Глава 10

Защита системы

10.1. Общие параметры

В одной из глав я обещал вам, что расскажу, как запретить вызов редактора реестра. В этой главе мы поговорим не только об этом, но и обо всем, что сделает вашу систему более защищенной.

10.1.1. Отключение редактора реестра

Неопытным пользователям не нужно разрешать запускать regedit. Для запрета запуска редактора реестра выполните следующие действия:

1. Добавьте ключ REG_DWORD DisableRegistryTools со значением 0 в раздел HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System.
2. Экспортируйте вышеуказанный раздел реестра в REG-файл.
3. Измените значение параметра DisableRegistryTools на 1.

Когда вам самим понадобится редактор реестра, вы сможете запустить созданный вами REG-файл для установки параметра DisableRegistryTools в 0, иначе запустить реестр у вас не получится.

10.1.2. Запрет запуска диспетчера задач

Существуют программы ограничения времени работы за компьютером. Например, вы можете установить такую программу, чтобы она контролировала время, проведенное за компьютером вашим ребенком. Но дети развиваются очень быстро, и если вчера ваш ребенок только осваивал азы работы с компьютером, то сегодня он вполне может запустить Диспетчер задач и завершить ненавистную ему программу — после этого он сможет играть в любимую игрушку без всяких ограничений. Чтобы такого не произошло, нужно запретить запуск диспетчера задач. Для этого в разделе HKCU\Software\

Microsoft\Windows\CurrentVersion\Policies\System создайте параметр REG_DWORD DisableTaskMgr и присвойте ему значение 1.

После этого запуск диспетчера задач будет невозможен, а вам останется лишь надеяться на то, что ваше чадо не узнает о существовании Total Commander, плагин TaskManager которого позволяет "убивать" процессы одним нажатием <F8>.

10.1.3. Запрет запуска Панели управления

Запрещать отдельные вкладки того или иного апплета **Панель управления** — это рутинная работа. Гораздо проще запретить запуск всей **Панели управления**. Для этого перейдите в раздел HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer и добавьте параметр REG_DWORD NoControlPanel со значением 1.

10.1.4. Запрет запуска программ

Вы можете составить "черный" список приложений: приложения из этого списка не могут быть запущены пользователем. Для этого создайте раздел HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun. Параметры в этом разделе создаются так:

имя параметра: N

тип: REG_SZ

значение: "имя exe-файла программы",

где N — это порядковый номер параметра. На рис. 10.1 приведен небольшой "черный" список программ.

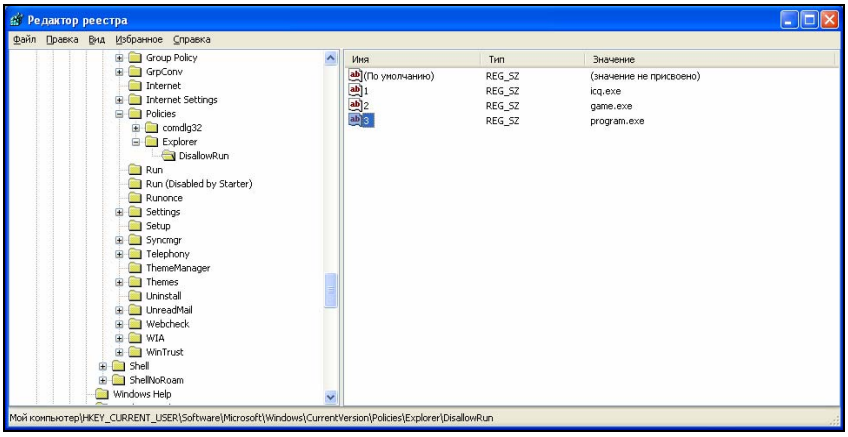

Рис. 10.1. "Черный" список программ

10.1.5. Запрет запуска командной строки

Для запрета запуска командной строки перейдите в раздел реестра HKCU\Software\Policies\Microsoft\Windows\System и добавьте параметр REG_DWORD DisableCMD. Вот допустимые значения этого параметра:

- 0 — разрешить использование командной строки;
- 1 — запретить использование командной строки;
- 2 — разрешить запуск командных файлов.

10.1.6. Запрещение изменения меню *Пуск*

Если вы не хотите, чтобы пользователь имел возможность редактировать меню **Пуск** (добавлять, удалять или изменять пункты меню), добавьте в раздел HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer параметр REG_DWORD NoChangeStartMenu со значением 1.

10.2. Вход в систему и пароли

10.2.1. Запрет кэширования пароля для входа в сеть

Windows кэширует пароль для входа в сеть на локальном компьютере, чтобы при повторном входе в сеть пользователь мог его не вводить. Из соображений безопасности рекомендуется отключить эту функцию. Конечно, при каждом входе в сеть пользователю придется вводить пароль заново, но это даже к лучшему. Во-первых, никто другой не сможет войти под именем пользователя, во-вторых, пользователь никогда не забудет свой пароль.

Запретить кэширование пароля можно с помощью параметра REG_DWORD DisablePwdCaching в разделе HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\. По умолчанию данного параметра нет, поэтому его придется создать и присвоить ему значение 1.

Также нужно запретить кэширование пароля домена: для этого необходимо присвоить значение, равное 1, параметру REG_DWORD NoDomainPwdCaching из раздела HKEY_LOCAL_MACHINE\Network\Logon.

10.2.2. Запрет кэширования интернет-паролей

Windows также запоминает пароли, которые пользователь вводит при входе на сайты, защищенные паролями, если активна опция сохранения пароля. Многие пользователи ленятся вводить пароль при каждом входе на сайт,

поэтому разрешают Windows запомнить пароль. Из соображений безопасности лучше отключить функцию запоминания пароля. Для этого выполните следующие действия:

- перейдите в раздел HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings;
- создайте параметр REG_DWORD DisablePasswordCaching и присвойте ему значение 1.

Включение данного параметра отключает возможность запоминания пароля при входе на сайт.

10.2.3. Запрет запоминания пароля сетевого подключения

Windows может запоминать пароли сетевых подключений (для удаленного доступа к сети). Для отключения этой возможности создайте параметр REG_DWORD DisableSavePassword в разделе HKLM\SYSTEM\CurrentControlSet\Services\RasMan\Parameters. Значение параметра, равное 1, отключает запоминание пароля сетевых подключений.

10.2.4. Установка минимальной длины пароля

С помощью параметра REG_DWORD MinPwdLen можно установить минимальную длину пароля пользователя. Данный параметр находится в разделе HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Network. Значение этого параметра — минимальная длина пароля (в символах).

Данный параметр бесполезен для домашних пользователей, но очень пригодится администраторам. Пользователи слишком часто устанавливают очень короткие пароли, например, "1" или "123", а с помощью этого параметра можно заставить пользователя придумать более длинный пароль.

> ***Примечание***
>
> В этом и в следующем совете имеются в виду пароли для входа в систему, а не пароли для доступа к сайту или пароли сетевых подключений.

10.2.5. Усложнение пароля

Вы можете установить минимальную длину пароля хоть 8, хоть 10 символов, а пользователь все равно установит пароль наподобие этого 12345678. Нужно заставить его придумать более оригинальный пароль. Для этого создайте

параметр REG_DWORD AlphanumPwds в разделе HKLM\SOFTWARE\Microsoft\ Windows\CurrentVersion\policies\Network. После присвоения этому параметру значения 1 Windows будет требовать от пользователя алфавитно-цифровой пароль, то есть пароль, содержащий как цифры, так и буквы.

10.2.6. Сообщение при входе в систему

Вы хотите, чтобы все пользователи видели установленное вами сообщение при входе в систему? Тогда перейдите в раздел HKLM\SOFTWARE\ Microsoft\Windows NT\CurrentVersion\Winlogon и создайте параметр REG_SZ LogonPrompt. В качестве значения введите любой текст.

10.2.7. Автоматический вход в систему

Если вы — единственный пользователь своего домашнего компьютера, можете настроить автоматический вход в систему. Тогда вам не придется каждый раз при запуске системы выбирать пользователя и вводить пароль.

Перейдите в раздел HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon и включите параметр REG_SZ AutoAdminLogon (присвойте ему значение 1). Затем присвойте значения следующим параметрам:

- REG_SZ DefaultUserName — имя пользователя для входа в систему;
- REG_SZ DefaultPassword — пароль для входа в систему;
- REG_SZ DefaultDomainName — домен по умолчанию (если вы работаете в сети);
- REG_SZ ForceAutoLogon — значение параметра, равное 1, обеспечивает принудительный вход в систему.

10.2.8. Требование пароля при выходе из спящего/ждущего режима

При выходе из спящего или ждущего режимов Windows обычно не требует пароль. А это нежелательно, поскольку на момент выхода компьютера из спящего режима за компьютером может оказаться совсем другой человек. Чтобы Windows запрашивала пароль, нужно создать параметр REG_DWORD PromptPasswordOnResume со значением 1 в разделе HKLM\SOFTWARE\Policies\ Microsoft\Windows\System\Power.

10.3. Сетевая безопасность

10.3.1. Запрет подключения сетевых дисков

Отключить появление кнопок **Подключить сетевой диск** и **Отключить сетевой диск** на панели инструментов Проводника можно с помощью параметра REG_DWORD NoNetConnectDisconnect в разделе HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer. Если параметру NoNetConnectDisconnect присвоено значение 1, пользователь не увидит данных кнопок.

10.3.2. Удаление значка "Вся сеть"

Параметр REG_DWORD NoEntireNetwork раздела HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Network при значении 1 удаляет значок **Вся сеть** в окне **Сетевое окружение**.

10.3.3. Запрет просмотра общих ресурсов анонимами

Параметр REG_DWORD RestrictAnonymous (значение 1) в разделе HKLM\System\CurrentControlSet\Control\Lsa позволяет запретить анонимным пользователям просматривать общие ресурсы и учетные записи пользователей.