** находится в разделе административных политик отдельного пользователя. Чтобы рабо-

тать с этой частью настроек, откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows** (User Configuration ⇒ Administrative Templates ⇒ Windows Components).

В этой главе мы рассматриваем только первый из перечисленных разделов.

В двух следующих параграфах мы обсудим общие подходы к использованию компонента **Настройка Internet Explorer** (Internet Explorer Maintenance), затем пройдемся по конкретным параметрам этого компонента, а в завершение покажем, как параметры раздела **Настройка Internet Explorer** (Internet Explorer Maintenance) можно экспортировать для последующего применения в автоматической настройке браузера.

Общая характеристика компонента Настройка Internet Explorer

Компонент **Настройка Internet Explorer** (Internet Explorer Maintenance) содержит шесть разделов (узлов, ветвей) с параметрами локальной групповой политики (рис. 6.1):

- **Пользовательский интерфейс обозревателя** (Browser User Interface);
- **Подключение** (Connection);
- **URL-адреса** (URLs);
- **Безопасность** (Security);
- **Программы** (Programs);
- **Дополнительно** (Advanced).

Работа с компонентом **Настройка Internet Explorer** (Internet Explorer Maintenance) может вестись в двух режимах. В режиме, который установлен по умолчанию, раздел **Дополнительно** (Advanced) не отображается. Чтобы увидеть его, необходимо переключиться в так называемый режим предпочтений. Для этого щелкните правой кнопкой мыши по названию компонента **Настройка Internet Explorer** (Internet Explorer Maintenance) и в появившемся контекстном меню выберите пункт **Режим предпочтений** (Preference Mode) (рис. 6.2).

Выбирая между обычным режимом редактирования ветви **Настройка Internet Explorer** (Internet Explorer Maintenance) и режимом предпочтений, следует учитывать два момента:

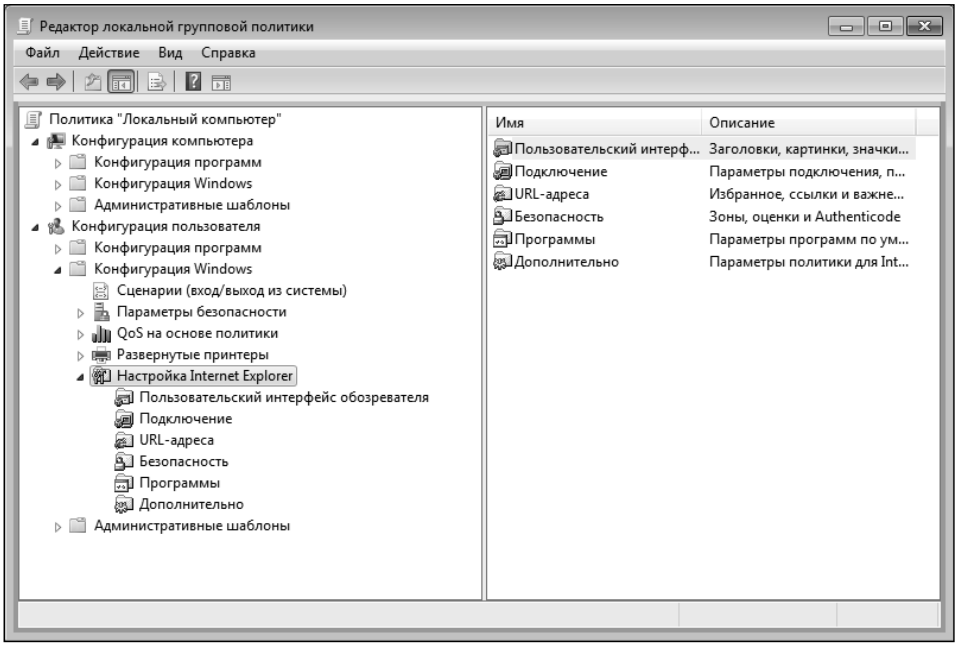


Рис. 6.1. *Окно* Редактора локальной групповой политики *с развернутым компонентом* Настройка Internet Explorer *в режиме предпочтений*

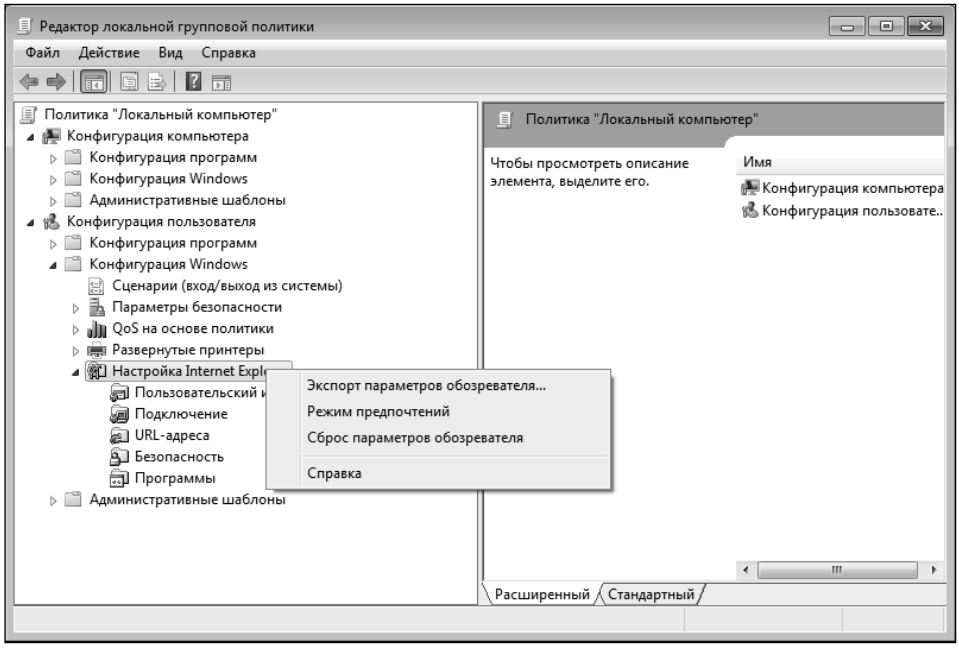


Рис. 6.2. *Окно* Редактора локальной групповой политики, *в котором вызвано контекстное меню для перехода в режим предпочтений*

- Переход в режим предпочтений делает доступной ветвь **Дополнительно** (Advanced), однако некоторые параметры других ветвей, которые открыты для изменения в обычном режиме, перестают быть редактируемыми. Например, в обычном режиме можно изменить заголовок обозревателя, а в режиме предпочтений этот параметр недоступен.
- Выбор режима следует осуществить в самом начале работы с разделом, поскольку его невозможно менять по ходу редактирования. Условием такого переключения является отсутствие пользовательских настроек в ветви **Настройка Internet Explorer** (Internet Explorer Maintenance). Если попытаться перейти в режим предпочтений после того, как отдельные параметры ветви были откорректированы, **Редактор локальной групповой политики** (Local Group Policy Editor) сначала предложит сбросить все внесенные изменения.

Чтобы выполнить сброс внесенных в ветвь **Настройка Internet Explorer** (Internet Explorer Maintenance) изменений, щелкните правой кнопкой мыши по названию ветви и в появившемся контекстном меню выберите команду **Сброс параметров обозревателя** (Reset Browser Settings). Ветвь приобретет свой первоначальный вид. Этой же командой осуществляется и возврат из режима предпочтений в обычный режим. Все внесенные изменения при этом также утрачиваются.

Среди описанных в этой главе параметров компонента **Настройка Internet Explorer** (Internet Explorer Maintenance) есть несколько, которые доступны только из **Редактора локальной групповой политики** (Local Group Policy Editor). Но все же большинство из них имеет аналоги в диалоговом окне **Свойства обозревателя** (Internet Options), которое должно быть хорошо знакомо каждому пользователю Internet Explorer. На это диалоговое окно мы далее будем неоднократно ссылаться. На всякий случай напомним, что попасть в него можно как минимум двумя способами:

- Способ первый. Любым удобным способом запустите Internet Explorer и в его окне выберите команду **Сервис ⇒ Свойства обозревателя** (Tools ⇒ Internet Options).
- Способ второй. Любым удобным способом откройте домашнюю страницу Панели управления и в ее окне выполните команду **Сеть и интернет ⇒ Свойства обозревателя** (Network and Internet ⇒ Internet Options).

Некоторые из параметров компонента **Настройка Internet Explorer** (Internet Explorer Maintenance) не требуется задавать вручную в **Редакторе локальной групповой политики** (Local Group Policy Editor). Вместо этого они

импортируется из текущих настроек операционной системы. Поэтому логично до начала работы с этим компонентом навести порядок в текущих подключениях Internet Explorer, настройках программ для работы с Интернетом, безопасности, конфиденциальности, ограничения доступа.

Сравнение компонента Настройка Internet Explorer и административных шаблонов

Повторимся, что в **Редакторе локальной групповой политики** (Local Group Policy Editor) есть несколько ветвей, которые имеют отношение к конфигурированию Internet Explorer. Поэтому важно понять различия между компонентом, который мы рассмотрим в этой главе, и административными шаблонами, которым посвящены другие главы данной книги.

Самое главное заключается в том, что рассматриваемая в этой главе **Настройка Internet Explorer** (Internet Explorer Maintenance) — это скорее совокупность рекомендаций, а административные шаблоны — средство принуждения пользователя.

Предположим, вы хотите назначить всем пользователям данного компьютера одну и ту же домашнюю страницу. У вас два пути:

- С одной стороны, вы можете открыть узел локальной политики **Конфигурация пользователя ⇒ Конфигурация Windows ⇒ Настройка Internet Explorer ⇒ URL-адреса** (User Configuration ⇒ Windows Settings ⇒ Internet Explorer Maintenance ⇒ URLs) и в параметре **Важные адреса URL** (Important URLs) задать домашнюю страницу.
- С другой стороны, узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Internet Explorer** (User Configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Internet Explorer) содержит параметр **Отключить изменение параметров домашней страницы** (Disable changing home page Settings). В этом параметре вы также можете ввести свое значение.

Если вы пойдете первым путем, пользователь, домашняя страница которого после применения политики однократно изменится, в любой момент сможет ввести вместо вашего значения любое другое. Для этого он должен пройти в диалоговое окно **Свойства обозревателя** (Internet Options) и на вкладке **Общие** (General) поменять домашнюю страницу.

Административный шаблон такую возможность исключает. При его применении элементы управления в диалоговом окне **Свойства обозревателя** (Internet Options), отвечающие за смену домашней страницы, будут недоступны. В нижней части диалогового окна пользователь увидит предупре-

ждение **Некоторыми параметрами управляет системный администратор** (Some Settings are managed by your system administrator).

Вместе с тем следует учитывать, что административные шаблоны позволяют, по сути, превратить параметры компонента **Настройка Internet Explorer** (Internet Explorer Maintenance) из рекомендательных в принудительные. Если вы хотите, чтобы настройки Internet Explorer, о которых пойдет речь в данной главе, обновлялись при обновлении объекта групповой политики, проделайте следующее:

1. Откройте узел **Конфигурация компьютера ⇒ Административные шаблоны ⇒ Система ⇒ Групповая политика** (Computer Configuration ⇒ Administrative Templates ⇒ System ⇒ Group Policy).
2. Дважды щелкните мышью по параметру **Обработка политики настройки Internet Explorer** (Internet Explorer Maintenance policy processing). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель политики в положение **Включить** (Enabled).
4. С помощью флажков раздела **Параметры** (Options) сформируйте оптимальный сценарий обработки этой политики.
5. Нажмите кнопку **OK**.

С этого момента параметры, которые вы внесли с помощью компонента **Настройка Internet Explorer** (Internet Explorer Maintenance), будут воспроизводиться. Если вернуться к рассмотренному выше примеру с изменением домашней страницы, то это означает следующее. Пользователь сможет в диалоговом окне **Свойства обозревателя** (Internet Options) поменять свою домашнюю страницу. Но после обновления групповой политики обозреватель вновь получит ту домашнюю страницу, которая предписана в компоненте **Настройка Internet Explorer** (Internet Explorer Maintenance). Например, это может произойти при перезагрузке операционной системы.

Настройка пользовательского интерфейса обозревателя

В ветви **Пользовательский интерфейс обозревателя** (Browser User Interface) есть только один параметр, который представляет практическую ценность для пользователей Windows 8 — он позволяет настроить название компании, отображаемое в заголовке окна браузера. Внести такие изменения из интерфейса Internet Explorer невозможно, хотя опытные пользователи могут для решения этой задачи прибегнуть к редактированию реестра.

Чтобы произвести настройку заголовка обозревателя средствами локальной групповой политики, проделайте следующее:

1. Откройте узел **Конфигурация пользователя ⇒ Конфигурация Windows ⇒ Настройка Internet Explorer ⇒ Пользовательский интерфейс обозревателя** (User Configuration ⇒ Windows Settings ⇒ Internet Explorer Maintenance ⇒ Browser User Interface).
2. Дважды щелкните мышью по параметру **Заголовок обозревателя** (Browser Title). Откроется диалоговое окно редактирования параметра политики.
3. Установите флажок **Изменить заголовки окон** (Customize Title Bars). Поле **Текст в заголовке** (Title Bar Text) станет доступным для редактирования.
4. Введите в поле **Текст в заголовке** (Title Bar Text) название компании, которое вы хотите видеть в заголовке браузера.
5. Нажмите кнопку **OK**.

Предположим, вы ввели в поле **Текст в заголовке** (Title Bar Text) слово **Радуга**. Если теперь запустить Internet Explorer, то его заголовок будет выглядеть так, как представлено на рис. 6.3.

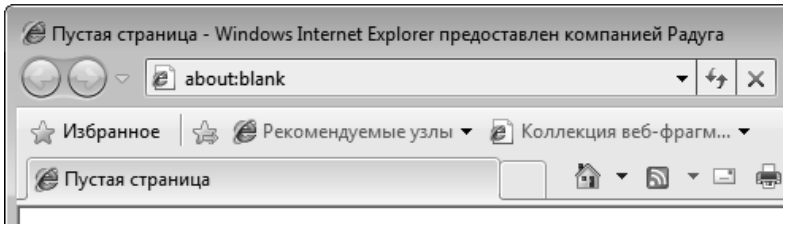


Рис. 6.3. ***Заголовок окна обозревателя Internet Explorer, к которому добавлен пользовательский текст***

В режиме предпочтений изменение заголовка обозревателя недоступно.

В ветви **Пользовательский интерфейс обозревателя** (Browser User Interface) также присутствуют разделы **Эмблема и анимированные рисунки** (Custom Logo and Animated Bitmaps) и **Настройка панели инструментов обозревателя** (Browser Toolbar Customizations). Они сохранились от устаревших версий Internet Explorer. Их редактирование не внесет никаких изменений в пользовательский интерфейс Internet Explorer версии 8.0 и выше, которая включена в состав операционной системы Windows 8.

Параметры подключения Internet Explorer

Обозреватель Internet Explorer позволяет гибко настраивать подключение к сети. Простейший способ начать работу с Интернетом — подключиться к нему посредством локальной сети, если она соединена с сетью глобальной и настроена. Также можно создать одно или несколько комментируемых подключений различных типов — через DSL, сетевой кабель, модем. Для каждого коммутируемого подключения определяются свой логин и пароль, конфигурируются параметры автоматической настройки обозревателя и прокси-сервера. Созданные подключения можно согласовать между собой: например, ноутбук, с которым вы много перемещаетесь, можно настроить таким образом, чтобы при наличии локальной сети Internet Explorer пытался подключиться через нее, а в случае отсутствия сети — инициировал запуск коммутируемого модемного соединения. Поверх созданных подключений можно использовать виртуальные частные сети (VPN).

Пользователь Internet Explorer может изменить все эти настройки на вкладке **Подключения** (Connections) диалогового окна **Свойства обозревателя** (Internet Options). Новичку ввод многочисленных настроек может показаться затруднительным, но чаще всего задача сводится к тому, чтобы следовать пошаговым инструкциям своего интернет-провайдера. В случае затруднений стоит в первую очередь воспользоваться справкой, встроенной в операционную систему. Чтобы обратиться к ней, достаточно, например, щелкнуть мышью на кнопке с вопросительным знаком в правом верхнем углу вкладки **Подключения** (Connections) диалогового окна **Свойства обозревателя** (Internet Options).

Локальная групповая политика добавляет в эту технологию возможность быстрого клонирования настроек по другим пользователям, а при необходимости — и по другим компьютерам. Чтобы распространить готовые параметры подключения к Интернету на других пользователей, сделайте следующее:

1. Откройте узел **Конфигурация пользователя ⇒ Конфигурация Windows ⇒ Настройка Internet Explorer ⇒ Подключение** (User Configuration ⇒ Windows Settings ⇒ Internet Explorer Maintenance ⇒ Connection).
2. Дважды щелкните мышью по параметру **Параметры подключения** (Connection Settings). Откроется диалоговое окно редактирования параметра политики.
3. Установите переключатель **Параметры подключения** (Connection Settings) в положение Импортировать текущие параметры подключения с этого компьютера (Import the current Connection Settings

from this machine). Кнопка **Изменить параметры** (Modify Settings) станет доступной.

4. Если вы не уверены в полноте и точности текущих настроек подключения, щелкните мышью по кнопке **Изменить параметры** (Modify Settings). Откроется уже упоминавшаяся вкладка **Подключения** (Connections), к которой мы ранее получали доступ из диалогового окна **Свойства обозревателя** (Internet Options).
5. Используя возможности открывшегося диалогового окна, просмотрите, а при необходимости — отредактируйте параметры текущих подключений компьютера. Внесенные изменения зафиксируйте кнопкой **OK**, в противном случае закройте диалоговое окно кнопкой **Отмена** (Cancel).
6. Если импорт настроек должен сопровождаться удалением существующих параметров подключения, установите флажок **Удалить существующие параметры подключения коммутируемого соединения** (Delete existing Dial-up Connection Settings) в нижней части диалогового окна **Параметры подключения** (Connection Settings).
7. Нажмите кнопку **OK**.

В результате пользователи, для которых формулировалась данная политика, получат унифицированный набор подключений Internet Explorer.

Автоматическая настройка обозревателя

Существует две разновидности автоматической настройки браузера Internet Explorer в локальной сети:

- Администратор может так настроить сеть, чтобы браузер, не имея никакой изначальной информации, находил настройки самостоятельно. Чтобы такой вариант заработал, следует определенным образом сконфигурировать серверы DHCP и DNS.
- При первоначальной настройке браузеру можно указать конкретные URL-адреса, по которым он получит файлы с настройками. При необходимости можно задать промежуток времени, через который браузер будет вновь обращаться по этим адресам за обновленной версией настроек.

Подробное описание этих способов содержится в документации к Пакету администрирования Internet Explorer.

Пользователь Internet Explorer может активировать указанные возможно-

сти из диалогового окна **Настройка параметров локальной сети** (Local Area Network (LAN) Settings). Чтобы попасть в это окно, следует любым удобным способом открыть диалоговое окно **Свойства обозревателя** (Internet Options), перейти на вкладку **Подключения** (Connections) и нажать кнопку **Настройка сети** (LAN Settings). Если в окне **Настройка параметров локальной сети** (Local Area Network (LAN) Settings) установить флажок **Автоматическое определение параметров** (Automatically detect Settings), вы включите первую возможность. А если в этом диалоговом окне установить флажок **Использовать сценарий автоматической настройки** (Use automatic Configuration script) и заполнить поле **Адрес** (Address), доступным станет второй вариант автонастройки.

Чтобы задействовать эти возможности в локальной групповой политике, сделайте следующее:

1. **Откройте узел Конфигурация пользователя ⇒ Конфигурация Windows ⇒ Настройка Internet Explorer ⇒ Подключение** (User Configuration ⇒ Windows Settings ⇒ Internet Explorer Maintenance ⇒ Connection).
2. Дважды щелкните мышью по параметру **Автоматическая настройка обозревателя** (Automatic Browser Configuration). Откроется диалоговое окно редактирования параметра политики.
3. Если необходимо активировать первую разновидность автоматической настройки браузера, установите флажок **Автоматически определять параметры настройки** (Automatically detect Configuration Settings).
4. Если необходимо активировать вторую разновидность автоматической настройки браузера, установите флажок **Разрешить автоматическую настройку** (Enable Automatic Configuration). Это сделает доступными остальные элементы управления диалогового окна. Введите в них URL-адреса, по которым браузер будет получать настройки, и промежуток времени, через который автонастройка должна повторяться.
5. Нажмите кнопку **OK**.

Теперь автоматическая настройка обозревателя будет сконфигурирована единообразно у всех пользователей, для которых была сформулирована данная политика.

Настройка параметров прокси-сервера

Прокси-сервер — это сетевая служба, которая опосредует запросы браузера к другим сетевым службам. Сначала обозреватель подключается к прокси-серверу и запрашивает какой-либо ресурс (например, страницу веб-сайта). Прокси-сервер в свою очередь обращается по указанному адресу и получает ресурс у него либо возвращает ресурс из собственного временного хранилища — кэша. Через прокси-серверы подключают своих пользователей многие организации и интернет-провайдеры — главным образом в целях упрощения маршрутизации, контроля и экономии трафика.

Настройки прокси-сервера может изменить каждый пользователь. Для этого следует любым удобным способом вызвать диалоговое окно **Свойства обозревателя** (Internet Options), перейти на вкладку **Подключения** (Connections) и нажать кнопку **Настройка сети** (LAN Settings). В открывшемся диалоговом окне **Настройка параметров локальной сети** (Local Area Network (LAN) Settings) задаются основные параметры прокси-сервера. Кнопка **Дополнительно** (Advanced) позволит открыть диалоговое окно расширенной настройки.

Локальные групповые политики позволяют настроить прокси-серверы сразу для нескольких пользователей. Чтобы сконфигурировать параметры прокси-серверов, сделайте следующее.

1. Откройте узел **Конфигурация пользователя ⇒ Конфигурация Windows ⇒ Настройка Internet Explorer ⇒ Подключение** (User Configuration ⇒ Windows Settings ⇒ Internet Explorer Maintenance ⇒ Connection).
2. Дважды щелкните мышью по параметру **Параметры прокси-сервера** (Proxy Settings). Откроется диалоговое окно редактирования параметра политики.
3. Установите флажок **Разрешить настройку прокси-сервера** (Enable proxy Settings). Станут доступными остальные элементы управления диалогового окна.
4. В группе полей **Адрес прокси-сервера** (Address of proxy) введите один или несколько адресов прокси-серверов. Чтобы использовать для всех служб в списке одинаковые настройки прокси-сервера, установите флажок **Использовать один прокси-сервер для всех адресов** (Use the same proxy server for all addresses).
5. В группе **Порт** (Port) введите номер порта для каждой службы. Значением по умолчанию является порт **80**.

6. В поле **Не использовать прокси-сервер для адресов, начинающихся с** (Do not use proxy server for addresses beginning with) введите конкретные адреса, обращение к которым должно осуществляться, минуя прокси-сервер. При необходимости в данном поле можно использовать подстановочный знак * — он заменяет ноль или несколько произвольных символов. Введенные адреса разделяются точкой с запятой. Общая длина списка исключений не должна превышать 2064 знака.
7. Чтобы отключить использование прокси-серверов для всех адресов во внутренней локальной сети, установите флажок **Не использовать прокси-сервер для локальных (внутрисетевых) адресов** (Do not use proxy server for local (intranet) addresses).
8. Нажмите кнопку **OK**.

В результате пользователи, для который формулировалась данная политика, получат унифицированные настройки проксирования.

Настройка строки обозревателя

Строка обозревателя (или по-другому — строка агента пользователя) — это текстовая информация, которую браузер посылает посещаемым серверам для идентификации. В первую очередь она необходима для сбора статистики интернет-трафика. Некоторые сайты корректируют содержимое вебстраницы в зависимости от того, какую строку агента прислал браузер.

Локальная групповая политика позволяет дополнить стандартную строку Internet Explorer пользовательским текстом. Чтобы внести такие изменения:

1. Откройте узел **Конфигурация пользователя ⇒ Конфигурация Windows ⇒ Настройка Internet Explorer ⇒ Подключение** (User Configuration ⇒ Windows Settings ⇒ Internet Explorer Maintenance ⇒ Connection).
2. Дважды щелкните мышью по параметру **Строка обозревателя** (User Agent String). Откроется диалоговое окно редактирования параметра политики.
3. Установите флажок **Настроить строку для присоединения к строке агента пользователя** (Customize string to be appended to User agent string), а затем введите в текстовое поле текст, которым хотите дополнить стандартную строку браузера.
4. Нажмите кнопку **OK**.

Данный параметр отсутствует в интерфейсе Internet Explorer, альтернативой применению локальной групповой политики в данном случае является непосредственное редактирование реестра. Впрочем, сама эта возможность ориентирована скорее на узкий круг специалистов. Обычному пользователю, не обладающему глубокими познаниями в интернет-технологиях, строку обозревателя менять не стоит.

В режиме предпочтений изменение строки обозревателя недоступно.

Настройка URL-адресов: Избранного, Ссылок, домашней страницы

В работе с браузером Internet Explorer важное место занимают коллекции **Избранное** (Favorites) и **Ссылки** (Links или Favorites Bar). В этих коллекциях пользователь накапливает адреса интернет-сайтов и отдельных страниц, которые заслуживают наибольшего внимания. Информацию о каком-либо ресурсе, сохраненную в браузере для последующего быстрого доступа из избранного или с панели ссылок, часто называют закладкой.

В момент установки Internet Explorer (или самой операционной системы Windows, в состав которой входит браузер) **Избранное** (Favorites) и **Ссылки** (Favorites Bar) автоматически пополняются несколькими стандартными элементами. Среди них, например, закладки на Домашнюю страницу Internet Explorer, портал MSN, принадлежащий компании Microsoft, сервисы семейства Windows Live и т. п. В дальнейшем пользователь изменяет свои закладки самостоятельно.

Локальные групповые политики позволяют централизованно распространять закладки среди пользователей. Чтобы добавить закладку на панель ссылок, проделайте следующее:

1. Откройте **узел Конфигурация пользователя ⇒ Настройка Internet Explorer ⇒ URL-адреса** (User Configuration ⇒ Internet Explorer Maintenance ⇒ URLs).
2. Дважды щелкните мышью по параметру **Избранное и ссылки** (Favorites and Links). Откроется диалоговое окно редактирования параметра политики. Если вы ранее не редактировали этот параметр, в списке доступных папок и ссылок присутствует два стандартных пункта — **Favorites** и **Links**.
3. Выделите элемент **Links** и нажмите кнопку **Добавить URL** (Add URL).
4. В появившемся диалоговом окне **Сведения** (Details) задайте обяза-

тельные параметры — имя закладки и URL-адрес сайта. При желании можно также указать значок сайта.

5. Нажмите кнопку **OK**. Диалоговое окно **Сведения** (Details) закроется, а в списке доступных папок и ссылок в разделе **Links** появится новый пункт.

Добавление элементов в Избранное выполняется аналогично, только в списке доступных папок и ссылок следует выбирать элемент **Favorites**.

Диалоговое окно **Избранное и ссылки** (Favorites and Links) содержит также ряд дополнительных инструментов для работы с закладками. В частности, пользователь имеет возможность:

- Объединять создаваемые закладки в папки. Чтобы поместить закладку внутрь собственной папки, сначала создайте папку с помощью кнопки **Добавить папку** (Add Folder), а затем, выделив эту папку в списке доступных, описанным выше способом поместите в ней новую ссылку.
- Изменять и удалять ранее добавленные ссылки. Для этого выделите необходимую ссылку и нажмите одну из кнопок — **Изменить** (Edit) или **Удалить** (Remove).
- В тестовых целях открывать ссылки в браузере. Для этого выделите соответствующую ссылку и нажмите кнопку **Проверить URL** (Test URL).
- Импортировать ранее созданный набор закладок. Для этого выделите необходимый элемент списка доступных папок и ссылок и нажмите кнопку **Импортировать** (Import). Откроется диалоговое окно **Обзор папок** (Browse for Folder), который позволит указать папку с закладками, намеченными для импорта.
- Задавать порядок расположения закладок. Для этого установите флажок **Расположить избранное и ссылки в начале списка в указанном порядке** (Place favorites and links at the top of the list in the order specified below). Это сделает доступными кнопки **Вверх** (Up) и **Вниз** (Down), с помощью которых измените очередность закладок.
- Принудительно удалять закладки, созданные до применения данной групповой политики. За различные аспекты этого действия отвечают флажки **Удалить существующее избранное и ссылки, если они есть** (Delete existing Favorites and Links, if present), **Удалить только созданное администратором избранное** (Only delete the favorites created by the administrator) и **Удалить существующие каналы, если они есть** (Delete existing channels, if present).

Когда работа в диалоговом окне **Избранное и ссылки** (Favorites and Links) завершена, нажмите кнопку **OK**.

Предположим, в **Редакторе локальной групповой политики** (Local Group Policy Editor) вы внесли следующие изменения:

- в раздел **Links** добавили закладку на сайт своей компании;
- в раздел **Favorites** — добавили URL-адреса поисковой системы Яндекс и русской версии онлайн-энциклопедии Википедия;
- установили флажок **Удалить существующее избранное и ссылки, если они есть** (Delete existing Favorites and Links, if present).

В результате браузер пользователя, на которого распространяется политика, примет вид, представленный на 6.4.

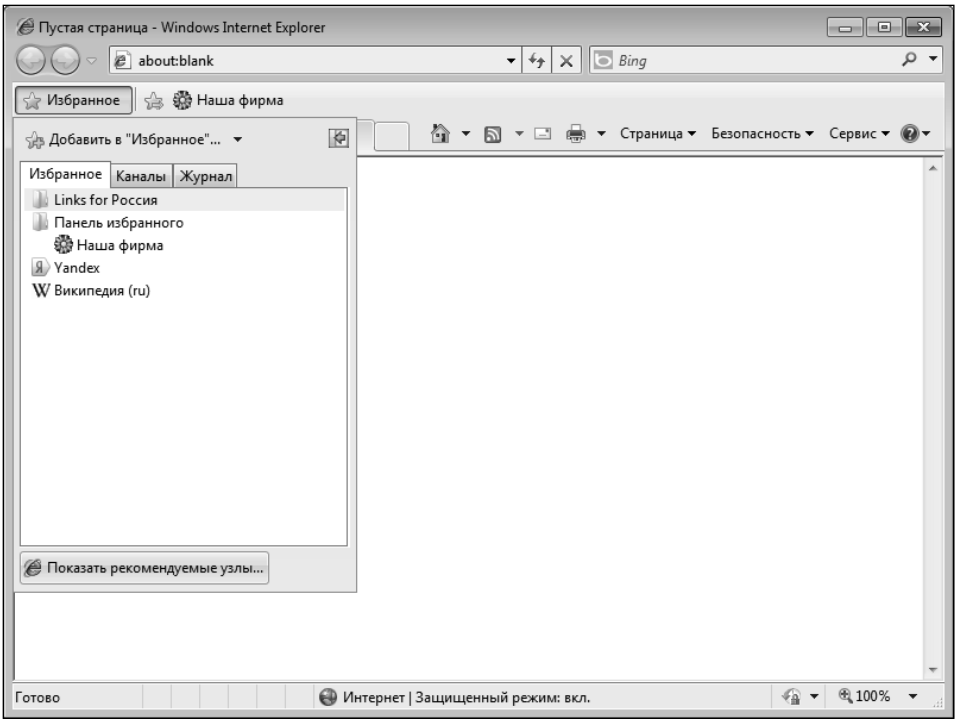


Рис. 6.4. ***Вид обозревателя Internet Explorer с настроенным*** **Избранным** ***и*** **Ссылками**

Важную роль в работе с браузером играет также домашняя страница — URL-адрес, который открывается при запуске обозревателя или при нажатии кнопки **Домой** (Home). Каждый пользователь может установить свою домашнюю страницу в диалоговом окне **Свойства обозревателя** (Internet Options) на вкладке **Общие** (General).

Локальные групповые политики позволяют централизовано назначать домашние страницы пользователей. Эта функция широко востребована во многих организациях, где принято устанавливать в качестве домашней главную страницу корпоративного сайта.

Чтобы выполнить такую настройку:

1. Откройте узел **Конфигурация пользователя ⇒ Настройка Internet Explorer ⇒ URL-адреса** (User Configuration ⇒ Internet Explorer Maintenance ⇒ URLs).
2. Дважды щелкните мышью по параметру **Важные адреса URL** (Important URLs). Откроется диалоговое окно редактирования параметра политики.
3. Установите флажок **Изменить адрес домашней страницы** (Customize Home page URL). Это сделает доступным поле для ввода адреса.
4. Введите в поле **URL-адрес домашней страницы** (Home page URL) необходимое значение. Учитывайте, что адрес в данном случае должен обязательно начинаться с указателя протокола. Например, программа отвергнет вариант **www.ya.ru**, необходимо ввести **http://www.ya.ru**.
5. Нажмите кнопку **OK**.

Глава 7.

Удаленное управление компьютером с Windows 8 через Интернет

7.1. Что такое удаленное администрирование и зачем оно может быть полезно

Программа Radmin предназначена для *удаленного администрирования* ПК. Прежде, чем начать изучение принципов работы с программой, дадим определение термину *удаленное администрирование*.

Под *удаленным администрированием* (УА) понимают возможность человека управлять *удаленным* (находящимся на достаточно большом расстоянии) компьютером с помощью аппаратных и программных средств. Под аппаратными средствами (в данном конкретном случае) стоит понимать персональный компьютер. Программные средства – это набор программ, позволяющих воспользоваться персональным компьютером для удаленного доступа, именно таким программным средством является Radmin. Radmin позволяет "превратить" один компьютер в терминал для другого. Т.е. на мониторе одного компьютера будет отображаться рабочий стол другого компьютера, при этом ваши клавиатура и мышь будут использоваться для управления удаленным ПК. В то же время все действия, производимые пользователем будут видны вам.

Теперь стоит рассмотреть случаи, в которых человеку может потребоваться *удаленный доступ* к компьютеру:

1. **При осуществлении должностных обязанностей**. Практически во всех крупных компаниях персональные компьютеры расположены на достаточно большом расстоянии друг от друга (особенно если у компании разветвленная сеть офисов). В таких условиях у человека, занимающегося обслуживанием компьютеров организации и не имеющего средств удаленного администрирования, большая часть времени уходила бы на перемещение между компьютерами пользователей. А имея такие средства, человек может спокойно

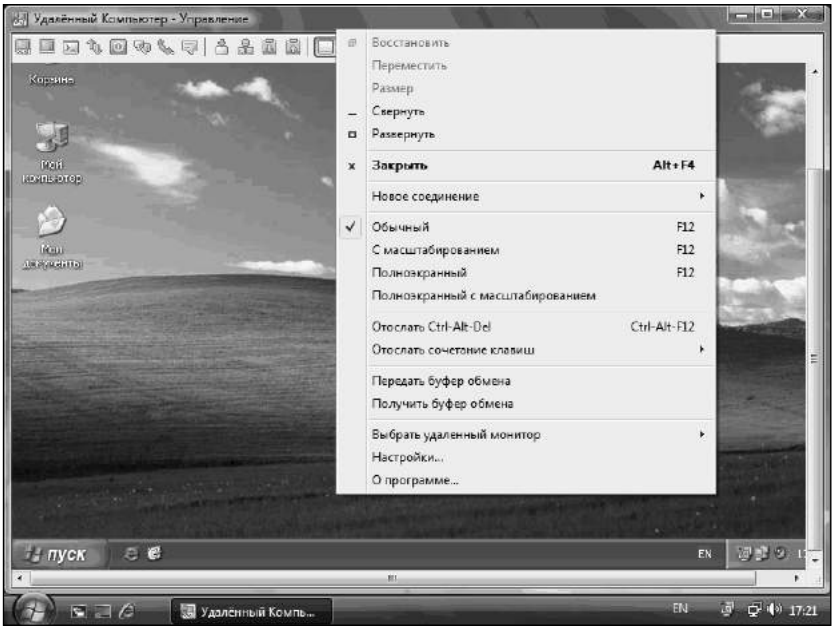


Рис. 7.1. Экран удаленного компьютера на экране вашего

подключиться к компьютеру пользователя и решить его проблемы. Также можно с помощью средств удаленного администрирования осуществлять обучение сотрудников.

Например, вам необходимо обучить сотрудника тому, как настраивать подключение к Интернету. Вы созваниваетесь с этим сотрудником, подключаетесь к его компьютеру и, производя необходимые для настройки Интернета на компьютере удаленного пользователя действия, поясняете ему, что вы делаете. Затем вы можете попросить сотрудника произвести настройку Интернета самому и следите за тем, чтобы он все сделал правильно.

Также с помощью средств удаленного администрирования вы сможете получить доступ к данным вашего домашнего ПК с рабочего компьютера и наоборот.

Руководителям средства удаленного администрирования позволят проконтролировать, чем заняты сотрудники в рабочее время.

2. **Для личных целей**. На первый взгляд, средства удаленного администрирования нужны лишь системным администраторам и программистам при осуществлении ими своих должностных обязанностей. Но это далеко не так! Обычные пользователи могут использовать средства удаленного администрирования для помощи своим

друзьям и родным. Получив удаленный доступ к другому компьютеру, вы сможете совместно с его владельцем решить проблему. Также вы сами можете прибегнуть к помощи другого человека.

Если вы уже решили для себя, что хотите узнать секрет того, как можно настроить и получить удаленный доступ к другому компьютеру с помощью программы Radmin, давайте приступим к ее рассмотрению.

7.2. Знакомство с программой

Системные требования

На сайте разработчика программы — www.radmin.ru — утверждают, что Radmin не предъявляет высоких системных требований к ПК, поэтому вам достаточно иметь установленную операционную систему семейства Microsoft Windows. Последняя версия Radmin полностью совместима с ОС Windows Vista и Windows 8.

Пробную 30-ти дневную версию программы вы можете скачать с сайта разработчика – www.radmin.ru или взять с диска, прилагаемого к книге. После окончания периода пробной эксплуатации вам необходимо будет приобрести программу. На момент написания данного материала последней версией программы являлась Radmin 3.5.

Установка Radmin на компьютере, который должен управляться

Прежде чем приступить к описанию процесса установки программы, стоит рассказать о том, что Radmin состоит из двух частей – серверной и клиентской.

Серверную часть Radmin необходимо установить на компьютеры, к которым вам необходимо получить удаленный доступ. Radmin Server дает возможность подключиться к удаленному компьютеру с помощью программы Radmin Viewer. Серверная часть дает возможность не только подключиться и управлять удаленным компьютером, но и обмениваться с ним файлами. Также благодаря серверной части программы Radmin вы сможете начать с пользователем удаленного компьютера текстовый или голосовой чат. В последней версии Radmin Server реализована возможность считывания данных непосредственно с экрана удаленного компьютера, что позволяет увеличить частоту обновления экрана и сэкономить сетевой трафик. Это особенно важно, если вы подключаетесь к удаленному компьютеру через Интернет.

При помощи клиентской части Radmin (Radmin Viewer) вы можете подключиться к удаленному компьютеру, на котором установлена серверная часть программы Radmin. Radmin Viewer в своем окне отображает рабочий стол удаленного компьютера. В окне Radmin Viewer вы можете управлять удаленным компьютером так, как если бы сидели непосредственно за ним.

7.3. Установка и настройка Radmin Server – на компьютере, с которого должно быть управление

Итак, приступим к установке серверной части. Помните, что серверную часть следует устанавливать на тех компьютерах, к которым вы хотите получить удаленный доступ. Для начала процесса установки Radmin Server запустите файл **rserv35ru.exe**. В первом окне нажмите кнопку **Далее**. Во втором окне вам необходимо принять лицензионное соглашение, после чего нажать кнопку **Далее**. В третьем окне нажмите кнопку **Установить**, чтобы начать процесс установки программы. Во время процесса установки все файлы программы будут скопированы в папку **C:\WINDOWS\system32\rserver30**. После установки вам будет предложено настроить права доступа к Radmin Server. Не снимая галочку напротив **Настроить права доступа для Radmin Server**, нажмите кнопку **Готово** в последнем окне мастера установки Radmin Server, перед вами откроется окно, показанное на рис. 7.2.

Рис. 7.2. Окно настройки Radmin Server

Нажав кнопку **Режим запуска,** вы сможете выбрать из двух вариантов **Ручной** или **Автоматический**. Лучше оставить вариант **Автоматический**.

Нажав кнопку **Настройки**, вы сможете настроить параметры **Radmin Server** (рис. 7.3).

Как вы можете видеть, все настройки Radmin Server'а представлены в виде дерева (слева на рис. 7.3). Рассмотрим их все.

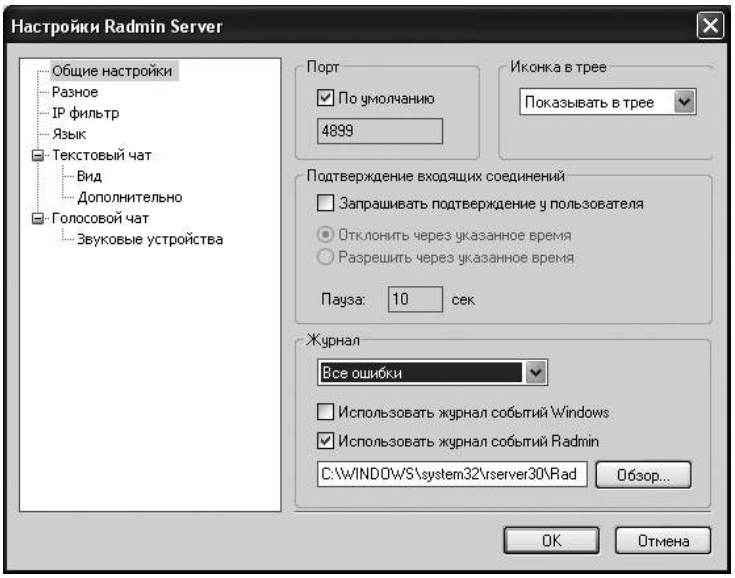


Рис. 7.3. Окно настроек параметров Radmin Server

Общие настройки. Параметры соединения

Общие настройки. Здесь вы сможете настроить параметры соединения с Radmin Server и настроить параметры журнала.

- **Порт**. Здесь вы можете указать порт, через который будет происходить подключение к серверу Radmin. По умолчанию указан порт **4899**. Если вы хотите указать другой порт – снимите галочку напротив **По умолчанию** и укажите нужный порт (этот порт не должен быть занят другим приложением). **Важно – если на компьютере, где установлен Radmin Server, работает файервол, вам необходимо задать в нем исключение для указанного вами в окне настроек Radmin Server порта.**
- **Иконка в трее**. Здесь вы можете задать режим отображения иконки Radmin Server в системном трее. Вы можете выбрать из двух вариантов **Показывать в трее** (иконка Radmin Server будет отображаться в трее только тогда, когда сервер Radmin будет запущен) и **Показывать всегда** (иконка в трее будет отображаться и в момент, когда сервер Radmin будет остановлен).
- **Подтверждение входящих соединений.** Если вы хотите, чтобы пользователь удаленного компьютера подтверждал ваше право на

получения доступа к его компьютеру, установите галочку напротив **Запрашивать подтверждение у пользователя**. После этого выберите из двух вариантов – **Отклонить через указанное время** (если пользователя не окажется перед компьютером, ваше соединение с Radmin Server будет разорвано через указанный промежуток времени) и **Разрешить через указанное время** (если пользователя удаленного ПК не окажется на месте, ваше право на подключение к его компьютеру будет подтверждено через указанный интервал времени). В поле **Пауза** укажите необходимый интервал времени, через который будет подтверждено или отклонено ваше право на подключение к удаленному компьютеру.

- **Журнал**. Здесь вы можете настроить параметры хранения журнала Radmin Server. В поле выбора вы сможете выбрать один из вариантов хранения информации о возникших в процессе работы Radmin Server'а ошибках. Выбрав вариант **Не вести журнал ошибок,** вы отключите возможность ведения журнала ошибок в работе Radmin Server'а. Если вы хотите хранить информацию об ошибках в работе Radmin Server в журнале событий Windows, установите галочку напротив **Использовать журнал событий Windows**. Так же вы сможете использовать *журнал событий Radmin*, установив галочку напротив соответствующего пункта настроек. Чтобы изменить папку, в которой будет храниться журнал событий Radmin, нажмите кнопку **Обзор**.

Параметры управления удаленным рабочим столом

Вкладка **Разное**. Здесь вы сможете настроить параметры управления удаленным рабочим столом. Для включения/отключения настроек поставьте/снимите галочки напротив соответствующих названий настроек.

- **Отключить режим управления**. Режим управления удаленным рабочим столом будет недоступен. В режиме управления удаленным рабочим столом вы можете управлять удаленным рабочим компьютером посредством мыши и клавиатуры локального компьютера, с которого вы подключаетесь к удаленному компьютеру; запускать программы; просматривать содержимое папок; открывать файлы и изменять их; отправлять документы на печать. В режиме управления удаленным рабочим столом вы будете работать так, как если бы вы сидели непосредственно за удаленным компьютером.
- **Отключить режим просмотра**. Режим просмотра будет недоступен. В режиме просмотра вы не сможете управлять удаленным компью

- тером, вы сможете только наблюдать за действиями пользователя удаленного компьютера.
- **Отключить режим передачи файлов**. Передача файлов с удаленного компьютера средствами Radmin будет невозможна. В данном режиме вы можете обмениваться файлами с удаленным компьютером.
- **Отключить режим Telnet**. При подключении к удаленному компьютеру вы не сможете отправлять на него текстовые команды. В данном режиме вы сможете посылать текстовые команды на удаленный компьютер.
- **Отключить использование как промежуточный сервер**. Данный сервер Radmin не сможет быть использован в качестве промежуточного сервера Radmin. Если данный режим включен, вы сможете использовать сервер Radmin для подключения к другим удаленным рабочим столам.
- **Отключить режим выключения**. Оставив включенным данный режим, вы сможете выключать и перезагружать удаленный компьютер, завершать сеанс работы пользователя. При работе в данном режиме вы сможете выключать и перезагружать удаленный компьютер.
- **Отключить текстовый чат**. Текстовый чат между вашим и удаленным компьютером будет отключен. В текстовом чате вы сможете обмениваться текстовыми сообщениями с пользователем удаленного компьютера.
- **Отключить голосовой чат**. Голосовой чат между вашим и удаленным компьютером будет отключен. В голосовом чате вы сможете пообщаться с собеседником (для этого на локальном и удаленном компьютере должны быть подключены колонки/наушники и микрофон).
- **Отключить передачу текстового сообщения**. Передача текстовых сообщений удаленному пользователю будет невозможна. Работая с удаленным компьютером в режиме передачи текстовых сообщений, вы сможете отправить удаленному пользователю сообщение, которое будет выведено на экран его монитора. Данный режим отличается от режима *текстовый чат* — в чате пользователь может отправить вам текстовое сообщение.
- **Не получать DNS имена для IP адресов**. Установите галочку напротив этой настройки, если вы не хотите, чтобы Radmin Server получал DNS-имена для входящих IP-адресов.

Настройка фильтрации и ограничения доступа по IP-адресу

Вкладка **IP фильтр**. В данном разделе настроек вы сможете указать IP-адрес или диапазон IP-адресов, с которых будет разрешено подключение к данному серверу Radmin. Для этого установите галочку напротив **Включить IP фильтрацию** и нажмите кнопку **Добавить**, перед вами откроется окно, в котором вы сможете указать **Один IP адрес** иди **Диапазон IP адресов** (рис. 7.4).

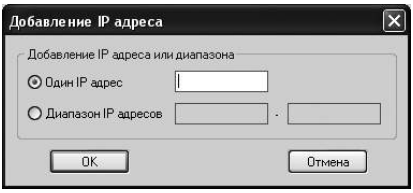


Рис. 7.4. Окно добавления IP адреса/диапазона IP-адресов в Radmin Server

Все добавленные IP-адреса и диапазоны IP-адресов вы сможете посмотреть в списке, показанном на рис. 7.5 (на рисунке данный список обведен прямоугольной рамкой).

Если вы хотите удалить отдельный IP-адрес или диапазон IP-адресов, выберите соответствующую запись в списке (рис. 7.5) и нажмите кнопку **Удалить**.

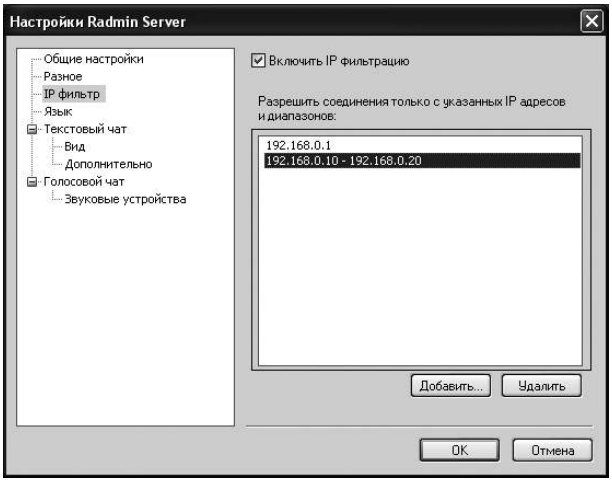


Рис. 7.5. Список IP-адресов и диапазонов IP-адресов, для которых разрешено подключение к Radmin Server

По желанию — настройка языка интерфейса программы

Вкладка **Язык**. Здесь вы можете указать язык интерфейса Radmin Server. Вы можете указать конкретное значение или установить галочку напротив **Выбрать язык автоматически** (язык интерфейса программы будет выбран в соответствии с настройками вашей системы). Для того чтобы языковые настройки вступили в силу, вам необходимо будет перезапустить Radmin Server.

Параметры организации текстового Чата между вашим и удаленным компьютерами

Вкладка **Текстовый чат** в окне настроек. Здесь вы сможете задать параметры текстового чата.

- В поле **Имя или псевдоним** укажите имя, которое будет отображаться в чате.
- В поле **Дополнительная информация** вы сможете указать дополнительную информацию о себе. **Сообщение для статуса 'Отошел'**: укажите здесь сообщение, которое будет отобраться, когда пользователь удаленного компьютера не будет совершать на нем никаких действий в течение определенного промежутка времени (как правило – 5 минут) или когда он заблокирует компьютер.
- Если хотите, чтобы данные параметры отображались только при получении входящих сообщений, включите опцию **Показывать только при получении приватных сообщений**.

В подразделе **Вид** (для раздела настроек **Текстовый чат**) вы сможете настроить параметры отображения сообщений в текстовом чате и окна чата:

- **Иконка в трее**, выбрав в данном поле одну из четырех настроек вы сможете настроить отображение окна текстового чата в системном трее.
- **Добавлять новые сообщения** — здесь вы сможете указать, как будут добавлять сообщения в текстовый чат – **Снизу** или **Сверху**.
- **Шрифт для элементов интерфейса текстового чата** – в данном поле вам необходимо выбрать элемент интерфейса текстового чата и затем настроить параметры шрифта (кнопка **Шрифт**) и цвета текста (кнопка **Цвет**).
- Так вы сможете настроить параметры для сообщений пользователя, к компьютеру которого подключаются удаленно – **Свои сообщения**;

параметры входящих сообщений – **Чужие сообщения**; параметры оповещений выводящихся на экран – **Оповещения**; параметры отображения сообщений об ошибках – **Сообщения об ошибках**; параметры цвета фона окна текстового чата – **Цвет фона** (для последнего варианта будет доступна только кнопка **Цвет**).

В подразделе **Дополнительно** (дополнительные параметры **Текстового чата**) вы сможете задать дополнительные настройки текстового чата:

- **Отображать имя перед моими сообщениями**. Включите эту опцию, если вы хотите, чтобы ваше имя (ник) отображались в начале вашего сообщения.
- **Отображать время перед сообщениями**. Включите эту опцию, чтобы перед сообщениями текстового чата (вашими и входящими) отображалось время.
- **Подтверждать отключение при открытых приватных каналах**. Включите данную опцию, чтобы вам выдавалось окно подтверждения отключения от чата при открытом приватном канале (сеансе общения в текстовом чате).
- **Подтверждать отключение при непрочитанных сообщениях**. Если в текстовом чате будут присутствовать непрочитанные сообщения – вам будет выдано окно подтверждения (при отключении от чата или закрытии программы).
- **Использовать специальные текстовые команды**. Если вы хотите использовать в текстовом чате специальные текстовые команды, включите данную опцию (описание текстовых команд приведено ниже в описании работы с Radmin Viewer).
- **Отображать текст справа налево**. Включите данную опцию для отображения текста в окне чата слева направо.

Если вы хотите хранить историю вашего общения в текстовом чате, установите галочку напротив **Сохранять сообщения в журнал**. Выберите один из двух форматов хранения журнала – **HTML** или **Текстовый** — и укажите папку, в которой будет храниться журнал сообщения, нажав кнопку **Обзор**.

Настройка голосового чата

Вкладка **Голосовой чат** окна настроек программы. Здесь вы сможете указать настройки голосового чата. Настройки данного раздела аналогичны настройкам для текстового чата – вы сможете указать имя, информацию о себе и сообщения для статуса ‘Отошел’.

Вкладка **Звуковые устройства** (для **Голосового чата**). Здесь вы сможете выбрать **Устройство для воспроизведения звука** и **Устройства для записи звука**. Перемещая ползунок, вы сможете настроить **Уровень чувствительности микрофона** – рис. 7.6.

После настройки всех необходимых параметров нажмите кнопку **ОК**.

Рис. 7.6. Настройка чувствительности микрофона в Radmin Server

7.4. Настройка прав доступа к удаленному компьютеру

Теперь необходимо настроить права доступа к удаленному компьютеру. Нажмите кнопку **Права доступа**, перед вами откроется окно, показанное на рис. 7.7.

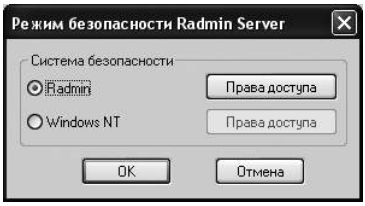


Рис. 7.7. Окно «Режим безопасности Radmin Server»

Рис. 7.8. Настройка прав доступа в Radmin Server

Как вы можете видеть, в данном окне вы можете настроить права доступа к Radmin Server для Radmin (при подключении к удаленному компьютеру вам необходимо будет указать логин и пароль) и Windows NT (вам необходимо указать, каким группам пользователей будет разрешено подключение к Radmin Server). Советую вам настраивать права доступа для варианта Radmin.

Выберите вариант Radmin и нажмите кнопку **Права доступа**, перед вами откроется окно, показанное на рис. 7.8.

Для примера настроим права доступа для двух пользователей *Администратор* (будут даны все права) и *Ученик*

(будет дано только право ‘Просмотр’, чтобы вы могли показать пользователю, подключившемуся к вашему компьютеру, работу с той или иной программой). Нажмите кнопку **Добавить** и в появившемся окне (рис. 7.9) укажите в качестве имени пользователя – *Администратор*. Затем укажите пароль и подтвердите его. Нажмите кнопку **ОК**.

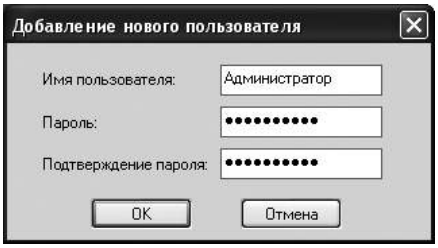


Рис. 7.9. Добавление нового пользователя

Нажмите кнопку **ОК** и установите галочку напротив **Полный доступ** в списке **Права пользователей** (все остальные галочки будут выставлены автоматически). Теперь добавим пользователя *Ученик*. Нажмите кнопку **Добавить**, укажите имя пользователя *Ученик* и пароль для него, после чего нажмите кнопку **ОК**. В списке **Права пользователей** установите галочку напротив **Просмотр** и напротив **Текстовый чат** и **Голосовой чат** (чтобы вы могли давать комментарии к своим действиям, при обучении удаленного пользователя).

Так, указывая различные наборы прав доступа, вы сможете создать учетные записи для всех пользователей, которым будет дано право доступа к вашему компьютеру.

Вернемся к окну настроек Radmin Server (рис. 7.2). Если вы приобрели лицензионную копию программы Radmin Server, вам необходимо активировать ее. Для этого нажмите кнопку **Активация** и укажите код активации Radmin Server. Если у вас нет соединения с Интернет, установите галочку напротив **Ручная активация**, после чего вы сможете **сохранить запрос на активацию в файл** или открыть имеющийся у вас **файл с лицензией**. После чего в окне настроек Radmin Server (рис. 7.2) будет отображена **информация о лицензии**.

Если вы хотите узнать IP-адрес вашего компьютера наведите курсор мыши на иконку Radmin Server в трее, и вам будет показано информационное сообщение с IP-адресом вашего компьютера – рис. 7.10.

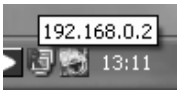


Рис. 7.10. Информация об IP-адресе компьютера, выдаваемая Radmin Server

IP-адрес компьютера вы также можете узнать при помощи средств Windows. Нажмите **Win + R**, введите команду ***cmd*** и нажмите клавишу «Enter». После чего в открывшемся окне введите команду ***ipconfig*** и нажмите клавишу «Enter».

Для остановки Radmin Server вы можете воспользоваться командой контекстного меню. Щелкните правой кнопкой мыши по иконке Radmin Server в трее и в появившемся списке выберите **Остановить Radmin Server**. Для запуска Radmin Server выполните **Программы → Radmin Sever 3 → Запустить Radmin Server**.

Для того чтобы посмотреть список входящих соединений, щелкните правой кнопкой мыши по иконке Radmin Server в трее и в появившемся контекстном меню выберите **Текущие соединения**.

Итак, мы установили и настроили Radmin Server, теперь нам необходимо установить и настроить Radmin Viewer – оба компьютера должны быть соединены по локальной сети или должны иметь подключение к Интернет.

7.5. Установка и настройка Radmin Viewer. Практика подключения к другому компьютеру

Стоит сразу сказать том, что Radmin Viewer в отличие от Radmin Server является абсолютно бесплатным. Вы можете установить Radmin Viewer на неограниченное количество компьютеров.

Для начала процесса установки Radmin Viewer вам необходимо запустить файл rview34ru.exe. В первом окне мастера установки нажмите кнопку **Далее**, после чего согласитесь с лицензионным соглашением и снова нажмите кнопку **Далее**. В третьем окне мастера установки Radmin Viewer укажите, для каких пользователей компьютера установить программу – только для вас или для всех пользователей. После чего нажмите кнопку **Далее**. В следующем окне укажите папку для установки программы, нажав кнопку **Обзор**, после чего нажмите кнопку **Далее**. Нажмите кнопку **Установить**, чтобы запустить процесс копирования файлов Radmin Viewer на ваш компьютер. По окончании процесса установки нажмите кнопку **Готово**, чтобы закрыть окно мастера установки Radmin Viewer.

Запустите Radmin Viewer, выполнив **Программы → Radmin Viewer 3 → Radmin Viewer 3**. Перед вами откроется окно Radmin Viewer 3 (рис. 7.11).

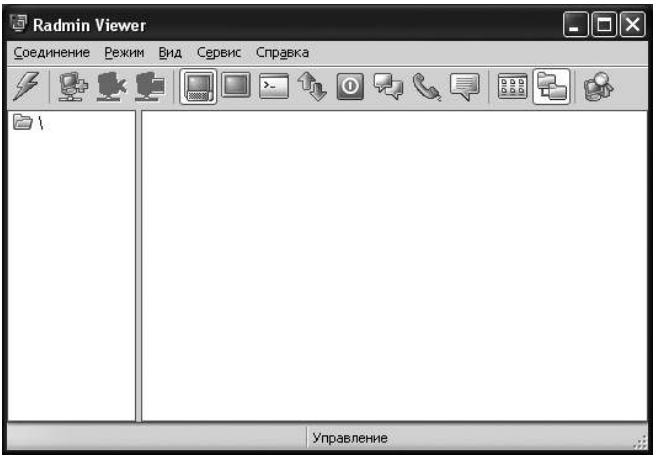


Рис. 7.11. Окно Radmin Viewer

Попробуем подключиться к удаленному компьютеру. На панели задач раскройте меню **Соединение** и выберите пункт **Соединиться с**. В появившемся окне укажите IP-адрес компьютера, к которому необходимо подключиться, в моем случае это 192.168.0.2 (рис. 7.12). Также вам необходимо указать режим подключения и порт для подключения (если при настройке Radmin Server вы указали значение, отличное от значения по умолчанию, снимите галочку напротив **По умолчанию** и в поле **Порт** укажите нужный номер порта).

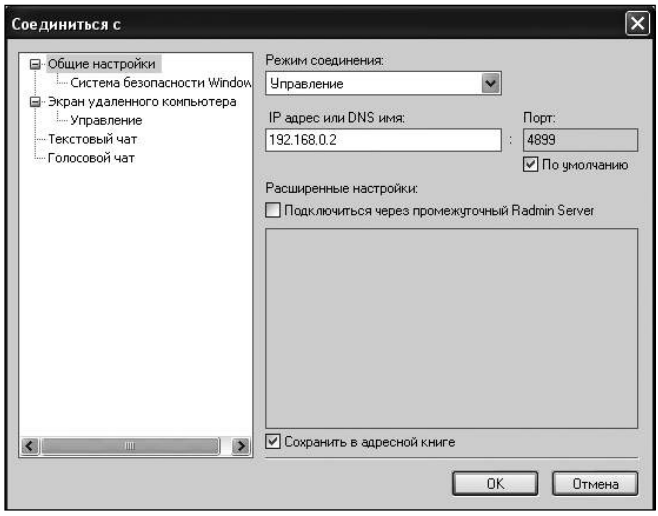


Рис. 7.12. Окно соединения с удаленным компьютером в Radmin Viewer

Если вы хотите сохранить введенное значение, оставьте установленной галочку напротив **Сохранить в адресной книге**, в противном случае снимите ее. Нажмите кнопку **ОК**. Программа попросит вас ввести логин и пароль для подключения к удаленному компьютеру – рис. 7.13. Чтобы при следующем подключении вновь не вводить логин, установите галочку напротив **Сохранить как данные по умолчанию**.

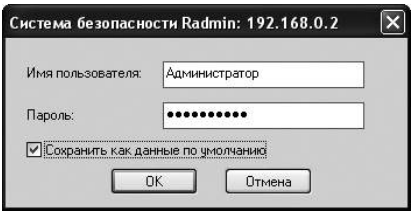


Рис. 7.13. Окно "Система безопасности Radmin Viewer"

Нажмите кнопку **ОК**. Если вы правильно указали параметры подключения, откроется окно, в котором будет показан удаленный рабочий стол – рис. 7.14.

В моем случае разрешение рабочего стола удаленного компьютера больше,

Рис. 7.14. Удаленный рабочий стол в окне Radmin Viewer

чем у компьютера, с которого производится подключение, поэтому изображение в окне Radmin Viewer выглядит бо́льшим по сравнению с изображением рабочего стола компьютера, с которого производится подключение. Это происходит потому, что выбран **Обычный** режим отображения – кнопка  . В Radmin Viewer существует 4 режима отображения:

- **Обычный** (кнопка ). В данном режиме изображение рабочего стола удаленного компьютера отображается в разрешении, установленном на удаленном компьютере.
- **С масштабированием** (кнопка ). Изображение с рабочего стола удаленного компьютера будет уменьшено/увеличено до размеров окна Radmin Viewer.
- **Полноэкранный** (кнопка ). В этом режиме изображение удаленного рабочего стола будет отображено *на весь экран*. В верхней части экрана будет расположена панель управления Radmin Viewer. В этом режиме изображение с рабочего стола удаленного компьютера будет передано в разрешении, установленном на удаленном компьютере.
- **Полноэкранный с масштабированием** (кнопка ). Изображение с рабочего стола удаленного компьютера будет увеличено/уменьшено до размеров экрана вашего монитора.

Настройка подключения к удаленному рабочему столу

Теперь подробно рассмотрим настройку подключения к удаленному рабочему столу и работу с Radmin Viewer. Закройте окно подключения к удаленному компьютеру и откройте окно программы Radmin Viewer, щелкнув левой кнопкой мыши по иконке программы в трее —  .

Добавим новую запись к списку подключений, для этого нажмите кнопку  или клавишу Insert или выполните **Соединение → Новое соединение**. Перед вами откроется окно, показанное на рис. 7.15.

В данном окне вы можете указать основные параметры соединения с удаленным рабочим столом. Все настройки в данном окне представлены в виде дерева (в левой части окна, показанного на рис. 7.15). Разберем их все по порядку:

1. **Общие настройки**. Здесь необходимо указать основные параметры подключения. В поле **Имя записи** укажите имя подключения к удаленному компьютеру (в списке подключений создаваемое вами подключение бу

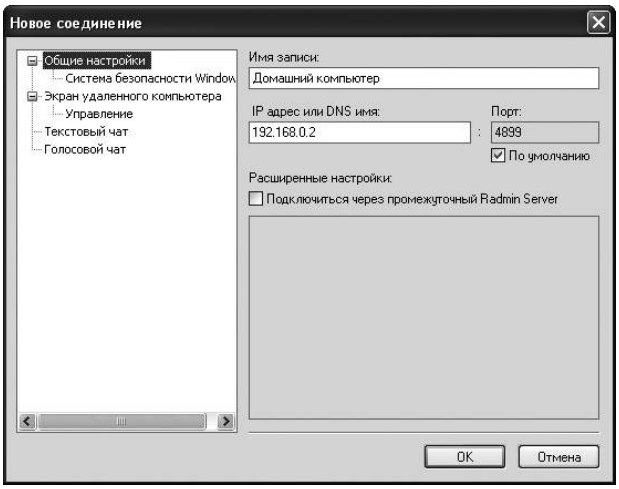


Рис. 7.15. Создание нового соединения в Radmin Viewer

1. дет отображаться под указанным вами именем). Укажите IP-адрес или DNS имя удаленного компьютера в поле с соответствующим названием. Если при настройке Radmin Server'а вы оставили порт по умолчанию, настройки порта менять не нужно, в противном случае снимите галочку напротив **По умолчанию** и укажите нужный порт. Если вы хотите подключиться к удаленному рабочему столу через промежуточный сервер Radmin, установите галочку напротив **Подключиться через промежуточный Radmin Server** и в списке выберите один из доступных промежуточных серверов Radmin, если таковых обнаружено не будет – список окажется пустым.

   Система безопасности Windows. Здесь вы можете указать параметры безопасности при подключении к удаленному рабочему столу. Вы можете отключить использование данных о вашей учетной записи Windows при подключении к удаленному рабочему столу, установив галочку напротив **Не использовать данные текущего пользователя**. Также вы сможете указать имя хоста для аутентификации по Kerberos в поле с соответствующим названием (если вы ничего не знаете про протокол аутентификации Kerberos – лучше оставьте это поле незаполненным).

2. **Экран удаленного компьютера**. Здесь вам необходимо указать параметры передачи изображения с рабочего стола удаленного компьютера. Очень важно верно задать параметры в данном разделе настроек. Если вы имеете хорошее (с высокой скоростью) подключение к удаленному рабочему столы вы можете указать максимальные настройки. Для подключений с низкой скоростью (в основном через Интернет) подберите оптимальные настройки для вашего подключения. Если для вас важ-

на экономия сетевого трафика – вам следует выбрать минимальные настройки.

- **Глубина цвета** – выберите одно из доступных значений (от 1 до 24), от значения этого параметра зависит качество передаваемого изображения и соответственно количество расходуемого на его передачу трафика.
- **Вид экрана**. Здесь вы можете указать, в каком режиме открывать окно соединения с удаленным компьютером: **Обычный**, **С масштабированием**, **Полноэкранный** и **Полноэкранный с масштабированием** (описание данных режимов приведено выше).
- **Максимальное количество обновлений экрана в секунду**. От значения параметра зависит частота обновления экрана удаленного компьютера и соответственно количество трафика, затрачиваемого на передачу данных с удаленного компьютера.

Управление. Здесь вы можете указать дополнительные параметры управления удаленным компьютером.

Режим отображения удаленного курсора. Здесь вам необходимо указать один из трех режимов отображения курсора в окне Radmin Viewer при подключении к удаленному компьютеру.

- **Не показывать удаленный курсор**. При выборе данного варианта удаленный курсор не будет отображаться в окне Radmin Viewer.
- **Локальный курсор принимает форму удаленного**. Данное значение установлено по умолчанию. В данном случае при попадании курсора в область окна Radmin Viewer он примет вид курсора, заданного на удаленном компьютере.
- **Отображать локальный и удаленный курсоры**. В данном режиме будут отображаться оба курсора —и локальный, и удаленный.

Передавать специальные сочетания клавиш. Данная опция установлена по умолчанию; когда она включена, все сочетания клавиш, вводимые вами на локальном компьютере, будут передаваться на удаленный компьютер.

3. **Текстовый чат**. В данном разделе настроек вам необходимо указать параметры текстового чата.
   - **Имя или псевдоним**. Укажите в данном поле имя, которое будет показано пользователю удаленного компьютера в текстовом чате.
   - **Информация о пользователе**. Укажите здесь дополнительную информацию о себе.

4. **Голосовой чат**. Здесь вам необходимо задать параметры голосового чата. Первые два из них (**Имя или псевдоним** и **Информация о пользователе**) аналогичны описанным параметрам текстового чата.

   Максимальная ширина канала, используемая голосовым чатом. Перемещая данный ползунок, укажите ширину канала (от этого будет зависеть качество передаваемого звука и соответственно количество, затрачиваемого на его передачу, трафика).

После того как вы укажите все необходимые параметры соединения нажмите кнопку **ОК**. Созданное соединение появится в окне Radmin Viewer – рис. 7.16.

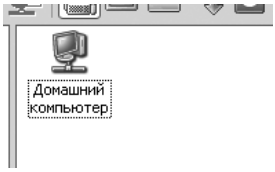


Рис. 7.16. Список соединений в Radmin Viewer

Если вы хотите удалить соединение из списка, выберите его, щелкнув по его значку левой кнопкой мыши, и нажмите клавишу Delete или нажмите кнопку  . Для изменения параметров выбранного соединения нажмите кнопку  . Вы можете создать ярлык для подключения к удаленному компьютеру прямо на рабочем столе. Для этого щелкните правой кнопкой мыши по значку подключения и в появившемся контекстном меню выберите **Создать ярлык на рабочем столе** и укажите режим подключения. После этого на рабочем столе появится ярлык, дважды щелкнув по которому левой кнопкой мыши, вы сможете открыть соединение с удаленным компьютером. Название ярлыка будет составляться из двух частей – названия подключения и режима.

7.6. Группировка списка подключений

Теперь стоит немного отвлечься и рассказать о группировке списка подключений. Вы могли обратить внимание, что при открытии Radmin Viewer в левой части экрана его окна находится панель со списком, в котором присутствует единственная запись —  . Выберите эту запись, щелкнув по ней левой кнопкой мыши, и нажмите клавишу «F7», чтобы создать новую папку для подключений. Укажите имя папки и нажмите клавишу Enter. Так вы можете создать несколько папок для различных типов подключений, что позволит вам быстрее находить нужное подключение – рис. 7.17.

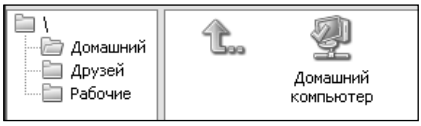


Рис. 7.17. Папка и подключения в ней (в программе Radmin Viewer)

7.7. Режимы управления удаленным рабочим столом и их включение

Режимы управления удаленным рабочим столом были рассмотрены нами ранее, при описании работы с Radmin Server. Теперь поговорим о включении этих режимов.

Включить тот или иной режим управления удаленным рабочим столом вы можете, выбрав его перед установкой соединения или в окне управления удаленным компьютером.

-  — режим управления.
-  — режим просмотра.
-  — открытие командной строки на удаленном компьютере.
-  — режим обмена файлами. При включении данного режима перед вами откроется окно показанное на рис. 7.18. В левой части данного окна отображаются данные локального компьютера, в правой – удаленного.

Рис. 7.18. Обмен файлами средствами Radmin

В данном окне вы не можете открывать файлы, расположенные на удаленном компьютере.

-  — выключение удаленного компьютера.

-  — открытие текстового чата.
-  — открытие голосового чата. Про работу в режимах текстового и голосового чата мы поговорим чуть ниже.
-  — отправка текстового сообщения пользователю удаленного компьютера. После нажатия данной кнопки перед вами откроется окно, в котором вы сможете написать текст сообщения для пользователя удаленного компьютера (рис. 7.19) и, нажав кнопку  , указать цвет текста сообщения.

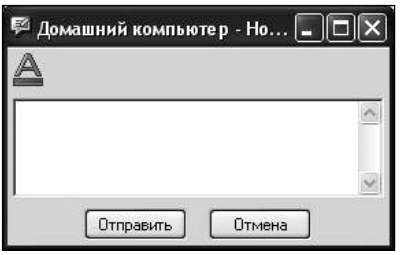


Рис. 7.19. Окно ввода текстового сообщения в Radmin Viewer

Глава 8.

Хакинг параметров безопасности Windows 8

Компоненты, обеспечивающие безопасность, являются одними из важнейших в современных операционных системах. Обычно по умолчанию эти компоненты настроены так, чтобы обеспечивать приемлемый уровень безопасности и не оказывать заметного влияния на производительность и удобство работы. Но иногда такого среднего уровня безопасности оказывается недостаточно, и в отдельных случаях операционная система настраивается таким образом, чтобы обеспечивалась максимальная безопасность, зачастую не только в ущерб удобству работы, но и ценой заметного снижения производительности системы. Конечно, рядовому пользователю такой уровень безопасности не нужен, но в некоторых случаях изменение всего нескольких параметров системы, отвечающих за безопасность могут заметно усилить защиту системы, практически никак не повлияв на удобство и скорость работы.

8.1. Пароли учетных записей

Параметры, собранные в узле **Конфигурация компьютера ⇒ Конфигурация Windows ⇒ Параметры безопасности ⇒ Политики учетных записей** (Computer Configuration ⇒ Windows Settings ⇒ Security Settings ⇒ Account Policies), предназначены для установки различных политик, связанных с паролями для входа в систему Windows. При использовании данных политик можно усложнить несанкционированный доступ к компьютеру.

Ведение журнала паролей

Настройка **Вести журнал паролей** (Enforce password history) определяет число новых уникальных паролей, которые назначаются пользователем до установки ранее использовавшегося пароля. Пользователь периодически может менять пароль для входа в систему. При этом он может использовать как новые пароли, так и ранее установленные. С помощью данной настройки устанавливается количество уникальных паролей (не использовавшихся ранее). Использовав установленное количество новых паролей, пользователь сможет задать ранее использовавшийся пароль.

Чтобы задать количество уникальных паролей, выполните следующие действия.

1. Откройте узел **Конфигурация компьютера ⇒ Конфигурация Windows ⇒ Параметры безопасности ⇒ Политики учетных записей ⇒ Политика паролей** (Computer Configuration ⇒ Windows Settings ⇒ Security Settings ⇒ Account Policies ⇒ Passwords policy).

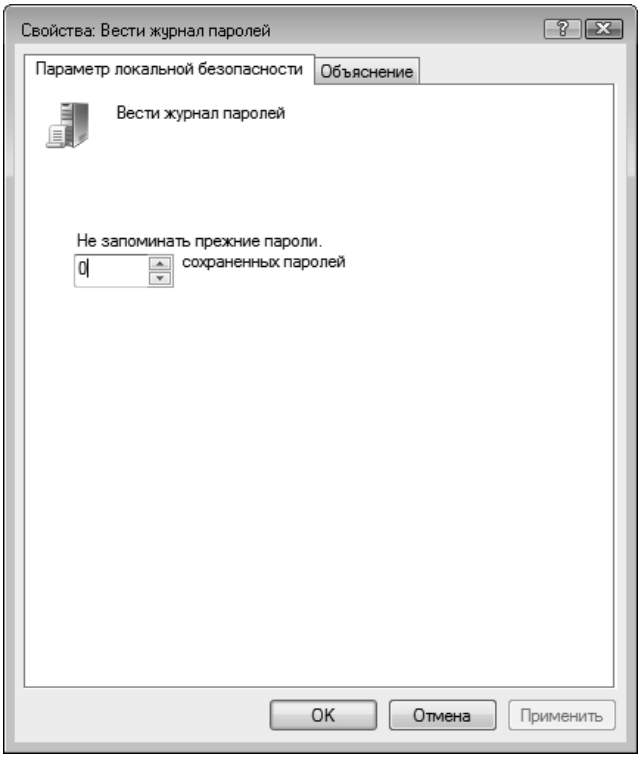


Рис. 8.1. ***Диалоговое окно настройки политики*** **Вести журнал паролей**

2. Дважды щелкните мышью по параметру **Вести журнал паролей** (Enforce password history). Появится диалоговое окно с единственным полем ввода (рис. 8.1).

По умолчанию в поле **Вести журнал для** (Keep password history for) указано значение 0 (ноль). Это означает, что журнал паролей не ведется, и пользователь может два и более раз подряд устанавливать один и тот же пароль для входа в систему. Увеличив это значение, например, до трех, вы зададите количество уникальных паролей, которые нужно будет установить, прежде чем захотите вернуться к ранее использовавшемуся паролю.

3. В поле **Вести журнал для** (Keep password history for) введите нужное количество паролей, которые будут храниться в журнале.

4. Нажмите кнопку **ОК**, чтобы применить изменения и закрыть диалоговое окно.

Теперь, если вы, не использовав указанное количество уникальных паролей, попытаетесь задать ранее использовавшийся пароль, на экране появится со-

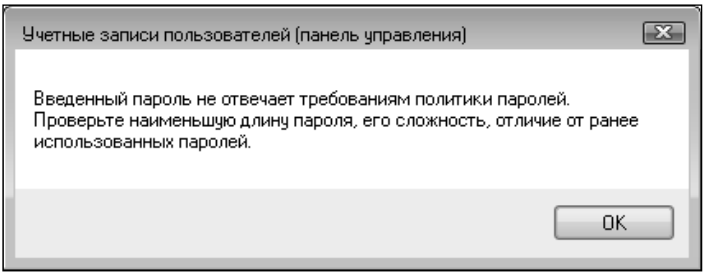


Рис. 8.2. ***Сообщение о том, что указанный пароль не соответствует установленным требованиям политики паролей***

общение о том, что указанный пароль не соответствует установленным требованиям политики паролей (рис. 8.2).

Закрыв появившееся сообщение, вы можете указать новый пароль. Если пароль будет уникальным или ранее вы уже использовали заданное количество уникальных паролей, данное сообщение не появится, и вы сможете установить желаемый пароль для входа в систему.

Изменения вступают в силу без перезагрузки компьютера.

Максимальный срок действия пароля

Параметр **Максимальный срок действия пароля** (Maximum password age) определяет, какое количество дней будет действовать пароль, установленный на вход в систему, до момента, когда пользователю будет предложено изменить пароль.

Диалоговое окно настройки **Максимальный срок действия пароля** (Maximum password age) вызывается щелчком по одноименному пункту в узле **Политика паролей** (Passwords policy).

Данное диалоговое окно содержит единственное поле со счетчиком. По умолчанию в данном поле установлено значение 0 (ноль). Это означает, что срок действия пароля неограничен. В данном поле вы можете указать нужный вам срок действия пароля (в днях). Максимальный срок действия пароля — 999 дней.

По истечении указанного периода при загрузке Windows вам будет предложено изменить пароль. Вы можете указать новый пароль или ввести тот же самый (если в настройке **Вести журнал паролей** (Enforce password history) указано значение 0 (ноль)).

Минимальный срок действия пароля

Настройка **Минимальный срок действия пароля** (Minimum password age) определяет срок, в течение которого пользователь должен использовать текущий пароль, прежде чем изменить его. Например, если установить минимальный срок действия пароля сроком на 7 дней, пользователь не сможет изменить пароль ранее, чем через семь дней.

Диалоговое окно данной настройки вызывается при двойном щелчке мышью по настройке **Минимальный срок действия пароля** (Minimum password age), расположенной в узле **Политика паролей** (Passwords policy).

В поле со счетчиком указывается минимальный срок действия пароля (в днях) от 1 до 998. Если в данном поле указать значение 0 (ноль), пользователь может изменять пароль в любое время без каких-либо ограничений.

Если пользователь попытается сменить пароль ранее указанного минимального срока (отсчет ведется от последней смены пароля), на экране появится сообщение о том, что указанный пароль не соответствует установленным требованиям политики паролей.

Минимальная длина пароля

Название настройки **Минимальная длина пароля** (Minimum password length) говорит само за себя. С помощью этой настройки задается минимальное количество знаков (букв или цифр), из которого может состоять пароль. Например, если вы зададите минимальную длину пароля в пять знаков, вы не сможете создать пароль, содержащий четыре и менее знаков. Ни для кого не является секретом, что чем длиннее пароль, тем сложнее его подобрать с целью несанкционированного доступа к компьютеру.

Диалоговое окно данной настройки вызывается двойным щелчком мыши по настройке **Минимальная длина пароля** (Minimum password length), расположенной в узле **Политика паролей** (Passwords policy).

Окно настройки содержит одно поле со счетчиком, в котором указывается минимально допустимая длина пароля. Если вы установите минимальную длину пароля, а затем попытаетесь указать новый пароль, длина которого ниже минимально допустимой, на экране появится сообщение о том, что указанный пароль не соответствует установленным требованиям политики паролей.

Минимальная длина пароля может составлять от 0 до 14 символов.

Требования сложности пароля

Настройка **Пароль должен отвечать требованиям сложности** (Password must meet complexity requirements), расположенная в узле **Политика паролей** (Passwords policy), позволяет исключить возможность ввода простых паролей. Многие пользователи создают пароли, совпадающие с именем учетной записи либо состоящие из одинаковых символов, например 11111. Злоумышленники в первую очередь пытаются подобрать пароль, используя подобные комбинации, а значит, такие пароли небезопасны.

При включении настройки **Пароль должен отвечать требованиям сложности** (Password must meet complexity requirements) пользователь не сможет создать пароль, если он не отвечает следующим требованиям:

- длина пароля должна составлять не менее шести символов;
- пароль не содержит имени учетной записи либо частей имени;
- содержать знаки трех из четырех категорий: латинские прописные буквы (A-Z), латинские строчные буквы (a-z), цифры (0-9), отличающиеся от букв и цифр знаки, например %, #, $.

Например, пароль **ABsa95** отвечает требованиям безопасности, поскольку он не совпадает с именем учетной записи, состоит не менее чем из шести символов, а также содержит и прописные, и строчные буквы, и цифры, то есть знаки из трех ранее указанных категорий.

Диалоговое окно настройки **Пароль должен отвечать требованиям сложности** (Password must meet complexity requirements) содержит всего один переключатель, с помощью которого можно включить либо отключить данную настройку. Если настройка включена, то при попытке создать пароль, не отвечающий требованиям сложности, на экране появится сообщение о том, что указанный пароль не соответствует установленным требованиям политики паролей.

Хранение паролей с использованием обратимого шифрования

Данная настройка определяет, будет ли использоваться метод обратимого шифрования для хранения паролей. Эта политика обеспечивает поддержку приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности.

Хранение паролей, использующих обратимое шифрование, не является безопасным, поэтому включение данной политики целесообразно только тогда,

когда требования приложения не станут более весомыми, чем требования по защите паролей.

8.2. Блокировка учетных записей

В узле **Политика блокировки учетных записей** (Account Lockout Policy) содержатся настройки, с помощью которых задаются параметры блокировки учетных записей.

Пороговое значение блокировки

Настройка **Пороговое значение блокировки** (Account lockout threshold) определяет количество неудачных попыток ввода пароля до блокировки системы. Диалоговое окно данной настройки вызывается при двойном щелчке мышью по настройке **Пороговое значение блокировки** (Account lockout threshold), расположенной в узле **Политика блокировки учетных записей** (Account Lockout Policy).

В диалоговом окне настройки **Пороговое значение блокировки** (Account lockout threshold) содержится всего одно поле со счетчиком. В данном поле указывается количество попыток неудачного ввода пароля, которое будет приводить к блокировке учетной записи.

Количество попыток ввода пароля может составлять от 0 до 999. При установке значения 0 (ноль) учетная запись не будет блокироваться вне зависимости от того, сколько раз был введен неправильный пароль. Иными словами, пользователь сможет вводить неверный пароль сколько угодно без каких-либо ограничений. Во всех остальных случаях количество попыток ввода неверного пароля будет ограничено. После того, как попытки ввода неверного пароля будут исчерпаны, учетная запись будет заблокирована. Разблокировка учетной записи может быть осуществлена администратором, либо разблокировка произойдет автоматически через заданное время.

Нетрудно догадаться, что блокировка учетной записи существенно усложняет процесс подбора пароля.

Продолжительность блокировки учетной записи

Изменение данной настройки возможно лишь, если в настройке **Пороговое значение блокировки** (Account lockout duration), описанной выше, установлено значение, отличное от нуля, то есть режим блокировки учетной записи включен. Настройка **Продолжительность блокировки учетной записи** (Account lockout duration) определяет интервал времени, в течение которо-

го учетная запись будет заблокирована в случае ввода неверного пароля заданное количество раз.

Продолжительность блокировки может составлять от нуля до 99999 минут. Если вы установите значение 0 (ноль), учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее вручную.

При блокировке учетной записи в окне приветствия Windows появляется сообщение о том, что учетная запись заблокирована и не может быть использована для входа в сеть. Следующие попытки входа в систему будут возможны по истечении указанного интервала блокировки.

Время до сброса счетчика блокировки

Настройка **Время до сброса счетчика блокировки** (Reset account lockout counter after) определяет интервал времени, через который будет осуществлен сброс счетчика блокировки после неудачной попытки ввода пароля. Допустим, у нас установлена блокировка учетной записи после трех неудачных попыток ввода пароля. И время до сброса счетчика блокировки установлено равным пяти минутам. Мы ввели неверный пароль (у нас осталось две попытки), но повторно пытаться не стали. По прошествии пяти минут счетчик блокировки сбрасывается, и у нас снова есть три попытки.

Интервал времени до сброса счетчика блокировки может быть назначен от 1 до 99999 минут.

8.3. Протоколирование действий в системе

Политики аудита расположены в узле **Конфигурация компьютера ⇒ Конфигурация Windows ⇒ Параметры безопасности ⇒ Локальные политики ⇒ Политики аудита** (Computer Configuration ⇒ Windows Settings ⇒ Security Settings ⇒ Local Policies ⇒ Audit Policy). В данном узле содержится несколько настроек, и каждая из них определяет, будет ли фиксироваться в системе то или иное событие. Тип события как раз и определяется конкретной настройкой. Все настройки в данном узле содержат одинаковые диалоговые окна, в которых присутствуют два флажка: **Успех** (Success) и **Отказ** (Failure) (рис. 8.3).

Если установлен флажок **Успех** (Success), будет фиксироваться успешное, то есть выполненное событие. Если же установить флажок **Отказ** (Failure), то фиксироваться будет так же незаконченное, то есть невыполненное событие, но при условии, что пользователь пытался выполнить это событие. Например, если установить флажок **Успех** (Success) в диалоговом окне на-

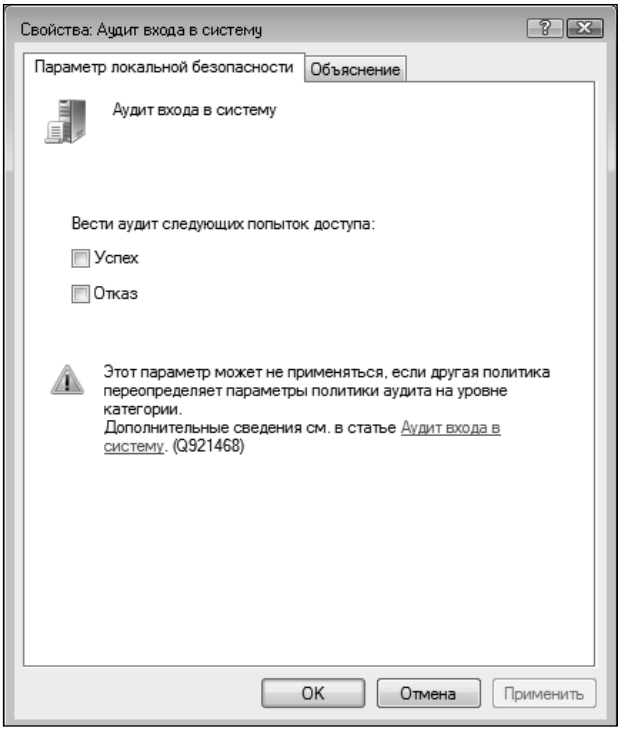


Рис. 8.3. ***Пример диалогового окна настройки одной из политик аудита***

стройки **Аудит входа в систему** (Audit account logon events), система будет фиксировать (администратор сможет просмотреть эти события) успешные входы и выходы пользователей в Windows. Неудачные попытки входа (например, в случае неправильно набранного пароля) фиксироваться не будут. Однако, если установить флажок **Отказ** (Failure), фиксироваться будут в том числе и неудачные попытки входа в систему.

Приведем настройки, доступные в узле **Политики аудита** (Audit Policy):

1. **Аудит входа в систему** (Audit account logon events). Аудиту подвергается успешный или не успешный вход в операционную систему, а также выход из нее;
2. **Аудит доступа к объектам** (Audit object access). Данная настройка выполняет аудит доступа к объектам, не относящимся к Active Directory. В качестве объектов могут выступать файлы, папки, принтеры, разделы системного реестра;
3. **Аудит доступа к службе каталогов** (Audit directory service access). Настройка выполняет аудит доступа к объектам, относящимся к Ac-

tive Directory, для которых указан список управления доступом;

4. **Аудит изменения политики** (Audit policy change). Нетрудно догадаться, что данная настройка ведет аудит изменения политик пользователем;
5. **Аудит изменений привилегий** (Audit privilege use). Даная настройка определяет, будет ли выполняться аудит попыток изменения политики назначения прав пользователям;
6. **Аудит отслеживания процессов** (Audit process tracking). Выполняет аудит событий, связанных с процессами, например, создания или завершения процесса, а также обработке дублирований и непрямого доступа к объектам;
7. **Аудит системных событий** (Audit system events). Выполняет аудит системных событий. К системным событиям можно отнести изменение системного времени, запуск и отключение системы безопасности, загрузку компонентов расширяемой проверки подлинности, потерю отслеживаемых событий, а также превышение размера журнала установленного уровня.
8. **Аудит событий входа в систему** (Audit logon events). Эта настройка определяет, будет ли операционная система выполнять аудит каждый раз при проверке данным компьютером учетных данных. При использовании этой политики создается событие для локального и удаленного входа пользователя в систему;
9. **Аудит управления учетными записями** (Audit account management). Данная политика определяет, будут ли создаваться события при управлении учетными записями в системе и, соответственно, будет ли выполняться аудит этих событий.

8.4. Назначение прав пользователя

В узле **Конфигурация компьютера ⇒ Конфигурация Windows ⇒ Параметры безопасности ⇒ Локальные политики ⇒ Назначение прав пользователя** (Computer Configuration ⇒ Windows Settings ⇒ Security Settings ⇒ Local Policies ⇒User Rights Assignment) сосредоточено более сорока политик, с помощью которых можно задать или ограничить права пользователя. То есть вы можете разрешить или запретить выполнять определенные действия для категорий пользователей или конкретных пользователей.

Все настройки имеют одинаковые диалоговые окна, в которых приводится список категорий пользователей. Чтобы разрешить выполнять выбран-

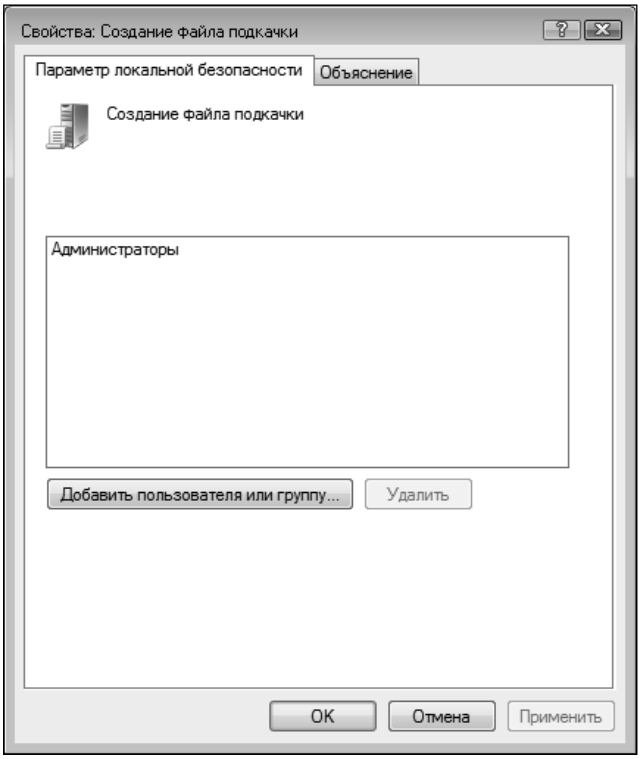


Рис. 8.4. ***Диалоговое окно настройки политики*** **Создание файла подкачки** ***(Create a page file)***

ное действие, нужно добавить в список или категорию пользователей, или конкретного пользователя. Например, настройка **Создание файла подкачки** (Create a page file) определяет пользователей, которым разрешено создавать файлы подкачки (рис. 8.4). По умолчанию данное действие позволено выполнять только администраторам.

Если мы хотим добавить категорию пользователей, которым разрешено создавать файлы подкачки, нужно выполнить следующие действия:

1. В диалоговом окне настройки данной политики нажать кнопку **Добавить пользователя или группу** (Add User or Group). На экране появится диалоговое окно выбора пользователей или групп (рис. 8.5).
2. С помощью появившегося диалогового окна найти пользователей или группы, которых хотите добавить в список разрешений.
3. Нажать кнопку **ОК**, чтобы закрыть диалоговое окно выбора пользователей или групп.

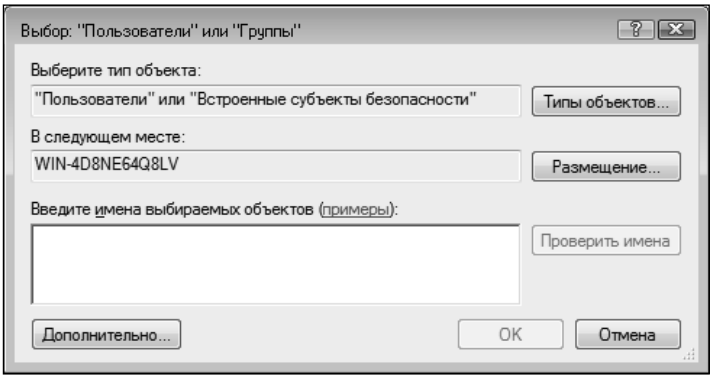


Рис. 8.5. ***Диалоговое окно выбора пользователей или групп***

4. Убедиться, что выбранные вами пользователи или группы появились в списке диалогового окна настройки политики.

5. Нажать кнопку **ОК**, чтобы закрыть диалоговое окно.

Группы пользователей можно выбрать, нажав кнопку **Типы объектов** (Object Types) в диалоговом окне выбора пользователей или групп. При нажатии данной кнопки появляется диалоговое окно со списком типов объектов. Для тех типов, которые вы хотите выбрать, следует установить флажки. Также вы можете добавить конкретных пользователей, выполнив их поиск на локальном и сетевых компьютерах.

С помощью кнопки **Размещение** (Locations) выбирается размещение пользователя (проще говоря — имя компьютера в сети или рабочая группа, в которой следует выполнить поиск имен). А с помощью кнопки **Проверить имена** (Check Names) выполняется проверка имен, указанных в поле слева. Проверка имен выполняется в размещении, указанном вами с помощью диалогового окна, появляющегося при нажатии кнопки **Размещение** (Locations).

Далее перечислим политики, расположенные в рассматриваемом нами узле:

- **Архивация файлов и каталогов** (Back up files and directories). Данная политика определяет, какие пользователи могут игнорировать разрешения для файлов, папок и других объектов с целью архивации системы;

- **Блокировать страницы в памяти** (Lock pages in memory). Эта политика определяет пользователей и группы, которые могут использовать процессы для сохранения данных в физической памяти для предотвращения сброса этих данных в виртуальную память на диске. Блокировка страниц в памяти уменьшает свободный объем ОЗУ, что сказывается на снижении быстродействия системы;

- **Восстановление файлов и каталогов** (Restore files and directories). Эта политика определяет пользователей, которым разрешено восстанавливать данные из ранее созданных архивных копий файлов и папок;
- **Вход в качестве пакетного задания** (Log on as a batch job). С помощью этой политики можно определить пользователей, которым разрешен вход в систему с помощью средства, использующего очередь пакетных заданий;
- **Вход в качестве службы** (Log on as a service). Данная политика позволяет субъекту безопасности (Локальная система, Локальная служба, Сетевая служба) входить в систему в качестве службы;
- **Выполнение задач по обслуживанию томов** (Perform volume maintenance tasks). Эта политика определяет пользователей, которым разрешено выполнять обслуживание томов, например, запускать удаленную дефрагментацию;
- **Добавление рабочих станций к домену** (Add workstations to domain). Название данной политики говорит само за себя (впрочем, как и большинства других политик). Данная политика определяет пользователей, которые имеют право добавлять рабочие станции в домен;
- **Доступ к диспетчеру данных от имени доверенного вызывающего** (Access Credential Manage as a trusted caller). Эта политика используется диспетчером учетных данных в ходе архивации и восстановления. Если добавить разрешения другим субъектам, учетные данные, сохраненные другими пользователями, могут быть скомпрометированы. Проще говоря, без особой необходимости эту настройку лучше не трогать;
- **Доступ к компьютеру из сети** (Access this computer from the network). Название этой политики вполне понятно. Она определяет, какие группы и пользователи могут подключаться к данному компьютеру по сети. То есть данной политикой вы можете ограничить круг пользователей, которые могут подключиться к конкретному компьютеру;
- **Завершение работы системы** (Shut down the system). Политика определяет пользователей и группы, которые могут завершить работу в операционной системе с помощью команды **Завершить работу** (Shut down). Проще говоря — корректно выйти из Windows;
- **Загрузка и выгрузка драйверов устройств** (Load and unload device

drivers). С помощью данной политики можно назначить права на динамическую загрузку или выгрузку драйверов устройств. По умолчанию такую привилегию имеет только администратор. Политика не распространяется на драйверы устройств Plug and Play;

- **Замена маркера уровня процесса** (Replace a process level token). Эта политика позволяет определить учетные записи, которым позволено вызывать процедуру API-интерфейса CreateProcessAsUser(). Данный интерфейс позволяет одной службе запускать другую;
- **Запретить вход в систему через службу удаленных рабочих столов** (Deny log on through Remote Desktop Services). Данная политика позволяет указать пользователей и группы, которым будет запрещено входить в систему как клиенту служб удаленных столов;
- **Запретить локальный вход** (Deny log on locally). Очень простая политика. С ее помощью можно определить пользователей и группы, которым будет отказано во входе в систему;
- **Изменение метки объекта** (Modify an object label). Эта политика определяет пользователей, которым разрешено изменять метки целостности объектов, владельцами которых являются другие пользователи. Примеры объектов — файлы, разделы реестра или процессы;
- **Изменение системного времени** (Change the system time). Эта политика определяет пользователей, которым разрешено изменять системное время и дату. По умолчанию привилегии применяются к администраторам и локальной службе;
- **Изменение часового пояса** (Change the Time Zone). Дает право на изменение часового пояса. По умолчанию право распространяется, в том числе, и на пользователей без прав администратора;
- **Локальный вход в систему** (Allow log on locally). С помощью данной политики можно указать пользователей или группы, которым разрешен вход в систему;
- **Настройка квот памяти для процесса** (Adjust memory quotas for a process). Здесь можно назначить пользователей и группы, которым разрешено изменять максимальный объем памяти, используемый процессом. По умолчанию разрешение выдано администраторам, а также локальным и сетевым службам;
- **Обход перекрестной проверки** (Bypass traverse checking). Политика определяет пользователей, которым разрешено производить обзор деревьев каталога при отсутствии разрешения на каталог. При этом пользователю не дается право на просмотр содержимого каталога;

- **Отказать в доступе к этому компьютеру из сети** (Deny access to this computer from the network). Название политики вполне однозначно. Здесь можно указать пользователей или группы, которые не смогут подключиться к компьютеру из сети. По умолчанию отказ в доступе распространяется на группу **Гость** (Guest);
- **Отказ во входе в качестве пакетного задания** (Deny log on as a batch job). Политика, обратная политике **Вход в качестве пакетного задания** (Log on as a batch job). То есть здесь вы, наоборот, указываете пользователей, которым запрещен вход в систему в виде пакетного задания;
- **Отказать во входе в качестве службы** (Deny log on as a service). Определяет пользователей или группы, которым будет отказано в регистрации процесса как службы. Политика не применяется к системе, а также локальной и сетевой службе;
- **Отключение компьютера от стыковочного узла** (Remove computer from docking station). С помощью этой политики можно назначить пользователей и группы, которым разрешено отстыковать портативный компьютер от стыковочного узла без выполнения входа в систему;
- **Отладка программ** (Debug programs). Дает право на подключение отладчика к процессу или ядру;
- **Принудительное удаленное завершение работы** (Force shutdown from a remote system). Нетрудно догадаться, что с помощью этой политики можно назначить пользователей, которые могут удаленно завершить работу на данном компьютере. По умолчанию разрешение дано только администраторам;
- **Смена владельцев файлов и других объектов** (Take ownership of files or other objects). Политика позволяет назначить пользователей, которые могут стать владельцами любого защищенного объекта в системе. Например, вы можете назначить пользователя, который будет иметь право изменять собственника файла или папки. По умолчанию разрешение дано администраторам;
- **Создание аудитов безопасности** (Generate security audits). Политика определяет субъекты, которые будут использоваться процессом для добавления в журнал безопасности. По умолчанию разрешение выдано локальной и сетевой службе;
- **Создание файла подкачки** (Create a pagefile). Дает право на управление (создание, изменение и удаление) файлом подкачки Windows.

По умолчанию разрешение дано администраторам;

- **Увеличение приоритета выполнения** (Increase scheduling priority). Политика определяет пользователей, которым разрешено использовать процесс, дающий право на повышение приоритета выполнения другого процесса;
- **Увеличение рабочего набора процессов** (Increase a process working set). Дает право на уменьшение или увеличение размера рабочего набора процесса, то есть набора страниц памяти, видимых процессу в физической оперативной памяти;
- **Управление аудитом и журналом безопасности** (Manage auditing and security log). Ранее мы рассматривали политики аудита. Данная политика как раз определяет пользователей, которые могут управлять политиками аудита. По умолчанию разрешение выдано администраторам.

8.5. Параметры безопасности

В узле **Конфигурация компьютера ⇒ Конфигурация Windows ⇒ Параметры безопасности ⇒ Локальные политики ⇒ Параметры безопасности** (Computer Configuration ⇒ Windows Settings ⇒ Security Settings ⇒ Local Policies ⇒ Security Options) сосредоточено огромное количество различных политик, отвечающих за безопасность данных и работы на компьютере. Диалоговые окна настройки политик достаточно просты и в большинстве случаев содержат единственный элемент управления: переключатель, раскрывающийся список, поле ввода или поле со счетчиком (рис. 8.6).

Перечислим политики, расположенные в узле **Параметры безопасности** (Security Options):

- **DCOM: Ограничения компьютера на доступ в синтаксисе SDDL** (DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax). Позволяет запретить или разрешить пользователям или группам пользователей локальный и удаленный доступ к COM-компонентам;
- **DCOM: Ограничения компьютера на запуск в синтаксисе SDDL** (DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax). Позволяет ограничить или разрешить пользователям или группам пользователей локальную или удаленную активацию и запуск COM-компонентов;
- **Аудит: аудит доступа глобальных системных объектов** (Audit: Audit the access of global system objects). С помощью данной полити-

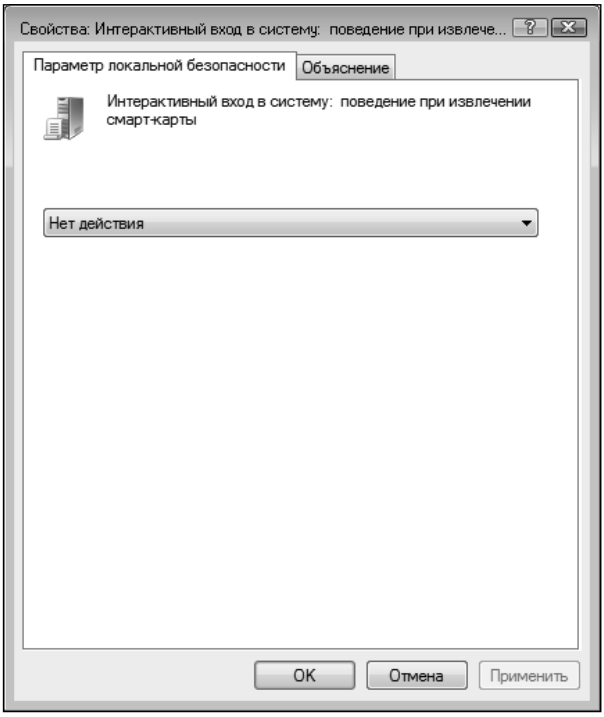


Рис. 8.6. ***Диалоговое окно настройки одной из политик*** **Параметры безопасности**

ки включается или отключается аудит доступа к глобальным системным объектам — мьютексам, семафорам и так далее;

- **Аудит: Аудит прав на архивацию и восстановление** (Audit: Audit the use of Backup and Restore privilege). С помощью данной политики можно включить или отключить аудит использования всех прав пользователя, включая архивацию и восстановление данных;
- **Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности** (Audit: Shut down system immediately if unable to log security audits). Если включить данную политику, то в случае невозможности системы внести запись о событии, подлежащем аудиту, происходит отключение системы. Одна из причин невозможности протоколирования событий — переполнение журнала аудита безопасности;
- **Доступ к сети: разрешить трансляцию анонимного SID в имя** (Network access: Allow anonymous SID/name translation). SID — идентификатор безопасности, соответствующий учетной записи пользователя. В операционных системах Windows идентификаторы безо-

пасности создаются в момент создания учетной записи пользователя, но для встроенных учетных записей, например **Администратор** (Administrator), они одинаковы, даже если их переименовать. Если включить данную политику, то по идентификатору SID можно получить реальное имя встроенной учетной записи администратора и использовать его в дальнейшем для проведения атак на компьютер;

- **Завершение работы: очистка файла подкачки виртуальной памяти** (Shutdown: Clear virtual memory pagefile). Если данная политика включена, при завершении работы системы автоматически будет выполняться очистка файла подкачки виртуальной памяти;
- **Завершение работы: разрешить завершение работы системы без выполнения входа в систему** (Shutdown: Allow system to be shut down without having to log on). По умолчанию действие этой политики не определено. Если включить данную политику, на экране входа в Windows появится команда для выхода из системы. То есть пользователь сможет выгрузить Windows, даже не входя в операционную систему;
- **Интерактивный вход в систему: поведение при извлечении смарт-карты** (Interactive logon: Smart card removal behavior). Данная политика определяет, что произойдет при извлечении смарт-карты. При извлечении смарт-карты может выполняться блокировка рабочей станции, принудительный выход из системы или отключение от системы (в случае удаленного сеанса служб удаленных рабочих столов);
- **Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему** (Interactive logon: Message title for users attempting to log on). Данная политика используется только, если в политике **Интерактивный вход в систему: текст сообщения для пользователей при входе в систему** (Interactive logon: Message text for users attempting to log on) указан какой-либо текст. Эта политика задает текст заголовка для сообщения, которое выводится в окне входа в Windows;
- **Интерактивный вход в систему: количество предыдущих подключений к КЭШу** (Interactive logon: Number of previous logons to cache (in case domain controller is not available)). Если компьютер подключен к локальной сети, использующей контроллер домена, то при входе пользователя в систему регистрационные данные будут проверяться на контроллере домена. На случай недоступности контроллера домена данные о предыдущих входах так же сохраняются на ком-

пьютере локально. Данная политика отвечает за количество сохраненных локально сведений о входе пользователя в систему на случай отказа контроллера домена;

- **Интерактивный вход в систему: напоминать пользователю об истечении срока действия пароля** (Interactive logon: Prompt user to change password before expiration). С помощью данной политики можно установить, за сколько дней до истечения срока действия пароля пользователь будет получать напоминание об окончании срока действия пароля. Напоминание происходит при входе пользователя в систему;
- **Интерактивный вход в систему: не отображать последнее имя пользователя** (Interactive logon: Do not display last user name). Данная политика позволяет включить или отключить режим отображение в окне входа в Windows имени последнего пользователя, выполнившего вход в систему;
- **Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL** (Interactive logon: Do not require CTRL+ALT+DEL). По умолчанию поведение политики не определено, и нажатия указанного сочетания клавиш для входа в систему не требуется, как это требовалось по умолчанию в Windows 2000. Однако вы можете включить запрос на нажатие сочетания клавиш **Ctrl**+**Alt**+**Del** для входа в систему;
- **Интерактивный вход в систему: отображать сведения о пользователе, если сеанс заблокирован** (Interactive logon: Display user information when the session is locked). С помощью данной политики вы можете задать тип сведений, которые будут отображаться на экране при заблокированном сеансе. На экране может отображаться выводимое имя пользователя, а также имена домена и пользователя, либо только имя пользователя. Также вы можете отключить вывод каких-либо сведений о пользователе;
- **Интерактивный вход в систему: текст сообщения для пользователей при входе в систему** (Interactive logon: Message text for users attempting to log on). С помощью данной политики можно указать текст, который будет выводиться на экране входа в Windows. Данный текст может содержать, например, какие-либо предупреждения или указания для всех пользователей, пытающихся войти в систему;
- **Интерактивный вход в систему: Требовать проверки на контроллере домена для отмены блокировки компьютера** (Interactive logon: Require Domain Controller authentication to unlock). Данная полити-

ка определяет, будет ли использоваться проверка на контроллере домена регистрационных данных для разблокировки компьютера или для этого будут использоваться регистрационные данные, кэшированные на данном компьютере;

- **Интерактивный вход: требовать смарт-карту** (Interactive logon: Require smart card). Данная политика определяет, будет ли требоваться смарт-карта для входа пользователя в систему. Если переключатель установлен в положение **Включен** (On), вход в систему без использования смарт-карты будет невозможен;
- **Клиент сети Microsoft: использовать цифровую подпись (всегда)** (Microsoft network client: Digitally sign communications (always)). Данный параметр определяет, будет ли использоваться цифровая подпись для пакетов данных, передаваемых по протоколу SMB — протоколу удаленного доступа к файлам, принтерам и сетевым ресурсам используемому в сетях. Если включить этот параметр, то данный протокол будет использоваться только для обмена данными с компьютерами, поддерживающими подпись пакетов;
- **Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера)** (Microsoft network client: Digitally sign communications (if server agrees)). При включении этого параметра клиентский компьютер перед обменом данными с сервером по протоколу SMB будет согласовывать использование цифровой подписи пакетов с сервером и использовать обмен подписанными пакетами данных, если такая возможность имеется. В противном случае пакеты данных не будут подписываться;
- **Сетевой клиент Майкрософт: отправить незашифрованный пароль для подключения к SMB-серверам сторонних компаний** (Microsoft network client: Send unencrypted password to connect to third-party SMB servers). Включение данной политики позволит отправлять пароль незашифрованным на SMB-сервер, не поддерживающий шифрование пароля;
- **Консоль восстановления: разрешить автоматический вход администратора** (Recovery console: Allow automatic administrative logon). Если политика включена, система не будет требовать пароль для входа учетной записи «Администратор»;
- **Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам** (Recovery console: Allow floppy copy and access to all drives and all folders). При включении данной политики становится доступной команда **SET** в консоли восстановления, с помо-

щью которой можно, например, использовать подстановочные знаки для некоторых команд, разрешить доступ к любым файлам и папкам, разрешить копировать файлы на съемные носители, отменить предупреждения при перезаписи уже существующих файлов;

- **Контроллер домена: запретить изменение паролей учетных записей компьютера** (Domain controller: Refuse machine account password changes). При включении этой политики пароли пользователей можно поменять только на контроллере домена;
- **Контроллер домена: разрешить операторам сервера задавать выполнение заданий по расписанию** (Domain controller: Allow server operators to schedule tasks). В операционных системах Windows помимо Планировщика заданий есть так же консольная утилита AT, обладающая схожими возможностями. При включении данной политики операторы контроллера домена имеют возможность выполнять различные команды по расписанию, используя эту утилиту;
- **Контроллер домена: требования цифровой подписи для LDAP-сервера** (Domain controller: LDAP server signing requirements). Если включить данный параметр, то сервер LDAP будет требовать у клиентов цифровую подпись для пакетов данных при подключении;
- **Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав** (User Account Control: Detect application installations and prompt for elevation). Если политика включена, то при установке приложений, если для продолжения выполнения установки требуется повышение прав, на экране появляется запрос на ввод имени и пароля администратора;
- **Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав** (User Account Control: Switch to the secure desktop when prompting for elevation). При включении этой политики все запросы, связанные с повышением прав, будут выводиться на безопасный рабочий стол, то есть рабочий стол пользователя будет отключаться, как при настройках контроля учетных записей по умолчанию;
- **Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором** (User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode). Эта политика определяет метод выведения запроса на повышение прав для администраторов. Возможно несколько вариантов от отсутствия запроса до требования ввода администраторского пароля на безопасном рабочем столе;

- **Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей** (User Account Control: Behavior of the elevation prompt for standard users). Данная политика определяет метод вывода запроса на повышение прав для пользователей. Запросы могут либо отклоняться, либо выводиться на рабочий стол, либо на безопасный рабочий стол;
- **Контроль учетных записей: повышать права только для UIAccess-приложений, установленных в безопасном местоположении** (User Account Control: Only elevate UIAccess applications that are installed in secure locations). При включении данной политики программы могут повышать права только в том случае, если такая необходимость указана разработчиком, а также если данные программы установлены в каталоги Program Files и Windows;
- **Контроль учетных записей: повышение прав только для подписанных и проверенных исполняемых файлов** (User Account Control: Only elevate executable files that are signed and validated). При включении данной политики повысить права могут только подписанные программы с верной электронной подписью;
- **Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в размещение пользователя** (User Account Control: Virtualize file and registry write failures to per-user locations). Данный параметр служит для уменьшения опасности программ. По умолчанию он включен, и если программа, не имеющая прав на запись данных в папку Program Files, Windows или в ветвь реестра HKLM\Software\, пытается выполнить такую операцию, то эти данные будут перенаправлены в пользовательскую область. Если параметр отключить, то такая операция будет завершаться ошибкой;
- **Контроль учетных записей: разрешать UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол** (User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop). При включении данного параметра UIAccess-приложения могут выводить запросы на повышение прав на обычный рабочий стол, если данная возможность не запрещена политикой **Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав** (User Account Control: Switch to the secure desktop when prompting for elevation). При отключенном параметре данной политики запросы на повышение прав будут выводиться UIAccess-приложениями, как и остальными программами на безопасный рабочий стол, если пользователь его не отключил;

- **Контроль учетных записей: использование режима одобрения администратором для встроенной учетной записи администратора** (User Account Control: Use Admin Approval Mode for the built-in Administrator account). При включении данного параметра для встроенной учетной записи Администратора будут выводиться запросы на подтверждение повышения прав для операций, как и для обычных учетных записей администраторов;
- **Параметры системы: использовать правила сертификатов для исполняемых файлов Windows для политик ограниченного использования программ** (System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies). Если включить данный параметр, то при попытке запуска программы будет проводиться проверка ее цифровой подписи, а также выполняться правила сертификатов — тип правил ограниченного использования программ, позволяющих запретить или разрешить выполнение программ с определенными цифровыми подписями;
- **Параметры системы: необязательные подсистемы** (System settings: Optional subsystems). Эта политика позволяет перечислить необязательные подсистемы — средства для запуска различных видов программ. По умолчанию в списке присутствует только Posix — подсистема для запуска специально подготовленных программ, написанных для операционных систем семейства Unix;
- **Сервер сети Microsoft: время бездействия до приостановки сеанса** (Microsoft network server: Amount of idle time required before suspending a session). Данный параметр позволяет установить время простоя до отключения сервером сеанса по протоколу SMB;
- **Сервер сети Microsoft: использовать цифровую подпись (всегда)** (Microsoft network server: Digitally sign communications (always)). Если данный параметр включен, то сервер откажет в соединении клиентам, не согласившимся на цифровую подпись пакетов данных;
- **Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента)** (Microsoft network server: Digitally sign communications (if client agrees)). Если включить данный параметр, то сервер будет согласовывать использование цифровой подписи пакетов данных с клиентами, в противном случае подпись сервером не будет использоваться. Эта политика обычно включается на контроллерах доменов;
- **Сетевой сервер (Майкрософт): отключать клиентов по истечении разрешенных часов входа** (Microsoft network server: Disconnect cli-

ents when logon hours expire). При включении этого параметра клиенты будут автоматически отключаться от сервера по истечении заданного для их учетных записей времени входа;

- **Сетевая безопасность: минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC)** (Network security: Minimum session security for NTLM SSP based (including secure RPC) clients). Данный параметр позволяет определить, какие типы протоколов должен использовать сервер, с которым клиент желает установить соединение;
- **Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC)** (Network security: Minimum session security for NTLM SSP based (including secure RPC) servers). Параметр аналогичный предыдущему, но для сервера. Если клиент не согласовывает с сервером какой-либо из указанных типов шифрования, то ему будет отказано в соединении;
- **Сетевая безопасность: настройка типов шифрования, разрешенных Kerberos** (Network security: Configure encryption types allowed for Kerberos). Данный параметр позволяет задать типы шифрования, разрешенные к использованию в службе Kerberos;
- **Сетевая безопасность: не хранить хэш-значения LAN Manager при следующей смене пароля** (Network security: Do not store LAN Manager hash value on next password change). Данная политика отвечает за хранение хэш-значения пароля, создаваемого по алгоритму аутентификации LAN Manager. Поскольку данный алгоритм не является достаточно криптостойким, данную политику желательно включить;
- **Сетевая безопасность: ограничения NTLM: аудит входящего трафика NTLM** (Network security: Restrict NTLM: Audit Incoming NTLM Traffic). При включении данной политики сервер будет регистрировать сквозные запросы на аутентификацию по протоколу NTLM. В зависимости от выбранного значения будут регистрироваться запросы учетных записей домена или всех учетных записей;
- **Сетевая безопасность: ограничения NTLM: аудит проверки подлинности NTLM в этом домене** (Network security: Restrict NTLM: Audit NTLM authentication in this domain). Данная политика позволяет регистрировать попытки входа с помощью аутентификации по протоколу NTLM;
- **Сетевая безопасность: ограничения NTLM: входящий трафик NTLM** (Network security: Restrict NTLM: Incoming NTLM traffic).

Запрет или разрешение запросов аутентификации по протоколу NTLM. В зависимости от выбранного значения можно разрешить аутентификацию, запретить для доменных учетных записей или для всех учетных записей;

- **Сетевая безопасность: ограничения NTLM: добавить исключения для серверов в этом домене** (Network security: Restrict NTLM: Add server exceptions in this domain). С помощью этого параметра можно задать список серверов домена, к которым клиенты могут подключаться, используя для аутентификации протокол NTLM, даже если данный протокол запрещен к использованию на серверах локальной сети контроллером домена;
- **Сетевая безопасность: ограничения NTLM: добавить удаленные серверы в исключения проверки подлинности NTLM** (Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication). Параметр аналогичен предыдущему, но применяется для создания списка серверов, не входящих в локальный домен;
- **Сетевая безопасность: ограничения NTLM: исходящий трафик NTLM на удаленные серверы** (Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers). Политика позволяет разрешить, запретить или включить аудит использования протокола NTLM для регистрации на удаленных серверах;
- **Сетевая безопасность: ограничения NTLM: проверка подлинности NTLM в этом домене** (Network security: Restrict NTLM: NTLM authentication in this domain). Позволяет ограничить или вообще запретить использование протокола NTLM в домене;
- **Сетевая безопасность: принудительный вывод из сеанса по истечении допустимых часов работы** (Network security: Force logoff when logon hours expire). При включении данного параметра подключения других компьютеров к данному по протоколу SMB будут автоматически разрываться по истечении заданного для них промежутка времени;
- **Сетевая безопасность: разрешить LocalSystem использовать нулевые сеансы** (Network security: Allow LocalSystem NULL session fallback). При включении данной политики программы и службы, запускаемые под учетной записью LocalSystem, могут использовать нулевые сеансы;
- **Сетевая безопасность: разрешить использование сетевых удостоверений в запросах проверки подлинности PKU2U к этому компьютеру** (Network security: Allow PKU2U authentication requests to

this computer to use online identities). Политика определяет возможность использования сетевых удостоверений для аутентификации при подключении к данному компьютеру;

- **Сетевая безопасность: разрешить учетной записи LocalSystem использовать удостоверение компьютера для NTLM** (Network security: Allow Local System to use computer identity for NTLM). Данный параметр определяет возможность для служб, запущенных под учетной записью Local System, использовать сетевое удостоверение компьютера для аутентификации по протоколу NTLM;
- **Сетевая безопасность: требование цифровой подписи для LDAP-клиента** (Network security: LDAP client signing requirements). Параметр аналогичен политике **Контроллер домена: требования цифровой подписи для LDAP-сервера** (Domain controller: LDAP server signing requirements), описанной выше, но применяется к клиентскому компьютеру;
- **Сетевая безопасность: уровень проверки подлинности LAN Manager** (Network security: LAN Manager authentication level). Политика определяет, какие протоколы аутентификации используются при удаленном подключении к компьютеру;
- **Сетевой доступ: запретить анонимный доступ к именованным каналам и общим ресурсам** (Network access: Restrict anonymous access to Named Pipes and Shares). При включении данного параметра анонимный доступ к общим ресурсам компьютера и именованным каналам будет запрещен. Исключение составляют каналы и данные, указанные в списках политик **Сетевой доступ: разрешать анонимный доступ к именованным каналам** (Network access: Named Pipes that can be accessed anonymously) и **Сетевой доступ: разрешать анонимный доступ к общим ресурсам** (Network access: Shares that can be accessed anonymously);
- **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей** (Network access: Sharing and security model for local accounts). Политика определяет, какими правами будут наделяться пользователи при входе в локальную сеть с использованием локальных учетных записей. В зависимости от выбранного значения пользователи будут авторизоваться либо под своими учетными данными и использовать те права, которые определены для их учетных записей, либо как гости и, соответственно, получать права гостевой учетной записи независимо от того, какими правами они пользуются на локальном компьютере;

- **Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями** (Network access: Do not allow anonymous enumeration of SAM accounts). Политика определяет возможность получения анонимными пользователями имен учетных записей домена;
- **Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями** (Network access: Do not allow anonymous enumeration of SAM accounts and shares). Политика определяет возможность получения анонимными пользователями имен общих сетевых ресурсов и учетных записей домена;
- **Сетевой доступ: не разрешать хранение паролей или учетных данных для сетевой проверки подлинности** (Network access: Do not allow storage of passwords and credentials for network authentication). Параметр определяет будут ли запоминаться диспетчером учетных данных данные учетной записи для последующей аутентификации на контроллере домена;
- **Сетевой доступ: разрешать анонимный доступ к именованным каналам** (Network access: Named Pipes that can be accessed anonymously). Данный параметр позволяет составить список именованных каналов, к которым в качестве исключения будет разрешен анонимный доступ;
- **Сетевой доступ: разрешать анонимный доступ к общим ресурсам** (Network access: Shares that can be accessed anonymously). Параметр аналогичен предыдущему, применяется для общих сетевых ресурсов;
- **Сетевой доступ: удаленно доступные пути и вложенные пути реестра** (Network access: Remotely accessible registry paths and subpaths). Политика содержит список ветвей реестра, к которым разрешен удаленный доступ;
- **Сетевой доступ: пути в реестре доступны через удаленное подключение** (Network access: Remotely accessible registry paths). В текстовом поле диалогового окна настройки данной политики можно указать пути реестра Windows, которые будут доступны по сети;
- **Сетевой сервер (Майкрософт): уровень проверки сервером имени участника-службы конечного объекта** (Microsoft network server: Server SPN target name validation level). Параметр позволяет задать уровень проверки имени участника-службы сервером при подключении к нему клиента по протоколу SMB;

- **Системная криптография: использовать FIPS 140-совместимые алгоритмы для шифрования, хеширования и подписывания** (System cryptography: Use FIPS 140 compliant cryptographic algorithms, including encryption, hashing and signing algorithms). При включении данного параметра в операционной системе для криптографических операций будут использоваться только протоколы, соответствующие стандарту FIPS 140;
- **Системная криптография: применять сильную защиту пользовательских ключей, хранящихся на компьютере** (System Cryptography: Force strong key protection for user keys stored on the computer). Параметр определяет необходимость ввода пользователем пароля при работе с закрытым ключом шифрования. В зависимости от выбранного значения пароль не будет требоваться, будет запрашиваться при первом или при каждом обращении к закрытому ключу;
- **Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов** (например, символических ссылок) (System objects: Strengthen default permissions of internal system objects (e.g., Symbolic Links)). При включении данного параметра пользователи, не являющиеся администраторами, по умолчанию будут иметь доступ к общим ресурсам домена только на чтение;
- **Системные объекты: учитывать регистр для подсистем, отличных от Windows** (System objects: Require case insensitivity for non-Windows subsystems). Данный параметр определяет, будет ли учитываться регистр при обращении к различным системным объектам, например каталогам, подсистемами, отличными от Windows, такими как POSIX;
- **Устройства: запретить пользователям установку драйверов принтеров при подключении к общим принтерам** (Devices: Prevent users from installing printer drivers when connecting to shared printers). При включении данной политики устанавливать сетевые принтеры смогут только администраторы. При выключенной политике устанавливать сетевые принтеры смогут все пользователи;
- **Устройства: Разрешать отстыковку без входа в систему** (Devices: Allow undock without having to log on). Эта политика определяет возможность отстыковки портативного компьютера без входа в систему. Если политика включена, вход в систему не требуется, и для отстыковки компьютера может быть использована внешняя аппаратная кнопка извлечения;
- **Устройства: разрешить доступ к дисководам гибких дисков только**

локальным пользователям (Devices: Restrict floppy access to locally logged-on user only). При включении данной политики доступ к дисководам гибких дисков будет доступнее только локальным пользователям;

- **Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям** (Devices: Restrict CD-ROM access to locally logged-on user only). То же, что и предыдущая политика, но доступ определяется для дисководов оптических дисков;
- **Устройства: разрешить форматирование и извлечение съемных носителей** (Devices: Allowed to format and eject removable media). Данная политика определяет группы пользователей, которые могут форматировать и извлекать NTFS-носители. Возможные варианты: Администраторы, Администраторы и опытные пользователи, Администраторы и интерактивные пользователи;
- **Учетные записи: переименование учетной записи администратора** (Accounts: Rename administrator account). С помощью данной политики вы можете изменить имя учетной записи администратора (по умолчанию — Администратор);
- **Учетные записи: переименование учетной записи гостя** (Accounts: Rename guest account). Данная политика позволяет изменить имя учетной записи гостя. По умолчанию — **Гость**;
- **Учетные записи: ограничить использование пустых паролей только консольным входом** (Accounts: Limit local account use of blank passwords to console logon only). С помощью данной политики можно запретить или разрешить использование пустых паролей при удаленном подключении к системе. Если параметр включен, то использовать учетную запись без пароля для входа в систему можно только с самого компьютера;
- **Учетные записи: состояние учетной записи «Администратор»** (Accounts: Administrator account status). С помощью этой политики вы можете включить или отключить учетную запись локального администратора;
- **Учетные записи: состояние учетной записи «Гость»** (Accounts: Guest account status). То же, что и предыдущая политика, но здесь вы можете включить или отключить гостевую учетную запись;
- **Член домена: всегда требуется цифровая подпись или шифрование данных безопасного канала** (Domain member: Digitally encrypt or sign secure channel data (always)). Параметр определяет необходи-

мость использования цифровой подписи пакетов данных или шифрования при установке безопасного канала связи с контроллером домена;

- **Член домена: максимальный срок действия пароля учетных записей компьютера** (Domain member: Maximum machine account password age). Параметр определяет срок действия пароля учетной записи компьютера;
- **Член домена: отключить изменение пароля учетных записей компьютера** (Domain member: Disable machine account password changes). Определяет возможность смены пароля учетной записи компьютера;
- **Член домена: требовать стойкий ключ сеанса (Windows 2000 или более поздней версии)** (Domain member: Require strong (Windows 2000 or later) session key). Политика определяет необходимость использования 128-битного ключа для шифрования при использовании безопасного канала связи с контроллером домена.
- **Член домена: подписывать данные безопасного канала, когда это возможно** (Domain member: Digitally sign secure channel data (when possible)). Политика определяет, будет ли компьютер требовать от контроллера домена подписи пакетов данных при использовании безопасного канала связи;
- **Член домена: шифровать данные безопасного канала, когда это возможно** (Domain member: Digitally encrypt secure channel data (when possible)). Политика определяет, будет ли компьютер требовать от контроллера домена шифрования данных при использовании безопасного канала связи.

8.6. Функция управления приложениями AppLocker

AppLocker — это новый компонент в Windows 8, с помощью которого можно указать, какие пользователи и группы могут запускать определенные приложения в зависимости от уникальных идентификаторов файлов. При использовании AppLocker можно создать правила, разрешающие или запрещающие запуск приложений.

Компонент **AppLocker** находится в узле **Конфигурация Windows ⇒ Параметры безопасности ⇒ Политики управления приложениями ⇒ AppLocker** (Computer Configuration ⇒ Windows Settings ⇒ Security Set-

tings ⇒ Application Control Policies ⇒ AppLocker). AppLocker работает с исполняемыми файлами (EXE и COM), файлами сценариев (JS, PSL, .VBS, CMD и BAT), а также с файлами установщика Windows (MSI и MSP). Для каждой из указанных групп файлов в узле **AppLocker** созданы группы, соответственно, **Исполняемые правила** (Executable Rules), **Правила сценариев** (Script Rules) и **Правила установщика** Windows (Windows Installer Rules). Работа с каждой из этих групп одинакова.

По умолчанию все три группы пусты, поскольку правила не созданы. Правила создаются одинаково для файлов каждой из указанных групп.

Чтобы создать, например, правило для исполняемых файлов, нужно выполнить следующие действия.

1. Щелкните по группе **Исполняемые правила** (Executable Rules) в узле **AppLocker**. В правой части окна редактора локальной групповой политики появится пустая таблица.
2. В окне редактора локальной групповой политики выберите команду меню **Действие ⇒ Создать новое правило** (Action ⇒ Create New Rule). На экране появится окно мастера создания правила.

   В левой части окна мастера находится список шагов, которые предстоит выполнить при создании правила. Перемещение между этими шагами осуществляется с помощью кнопки **Далее** (Next).

   Первая страница мастера создания правил содержит информационный текст. Здесь не выполняется никаких действий.
3. Нажмите кнопку **Далее** (Next). Появится вторая страница мастера создания правила (рис. 8.7).

Переключателем **Действие** (Action) задается действие, которое будет определяться правилом:

- **Разрешить** (Allow). Запуск приложения будет разрешен;
- **Запретить** (Deny). Запуск приложения будет запрещен.

Ниже располагается поле, в котором отображается группа пользователей (по умолчанию — Все), на которых распространяется данное правило. Группы пользователей можно выбрать в диалоговом окне, появляющемся при нажатии кнопки **Выбрать** (Select). Также можно выбрать конкретного пользователя, на которого будет распространяться создаваемое правило. Например, если вы выберете группу **Администраторы**, создаваемое правило будет распространяться только на пользователей, вошедших под учетной записью **Администратор**.

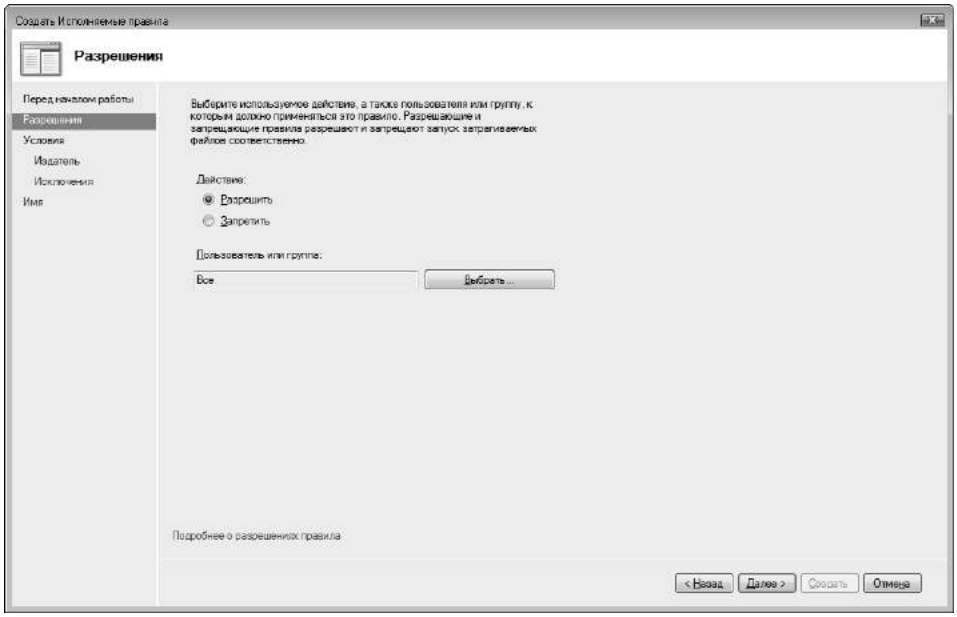


Рис. 8.7. ***Второе окно мастера настройки создания правила*** **AppLocker**

4. С помощью переключателя **Действие** (Action) выберите действие для правила.
5. Выберите группы пользователей, на которых будет распространяться создаваемое правило.
6. Нажмите кнопку **Далее** (Next). Появится третье окно мастера создания правила (рис. 8.8).

В третьем окне мастера создания правила выбирается тип основного условия, которое следует создать. Вы можете разрешить или запретить запуск программ по их издателю (здесь учитываются имя издателя, имя файла, название продукта, версия файла), по конкретному пути или по хэшу файла. Выбор типа основного правила выбирается с помощью переключателя.

7. Выберите тип основного условия с помощью переключателя в третьем окне мастера настройки правила.
8. Нажмите кнопку **Далее** (Next). Появится четвертое окно мастера создания правила (рис. 8.9).

Содержимое четвертого окна мастера создания правила меняется в зависимости от того, какой тип правила был выбран на предыдущем шаге. В нашем примере был выбран тип **Издатель** (Publisher).

9. С помощью элементов управления в четвертом окне мастера созда-

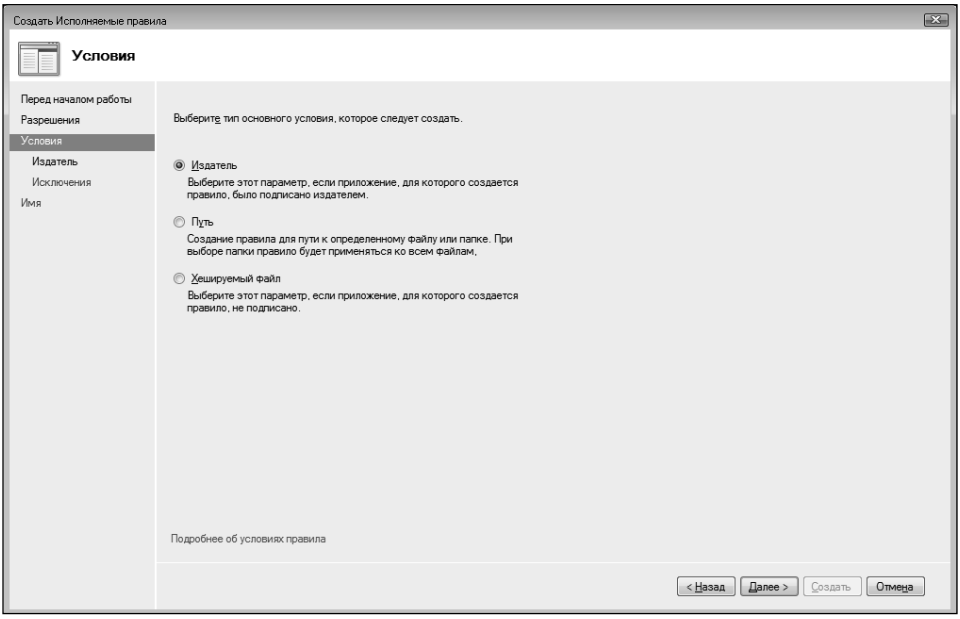


Рис. 8.8. ***Выбор типа основного условия***

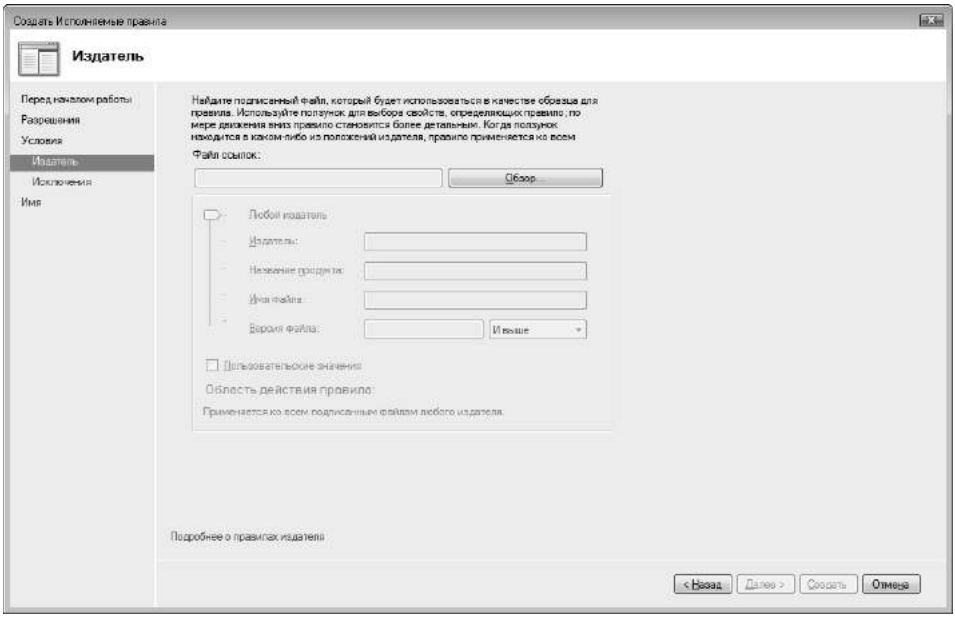


Рис. 8.9. ***Четвертое окно мастера создания правила***

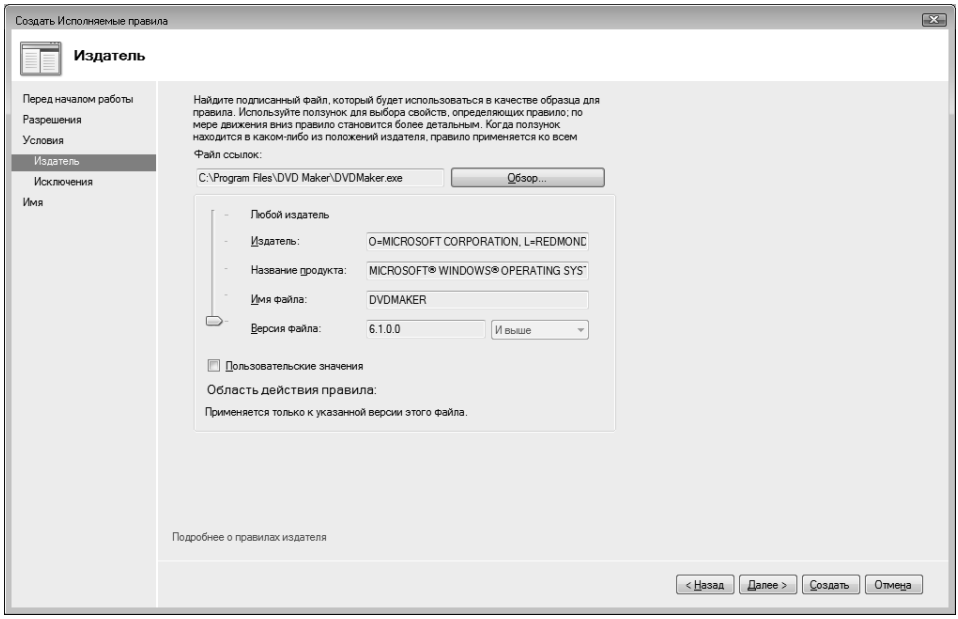


Рис. 8.10. ***Программа выбрана***

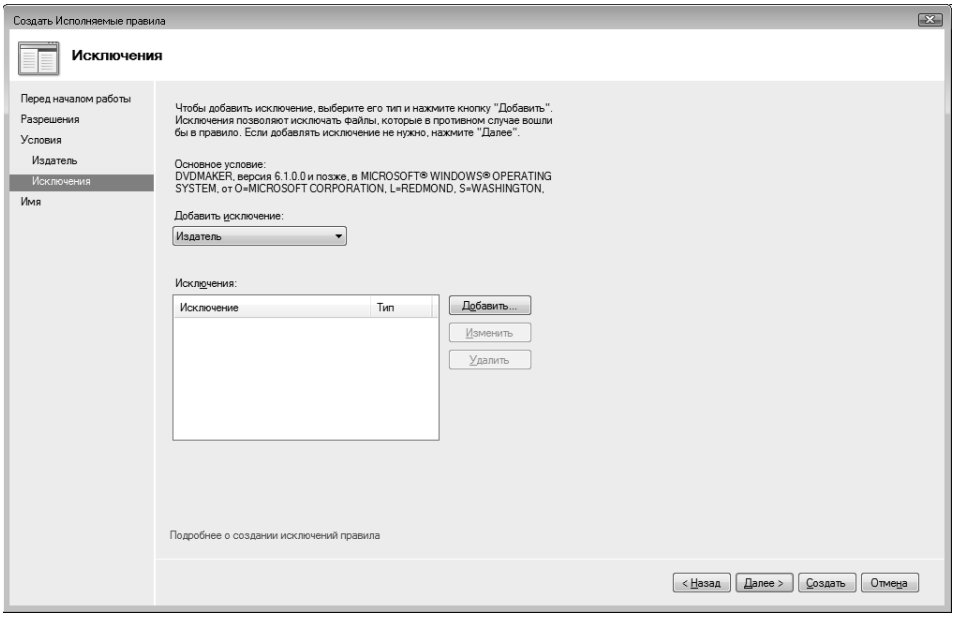


Рис. 8.11. ***В этом окне задаются исключения для правила***

ния правила укажите программу (сценарий или установщик), для которой создается правило. В нашем примере мы создали запрет на запуск программы DVDMaker (рис. 8.10).

10. Нажмите кнопку **Далее** (Next). Появится следующее окно мастера создания правила, в котором задаются исключения (рис. 8.11).

С помощью исключений вы можете добавить объекты (файлы, сценарии и установщики), на которые не будет распространяться правило.

11. Нажмите кнопку **Далее** (Next). Появится последнее окно мастера создания правила (рис. 8.12).

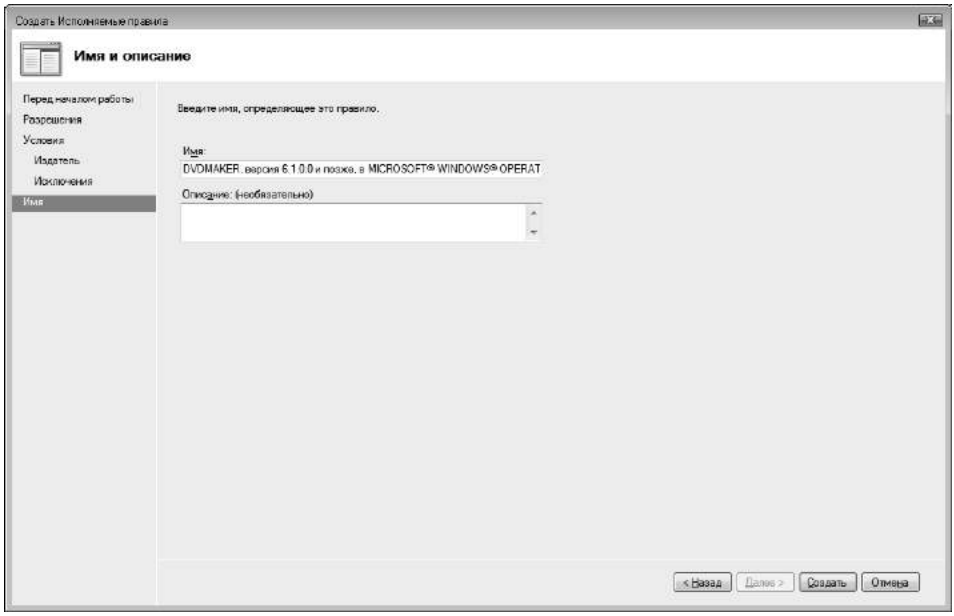


Рис. 8.12. ***Последняя страница мастера создания правила***

В появившемся окне задается имя для созданного правила, а также его описание. Имя правила может быть любым понятным пользователю или администратору, например **Запрет на запуск игры Паук**. Описание тоже может быть любым. В нем можно привести более подробную информацию о правиле.

12. Укажите имя для созданного правила в поле **Имя** (Name).
13. При необходимости укажите описание для правила в поле **Описание** (Description).
14. Нажмите кнопку **Создать** (Create). Автоматически будет создано не-

сколько правил общего характера и правило с заданными вами условиями (рис. 8.13).

Созданные вами правила располагаются в списке, который отображается при выделении соответствующей группы в узле **AppLocker**.

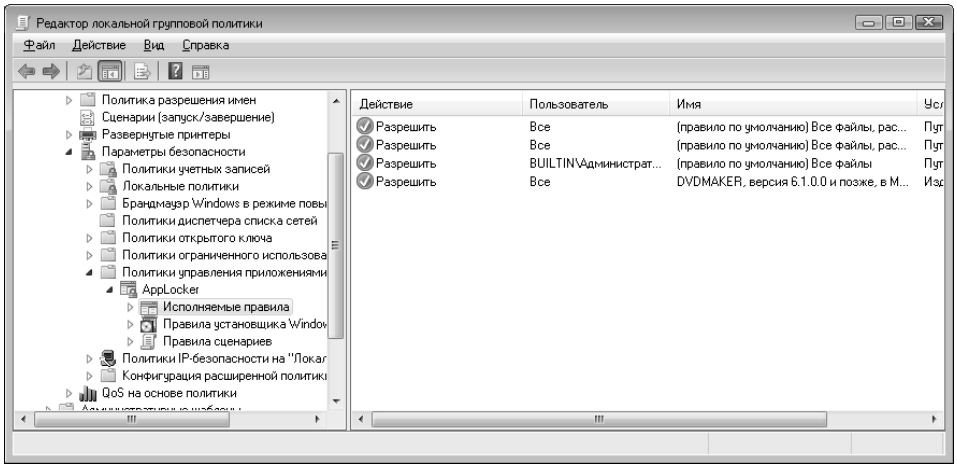


Рис. 8.13. ***Правило создано***

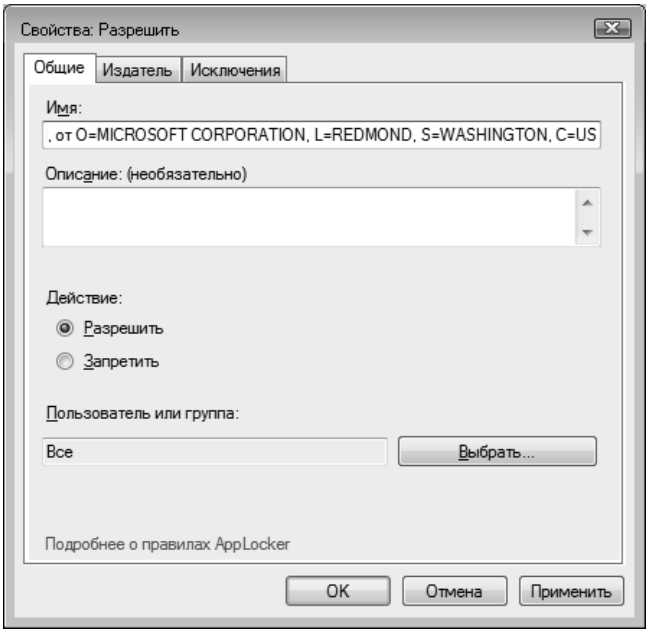


Рис. 8.14. ***Диалоговое окно редактирования свойств правила*** **AppLocker**

Ранее созданное правило можно изменить. Для этого нужно дважды щелкнуть мышью по пункту, соответствующему правилу, которое вы хотите изменить. При этом появится диалоговое окно свойств правила (рис. 8.14).

Диалоговое окно свойств правила, хоть и отличается от мастера создания правила, но содержит те же самые элементы управления, которые, в свою очередь, располагаются на разных вкладках. Здесь вы не можете изменить только тип основного условия, все остальные параметры правила можно менять.

Удалить ранее созданное правило можно двумя способами:

- выделить правило в списке и нажать клавишу **Del**;
- щелкнуть правой кнопкой мыши на пункте правила и в появившемся контекстном меню выбрать команду **Удалить** (Delete).

В обоих случаях последует запрос, в котором нужно подтвердить намерение удалить правило. Правила удаляются без возможности восстановления.

Таким образом, можно создать множество правил, ограничивающих использование тех или иных объектов для тех или иных групп пользователей. В результате даже на одном и том же компьютере доступ к определенным программам, сценариям или установщикам может быть кому-то разрешен, а кому-то запрещен.

8.7. Брандмауэр Windows в режиме повышенной безопасности

С помощью политики **Брандмауэр Windows в режиме повышенной безопасности** (Windows Firewall with Advanced Security), расположенной в узле **Конфигурация Windows ⇒ Параметры безопасности ⇒ Брандмауэр Windows в режиме повышенной безопасности** (Computer Configuration ⇒ Windows Settings ⇒ Security Settings ⇒ Windows Firewall with Advanced Security), можно тонко настроить правила безопасности сети для компьютеров под управлением Windows.

Здесь вы можете создать правила для входящих, исходящих подключений, а также правила безопасности подключения. Например, вы можете создать правило, блокирующее доступ к компьютеру через определенный порт. Или правило, запрещающее доступ какой-либо программе к вашему компьютеру по сети.

Правила настраиваются с помощью мастера. Предварительно следует выделить тип подключения в узле **Брандмауэр Windows в режиме повышенной**

безопасности (Windows Firewall with Advanced Security). Рассмотрим пример создания правила для программы, использующей входящее подключение. Для создания такого правила нужно выполнить следующие действия.

- Выделите пункт **Правила для входящих подключений** (Inbound Rules) в узле **Брандмауэр Windows в режиме повышенной безопасности** (Windows Firewall with Advanced Security). В правой части окна редактора локальной групповой политики появится таблица, содержащая список правил. Но, поскольку правила еще не созданы, таблица пуста.
- В окне редактора локальной групповой политики выберите команду меню **Действие ⇒ Создать правило** (Action ⇒ New Rule). На экране появится окно мастера создания правила (рис. 8.15).

В левой части окна мастера создания правила приведен список шагов, которые нужно выполнить для создания правила. Переход к следующему шагу осуществляется с помощью кнопки **Далее** (Next).

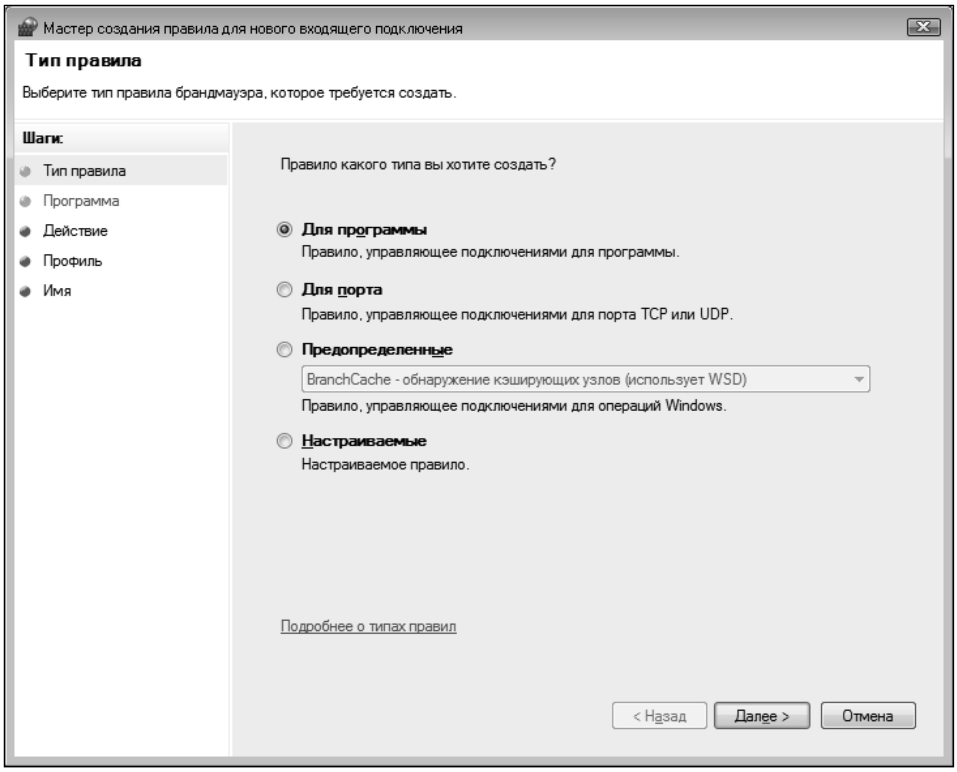


Рис. 8.15. ***Первое окно мастера создания правила***

На первой странице мастера создания правила предлагается выбрать тип правила. Правило можно создать для программы, порта, а также предопределенное (готовое решение) или настраиваемое. Мы настраиваем правило для программы.

- Выберите тип правила с помощью переключателя в окне мастера создания правила. Мы выберем положение **Для программы** (Program).
- Нажмите кнопку **Далее** (Next). Появится вторая страница мастера создания правила (рис. 8.16).

Содержимое второй страницы мастера создания правила (а также количество этих страниц) зависит от выбранного вами типа правила. В нашем примере предлагается применить создаваемое правило ко всем программам или к конкретной программе, путь к которой указывается в поле **Путь программы** (This program path).

- Нажмите кнопку **Обзор** (Browse) и в появившемся диалоговом окне найдите и выделите исполняемый файл программы, для которой соз-

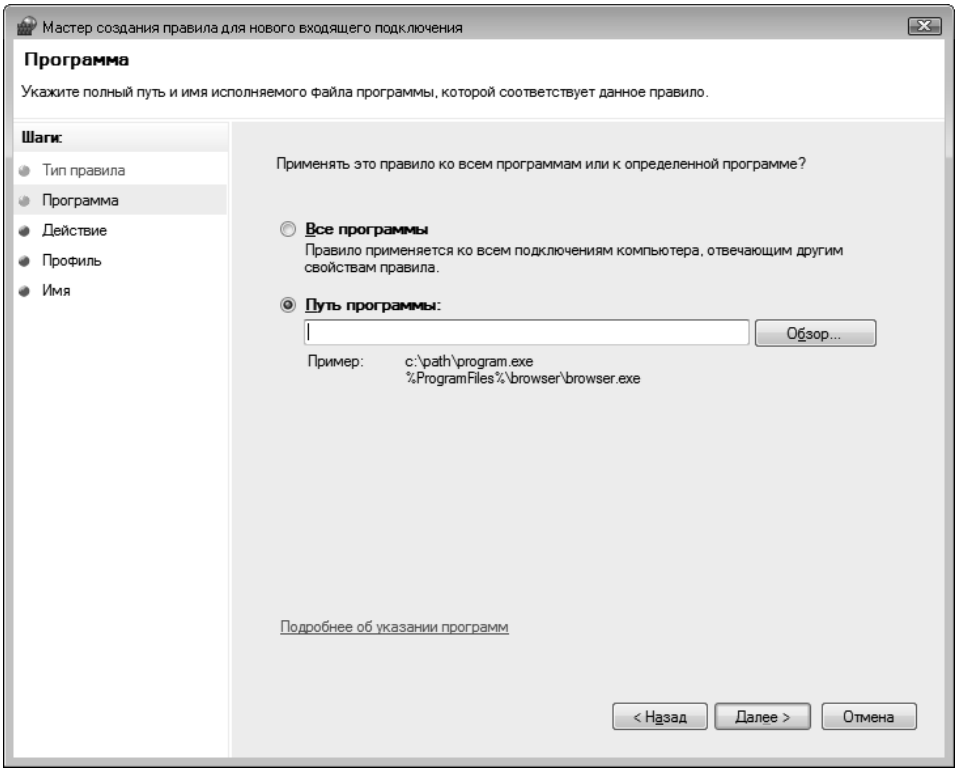


Рис. 8.16. ***Второе окно мастера создания правила***

дается правило, после чего нажмите кнопку **Открыть** (Open) диалогового окна. Диалоговое окно закроется, а путь к указанной программе появится в поле на второй странице мастера создания правила.

- Нажмите кнопку **Далее** (Next). Будет осуществлен переход к следующей странице мастера создания правила, на которой указывается действие для правила (рис. 8.17).

Для указанной программы можно разрешить подключение, разрешить безопасное подключение (с проверкой подлинности) или заблокировать подключение. Действие определяется с помощью переключателя.

- Установите переключатель в положение, соответствующее выбранному действию.
- Нажмите кнопку **Далее** (Next). Появится следующая страница мастера создания правила (рис. 8.18).

На появившейся странице предлагается указать профиль подключения:

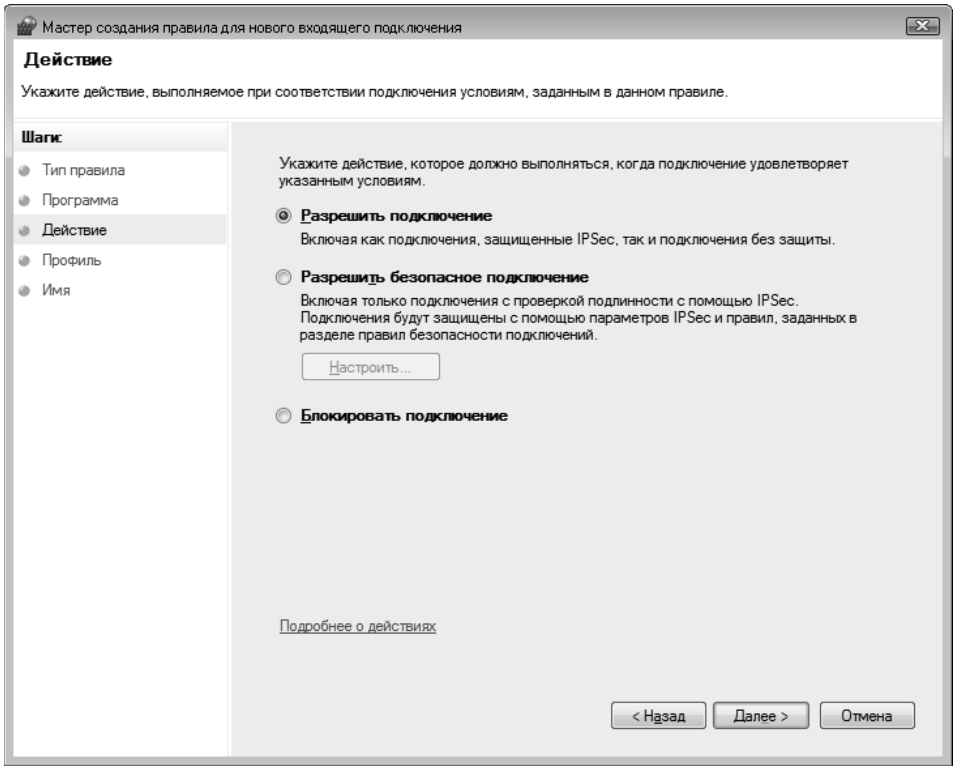


Рис. 8.17. ***Выбор действия для правила***

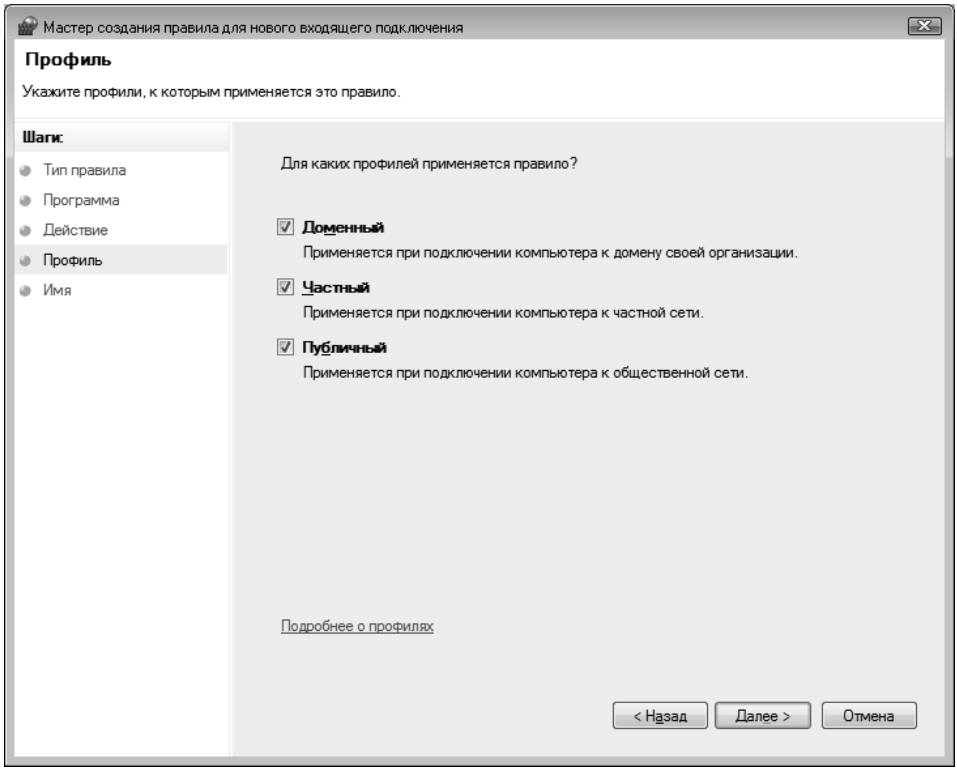


Рис. 8.18. ***Выбор профиля***

1. **Доменный** (Domain), использующийся при подключении компьютера к домену организации;
2. **Частный** (Private), использующийся для подключения к частной сети;
3. **Публичный** (Public), использующийся для подключения к общественной сети.

Обратите внимание, вы можете выбрать несколько профилей одновременно или все сразу. По умолчанию включены все профили.

- Сбросьте флажки для тех профилей, на которые создаваемое правило не будет распространяться.
- Нажмите кнопку **Далее** (Next). Появится последняя страница мастера создания правила (рис. 8.19).

На последней странице мастера создания правила следует ввести название правила и его описание. Ввод описания не является обязательным условием.

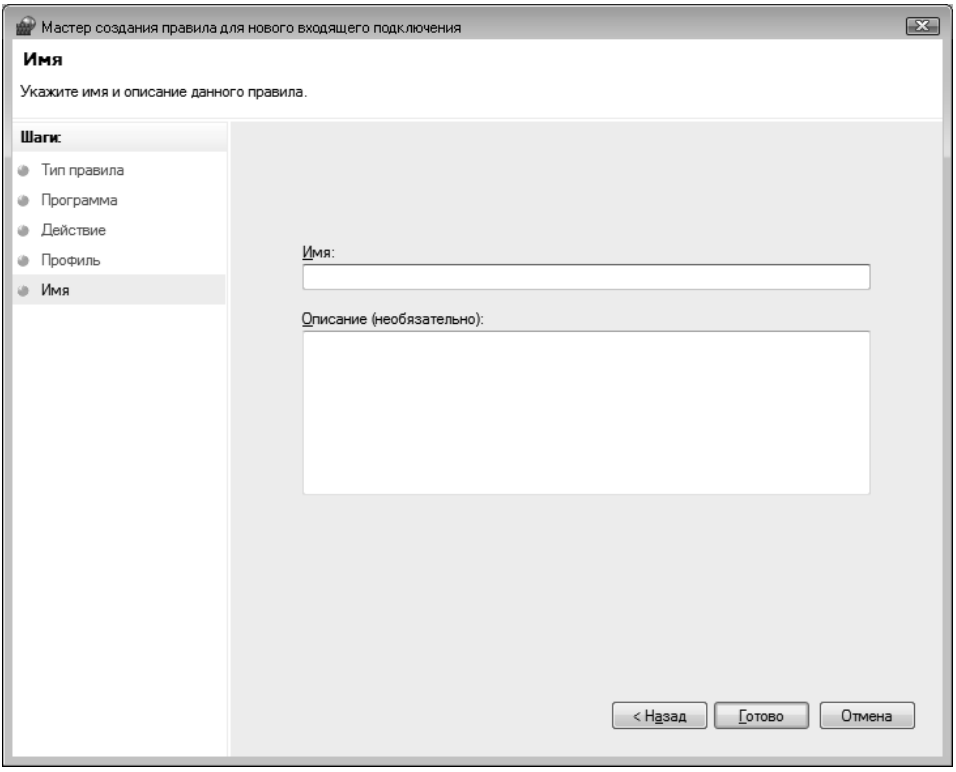


Рис. 8.19. ***Последняя страница мастера создания правила***

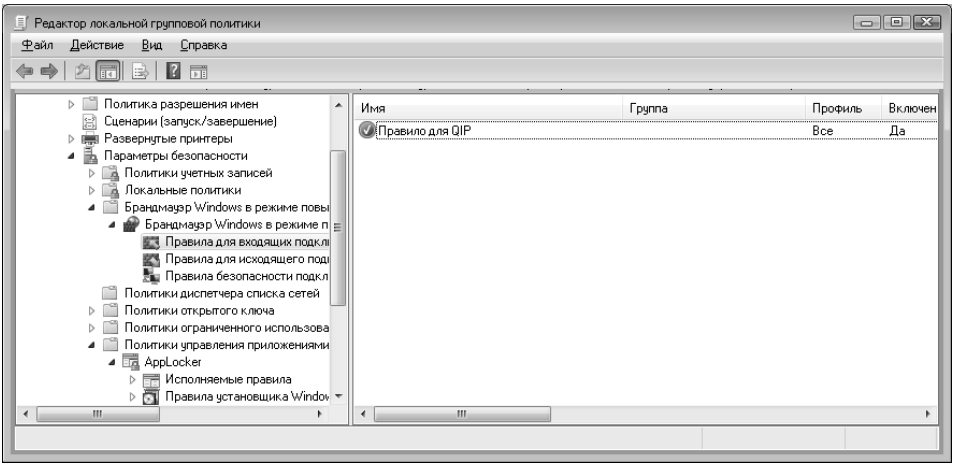


Рис. 8.20. ***Правило создано***

- В поле **Имя** (Name) введите название для создаваемого правила. Название может быть любым.
- При необходимости в поле **Описание** (Description) введите описание правила.
- Нажмите кнопку **Готово** (Finish). Правило появится в списке группы **Правила входящих подключений** (Inbound Rules) (рис. 8.20).

Таким образом, можно создать множество правил подключения для разных программ или портов. Отметим, что при выборе настраиваемого правила вы можете указать не только программы и порты, но также IP-адреса, к которым производится подключение.

Ранее созданное правило можно редактировать. Это делается в диалоговом окне свойств правила, которое вызывается двойным щелчком по правилу в списке (рис. 8.21).

Диалоговое окно свойств правила содержит тот же набор элементов управления, что и мастер создания правила. Элементы управления содержатся на разных вкладках диалогового окна.

Чтобы удалить правило, достаточно щелкнуть по нему правой кнопкой мыши и в появившемся контекстном меню выбрать команду **Удалить** (Delete).

Вы можете отключить правило, не удаляя его. Отключенное правило не будет действовать до тех пор, пока вы снова его не включите. Чтобы отключить правило, следует щелкнуть по нему правой кнопкой мыши и в появившемся контекстном меню выбрать команду **Отключить правило** (Disable Rule). Для включения правила в контекстном меню выбирается команда **Включить правило** (Enable Rule). Если правило отключено, значок, расположенный в левой части правила в списке, становится серым.

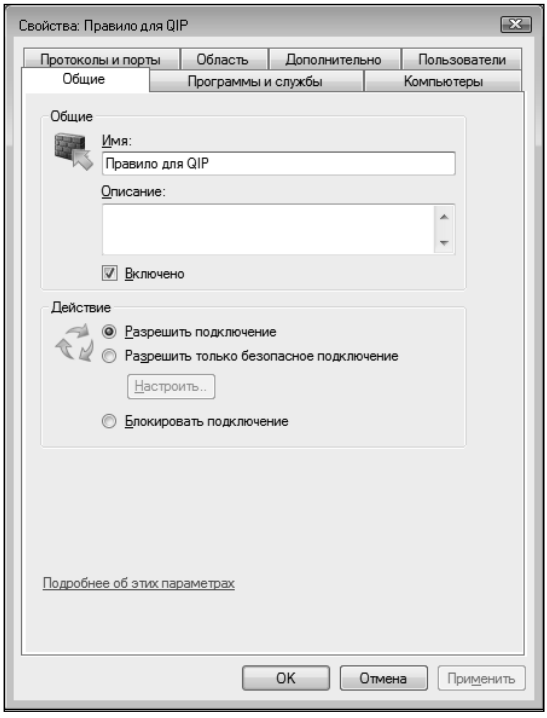


Рис. 8.21. ***Диалоговое окно свойств правила***

Глава 9.

Хакинг браузера Internet Explorer

9.1. Настройка меню и панелей инструментов браузера

Основная часть доступных пользователю команд управления браузером располагается в меню и на панелях инструментов. Обычно отображение строки меню, количество кнопок на панелях инструментов и их расположение задаются пользователями самостоятельно, но не все пользователи знают, как выполняются те или иные настройки. Иногда администратору нужно настроить браузер таким образом, чтобы его интерфейс максимально был похож на интерфейс предыдущих версий, например, если на предприятии происходит замена операционной системы Windows XP на Windows 8\Windows Server 2008 или просто обновление версии браузера. В других случаях требуется запретить использование отдельных команд меню или скрыть отдельные кнопки. Все перечисленные выше операции можно выполнить с помощью редактора политик.

Настройка меню

За настройку меню браузера отвечает узел **Меню браузера** (Browser menus). Этот узел располагается только в кусте **Конфигурация пользователя** (User Configuration), поэтому данные политики могут применяться только к конкретным пользователям или группам пользователей.

С помощью узла **Меню браузера** (Browser menus) можно отключать отдельные команды меню браузера. Как правило, политики этого узла используются для того, чтобы пользователи не могли совершать определенные действия с помощью команд меню браузера, например, сохранять веб-страницы корпоративного сайта на локальный диск.

Поскольку политики рассчитаны на работу с различными версиями браузеров, некоторые названия команд в политиках могут отличаться от названий пунктов меню браузера, например, политика **Меню Файл: Отключить пункт «Создать»** (File menu: Disable New menu options) отключает не только указанную команду в скрытом по умолчанию классическом меню, но и команду на панели команд **Страница ⇒ Новое окно** (Page ⇒ New Window).

В качестве примера отключим возможность сохранять просматриваемые веб-страницы на жесткий диск пользователям, не входящим в группу администраторов.

1. Откройте консоль управления и выберите оснастку **Политика «Локальный компьютер\Не администраторы»** (Local Computer\Non-Administrators Policy).

2. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒**

   Компоненты Windows ⇒ Internet Explorer ⇒ Меню браузера (User Configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Internet Explorer ⇒ Browser menus). В этом узле располагаются семнадцать параметров, позволяющих управлять различными элементами меню браузера.

3. Дважды щелкните мышью по параметру **Меню Файл: Отключить пункт «Сохранить как»** (File menu: Disable Save As... menu options). В открывшемся диалоговом окне редактирования параметра политики установите переключатель в положение **Включить** (Enabled). При необходимости введите в поле ввода **Комментарий** (Comment) комментарий к вашим действиям.

4. Нажмите кнопку **ОК**. Теперь команда меню **Файл ⇒ Сохранить как** (File ⇒ Save As...) и командной панели **Страница ⇒ Сохранить как** (Page ⇒ Save As...) будут недоступны.

Повторите шаги 4-5 для параметра **Отключить контекстное меню** (Disable Context menu), чтобы пользователи не могли воспользоваться командой контекстного меню **Сохранить объект как** (Save Target As...) для загрузки и сохранения веб-страниц по ссылкам.

Если вы желаете оставить пользователям возможность сохранять текстовые данные с веб-страниц, то вместо **Меню Файл: Отключить пункт «Сохранить как»** (File menu: Disable Save As... menu options) используйте параметр **Меню Файл: Отключить пункт «Сохранить как веб-страницу, полностью»** (File menu: Disable Save As Web Page Complete). Эта политика позволит пользователям сохранять просматриваемую страницу в виде простого текстового файла или в виде простого HTML-файла без графических элементов, таблиц стилей и скриптов.

Приведенный выше пример можно дополнить запретом на печать веб-страниц.

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒**

Компоненты Windows ⇒ Internet Explorer ⇒ Меню браузера (User Configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Internet Explorer ⇒ Browser menus).

2. Дважды щелкните мышью по параметру **Выключить отображение меню** (Turn off Print Menu). В открывшемся диалоговом окне редактирования параметра политики установите переключатель в положение **Включить** (Enabled). При необходимости введите в поле ввода **Комментарий** (Comment) комментарий к вашим действиям.
3. Нажмите кнопку **ОК**. Теперь команды меню **Файл ⇒ Печать** (File ⇒ Print...) и **Файл ⇒ Предварительный просмотр** (File ⇒ Print Preview...) и **Файл ⇒ Параметры страницы** (File ⇒ Page Setup...) будут недоступны, а при нажатии кнопки **Печать** (Print) на панели команд будет выведено сообщение о том, что данная операция запрещена администратором (рис. 9.1).

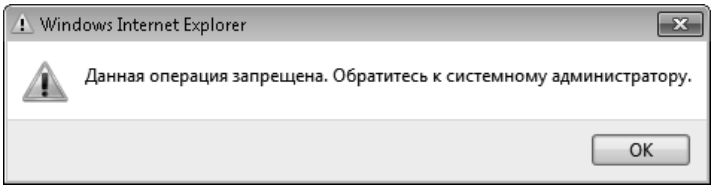


Рис. 9.1. ***Сообщение о попытке выполнения запрещенной операции***

Еще одна полезная политика, позволяющая не только повысить безопасность компьютера, но и сэкономить немалый объем трафика — **Отключить параметр «Сохранить эту программу на диске»** (Disable Save this program to disk option). Если установить параметр этой политики в положение **Включить** (Enabled), то пользователи не смогут сохранять загружаемые программы и другие файлы на компьютере. Если в диалоговом окне, появляющемся при загрузке файла, нажать кнопку **Сохранить** (Save) — пользователь получит предупреждение о невозможности этой операции (рис. 9.2), а загрузка будет отменена.

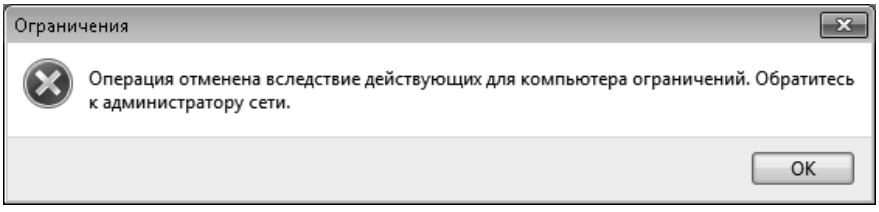


Рис. 9.2. ***Предупреждение о невозможности совершения операции***

Помимо отключения команд меню, с помощью политик этого узла можно полностью скрыть пункт меню **Избранное** (Favorites), при этом вкладка **Избранное** (Favorites) в центре управления избранным также перестанет отображаться, можно также запретить просмотр исходного кода страниц и другие действия, выполняемые с помощью команд меню.

Настройка панелей инструментов

Помимо элементов меню, с помощью политик можно настроить и панели инструментов браузера. Сделать это можно с помощью политик узла **Панели инструментов** (Toolbars). Политики этого узла позволяют управлять расположением кнопок **Обновить** (Refresh) и **Остановить** (Stop), скрывать панель команд и строку состояния, настраивать подписи команд и кнопки, а также запрещать их настройку. Последний вариант бывает полезен в случаях, когда дополнительные панели требуются для придания браузеру требующейся в работе функциональности или служат для повышения безопасности. Этот вариант мы и рассмотрим в качестве примера.

Для отключения возможности настройки панелей инструментов следует отключить функцию скрытия и отображения панелей инструментов, установленных в браузере, и кнопок на стандартных панелях инструментов — **Панели Избранного** (Favorites Bar) и **Панели Команд** (Command Bar).

1. Откройте консоль управления и выберите оснастку **Политика «Локальный компьютер\Не администраторы»** (Local Computer\Non-Administrators Policy).
2. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒**

   Компоненты Windows ⇒ Internet Explorer ⇒ Панели инструментов (User Configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Internet Explorer ⇒ Toolbars).

Дважды щелкните мышью по параметру **Отключить настройку панелей инструментов браузера** (Disable customizing browser toolbars). В открывшемся диалоговом окне редактирования параметра политики установите переключатель в положение **Включить** (Enabled). При необходимости введите в поле ввода **Комментарий** (Comment) комментарий к вашим действиям.

Нажмите кнопку **ОК**.

Повторите шаги 4-5 для параметра **Отключить настройку кнопок панели инструментов браузера** (Disable customizing browser toolbar buttons), чтобы отключить функцию отображения и скрытия кнопок на стандартных панелях инструментов браузера.

Теперь пользователь сможет отображать или скрывать только стандартные панели и строку статуса. Пункты меню, отвечающие за отображение остальных панелей инструментов и кнопок на стандартных панелях, будут неактивны.

9.2. Параметры журнала браузера

В последних версиях Internet Explorer журнал браузера помимо списка посещенных веб-страниц хранит данные, введенные в веб-формы, и пароли к сайтам. Кроме того, в журнале хранятся cookie-файлы. С помощью диалогового окна **Удаление истории обзора** (Delete Browsing History) пользователи могут удалять некоторые группы данных или вообще полностью очищать журнал. В то же время журнал браузера позволяет более точно контролировать работу пользователей и, например, в случае загрузки вируса на компьютер, установить, когда и с какого ресурса произошла загрузка вредоносной программы. Политики узла **Удалить журнал браузера** (Delete Browsing History) позволяют лишить пользователей возможности удалять некоторые группы данных из журнала браузера или вообще отключить возможность его ручной очистки.

Обычно для контроля за посещаемыми сайтами используется только список посещенных веб-страниц.

1. Для отключения возможности очистки списка посещенных веб-страниц откройте консоль управления и выберите оснастку **Политика «Локальный компьютер\Не администраторы»** (Local Computer\Non-Administrators Policy).

2. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒**

   Компоненты Windows ⇒ Internet Explorer ⇒ Удалить журнал браузера (User Configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Internet Explorer ⇒ Delete Browsing History). Узел содержит одиннадцать политик, позволяющих запретить пользователям отдельные или все операции с журналом.

3. Дважды щелкните мышью по параметру **Предотвращать удаление посещенных пользователем веб-сайтов** (Prevent Deleting Web sites that user has Visited). В открывшемся диалоговом окне редактирования параметра политики установите переключатель в положение **Включить** (Enabled). При необходимости введите в поле ввода **Комментарий** (Comment) комментарий к вашим действиям.

4. Нажмите кнопку **ОК**.

После завершения настроек в диалоговом окне **Удаление истории обзора** (Delete Browsing History) пункт **Журнал** (History) будет неактивен (рис. 9.3), а в нижней его части будет отображаться уведомление о том, что отдельные параметры управляются системным администратором.

Рис. 9.3. ***Диалоговое окно*** **Удаление истории обзора** ***с неактивным пунктом*** **Журнал**

9.3. Средства безопасности

Параметров, отвечающих за безопасность браузера, в Internet Explorer предусмотрено достаточно много, а политик, обеспечивающих ее, еще больше. Часть политик, отвечающих за обеспечение безопасности, собрана в узле **Средства безопасности** (Security Features). Этот узел есть и в кусте **Конфигурация компьютера** (Computer Configuration), и в кусте **Конфигурация пользователя** (User Configuration). В зависимости от того, с какой целью выполняются настройки, следует использовать различные кусты. Отмечу также, что количество политик узла в обоих кустах неодинаково — куст **Конфигурация компьютера** (Computer Configuration) содержит дополни-

тельный параметр **Отключить предотвращение выполнения данных** (Turn off Data Execution Prevention), отвечающий за работу функции предотвращения выполнения данных DEP для браузера.

Большая часть политик этого узла настраивается однотипно и содержит три параметра, отвечающих за различные области применения политики:

4. **Все процессы** (All Processes) — для применения политики ко всем процессам, выполняющимся на компьютере, кроме процессов Internet Explorer.
5. **Процессы Internet Explorer** (Internet Explorer Processes) — для применения политики к процессам Internet Explorer.
6. **Список процессов** (Process List) — применяет политику к заданному списку процессов.

Одна из наиболее явно сказывающихся на работе браузера политик узла **Средства безопасности** (Security Features) — **Управление надстройками** (Add-on Management).

К надстройкам относятся различные плагины, элементы ActiveX и дополнительные панели инструментов. Часто из-за ошибок в коде таких надстроек нарушается стабильность работы браузера. Кроме того, под видом полезных надстроек к браузеру распространяются некоторые виды вредоносных программ. Наиболее простой способ оградить браузер от проблем с надстройками — запретить загрузку любых надстроек, кроме внесенных в список разрешенных. В качестве примера создадим список разрешенных надстроек для пользователей, не входящих в группу администраторов, а загрузку остальных надстроек запретим.

1. Откройте консоль управления и выберите оснастку **Политика «Локальный компьютер\Не администраторы»** (Local Computer\Non-Administrators Policy)
2. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒**

   Компоненты Windows ⇒ Internet Explorer ⇒ Средства безопасности ⇒ Управление надстройками (User Configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Internet Explorer ⇒ Add-on Management).
3. Дважды щелкните мышью по параметру **Список надстроек** (Add-on List). В открывшемся диалоговом окне редактирования параметра политики установите переключатель в положение **Включить** (Enabled) и нажмите кнопку **Показать** (Show).

4. В открывшемся диалоговом окне **Вывод содержания** (Show Contents) (рис. 9.4) в поле **Имя значения** (Value name) введите идентификатор класса CLSID, соответствующий надстройке, а в поле ввода **Значение** (Value) введите числовое значение, соответствующее действию браузера по отношению к указанной настройке:
   - **0** — не загружать указанную надстройку.
   - **1** — загружать указанную надстройку. При установке этого параметра надстройка будет загружаться независимо от желания пользователя. Этот параметр желательно установить для надстроек, обеспечивающих дополнительную безопасность браузера, например, AVG Safe Search — компонент антивирусной программы для проверки безопасности вебстраниц AVG LinkScannerFree.
   - **2** — загружать надстройку и разрешить пользователям управление ею средствами браузера. При установке этого параметра пользователи имеют возможность самостоятельно разрешать или запрещать загрузку этой надстройки с помощью диалогового окна **Надстройки** (Manage Add-ons).
5. После ввода данных в первую строку в диалоговом окне автоматически отобразится вторая строка для нового элемента списка.
6. Нажмите кнопку **ОК** для сохранения списка. При необходимости введите в поле ввода **Комментарий** (Comment) комментарий к вашим действиям в диалоговом окне настройки параметров политики и нажмите кнопку **ОК,** чтобы применить политику.
7. Дважды щелкните мышью по параметру **Запрещать все надстройки, кроме заданных политикой «Список надстроек»** (Deny all add-ons unless specifically allowed in the Add-on List). В открывшемся диалоговом окне редактирования параметра политики установите переключатель в положение **Включить** (Enabled) и нажмите кнопку **ОК**. Если не настраивать этот параметр, то браузер не будет загружать только те политики, для которых в списке надстроек указано значение **0**. Таким образом, можно явно запретить загрузку или настройку конкретных надстроек, оставив управление остальными на усмотрение пользователей.

Теперь при работе браузера будут использоваться только те надстройки, которые были внесены в список как разрешенные. Узнать идентификатор класса CLSID надстройки, установленной в системе, можно, дважды щелкнув по ее названию в диалоговом окне **Надстройки** (Manage Add-ons), вызывае-

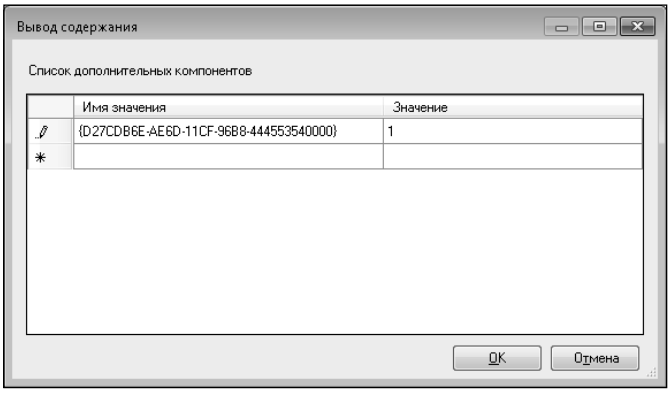


Рис. 9.4. *Диалоговое окно* Вывод содержания

мом командой меню **Сервис ⇒ Надстройки** (Tools ⇒ Manage Add-ons). В приведенном выше примере указан идентификатор для элемента ActiveX Adobe Shockwave Flash Object, используемого для воспроизведения флеш-анимации на веб-страницах.

9.4. Доступ к элементам управления ActiveX

Иногда нужно запретить пользователям просматривать определенные типы данных, например, для экономии трафика можно запретить воспроизведение потокового видео и аудио. Сделать это можно с помощью политик узла **Элементы управления, допущенные администратором** (Administrator Approved Controls). В этом узле располагаются политики, позволяющие запретить или разрешить для различных зон безопасности использование элементов управления ActiveX, таких как Shockwave Flash или **Универсальный проигрыватель** (Audio/Video Player), использующихся для воспроизведения различных данных на веб-страницах. По умолчанию все политики данного узла запрещают использование элементов управления, но настройки браузера игнорируют данный запрет. Таким образом, для запрета использования каких-либо элементов управления следует разрешить или запретить отдельные элементы управления, а затем, с помощью редактора групповой политики или самого браузера, настроить зоны безопасности таким образом, чтобы политики узла **Элементы управления, допущенные администратором** (Administrator Approved Controls) не игнорировались.

В качестве примера запретим пользователям использование **Универсального проигрывателя** (Audio/Video Player) при работе в зоне **Интернет** (Internet).

Отметим элемент управления **Универсальный проигрыватель** (Audio/Video Player) как запрещенный к использованию.

1. Для отключения возможности воспроизведения звука и потокового видео на веб-страницах откройте консоль управления и выберите оснастку **Политика «Локальный компьютер\Не администраторы»** (Local Computer\Non-Administrators Policy).
2. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Internet Explorer ⇒ Элементы управления, допущенные администратором** (User Configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Internet Explorer ⇒ Administrator Approved Controls). Узел содержит политики, позволяющие пользователям использовать различные элементы управления.
3. Дважды щелкните мышью по параметру **Универсальный проигрыватель** (Audio/Video Player). В открывшемся диалоговом окне редактирования параметра политики установите переключатель в положение **Отключить** (Disabled). При необходимости введите в поле ввода **Комментарий** (Comment) комментарий к вашим действиям.
4. Нажмите кнопку **ОК**.
5. Повторите действия 3 и 4 для остальных политик узла. Для элементов управления, которые вы хотите разрешить для использования, следует установить параметр политики в положение **Включить** (Enabled).

Теперь внесем соответствующие изменения в параметры зоны **Интернет** (Internet). Сделать это можно двумя способами:

1. Откройте узел **Конфигурация пользователя ⇒ Конфигурация Windows ⇒ Настройка Internet Explorer ⇒ Зоны безопасности и оценка содержимого** (User Configuration ⇒ Windows Settings ⇒ Internet Explorer Maintenance ⇒ Security ⇒ Security Zones and Content Ratings).
2. В открывшемся диалоговом окне **Зоны безопасности и оценка содержимого** (Security Zones and Content Ratings) установите переключатель **Зоны безопасности и конфиденциальность** (Security Zones and Privacy) в положение **Импортировать текущие параметры безопасности и конфиденциальности** (Import the current security zones and privacy settings) и нажмите кнопку **Изменить параметры** (Modify Settings).
3. В открывшемся диалоговом окне **Свойства Интернет** (Internet Prop-

erties) выберите зону, которую вы хотите настроить, например **Интернет** (Internet), и нажмите кнопку **Другой** (Custom Level). Откроется диалоговое окно **Параметры безопасности — зона Интернета** (Security Settings — Internet Zone) (рис. 9.5).

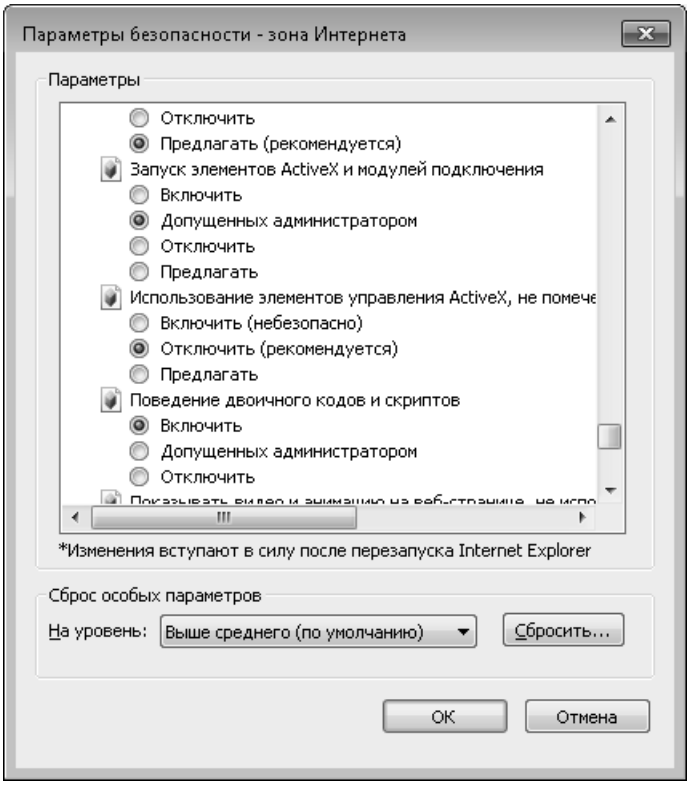


Рис. 9.5. *Диалоговое окно* Параметры безопасности — зона Интернета

4. В этом диалоговом окне найдите переключатель **Запуск элементов ActiveX и модулей подключения** (Run ActiveX controls and plug-ins) и установите его в положение **Допущенных администратором** (Administrator approved). Этот параметр можно также настроить, установив параметр **Запуск элементов ActiveX и модулей подключения** (Run ActiveX controls and plug-ins) в узле **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Internet Explorer ⇒ Панель управления браузером ⇒ Вкладка безопасности ⇒ Зона Интернета** (User Configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Internet Explorer ⇒ Internet Control Panel ⇒ Security Page ⇒ Internet Zone) в положение

Включен (Enabled) и выбрав в раскрывающемся списке **Запускать элементы ActiveX и подключаемые модули** (Run ActiveX controls and plug-ins) положение **Разрешено администратором** (Administrator approved).

5. Нажмите кнопку **ОК** для сохранения примененных настоек. После завершения настройки переключатель **Запуск элементов ActiveX и модулей подключения** (Run ActiveX controls and plug-ins) в диалоговом окне браузера **Параметры безопасности — зона Интернета** (Security Settings — Internet Zone) будет неактивен.

Теперь при открытии в Internet Explorer веб-страницы, содержащей видео- или аудиофайлы, на панели информации отобразится предупреждение о невозможности запуска надстройки для отображения части содержимого страницы.

9.5. Панель управления браузером

На вкладках **Дополнительно** (Advanced) и **Безопасность** (Security) диалогового окна **Свойства обозревателя** (Internet Options) располагается большое количество параметров, от которых зависит стабильность и безопасность работы браузера. Такие важные настройки не обойдены вниманием и в редакторе политик. Узел **Панель управления браузером** (Internet Control Panel) содержит политики, дублирующие настройки браузера, расположенные на этих вкладках, а также политики, позволяющие отключить отдельные вкладки диалогового окна **Свойства обозревателя** (Internet Options). При этом параметры, явно заданные политиками, запрещают изменение соответствующих настроек средствами браузера.

Вкладка «Дополнительно»

В этом узле располагается ряд параметров, которые заметно влияют на безопасность как браузера, так и операционной системы в целом. Ниже перечислены параметры, которые рекомендуется изменить:

- **Проверять, не отозван ли сертификат сервера** (Check for server certificate revocation) — этот параметр желательно включить в качестве дополнительной защиты от мошенничества, поскольку по умолчанию проверка действительности электронного сертификата веб-сервера не производится.
- **Запретить сброс параметров Internet Explorer** (Do not allow resetting Internet Explorer settings) — включение данного параметра сде-

лает кнопку **Сброс** (Reset) на вкладке **Дополнительно** (Advanced) диалогового окна **Свойства обозревателя** (Internet Options) неактивной, и пользователи не смогут случайно или намеренно сбросить настройки браузера на первоначальные.

- **Проверка подписи для загруженных программ** (Check for signatures on downloaded programs) и **Разрешать установку или выполнение программ с недействительной цифровой подписью** (Allow software install even if the signature is invalid) — часто недействительная цифровая подпись является признаком подделки или модификации оригинальной программы злоумышленником. По умолчанию при попытке установить такую программу операционная система выводит предупреждение о недействительности цифровой подписи, и пользователи могут разрешить или запретить установку. Но многие могут либо не знать, что такое электронная подпись, либо не обратить на это предупреждение внимания. В связи с этим, параметр **Проверка подписи для загруженных программ** (Check for signatures on downloaded programs) рекомендуется включить, а параметр **Разрешать установку или выполнение программ с недействительной цифровой подписью** (Allow software install even if the signature is invalid) отключить, чтобы пользователи получали предупреждение о достоверности электронной цифровой подписи для загружаемых программ и не могли загружать на компьютер программы и элементы ActiveX с недействительными подписями.

- **Не сохранять шифрованные страницы на диске** (Do not save encrypted pages to disk) — для работы с некоторыми веб-сервисами используется передача данных по защищенному протоколу HTTPS с использованием протоколов шифрования. Как правило, по таким протоколам передается различная конфиденциальная информация, например регистрационные данные, данные о проводимых платежах и состоянии счета в электронных платежных системах. По умолчанию веб-страницы, загружаемые по защищенным протоколам, сохраняются в кэше браузера, как и те, которые загружаются по обычным протоколам, и могут быть скопированы и переданы злоумышленнику с помощью различных вредоносных программ. Если данный параметр включить, то страницы, передаваемые по протоколу HTTPS, не будут кэшироваться на жесткий диск. Этот параметр может замедлить работу браузера, но повысит безопасность.

- **Отключить поддержку шифрования** (Turn off Encryption Support) — поскольку некоторые протоколы шифрования, например SSL 2.0, на данный момент не являются надежными, имеет смысл отключить

возможность их использования, чтобы они не использовались при взаимодействии с веб-серверами по защищенным протоколам связи. Для этого данный параметр следует включить и в раскрывающемся списке **Сочетания безопасных протоколов** (Secure Protocol combinations) диалогового окна настройки параметра выбрать нужное сочетание разрешенных протоколов шифрования.

Помимо перечисленных выше параметров, можно включить параметр **Удалять все файлы из временной папки Интернета при закрытии браузера** (Empty Temporary Internet Files when browser is closed). Этот параметр позволит сэкономить место на жестком диске и обезопасить себя или других пользователей от просмотра кэшированных веб-страниц с конфиденциальной информацией, полученных по обычным протоколам, например, с почтовых сервисов или блогов.

Настройка зон безопасности

Взаимодействие Internet Explorer с веб-страницами, скриптами, программами, видео и звуковыми фрагментами и другими элементами, загружаемыми из локальной сети или Интернета, определяется параметрами безопасности. Таких параметров довольно много, и для облегчения работы с ними используются уровни безопасности — варианты настроек параметров безопасности, обеспечивающие определенный уровень защиты браузера.

В свою очередь все веб-узлы, с которыми взаимодействует браузер, разделяются на четыре зоны, для которых может быть установлен определенный уровень безопасности:

- **Зона Интернета** (Internet) — к этой зоне относятся все веб-узлы, не входящие в другие зоны. Для данной зоны уровень безопасности не может быть ниже умеренного.
- **Местная интрасеть** (Local intranet) — веб-узлы и страницы, располагающиеся в локальной или корпоративной сети. Для этой зоны можно выбрать любой уровень безопасности.
- **Надежные узлы** (Trusted sites) — веб-узлы, располагающиеся в Интернете или локальной сети, но специально включенные в список надежных узлов. Для таких узлов, как и для узлов интрасети, можно установить любой уровень безопасности.
- **Ограниченные узлы** (Restricted sites) — к этой зоне относятся потенциально-опасные веб-узлы, внесенные в соответствующий список. Уровень безопасности для таких узлов не может быть ниже высокого.

Настройка зон безопасности осуществляется в диалоговом окне **Свойства обозревателя** (Internet Options) на вкладке **Безопасность** (Security). Уровень безопасности для каждой из четырех зон задается с помощью ползункового регулятора, а отдельные параметры можно настроить с помощью диалогового окна, вызываемого кнопкой **Другой** (Custom). Обычно параметры безопасности настраивают, выбрав один из уровней в качестве шаблона, а затем изменив один или несколько отдельных параметров вручную.

Пользуясь этими элементами управления, пользователи могут изменить параметры безопасности, заданные по умолчанию для отдельных зон, например, разрешить загрузку неподписанных элементов ActiveX и тем самым нарушить безопасность браузера и всей системы.

Избежать подобной ситуации можно, настроив необходимые параметры уровней безопасности зон и скрыв вкладку **Безопасность** (Security) от пользователей. Последнее действие может быть необязательным, поскольку параметры зон безопасности, заданные политиками, не позволяют изменить настройки средствами браузера.

Проще всего закрепить с помощью редактора политик за каждой зоной соответствующий уровень безопасности.

1. Для настройки уровня безопасности зон откройте консоль управления и выберите оснастку **Политика «Локальный компьютер\Не администраторы»** (Local Computer\Non-Administrators Policy) или оснастку **Политика «Локальный компьютер»** (Local Computer Policy), если настройки будут применяться для всех пользователей, работающих за данным компьютером.

2. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Internet Explorer ⇒ Панель управления браузером ⇒ Вкладка безопасности** (User Configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Internet Explorer ⇒ Internet Control Panel ⇒ Security Page). Если настройки будут применяться для всех пользователей, работающих за компьютером, узел следует открывать в кусте **Конфигурация Компьютера** (Computer Configuration).

3. Дважды щелкните мышью по параметру **Шаблон зоны Интернета** (Internet Zone Template) для настройки зоны Интернета.

4. В открывшемся диалоговом окне установите переключатель в положение **Включить** (Enabled) и в раскрывающемся списке **Интернет** (Internet) выберите уровень безопасности, который будет применяться для веб-узлов, отнесенных к зоне Интернета, например **Уме-**

ренно высокий (Medium High).

5. Нажмите кнопку **ОК**.
6. Повторите действия 3 — 5 для остальных шаблонов зон безопасности.

После завершения настройки ползунковый регулятор выбора уровня безопасности зоны не будет отображаться (рис. 9.6), и пользователи не смогут самостоятельно изменять уровень безопасности зоны Интернета, а в нижней части диалогового окна **Свойства браузера** (Internet Options) на вкладке **Безопасность** (Security) будет отображаться уведомление **Некоторыми параметрами управляет системный администратор** (Some settings are managed by your system administrator). Параметры безопасности в диалоговом окне, вызываемом кнопкой **Другой** (Custom), будут также недоступны для изменения.

В некоторых случаях предлагаемые настройки уровней безопасности могут не устраивать администратора, например, параметры уровня **Выше средне-**

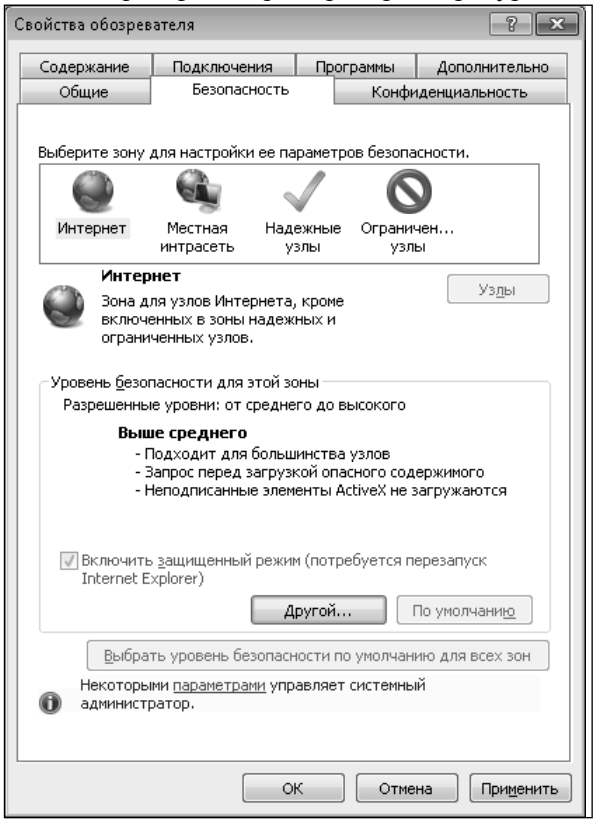


Рис. 9.6. ***Диалоговое окно*** **Свойства обозревателя** ***после закрепления уровня безопасности***

го (Medium-high) могут не обеспечивать нужной безопасности, а параметры уровня **Высокий** (High) сильно ограничивают функциональность браузера. С помощью политик уже упоминавшегося выше узла **Зона Интернета** (Internet Zone), располагающегося в узле **Вкладка безопасности** (Security Page), можно изменить отдельные параметры для выбранного уровня безопасности, например, запретить загрузку неподписанных элементов управления ActiveX.

1. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Internet Explorer ⇒ Панель управления браузером ⇒ Вкладка безопасности ⇒ Зона Интернета** (User Configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Internet Explorer ⇒ Internet Control Panel ⇒ Security Page⇒ Internet Zone).
2. Дважды щелкните мышью по выбранному для настройки параметру, например, **Загрузка неподписанных элементов ActiveX** (Download unsigned ActiveX controls). В открывшемся диалоговом окне редактирования параметра политики доступно три варианта политики:

- **Отключено** (Disabled) — пользователи не смогут загружать неподписанные элементы ActiveX.
- **Включено** (Enabled) — при установке переключателя в это положение будет доступен раскрывающийся список **Загружать неподписанные элементы ActiveX** (Download unsigned ActiveX controls), в котором можно выбрать, будут ли элементы ActiveX загружаться автоматически или перед загрузкой таких элементов будет выводиться запрос пользователю. Либо эти элементы не будут загружаться вообще.
- **Не задано** (Not configured) — действия определяются текущими настройками браузера и могут быть изменены пользователями.
- Установите переключатель в положение **Включено** (Enabled) и в раскрывающемся списке **Загружать неподписанные элементы ActiveX** (Download unsigned ActiveX controls) выберите **Отключить** (Disable) для отключения возможности загружать неподписанные компоненты. При необходимости введите в поле ввода **Комментарий** (Comment) комментарий к вашим действиям.

3. Нажмите кнопку **ОК**.
4. При необходимости повторите действия 3 и 4 для остальных параметров узла.

После завершения настройки уровень безопасности для выбранной зоны из-

менится на **Другой** (Custom), а настроенные с помощью редактора групповой политики параметры будут недоступны для изменения средствами браузера.

Отключение вкладок диалогового окна Свойства обозревателя

Как уже упоминалось выше, при изменении настроек безопасности браузера вкладку **Безопасность** (Security) лучше отключить. Эта рекомендация приводится и в редакторе политик.

Впрочем, при желании или необходимости можно отключить любую вкладку диалогового окна **Свойства обозревателя** (Internet options), поскольку большинство элементов управления на этих вкладках так или иначе влияют на безопасность браузера.

1. Для отключения вкладки **Безопасность** (Security) диалогового окна **Свойства обозревателя** (Internet options) для всех пользователей, не являющихся администраторами, откройте консоль управления и выберите оснастку **Политика «Локальный компьютер\Не администраторы»** (Local Computer\Non-Administrators Policy).
2. Откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Internet Explorer ⇒ Панель управления браузером** (User Configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Internet Explorer ⇒ Internet Control Panel).
3. Дважды щелкните мышью по параметру **Отключить вкладку «Безопасность»** (Disable the Security page).
4. В открывшемся диалоговом окне установите переключатель в положение **Включить** (Enabled). При необходимости введите в поле ввода **Комментарий** (Comment) комментарий к вашим действиям.
5. Нажмите кнопку **ОК**.
6. При необходимости повторите действия 3 - 5 для остальных параметров.

После завершения настройки в диалоговом окне **Свойства обозревателя** (Internet options) будут отображаться только разрешенные вкладки (рис. 9.7).

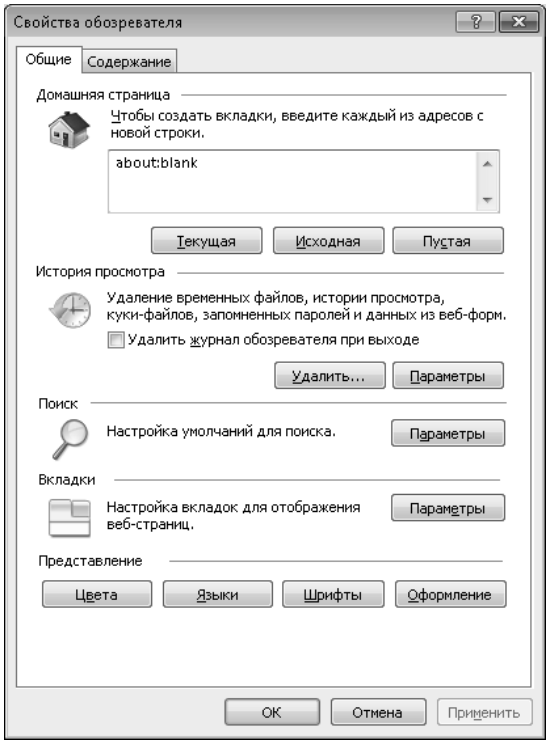


Рис. 9.7. ***Диалоговое окно*** **Свойства обозревателя** ***после отключения отдельных вкладок***

Заключение

Описанные в этой главе политики составляют весьма небольшую часть от имеющихся в редакторе. Большая часть не рассмотренных в этой главе политик, относящихся к настройке браузера, имеет довольно подробное описание и рекомендации по использованию, понятные даже неспециалисту. С этими описаниями настоятельно рекомендуется внимательно ознакомиться перед изменением настроек, даже если название политики четко говорит о ее назначении, поскольку действие некоторых политик распространяется только на старые версии браузера, а иногда и операционной системы.


Windows 8

Глава 10.

Хакинг среды Windows 8 (Проводник и т.д.)

Проводник Windows представляет собой удобное средство, реализующее графический интерфейс доступа к файлам и папкам операционной системы, то есть Проводник Windows является стандартным файловым менеджером операционной системы Windows. В Редакторе локальной групповой политики имеется специальный узел **Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (Administrative Templates ⇒ Windows Components ⇒ Windows Explorer), в котором можно найти несколько десятков параметров политик, позволяющих произвести настройку Проводника Windows и компонентов операционной системы, использующих Проводник. Также в этом узле находятся параметры политик, напрямую не связанные с работой Проводника Windows, решающие более глобальные вопросы, например вопросы безопасности операционной системы.

В данной главе будут рассмотрены параметры политик узла **Проводник Windows** (Windows Explorer). Даже если при работе с компьютером вы не используете Проводник Windows, а пользуетесь файловым менеджером стороннего производителя, рекомендуется не пропускать эту главу, ведь в указанном узле содержится множество интересных и важных параметров политик, имеющих к Проводнику Windows неочевидное отношение. Знания, полученные в данной главе, помогут повысить уровень безопасности операционной системы и сделать работу с компьютером удобнее.

10.1. Настройки отображения Проводника Windows

Наверное, ни для кого не будет открытием тот факт, что удобство рабочей среды может значительно сказаться на производительности и качестве работы. Если говорить о работе с файлами и папками компьютера, то удобно настроенный Проводник Windows может сделать работу несколько проще и поможет сэкономить немало времени. Для каждого пользователя операционной системы понятие удобства является сугубо индивидуальным. Именно для этого в программе Проводник Windows имеется такое большое количество настроек отображения, доступных также при помощи групповых политик. Впрочем, некоторые настройки отображения доступны только при помощи групповых политик.

Настройка интерфейса Проводника Windows

Многие из политик настройки интерфейса Проводника Windows имеют свое отражение в меню самой программы, впрочем, в некоторых случаях удобнее использовать именно групповые политики.

По умолчанию отображение строки меню Проводника Windows отключено. Ее отображение можно включить, выбрав пункт меню **Упорядочить ⇒ Представление ⇒ Строка меню** (Organize ⇒ Layout ⇒ Menu bar). Этого же результата можно добиться, используя параметр политики **Отображать строку меню в проводнике Windows** (Display the menu bar in Windows Explorer). Данный параметр может быть найден в узле **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer).

> **Примечание.** Получить доступ к строке меню, даже если она не отображается, можно нажатием клавиши **Alt**.

При помощи групповой политики также можно определять, будут ли отображаться определенные области Проводника Windows. При этом, хотя схожие настройки имеются в меню Проводника Windows, групповые политики имеют больший приоритет: если отключить отображение области при помощи групповой политики, то при помощи меню Проводника Windows вернуть ее обратно не удастся. Для отключения области Проводника Windows:

1. Выберите необходимый объект оснастки и запустите соответствующий редактор. Данную политику можно определять для каждого пользователя системы отдельно.
2. В дереве политик откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows ⇒ Область кадра проводника** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer ⇒ Explorer Frame Pane).
3. Если необходимо:
   - Отключить **Область сведений** (Details Pane) Проводника Windows, то дважды щелкните мышью по параметру **Отключить область сведений** (Turn off Details Pane). Откроется диалоговое окно редактирования параметра политики.
   - Отключить **Область просмотра** (Preview Pane) Проводника Windows, то дважды щелкните мышью по параметру **Отключить область просмотра** (Turn off Preview Pane). Откроется ди-

алоговое окно редактирования параметра.

4. Чтобы групповая политика вступила в силу, установите переключатель в положение **Включить** (Enable). Не забудьте оставить примечание в поле ввода **Комментарий** (Comments), если вы документируете все свои действия в отношении групповых политик.

5. Нажмите кнопку **ОК**.

Если параметры политики не включены, **Область сведений** (Details Pane) и **Область просмотра** (Preview Pane) отображаются в Проводнике Windows, если иное не предусмотрено настройками программы.

По умолчанию в Проводнике Windows отображаются эскизы файлов: для графических изображений это будут их уменьшенные копии, для видеофайлов — уменьшенный кадр видеофайла. Использование эскизов файлов позволяет экономить время и делает работу с графическими и видеофайлами более удобной — эскиз загружается гораздо быстрее, чем файл в полном размере. Однако в некоторых случаях использование эскизов может оказаться неудобным. Одной из таких ситуаций является просмотр папки с большим количеством графических или видеоизображений очень высокого качества — загрузка их эскизов может быть неоправданно долгой. Особенно если вы хотите открыть конкретный файл, имя которого вам известно — в этом случае нет необходимости загружать эскизы остальных файлов в папке.

В этом случае вы можете отключить использование эскизов файлов и заменить их стандартными значками. Это можно сделать, установив соответствующий значок в диалоговом окне **Параметры папок** (Folder Options) на вкладке **Вид** (View). Чтобы открыть данное диалоговое окно, выберите пункт меню **Упорядочить ⇒ Параметры папок и поиска** (Organize ⇒ Folder and search options) Проводника Windows.

Эту задачу можно также решить при помощи параметра политики **Отключить отображение эскизов и отображать только значки** (Turn off the display of thumbnails and only display icons), доступного на узле **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer).

Особенно остро вопрос отображения эскизов стоит при работе с папкой удаленно. При низкой скорости доступа к сети загрузка даже небольшого количества эскизов может занимать значительное время, раздражать пользователя и отнимать драгоценное время. При помощи параметра политики **Отключить отображение эскизов и отображать только значки в сетевых папках**

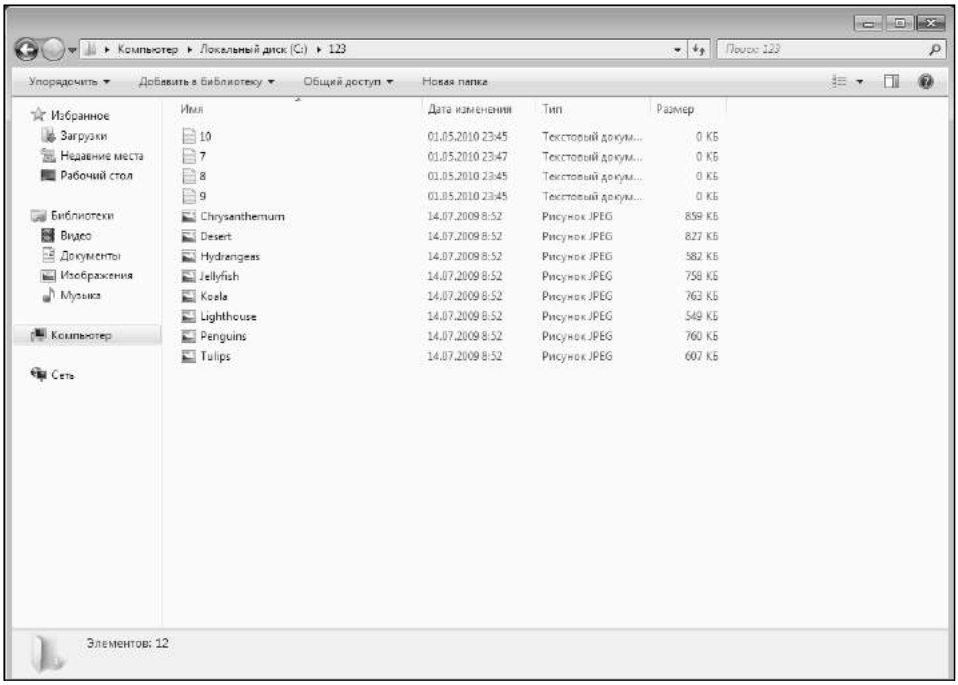


Рис. 10.1. ***Проводник Windows с отключенной функцией числового упорядочивания***

(Turn off the display of thumbnails and only display icons on network folders) можно отключить отображение эскизов только для сетевых папок, при этом для всех остальных папок эскизы отображаться будут, тем самым не снижается удобство работы с локальными ресурсами. Данный параметр политики располагается в том же узле, что и предыдущий.

Многие пользователи, перейдя с Windows 2000 и более ранней версии операционной системы семейства Windows на более новые, ощущали некоторый дискомфорт при работе с именами файлов в программе Проводник Windows. Одной из причин неудобств оказалось то, что в старых версиях операционных систем использовалось алфавитное упорядочивание числовых имен, то есть каждый разряд числа распознавался как отдельный символ, сравнение имен происходило посимвольно. Так, получалось, что файл с именем «10.jpg» отображался в папке раньше, чем файл «9.jpg» (рис. 10.1). Конечно, большинству пользователей это создавало некоторые неудобства, поэтому в новых версиях операционных систем семейства Windows используется числовое упорядочивание числовых имен. То есть сравнение числовых имен осуществляется не посимвольно, а по увеличению значения числа. То есть файл с именем «9.jpg» отображается в папке раньше, чем файл «10.jpg».

Впрочем, многим пользователям такая система кажется неудобной — хочется вернуться к универсальному алфавитному упорядочиванию. В узле **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer) для таких случаев доступен параметр политики **Отключить числовое упорядочивание проводника Windows** (Turn off numerical sorting in Windows Explorer).

Интерфейс операционной системы Windows и ее компонентов, таких как Проводник Windows, тщательно продуман огромной командой разработчиков фирмы Microsoft: они сделали все, чтобы работа с компьютером была приятнее и удобнее. К тому же вы имеете огромное число инструментов, позволяющих подстроить настройки отображения под свой вкус. Однако в некоторых ситуациях предпочтительнее отказаться от некоторых визуальных излишеств, например от анимации элементов управления и окон. Это позволяет сделать удобнее работу пользователей с ограниченными зрительными способностями. При этом не стоит забывать, что использование анимации отнимает некоторое количество системных ресурсов: отказ от анимации позволяет несколько повысить производительность системы и снизить расход батареи мобильных компьютеров.

Для того чтобы отказаться от использования анимации общих элементов управления и окон, необходимо открыть узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer) и применить параметр политики **Отключить анимацию общих элементов управления и окон** (Turn off common control and windows animation).

Пункт меню **Файл** (File) командной панели проводника Windows предоставляет доступ ко многим важнейшим инструментам программы: создание библиотек и ярлыков, удаление файлов и папок, возможность смены имен файлов и папок, а также доступ к их свойствам. В определенных ситуациях бывает необходимо запретить доступ к этому пункту меню. Сделать это очень просто: в узле **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer) вы можете найти политику **Удалить меню «Файл» из проводника Windows** (Remove File menu from Windows Explorer).

> **Примечание**. Данный параметр только лишь скрывает пункт меню **Файл** (File) строки (рис. 10.2), при этом пользователь может использовать другие способы выполнения задач, представленные в пункте меню **Файл** (File) строки меню.

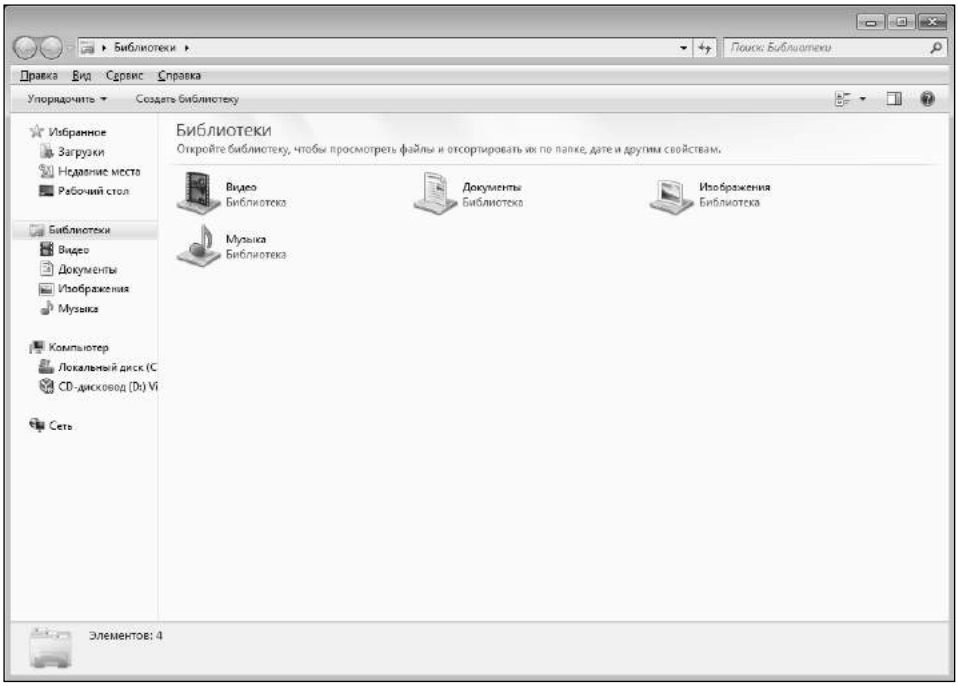


Рис. 10.2. ***Окно Проводника Windows с отключенным пунктом меню Файл командной панели***

Если вы интересуетесь вопросами безопасности, вас должен заинтересовать параметр политики **Удалить команду «Свойства папки» из меню «Сервис»** (Removes the Folder Options menu item from the Tools menu) узла **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer). Данный параметр позволяет запретить доступ к диалоговому окну **Свойства папки** (Folder Options) из всех меню Проводника Windows, а также Панели управления. В диалоговом окне **Свойства папки** (Folder Options) можно устанавливать различные параметры Проводника Windows, например параметры рабочего стола Active Desktop или представления папок в виде веб-страниц, скрытых системных и автономных файлов.

Также с точки зрения безопасности представляет большой интерес параметр политики **Скрыть команду «Управление» из контекстного меню проводника Windows** (Hides the Manage item on the Windows Explorer context menu) узла **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer).

Данный параметр позволяет запретить вызов консоли **Управление компьютером** (Computer management) из меню Проводника Windows. Напомним, что данная консоль предоставляет пользователю комплекс инструментов конфигурирования операционной системы и, по сути, представляет собой совокупность консолей **Просмотр событий** (Event Viewer), **Диспетчер устройств** (Device Manager) и **Управление дисками** (Disk Management).

Данный параметр не запрещает вызов консоли **Управление компьютером** (Computer management) другими способами, минуя Проводник Windows. Помимо уже известных из предыдущих глав методов запуска консоли, можно воспользоваться командой меню **Администрирование ⇒ Управление компьютером** (Administrative Tools ⇒ Computer management).

Некоторые системные администраторы предпочитают запретить подключение и отключение сетевых дисков, используя Проводник Windows. Это очень просто сделать при помощи параметра групповой политики **Удалить команды «Подключить сетевой диск» и «Отключить сетевой диск»** (Remove «Map Network Drive» and «Disconnect Network Drive») узла **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer).

Стоит отметить, что данный параметр не запрещает пользователям подключаться к другим компьютерам — он лишь удаляет команды **Подключить сетевой диск** (Map Network Drive) и **Отключить сетевой диск** (Disconnect Network Drive) из меню Проводника Windows и окна **Сеть** (Network Locations).

Наверное, вы уже обратили внимание, что многие из только что рассмотренных параметров политик, например, такие как **Скрыть команду «Управление» из контекстного меню проводника Windows** (Hides the Manage item on the Windows Explorer context menu), оставляют за пользователем возможность получить доступ к запрещенному элементу другим путем. Зачастую решить эту задачу можно запретив вызов всех контекстных меню по умолчанию в Проводнике Windows и Рабочем столе. Для этого можно воспользоваться параметром политики **Запретить вывод контекстного меню по умолчанию для проводника Windows** (Remove Windows Explorer's default context menu), что располагается в узле **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer). После применения политики щелчок правой кнопкой мыши по любому элементу интерфейса Проводника Windows или Рабочего стола не будет иметь какого-либо результата. Однако стоит за-

метить, что данный параметр политики запрещает только лишь вызов контекстных меню. Пользователь по-прежнему может получить доступ другими способами к функциям, заключенным в пунктах этих контекстных меню.

В ранних версиях операционных систем семейства Windows не существовало встроенного программного средства записи компакт-дисков, что создавало пользователям немало проблем: после приобретения соответствующего устройства необходимо было покупать дополнительное дорогостоящее программное обеспечение, позволяющее использовать функции записи. В современных операционных системах семейства Windows Проводник имеет встроенную функцию записи компакт-дисков. Однако многие пользователи считают возможности записи компакт-дисков Проводника Windows довольно бедными и предпочитают ему платные альтернативы.

Скрыть возможности записи компакт-дисков Проводника Windows очень просто: достаточно включить параметр политики **Удалить возможности записи компакт-дисков** (Remove CD Burning features) узла **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer). При этом стоит заметить, что данный параметр политики не запрещает запись и перезапись компакт-дисков в данной операционной системе — он всего лишь скрывает эти возможности в Проводнике Windows, записывать компакт-диски можно будет по-прежнему, воспользовавшись любым другим программным средством с данной функцией.

Рассмотрим еще три параметра политики узла **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer): **Удалить вкладку «Оборудование»** (Remove Hardware tab), **Удалить вкладку DFS** (Remove DFS tab) и **Удалить вкладку «Безопасность»** (Remove Security tab). Данные параметры политики предназначены, в некоторой степени, помочь администратору в организации политики безопасности системы.

Параметр политики **Удалить вкладку «Оборудование»** (Remove Hardware tab) удаляет вкладку **Оборудование** (Hardware) из диалоговых окон **Мышь** (Mouse), **Клавиатура** (Keyboard) и **Звуки и аудиоустройства** (Audio Devices) Панели управления, а также из диалогового окна **Свойства** (Properties) всех локальных дисков, включая жесткие диски, дискеты и компакт-диски. Вкладка **Оборудование** (Hardware) данных диалоговых окон предоставляет пользователю доступ к списку устройств и свойств этих устройств. Также при помощи кнопки **Устранение неполадок** (Troubleshoot) диалогового окна **Оборудование** (Hardware) можно искать и устранять связанные с

устройствами неполадки. В интересах безопасности системы необходимо максимально сузить круг лиц, которые имеют доступ к диалоговому окну настройки оборудования.

Параметр политики **Удалить вкладку DFS** (Remove DFS tab) удаляет вкладку **DFS** (DFS) из Проводника Windows и других программ, использующих окно Проводника Windows, таких как, например, Мой компьютер. Данная вкладка используется для просмотра и изменения свойств общих ресурсов распределенной файловой системы DFS, доступных на этом компьютере. Данный параметр политики, подобно своим соседям, лишь удаляет элементы управления из окна Проводника Windows, оставляя за пользователем возможность получить доступ к DFS другими способами.

Параметр политики **Удалить вкладку «Безопасность»** (Remove Security tab) должен заинтересовать любого системного администратора: он удаляет вкладку **Безопасность** (Security) диалогового окна **Свойства** (Properties) (рис. 10.3) любых объектов файловой системы, открытых при помощи Проводника Windows. Элементы данной вкладки позволяют произвести настройку параметров безопасности и просматривать список пользователей, имеющих доступ к этому ресурсу.

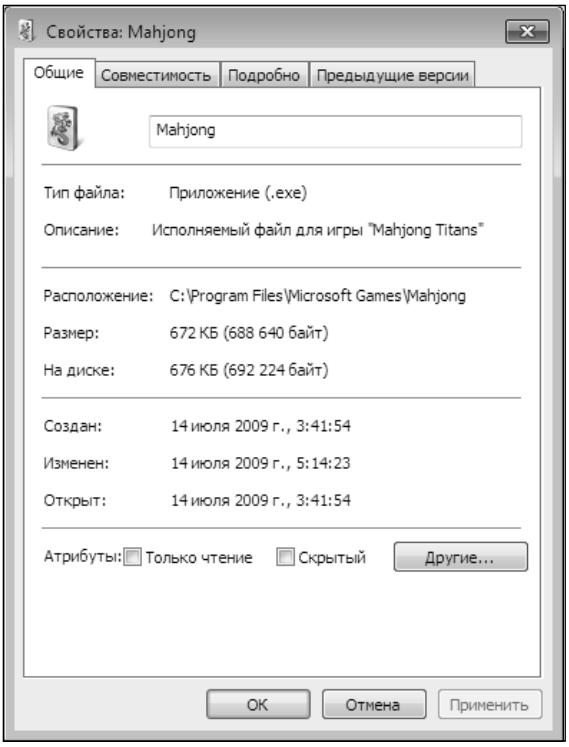


Рис. 10.3. ***Диалоговое окно*** **Свойства** ***с удаленной вкладкой*** **Безопасность**

Настройка диалоговых окон открытия и сохранения файлов

Стандартное диалоговое окно открытия и сохранения файлов видел каждый пользователь операционной системы Windows: эти окна присутствуют практически во всех программах, в которых осуществляется работа с внешними файлами. Естественно, при разработке операционной системы Windows было создано несколько групповых политик, определяющих работу этих диалоговых окон. Часть этих групповых политик находится в узле конфигурирования Проводника Windows, рассматриваемом в данной главе.

Для удобства пользователей система автоматически сохраняет историю последних посещенных папок. Если возникнет необходимость, можно быстро открыть недавно посещенную папку, нажав кнопку **Назад** (Back) диалогового окна или воспользовавшись раскрывающимся списком недавно открывавшихся файлов.

Некоторые пользователи предпочитают скрывать информацию о посещенных ими папках и открытых файлах. Сделать это можно при помощи параметров групповой политики **Скрыть раскрывающийся список недавно открывавшихся документов** (Hide the dropdown list of recent files) и **Скрыть кнопку «Назад» в общих диалогах открытия файлов** (Hide the common dialog back button) узла **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows ⇒ Общее диалоговое окно открытия файлов** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer ⇒ Common Open File Dialog).

Параметр политики **Скрыть раскрывающийся список недавно открывавшихся документов** (Hide the dropdown list of recent files) удаляет список недавно открывавшихся файлов из диалогового окна открытия файлов. Если включить данный параметр политики, то раскрывающийся список **Имя файла** (File name) превратится в обычное поле ввода.

Параметр политики **Скрыть кнопку «Назад» в общих диалогах открытия файлов** (Hide the common dialog back button) позволяет отключить отображение кнопки **Назад** (Back) во всех диалоговых окнах открытия и сохранения файлов. Данная кнопка была добавлена в версии Windows 2000 Professional и позволяет вернуться к отображению в диалоговом окне предыдущей посещенной папки.

> **Примечание.** Параметры политики **Скрыть раскрывающийся список недавно открывавшихся документов** (Hide the dropdown list of recent files) и **Скрыть кнопку «Назад» в общих диалогах открытия файлов** (Hide the common dialog back button) оказывают свое действие только на стандартные диалоговые окна открытия и сохранения файлов и не распространяются на прочие диалоговые окна.

Прочие настройки интерфейса

Для ускорения работы Проводника Windows, чтобы повторно полностью не загружать и обрабатывать файлы с целью создания их эскизов, создаются кэш-файлы. Они позволяют при повторном обращении пользователя к папке быстро загрузить эскизы всех содержащихся там элементов. Функция кэширования эскизов файлов включена в операционной системе Windows 8 по умолчанию, однако в некоторых случаях ее бывает необходимо отключить. Дело в том, что если на компьютере обрабатывают определенную информацию ограниченного доступа, то использование кэша может ставить ее конфиденциальность под сомнение, поскольку сохраненный кэш может быть легко прочитан другими пользователями.

На этот случай имеется следующий параметр групповой политики. Для отключения кэширования эскизов выполните следующие действия:

1. Выберите необходимый объект оснастки и запустите соответствующий редактор. Данную политику можно определять для каждого пользователя системы отдельно.
2. В дереве политик откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer).
3. Дважды щелкните мышью по параметру **Отключить кэширование эскизов изображений** (Turn off the caching of thumbnail pictures). Откроется диалоговое окно редактирования параметра политики.
4. Чтобы групповая политика вступила в силу, установите переключатель в положение **Включить** (Enable).
5. Не забудьте оставить примечание в поле ввода **Комментарий** (Comments), если вы документируете все свои действия в отношении групповых политик. Нажмите кнопку ОК.

После отключения кэширования эскизов работа с Проводником Windows может стать заметно медленнее — такова расплата за повышение уровня безопасности системы.

10.2. Полезные функции

В рассматриваемом узле, помимо параметров групповых политик, направленных непосредственно на работу Проводника Windows, имеются также параметры, решающие другие вопросы, напрямую не связанные с Прово-

дником. Многие из них могут оказаться действительно очень полезны администратору системы, например, параметры политик, направленные на решение вопросов обеспечения безопасности системы.

Вопросы обеспечения безопасности системы

Существует огромное количество параметров групповых политик, предназначенных для решения вопросов безопасности операционной системы. Эти параметры разбросаны по множеству узлов оснастки, узел настройки Проводника Windows — **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer) — не является в данном случае исключением.

Как правило, в наши дни на одном компьютере имеется более одного раздела жесткого диска. Нередко пользователи наделяют различные разделы различными функциями: первый раздел может содержать операционную систему и связанные с ней данные, второй — различное программное обеспечение, третий — различные документы, четвертый — некоторую конфиденциальную информацию. Очевидно, что к первому и четвертому разделам жесткого диска желательно запретить доступ, а то и вовсе скрыть их от посторонних глаз. Данная задача может быть легко разрешима при помощи групповой политики:

1. Выберите необходимый объект оснастки и запустите соответствующий редактор. Данную политику можно определять для каждого пользователя системы отдельно.
2. В дереве политик откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer).
3. Если вы хотите:

- Скрыть некоторые разделы жесткого диска, то дважды щелкните мышью по параметру **Скрыть выбранные диски из окна «Мой компьютер»** (Hide these specified drives in My Computer). Откроется диалоговое окно редактирования параметра политики. Данный параметр политики удаляет значки выбранных разделов дисков из программ Мой компьютер, Проводник Windows и стандартных диалоговых окон **Открыть** (Open), **Сохранить** (Save), **Сохранить как** (Save As) (рис. 10.4).
- Запретить доступ к некоторым разделам жесткого диска, то дважды

щелкните мышью по параметру **Запретить доступ к дискам через «Мой компьютер»** (Prevent access to drives from My Computer). Откроется диалоговое окно редактирования параметра политики. Данный параметр политики не удаляет значки выбранных разделов дисков из программ Мой компьютер, Проводник Windows и стандартных диалоговых окон **Открыть** (Open), **Сохранить** (Save), **Сохранить как** (Save As), однако в случае обращения пользователя к запрещенным разделам системой будет выведено сообщение об ошибке, а доступ предоставлен не будет.

4. Чтобы групповая политика вступила в силу, установите переключатель в положение **Включить** (Enable). Раскрывающийся список **Выберите одну из указанных комбинаций** (Pick one of the following combinations) области **Параметры** (Options) станет активным.

5. В раскрывающемся списке **Выберите одну из указанных комбинаций** (Pick one of the following combinations) выберите необходимую комбинацию разделов жесткого диска. Пункт **Ограничить доступ ко всем дискам** (Restrict all drives) запретит обращение пользователя к любому разделу жесткого диска. Пункт **Не ограничивать доступ к дискам** (Do not restrict drives) снимает все ограничения на доступ к любому разделу жесткого диска.

6. Не забудьте оставить примечание в поле ввода **Комментарий** (Comments), если вы документируете все свои действия в отношении групповых политик. Нажмите кнопку **ОК**.

Обратите внимание: данные параметры политик не запрещают получить доступ к указанным разделам жесткого диска при помощи других программ и методов. Например, можно обратиться к необходимому диску при помощи диалогового окна **Выполнить** (Run).

Также при помощи групповой политики можно ограничить доступ только к конкретным папкам. Реализуется это при помощи параметра политики **Отключить известные папки** (Disable Known Folders):

1. Выберите необходимый объект оснастки и запустите соответствующий редактор. Данную политику можно определять для каждого пользователя системы отдельно.

2. В дереве политик откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer).

3. Дважды щелкните мышью по параметру **Отключить известные пап-**

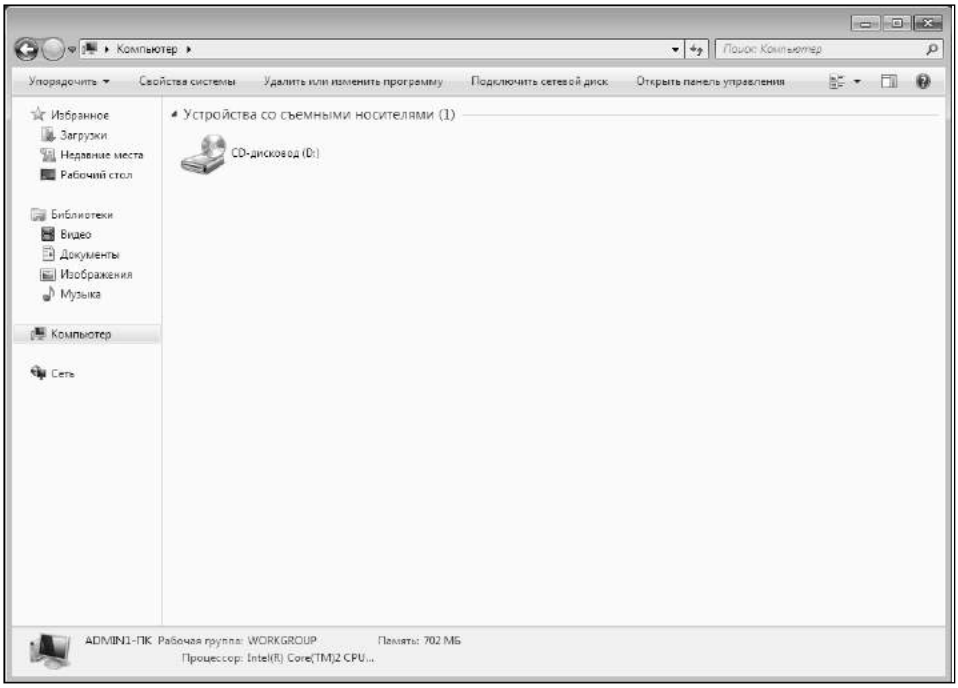


Рис. 10.4. ***Проводник Windows, в котором скрыты все разделы дисков, кроме D***

ки (Disable Known Folders). Откроется диалоговое окно редактирования параметра политики.

4. Чтобы групповая политика вступила в силу, установите переключатель в положение **Включить** (Enable). Кнопка **Показать** (Show) области **Параметры** (Options) станет активной.

5. Щелкните мышью по кнопке **Показать** (Show). Откроется диалоговое окно **Вывод содержания** (Show contents).

6. В диалоговом окне **Вывод содержания** (Show contents) (рис 10.5) в полях ввода укажите имена папок, к которым необходимо ограничить доступ. Имена можно указывать с помощью канонического имени или идентификатора. Например, папка **Образцы видео** (Sample Videos) может иметь имена «SampleVideos» или «{440fcffd-a92b-4739-ae1a-d4a54907c53f}».

7. Не забудьте оставить примечание в поле ввода **Комментарий** (Comments), если вы документируете все свои действия в отношении групповых политик. Нажмите кнопку **ОК**.

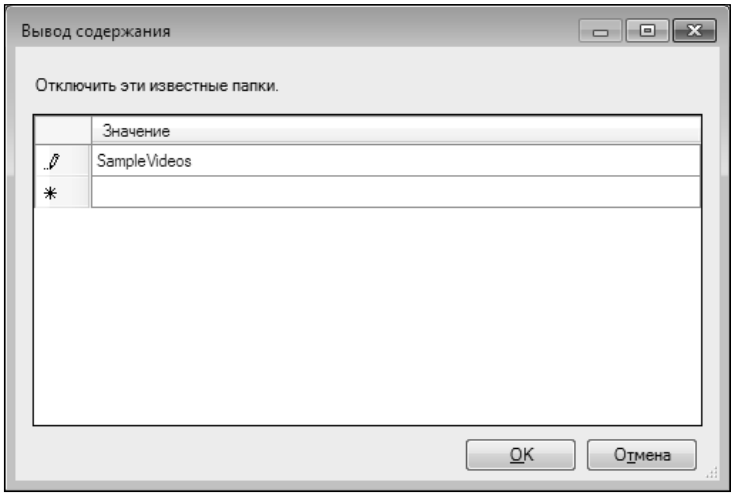


Рис. 10.5. *Диалоговое окно* Вывод содержания

Отключение известной папки запретит создавать в ней вложенные файлы и папки с помощью API папки. Однако если вложенные файлы и папки уже существовали до применения параметра политики, после применения параметра они автоматически удалены не будут — политика блокирует лишь создание новых файлов и папок. При необходимости удалить уже существовавшие вложенные элементы можно вручную.

> **Примечание.** При отключении известной папки приложения, работа которых зависит от существования этой папки, могут неправильно функционировать или вовсе прекратить свою работу.

Жесткие диски компьютера, подобно человеческому жилищу, требуют порядка при работе и периодической уборки. Если оставить дело на самотек, на компьютерах многих пользователей со временем становится непонятно, что и где находится. Часто это бывает связано с тем, что файлы и папки создаются в случайных местах. Особенно неприятно смотрится такой беспорядок в корневых каталогах. При помощи групповой политики можно запретить пользователям сохранять файлы и папки в корневых каталогах с файлами пользователя — это позволяет в некоторой степени помочь сохранению порядка. Данная задача реализуется при помощи параметра политики **Запретить пользователям добавлять файлы в корневую папку с файлами пользователя** (Prevent users from adding files to the root of their Users Files folders), который можно найти в узле **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Com-

ponents ⇒ Windows Explorer). Однако стоит заметить, что данный параметр не запрещает пользователям сохранять файлы и папки в настоящую папку профиля файловой системы, находящуюся в «%userprofile%».

Использование сочетаний клавиш с использованием клавиши **Windows** позволяют быстро запустить многие важные приложения операционной системы. Так, например, для быстрого запуска Проводника Windows можно использовать сочетание клавиш **Windows**+**E**, диалоговое окно **Выполнить** (Run) можно вызвать сочетанием клавиш **Windows**+**R**, для быстрого доступа к функции поиска используется сочетание клавиш **Windows**+**F**. Отключить использование сочетаний клавиш с использованием клавиши **Windows** можно при помощи групповой политики **Отключить сочетания клавиш Windows+X** (Turn off Windows+X hotkeys) узла **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer).

Параметр политики **Отключить защищенный режим протокола оболочки** (Turn off shell protocol protected mode) определяет функциональные возможности протокола оболочки. Так, при использовании всех возможностей протокола оболочки приложения могут беспрепятственно обращаться к любым файлам и папкам. В безопасном режиме приложения несколько ограничены в правах: могут открыть только определенные папки, а также не смогут запускать файлы.

По умолчанию протокол оболочки используется в защищенном режиме, что позволяет повысить уровень безопасности операционной системы. При необходимости можно отключить защищенный режим протокола оболочки, включив параметр политики **Отключить защищенный режим протокола оболочки** (Turn off shell protocol protected mode). Данный параметр может быть найден в узле **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer).

Отключение функции отслеживания ярлыков оболочки при перемещении

Использование ярлыков помогает существенно упростить работу с компьютером: достаточно пары щелчков мышью для запуска необходимого приложения или открытия папки. Ярлыки содержат абсолютный путь к исходному файлу ярлыка и относительный путь к текущему файлу. Если по какой-то причине, например, в случае перемещения элемента, система не находит те-

кущий путь, по умолчанию производится поиск файла назначения на исходном пути. В случае если ярлык был перенесен с другого компьютера, исходный путь может указывать на удаленный компьютер, например, на некоторый сервер в Интернете.

Параметр политики **Не отслеживать ярлыки оболочки при перемещении** (Do not track Shell shortcuts during roaming) определяет будет ли производиться поиск источников ярлыков системой в случае, если объектов, на который ссылается ярлык отсутствует на локальном компьютере. Данный параметр может быть найден в узле **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer). Если параметр включен, операционная система использует только текущий путь назначения, а поиск по исходному пути не осуществляется ни при каких обстоятельствах.

10.3. Настройки функции поиска

Каждый пользователь когда-нибудь пользовался функцией поиска: в наши дни, когда компьютеры располагают огромными массивами памяти, потерять на жестком диске необходимый файл не составляет труда. При этом многие пользователи зачастую сталкиваются с определенными проблемами: отыскать нужный файл бывает не так-то просто, а иногда функция поиска может оказаться бесполезной, так как не способна ощутимо помочь. Проводник Windows предоставляет большое количество настроек функции поиска. Доступ к диалоговому окну настройки функции поиска можно получить, выбрав пункт меню **Упорядочить ⇒ Параметры папок и поиска** (Organize ⇒ Folders and search options) Проводника Windows. В появившемся диалоговом окне **Параметры папок** (Folder options) содержатся различные настройки Проводника, настройки функции поиска находятся на вкладке **Поиск** (Search).

Многих пользователей данные настройки могут удовлетворить полностью. Если вы не относитесь к их числу, то можете воспользоваться возможностями групповых политик и получить еще несколько ценных инструментов для работы с функцией поиска.

Специфические настройки функции поиска Проводника Windows

После первой попытки поиска ключевых слов, в экране Проводника Win-

dows будет отображен список найденных файлов и папок. Вам также будет предложено повторить поиск в другом месте. По умолчанию вы увидите три кнопки для быстрого поиска: **Компьютер** (Computer), **Другое** (Custom) и **Интернет** (Internet). Кнопка **Компьютер** (Computer) продолжит поиск среди всех индексированных, неиндексированных, системных и скрытых файлов на компьютере. Кнопка **Другое** (Custom) позволяет настроить место поиска вручную — по ее нажатии будет вызвано диалоговое окно **Выберите место расположения для поиска** (Choose search location), в котором пользователь может точно определить области поиска. Кнопка **Интернет** (Internet) позволяет продолжить поиск в глобальной сети Интернет, то есть вне встроенных ресурсов компьютера. При этом будет открыт браузер Internet Explorer.

Если вы не хотите, чтобы пользователи при повторном поиске не могли быстро обратиться к поиску в Интернете, можно скрыть кнопку **Интернет** (Internet). Для этого:

1. Выберите необходимый объект оснастки и запустите соответствующий редактор. Данную политику можно определять для каждого пользователя системы отдельно.
2. В дереве политик откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer).
3. Дважды щелкните мышью по параметру **Удалить ссылку «Повторить поиск» при поиске в Интернете** (Remove the Search the Internet «Search again» link). Откроется диалоговое окно редактирования параметра политики.
4. Чтобы групповая политика вступила в силу, установите переключатель в положение **Включить** (Enable). Не забудьте оставить примечание в поле ввода **Комментарий** (Comments), если вы документируете все свои действия в отношении групповых политик.
5. Нажмите кнопку **ОК**.

По умолчанию данная политика отключена, программа Проводник Windows позволяет осуществлять функцию поиска в Интернете непосредственно из своего окна.

Если функция поиска в Интернете используется на компьютере довольно часто, то при помощи групповых политик можно сделать поиск удобнее. Параметр политики **Прикрепить поисковые веб-сайты к ссылкам «Повторить поиск» и меню «Пуск»** (Pin Internet search sites to the «Search again» links

and the Start menu) позволяет добавить к стандартным ссылкам области **Повторить поиск** (Search again) Проводника Windows внешние веб-сайты и сайты локальной интрасети**.** При определении параметра политики вы должны указать URL-адрес поискового веб-сайта и его отображаемое имя. URL-адрес вводится в формате OpenSearch.

Итак, для того, чтобы добавить кнопку поискового веб-сайта к области **Повторить поиск** (Search again in):

1. Выберите необходимый объект оснастки и запустите соответствующий редактор. Данную политику можно определять для каждого пользователя системы отдельно.
2. В дереве политик откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer).
3. Дважды щелкните мышью по параметру **Прикрепить поисковые веб-сайты к ссылкам «Повторить поиск» и меню «Пуск»** (Pin Internet search sites to the «Search again» links and the Start menu). Откроется диалоговое окно редактирования параметра политики (рис. 10.6).
4. Чтобы групповая политика вступила в силу, установите переключатель в положение **Включить** (Enable). Поля ввода области **Параметры** (Options) станут активными.
5. В поле ввода **URL-адрес сайта** (Site URL) необходимо ввести URL-адрес сайта в формате OpenSearch с ключевыми словами в качестве строки запроса. Например, вы можете ввести строку вида «http://www.example.com/results.aspx?q={ключевые слова}». В поле ввода **Имя сайта** (Site Name) введите отображаемое имя поискового сайта. В общей сложности вы можете определить до 5 дополнительных адресов. Данные ссылки являются общими для внешних веб-сайтов и соединителей или библиотек поиска. При этом ссылки поиска в Интернете имеют меньший приоритет, чем ссылки соединителей или библиотек поиска.
6. Не забудьте оставить примечание в поле ввода **Комментарий** (Comments), если вы документируете все свои действия в отношении групповых политик. Нажмите кнопку **ОК**.

Стоит отметить, что не все из указанных поисковых веб-сайтов будут отображены — вы увидите только несколько первых ссылок, обычно их число равняется четырем.

При этом имеется следующий приоритет ссылок: если ссылка **Еще результаты** (See more results) не отключена групповой политикой, то она по умолчанию прикрепляется первой. Затем по приоритету следует ссылка **Поиск в Интернете** (Search the Internet). Однако по умолчанию ее отображение отключено, включить ее отображение можно при помощи соответствующей групповой политики. Третьими по приоритету следуют пользовательские ссылки поиска в Интернете, прикрепленные с помощью групповой политики. Ниже по приоритету идут прикрепленные внешние и локальные ссылки, прикрепленные соединители и библиотеки поиска. Ссылки поиска в Интернете и локальной интрасети имеют меньший приоритет, чем ссылки соединителей и библиотек поиска.

Помимо ссылок на поисковые веб-сайты, вы также можете прикрепить ссылки на библиотеки или соединители поиска к стандартным ссылкам области **Повторить поиск** (Search again) Проводника Windows. Задача реализуется параметром политики **Прикрепить библиотеки или соединители поиска к ссылкам «Повторить поиск»** (Pin libraries and Search Connectors to the «Search again» links and the Start menu), который вы можете найти в том же узле, в котором находился последний рассмотренный параметр политики.

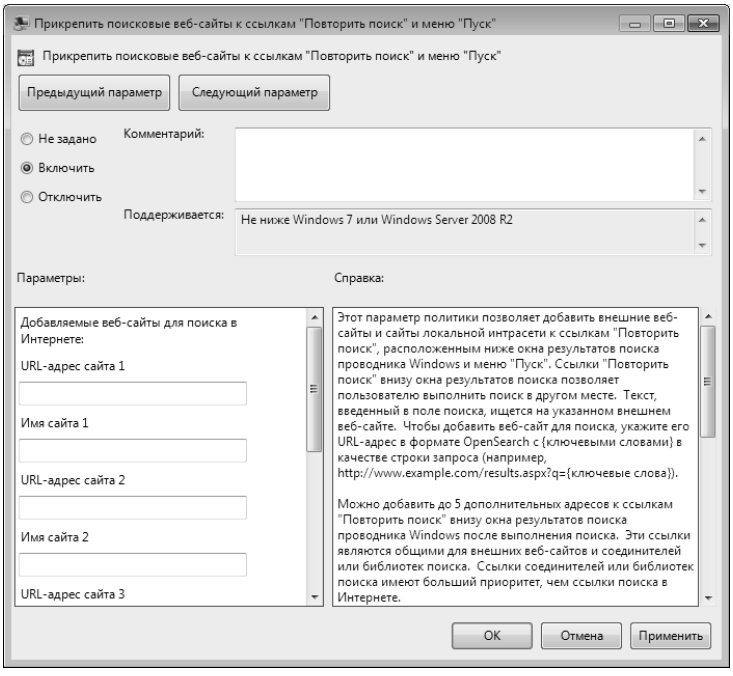


Рис. 10.6. *Диалоговое окно редактирования политики* Прикрепить поисковые веб-сайты к ссылкам «Повторить поиск» и меню «Пуск»

Файлы библиотек документов имеют расширение «.library-ms», файлы соединителей поиска имеют расширение «.searchConnector-ms». В диалоговом окне редактирования параметра политики будет необходимо указать размещение файла библиотеки или соединителя поиска — это необходимо сделать в поле ввода **Размещение** (Location) области **Параметры** (Options). Будьте внимательны при вводе: прикрепленная ссылка правильно сработает только в случае, если вы безошибочно укажете допустимый путь, а в указанной папке окажется необходимый файл с расширением «.library-ms» или «.searchConnector-ms». В общей сложности вы можете определить до 5 ссылок.

Отключение функции отображения прошлых запросов поиска

Довольно часто пользователь системы не желает по тем или иным причинам, чтобы его запросы поиска были сохранены в памяти компьютера и отображались в будущем при обращении к функции поиска. Такая ситуация может, например, возникнуть, если к одной учетной записи имеют доступ несколько человек и необходимо скрыть поисковые запросы от других пользователей этой же учетной записи.

Итак, чтобы отключить функцию отображения прошлых запросов поиска:

1. Выберите необходимый объект оснастки и запустите соответствующий редактор. Данную политику можно определять для каждого пользователя системы отдельно.
2. В дереве политик откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer).
3. Дважды щелкните мышью по параметру **Отключить отображение прошлых запросов поиска в поле поиска проводника Windows** (Turn off display of recent search entries in the Windows Explorer search box). Откроется диалоговое окно редактирования параметра политики.
4. Чтобы групповая политика вступила в силу, установите переключатель в положение **Включить** (Enable). Не забудьте оставить примечание в поле ввода **Комментарий** (Comments), если вы документируете все свои действия в отношении групповых политик.
5. Нажмите кнопку **ОК**.

Когда пользователь вводит некоторые данные в поле ввода поиска, Проводник Windows считывает данные прошлых введенных запросов поиска из реестра операционной системы и выводит на их основе подходящие результаты (рис. 10.7). После применения данного параметра политики запросы, введенные в поле ввода поиска, не будут сохраняться в реестре операционной системы.

10.4. Работа с «Корзиной» Windows

В рассматриваемом узле имеются также параметры групповой политики, отвечающие за работу «Корзины» Windows. Напомним, что при удалении файлов и папок с помощью Проводника Windows их копия сохраняется в «Корзине», для того, чтобы пользователь имел возможность в течение некоторого времени восстановить удаленную информацию.

Очевидно, что пока копии удаленных файлов находятся в «Корзине», они занимают драгоценное место на вашем жестком диске. При удалении большого количества файлов из системы, размер «Корзины» может быть довольно существенным. Не стоит говорить о ценности такого ресурса как память — памяти много не бывает. Впрочем, при помощи групповых политик вы можете повлиять на работу операционной систему с «Корзиной».

Так, например, отключить ее использование. Для этого:

1. Выберите необходимый объект оснастки и запустите соответствующий редактор. Данную политику можно определять для каждого пользователя системы отдельно.
2. В дереве политик откройте узел **Конфигурация пользователя ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer).
3. Дважды щелкните мышью по параметру **Не перемещать удаляемые файлы в «Корзину»** (Do not move deleted files to the Recycle Bin). Данный параметр политики не имеет дополнительных настроек, его можно лишь включить или включить.
4. Чтобы групповая политика вступила в силу, установите переключатель в положение **Включить** (Enable). Не забудьте оставить примечание в поле ввода **Комментарий** (Comments), если вы документируете все свои действия в отношении групповых политик.

Рис. 10.7. ***Функция отображения прошлых запросов поиска программы Проводник Windows***

5. Нажмите кнопку **ОК**.

Настоятельно не рекомендуется отключать использование «Корзины»: при необходимости вы попросту не сможете восстановить случайно удаленные файлы. Конечно, есть специальные средства для восстановления окончательно удаленных из системы файлов и папок, но их использование не всегда приводит к положительным результатам, к тому же это довольно сложный и утомительный процесс — гораздо проще пожертвовать немного места на вашем жестком диске и тем самым обезопасить себя от нежеланных потерь.

Еще одним параметром политики, имеющим непосредственное отношение к «Корзине» Windows, является параметр политики **Запрашивать подтверждение при удалении файлов** (Display confirmation dialog when deleting files) узла **Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows ⇒** (User configuration ⇒ Administrative Templates ⇒ Windows Components ⇒ Windows Explorer). Данный параметр политики отвечает за отображение диалогового окна подтверждения удаления файлов и папок. Данное диалоговое окно отображается как при перемещении файлов и папок в «Корзину» Windows, так и при полном их удалении.

Если данный параметр политики включен, то при удалении или перемещении в «Корзину» файлов и папок пользователь увидит диалоговое окно подтверждения удаления. Если параметр не определен или отключен, что является положением по умолчанию, диалоговое окно отображено не будет.

Заключение

Узел **Административные шаблоны ⇒ Компоненты Windows ⇒ Проводник Windows** (Administrative Templates ⇒ Windows Components ⇒ Windows Explorer) довольно объемен: он насчитывает несколько десятков параметров политик, решающих вопросы настройки визуализации Проводника Windows и различных компонентов операционной системы, работы функции поиска и «Корзины» Windows, а также некоторых специфических функций операционной системы. В данной главе были рассмотрены почти все параметры политик узла **Проводник Windows (**Windows Explorer). Надеемся, что материал главы показался вам довольно легким, и у вас не возникло проблем при использовании его на практике: принцип работы большинства параметров политик узла очевиден, поэтому их описание в главе было несколько поверхностным. Если суть работы некоторых параметров политик осталась вам не ясна, рекомендуем перечитать текст главы или обратиться к разделу справочной информации данного параметра.


Windows 8

«Горячие» клавиши Windows 8

-  : Переключение между меню Пуск и последним использованным приложением
-  + C: Доступ к дополнительной панели
-  + Tab: Доступ к новой панели задач
-  + I: Доступ к настройкам приложения на дополнительной панели
-  + H: Доступ к меню “Отправить” на дополнительной панели
-  + K: Доступ к меню “Устройства” на дополнительной панели
-  + Q: Доступ к экрану поиска приложения
-  + F: Доступ к экрану поиска файлов
-  + W: Доступ к экран настроек поиска
-  + P: Доступ к настройкам дополнительного экрана поиска
-  + Z: Открыть панель дополнительных возможностей, когда открыто приложение в Metro-UI
-  + X: Доступ к меню Windows-приложений
-  + O: Закрепить ориентацию экрана
-  + . : Переместить приложения к правому краю
-  + Shift + . : Переместить приложения к левому краю
-  + V: Просмотреть уведомления
-  + Shift + V: Просмотреть уведомления в обратном порядке
-  + PrtScn: Снять снимок экрана. Он автоматически появится в библиотеке, в паке Картинки
-  + Enter: Запустить Рассказчик

-  + E: Открыть Мой компьютер
-  + R: Открыть окно «Выполнить
-  + U: Открыть центр для быстрого доступа
-  + Ctrl + F: Открыть окно для поиска компьютеров
-  + Pause/Break: Открыть системную страницу
-  + 1..10: Запустить программу, прикреплённую к панели задач, где число – номер программы
-  + Shift + 1..10: Запустить новую копию программы, прикреплённую к панели задач.
-  + Ctrl + 1..10: Доступ к последнему активному состоянию программы, прикреплённую к панели задач
-  + Alt + 1..10: Открыть окно с дополнительными настройками программы, прикреплённой к панели задач
-  + B: Выделить первый пункт в списке. Используйте клавиши со стрелками для перемещения по меню
-  + Ctrl + B: Быстрый доступ к приложению, которое показало уведомление
-  + T: Прокрутить элементы в диспетчере задач
-  + M: Свернуть все окна
-  + Shift + M: Развернуть все свернутые окна
-  + D: Скрыть/показать рабочий стол
-  + L: Заблокировать систему
-  + Стрелка вверх: Увеличить программу
-  + Стрелка вниз: Свернуть/развернуть программу
-  + Home: Свернуть все окна, кроме текущего
-  + Стрелка влево: Прикрепить окно слева

-  + Стрелка вправо: Прикрепить окно справа
-  + Shift + Стрелка вверх: Переместить приложение сверху вниз
-  + Shift + Левая/Правая стрелка: Переместить приложение на следующий/предыдущий экран
-  + F1: Запустить справку и поддержку
- PageUp: Пролистать дальше
- PageDown: Пролистать назад
- Esc: Закрыть дополнительную панель
- Ctrl + Esc: Переключить между меню Пуск и последним использованным приложением
- Ctrl + колесо мыши: Активировать увеличение для нового меню Пуск
- Alt: Показать все скрытые меню
- Alt + D: Переместить курсор в адресную строку
- Alt + P: Показать панель предпросмотра в Проводнике
- Alt + Tab: Прокрутить вперед по открытым окнам
- Alt + Shift + Tab: Прокрутить назад по открытым окнам
- Alt + F: Открыть диалог главного меню окна
- Alt + Пробел: Доступ к дополнительному меню текущего окна
- Alt + Esc: Перелистывание открытых окон
- Alt + Enter: Открыть диалог Свойств выделенного элемента
- Alt + PrtScn: Снять снимок экрана и поместить его в буфер обмена
- Alt + Стрелка вверх: Перейти на один уровень вверх в Проводнике
- Alt + Стрелка влево: Показать предыдущую папку
- Alt + Стрелка вправо: Показать следующую папку
- Shift + Insert: CD/DVD Загрузка CD/DVD без Автозапуска
- Shift + Delete: Навсегда удалить выделенный элемент (без помещения его в Корзину)
- Shift + F6: Пролистать возможные варианты установки курсора в окне
- Shift + F10: Доступ к контекстному меню выделенного элемента

- Shift + Tab: Пролистать возможные варианты установки курсора в окне
- Shift + Клик мыши: Выделить группу элементов
- Shift + Клик мыши на программе на Панели задач: Запустить новую копию программы
- Shift + Клик правой кнопкой мыши на программе на Панели задач: Доступ к контекстному меню выделенного элемента
- Ctrl + A: Выделить всё
- Ctrl + C: Копировать
- Ctrl + X: Вырезать
- Ctrl + V: Вставить
- Ctrl + D: Удалить
- Ctrl + Z: Отменить
- Ctrl + Y: Повторить
- Ctrl + N: Открыть новое окно в Проводнике
- Ctrl + W: Закрыть окно в Проводнике
- Ctrl + E: Поставить курсор в окно поиска в правом верхнем углу окна
- Ctrl + Shift + N: Сделать новую папку
- Ctrl + Shift + Esc: Открыть диспетчер задач
- Ctrl + Alt + Tab: Открыть диспетчер задач. Используйте клавиши со стрелками, чтобы выбрать элемент
- Ctrl + Alt + Delete: Доступ к экрану блокировки
- Ctrl + Click: Выделить выделенные фрагменты
- Ctrl + Click и перенос элемента: Копировать элемент(ы) в данную папку
- Ctrl + Shift + Click и перенос элемента: Сделать ярлык данного элемента в этой папке
- Ctrl + Tab: Перейти вперед по закладкам
- Ctrl + Shift + Tab: Перейти назад по закладкам
- Ctrl + Shift + Click на Панели задач: Запустить новую копию программу от имени Администратора
- Ctrl + Click группе открытых окон на Панели задач: Пролистать программы в группе

- F1: Помощь
- F2: Переименовать файл
- F3: Открыть поиск
- F4: Показать подсказки для адресной строки
- F5: Обновить экран
- F6: Прокручивать по списку элементы в окне
- F7: Показать историю команд в командной строке
- F10: Показать скрытые меню
- F11: Развернуть окно во весь экран
- Tab: Пролистать возможные элементы в окне или диалоге выбора
- PrtScn: Снять снимок экрана и поместить его в буфер обмена
- Home: Идти наверх активного окна
- End: Идти вниз активного окна
- Delete: Удалить выбранный элемент
- Backspace: Показать предыдущую папку в Проводнике или вверх в иерархии папок или диалога сохранения
- Esc: Закрыть диалог [14]

Уважаемые господа!
Книги издательства «Наука и Техника»

Вы можете заказать наложенным платежом
в нашем интернет-магазине

www.nit.com.ru,

а также приобрести

➢ **в крупнейших магазинах г. Москвы:**

Т Д «БИБЛИО-ГЛОБУС»	ул. Мясницкая, д. 6/3, стр. 1, ст. М «Лубянка» тел. (495) 781-19-00, 624-46-80
Московский Дом Книги, «ДК на Новом Арбате»	ул.Новый Арбат, 8, ст. М «Арбатская», тел. (495) 789-35-91
Московский Дом Книги, «Дом технической книги»	Ленинский пр., д.40, ст. М «Ленинский пр.», тел. (499) 137-60-19
Московский Дом Книги, «Дом медицинской книги»	Комсомольский пр., д. 25, ст. М «Фрунзенская», тел. (499) 245-39-27
Дом книги «Молодая гвардия»	ул. Б. Полянка, д. 28, стр. 1, ст. М «Полянка» тел. (499) 238-50-01
Сеть магазинов «Новый книжный»	тел. (495) 937-85-81, (499) 177-22-11

➢ **в крупнейших магазинах г. Санкт-Петербурга:**

Санкт-Петербургский Дом Книги	Невский пр. 28 тел. (812) 448-23-57
«Энергия»	Московский пр. 57 тел. (812) 373-01-47
«Аристотель»	ул. А. Дундича 36, корп. 1 тел. (812) 778-00-95
Сеть магазинов «Книжный Дом»	тел. (812) 559-98-28

➢ **в регионах России:**

г. Воронеж, пл. Ленина д. 4	«Амиталь»	(4732) 24-24-90
г. Екатеринбург, ул. Антона Валека д. 12	«Дом книги»	(343) 253-50-10
г. Екатеринбург	Сеть магазинов «100 000 книг на Декабристов»	(343) 353-09-40
г. Нижний Новгород, ул. Советская д. 14	«Дом книги»	(831) 277-52-07
г. Смоленск, ул. Октябрьской революции д. 13	«Кругозор»	(4812) 65-86-65
г. Челябинск, ул. Монакова, д. 31	«Техническая книга»	(904) 972 50 04
г. Хабаровск	Сеть книжно-канцелярских магазинов фирмы «Мирс»	(4212) 26-87-30

➢ **и на Украине (оптом и в розницу) через представительство издательства**

г. Киев, ул. Курчатова 9/21, «Наука и Техника», ст. М «Лесная»
(044) 516-38-66
e-mail: nits@voliacable.com

Мы рады сотрудничеству с Вами!

Уважаемые господа!
Книги издательства «Наука и Техника»

Вы можете заказать наложенным платежом
в нашем интернет-магазине

www.nit.com.ru,

а также приобрести

➢ **в крупнейших магазинах г. Москвы:**

Т Д «БИБЛИО-ГЛОБУС»	ул. Мясницкая, д. 6/3, стр. 1, ст. М «Лубянка» тел. (495) 781-19-00, 624-46-80
Московский Дом Книги, «ДК на Новом Арбате»	ул.Новый Арбат, 8, ст. М «Арбатская», тел. (495) 789-35-91
Московский Дом Книги, «Дом технической книги»	Ленинский пр., д.40, ст. М «Ленинский пр.», тел. (499) 137-60-19
Московский Дом Книги, «Дом медицинской книги»	Комсомольский пр., д. 25, ст. М «Фрунзенская», тел. (499) 245-39-27
Дом книги «Молодая гвардия»	ул. Б. Полянка, д. 28, стр. 1, ст. М «Полянка» тел. (499) 238-50-01
Сеть магазинов «Новый книжный»	тел. (495) 937-85-81, (499) 177-22-11

➢ **в крупнейших магазинах г. Санкт-Петербурга:**

Санкт-Петербургский Дом Книги	Невский пр. 28 тел. (812) 448-23-57
«Энергия»	Московский пр. 57 тел. (812) 373-01-47
«Аристотель»	ул. А. Дундича 36, корп. 1 тел. (812) 778-00-95
Сеть магазинов «Книжный Дом»	тел. (812) 559-98-28

➢ **в регионах России:**

г. Воронеж, пл. Ленина д. 4	«Амиталь»	(4732) 24-24-90
г. Екатеринбург, ул. Антона Валека д. 12	«Дом книги»	(343) 253-50-10
г. Екатеринбург	Сеть магазинов «100 000 книг на Декабристов»	(343) 353-09-40
г. Нижний Новгород, ул. Советская д. 14	«Дом книги»	(831) 277-52-07
г. Смоленск, ул. Октябрьской революции д. 13	«Кругозор»	(4812) 65-86-65
г. Челябинск, ул. Монакова, д. 31	«Техническая книга»	(904) 972 50 04
г. Хабаровск	Сеть книжно-канцелярских магазинов фирмы «Мирс»	(4212) 26-87-30

➢ **и на Украине (оптом и в розницу) через представительство издательства**

г. Киев, ул. Курчатова 9/21, «Наука и Техника», ст. М «Лесная»
(044) 516-38-66
e-mail: nits@voliacable.com

Мы рады сотрудничеству с Вами!

Группа подготовки издания:

Зав. редакцией компьютерной литературы: *М. В. Финков*

Редактор: *М. А. Финкова*

Корректор: *А. В. Громова*

ООО «Наука и Техника»

Лицензия №000350 от 23 декабря 1999 года.

198097, г. Санкт-Петербург, ул. Маршала Говорова, д. 29.

Подписано в печать 25.12.2013. Формат 70x100 1/16.

Бумага писчая. Печать офсетная. Объем 19 п. л.

Тираж . Заказ