Настройка безопасности Windows XP

Владимир Безмалый, консультант по вопросам информационной безопасности "БМС Консалтинг"

Введение

В настоящее время одной из наиболее распространенных клиентских операционных систем является Microsoft Windows® XP. Именно о защите клиентского компьютера (компьютера домашнего или офисного пользователя) и будет идти речь. Не секрет, что любую атаку гораздо проще начинать именно с клиентского рабочего места. Ведь основное внимание в вопросах защиты традиционно уделяется серверам локальных сетей. Несомненно, на рабочих местах необходима и антивирусная защита и усиленные меры идентификации и аутентификации пользователей. Но все же в первую очередь, с моей точки зрения, необходимо обеспечить защиту с помощью встроенных средств операционной системы.

Для кого предназначена данная статья

Данная статья предназначена в первую очередь для консультантов, специалистов в сфере безопасности, системных разработчиков и специалистов по информационным технологиям, ответственных за планирование инфраструктуры, использование приложений и развертывание рабочих станций под управлением Windows XP в корпоративной ИТ-инфраструктуре. Статья предназначена для следующих специалистов:

- системные разработчики и проектировщики, ответственные за вопросы, связанные с архитектурой рабочих станций организации;
- специалисты по безопасности информационных технологий, ответственные за обеспечение межплатформенной безопасности в рамках организации;
- аналитики и лица, принимающие важные деловые решения, которые в процессе своей деятельности активно используют компьютер;
- консультанты (как средство обучения корпоративных клиентов).

Дополнительные сведения

Для получения дополнительных сведений о настройке параметров безопасности в Microsoft Windows XP ознакомьтесь с руководством **Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP**, которое можно загрузить с веб-узла по адресу: http://go.microsoft.com/fwlink/?LinkId=15159.
Для получения сведений об использовании **Microsoft Operations Framework (MOF)** на предприятии посетите следующую веб-страницу:
http://www.microsoft.com/business/services/mcsmof.asp.
Сведения о Стратегической программе защиты технологий можно получить по следующему адресу:
http://microsoft.com/security/mstpp.asp.
Сведения о **Microsoft Security Notification Service** можно получить по следующему адресу:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ notify.asp.
Для получения дополнительных сведений о восстановлении и защите данных ознакомьтесь со следующей веб-страницей:
http://www.microsoft.com/windowsxp/pro/techinfo/administration/recovery/default.asp.

Настройка операционной системы

Все мы прекрасно знаем, что нельзя настраивать встроенные средства безопасности на файловой системе FAT32. В связи с этим необходимо либо на этапе установки операционной системы (разметки диска) выбрать файловую систему NTFS, либо приступить к преобразованию файловой системы сразу же после установки ОС.

Преобразование файловой системы

Чтобы преобразовать диск из **FAT (FAT32)** в **NTFS**, воспользуйтесь утилитой **Convert**.

Синтаксис команды

CONVERT том: /FS:NTFS [/V] [/CvtArea:имя_файла] [/NoSecurity] [/X]

- **том** – определяет букву диска (с последующим двоеточием) точку подключения или имя тома.

- **/FS:NTFS** Конечная файловая система: NTFS.
- **/V** Включение режима вывода сообщений.
- **/CVTAREA:имя_файла** Указывает непрерывный файл в корневой папке для резервирования места для системных файлов NTFS.
- **/NoSecurity** Параметры безопасности для преобразуемых файлов и папок будут доступны для изменения всем.
- **/X** Принудительное снятие этого тома (если он был подключен). Все открытые дескрипторы этого тома станут недопустимыми.

Если в вашей организации используется большое количество компьютеров, то необходимо продумать процесс автоматизации установки ОС.

Существует два возможных варианта автоматизации процесса установки:

1. **Автоматизированная установка.** В этом случае используется пакетный файл и сценарий (называемый файлом ответов[1]), благодаря этому отключаются запросы операционной системы, а необходимые данные выбираются из файлов ответов автоматически. Существует пять режимов автоматической установки.
2. **Копирование диска (клонирование).** В этом случае запускается утилита подготовки системы к копированию (Sysprep.exe), которая удаляет идентификатор безопасности (Security Identifier - SID). Затем диск копируется с помощью программы клонирования дисков, например Ghost (Symantec) (http://www.symantec.com/ghost) или Drive Image (Power Quest) (http://www.powerquest.com/driveimage). После копирования будет выполнена «сжатая» процедура установки (5-10 минут).[2]

Вы установили операционную систему, однако, самая тяжелая и продолжительная часть работы еще впереди.

Установка необходимых обновлений

Не взирая на то, что, согласно документации, установка ОС занимает около 1 часа, на самом деле установка, настройка, установка всех критических патчей (обновлений) займет у вас по меньшей мере 4-5 часов (это при условии, что все патчи уже есть у вас на жестком диске или CD-ROM и вам не нужно вытягивать их из Internet).

Итак, вы установили операционную систему. Для дальнейшей установки патчей у вас есть два пути:

1. Воспользоваться службой автоматического обновления **Windows Update**. Этот путь достаточно хорошо описан в литературе и не требует никаких усилий со стороны программиста. Однако, предположим, что в вашей организации хотя бы 20 компьютеров. Таким образом, вам придется 20 раз воспользоваться этой службой. Это не самый лучший способ, однако если у вас быстрый канал и ваше руководство не против выбрасывать таким способом деньги, то вам подходит этот путь. Но учтите, что при переустановке ОС вам придется все вытягивать заново.[3]
2. Воспользоваться каким-то сканером безопасности для поиска необходимых патчей (обновлений). Для примера рассмотрим бесплатный сканер Microsoft Base Security Analyzer (в данной статье не будет подробно рассматриваться вопрос о методах работы с данным сканером). Данный сканер можно бесплатно загрузить с сайта

---

[1] Создается с помощью утилиты deploy.cab. Для работы создайте папку, разверните туда архив deploy.cab. Вложенный файл setupmgr.exe является Менеджером установки (Microsoft Setup Manager Wizard), который используется для создания файлов ответов.

[2] В больших фирмах с сетями под управлением серверов Windows 2000 Server или Windows 2003 Server развертывание Windows XP может быть выполнено благодаря службам удаленной установки (Remote Installation Services-RIS) и серверу управления системами Microsoft (Systems Management Server – SMS). Подробнее о RIS можно прочесть http://www.microsoft.com/windows/server
SMS позволяет управлять установкой централизованно (http://www.microsoft.com/smsmgmt

[3] Для проведения обновлений можно воспользоваться Microsoft Software Update Services (SUS) (подробнее см. http://www.microsoft.com/windowsserversystem/sus/default.mspx).

Microsoft из раздела TechNet. 4. До начала тестирования необходимо будет извлечь файл Mssecure.xml файл из http://download.microsoft.com/download/xml/security/1.0/nt5/en-us/mssecure.cab Файл Mssecure.xml должен быть помещен в ту же папку, в которой развернут Microsoft Base Security Analyzer

Результатом сканирования будет перечень необходимых патчей, который вы должны будете установить на вашем компьютере.

На мой взгляд, удобнее применять коммерческие сканеры безопасности типа LAN Guard Network Scanner или XSpider.

Рассмотрим более подробно LAN Guard Network Scanner.

Этот сканер предназначен для поиска уязвимостей в компьютерных сетях не только на базе Windows. Однако, в нашем случае, можно легко воспользоваться ним для поиска уязвимостей на отдельном компьютере. Вам будет рекомендовано посетить конкретные страницы бюллетеня безопасности от Microsoft.

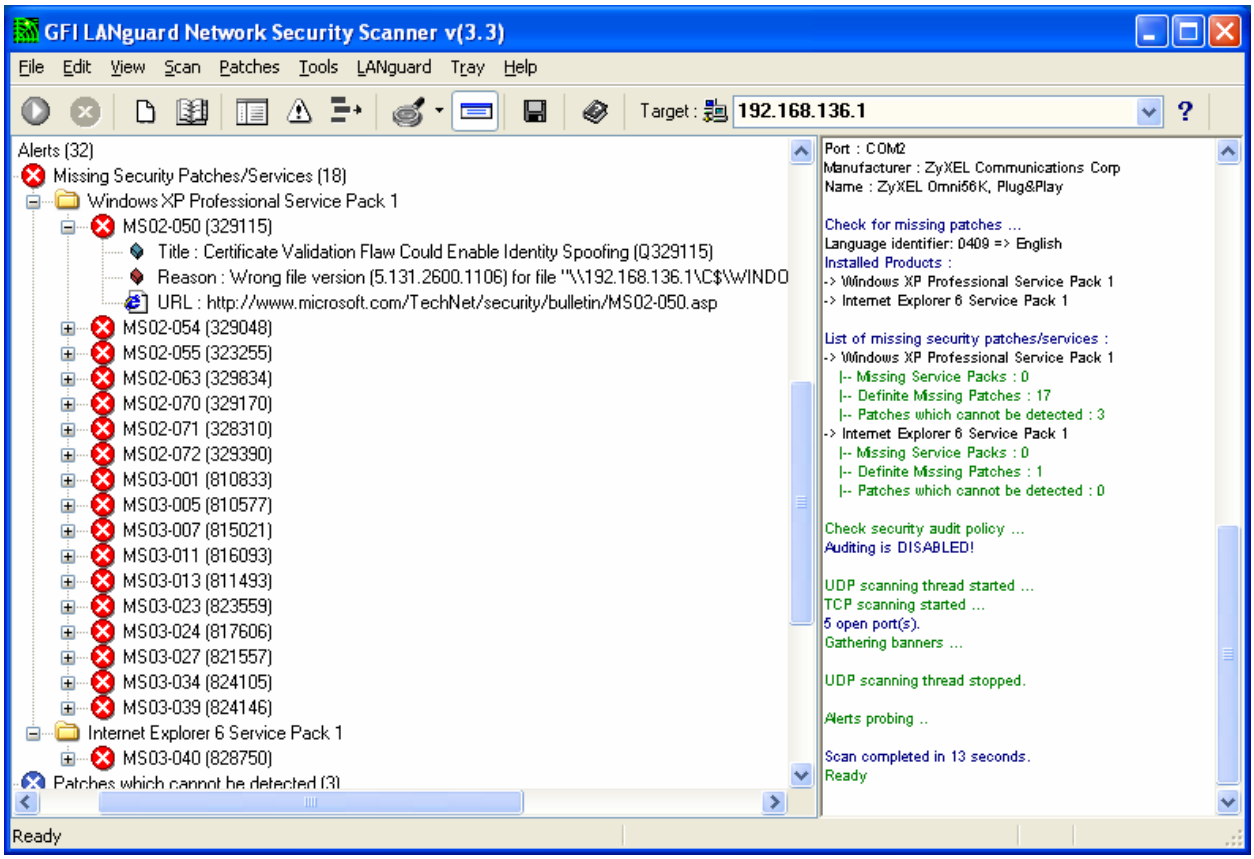

Рис. 1 Результат работы LAN Guard Network Scanner

В таком случае гораздо проще устанавливать обновления и появляется возможность узнать для решения какой уязвимости создано данное обновление.

Анализ процесса установки патчей приведен на рис.2

[4] Существует ряд сканеров безопасности третьих фирм, они описаны в приложении 1 к данной статье

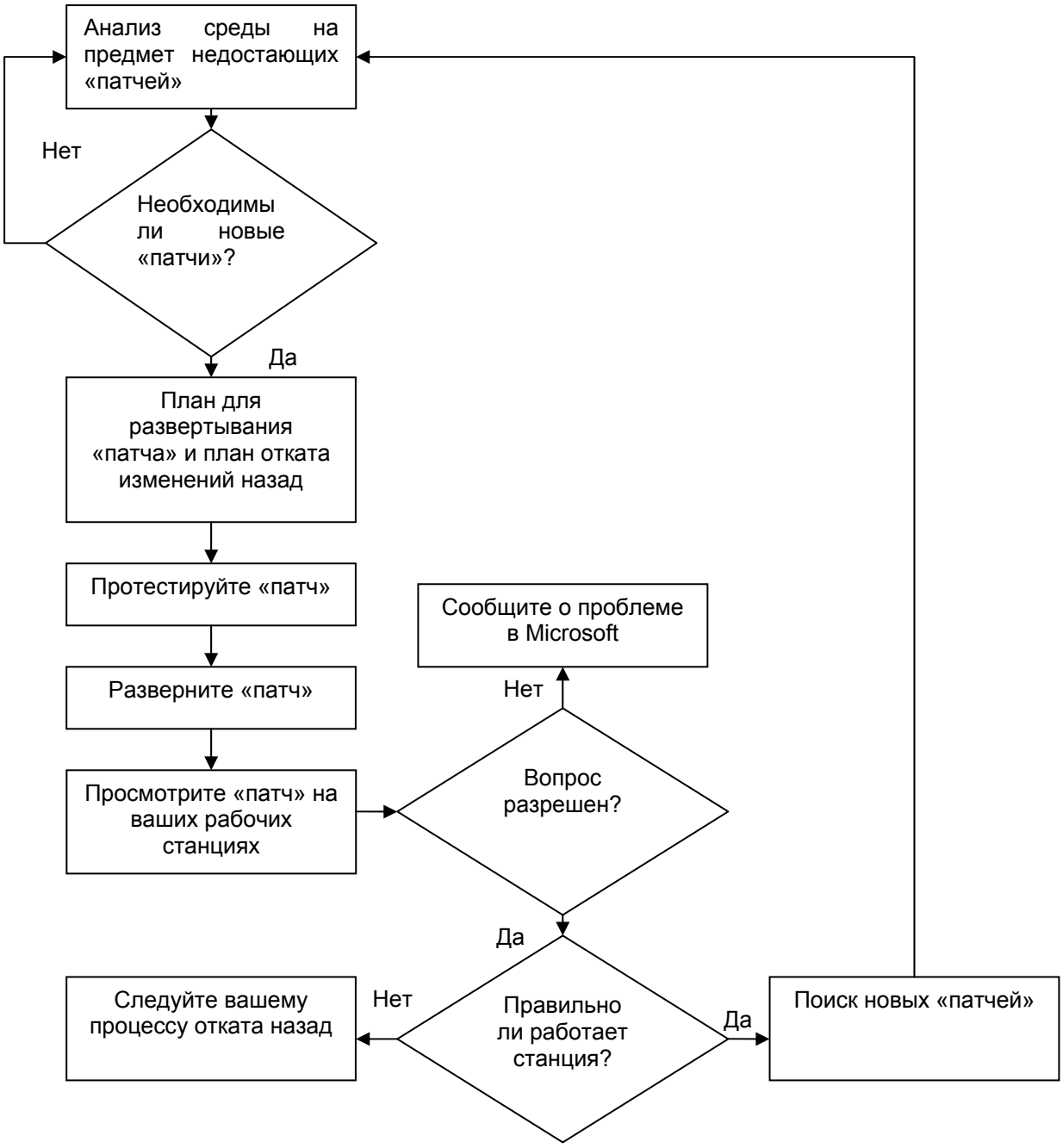

Рис 2. Процесс управления установкой обновлений

Стоит исследовать эти шаги подробнее:

- **Анализ**. Посмотрите на текущую среду и потенциальные угрозы. Определите патчи, которые вы должны инсталлировать, чтобы сократить количество угроз вашей среде.
- **План**. Установите, какие патчи надо инсталлировать, чтобы сдерживать потенциальные угрозы и обнаруженные вами уязвимые места. Определитесь, кто будет осуществлять тестирование и инсталляцию, и какие шаги нужно сделать.
- **Тестирование**. Просмотрите доступные патчи и разделите их на категории для вашей среды.
- **Инсталляция**. Инсталлируйте нужные патчи, чтобы защитить вашу среду.
- **Мониторинг**. Проверьте все системы после инсталляции патчей, чтобы удостовериться в отсутствии нежелательных побочных эффектов.
- **Просмотр**. Важной частью всего процесса является тщательный просмотр новых изданных патчей, вашей среды, и выяснение, какие из патчей нужны вашей компании.

Если во время просмотра вы обнаружите, что необходимы новые патчи, начните снова с первого шага.

Примечание: Настоятельно рекомендуется сделать резервную копию всей рабочей системы до инсталляции патчей.

Проверка среды на предмет недостающих патчей

Так как это непрерывный процесс, вам нужно убедиться в том, что ваши патчи соответствуют последним установкам. Рекомендуется постоянно следить за тем, чтобы иметь новейшую информацию о патчах. Иногда выпускается новый патч, и вам необходимо установить его на всех станциях. В других случаях в сети появляется новая станция, и на ней нужно установить все необходимые обновления. Вам следует продолжать проверять все ваши станции, чтобы убедиться в том, что на них установлены все необходимые новейшие патчи. Вообще, вопрос установки патчей далеко не так прост, как кажется на первый взгляд и полное рассмотрение этого вопроса выходит за пределы нашей статьи.

Следует учесть, что иногда после установки последующего патча необходимо переустановить предыдущий. В частности в моей практике такое встречалось неоднократно.

Итак, предположим, что все патчи установлены и ваша система не имеет дырок, связанных с их отсутствием. Учтите, что это состояние только на текущий момент времени, завтра возможно вам придется устанавливать новые патчи. Этот процесс, увы, беспрерывен.

Восстановление системных файлов

Полезная функция, если ваш компьютер не используется исключительно для ресурсоемких задач типа игр. Так что лучше оставить ее включенной. При этом компьютер периодически создает слепки критичных системных файлов (файлы реестра, COM+ база данных, профили пользователей и т.д.) и сохраняет их как "точку отката". Если какое-либо приложение "снесет" вашу систему, или что-то важное будет испорчено, вы можете обратить компьютер в предыдущее состояние – в точку отката.

Точки отката автоматически создаются службой "Восстановления системы" (System Restore) при возникновении некоторых ситуаций типа установки нового приложения, обновления Windows, установки неподписанного драйвера и т.д. Вы можете и вручную создавать точки отката через интерфейс Восстановления системы (System Restore), который можно вызвать, пройдя путь: Пуск → Программы → Стандартные → Служебные → Восстановление системы (Start → Programs → Accessories → System Tools → System Restore).

Аналогичный результат можно получить с помощью утилиты msconfig, запускаемой из режима командной строки или Пуск →Выполнить

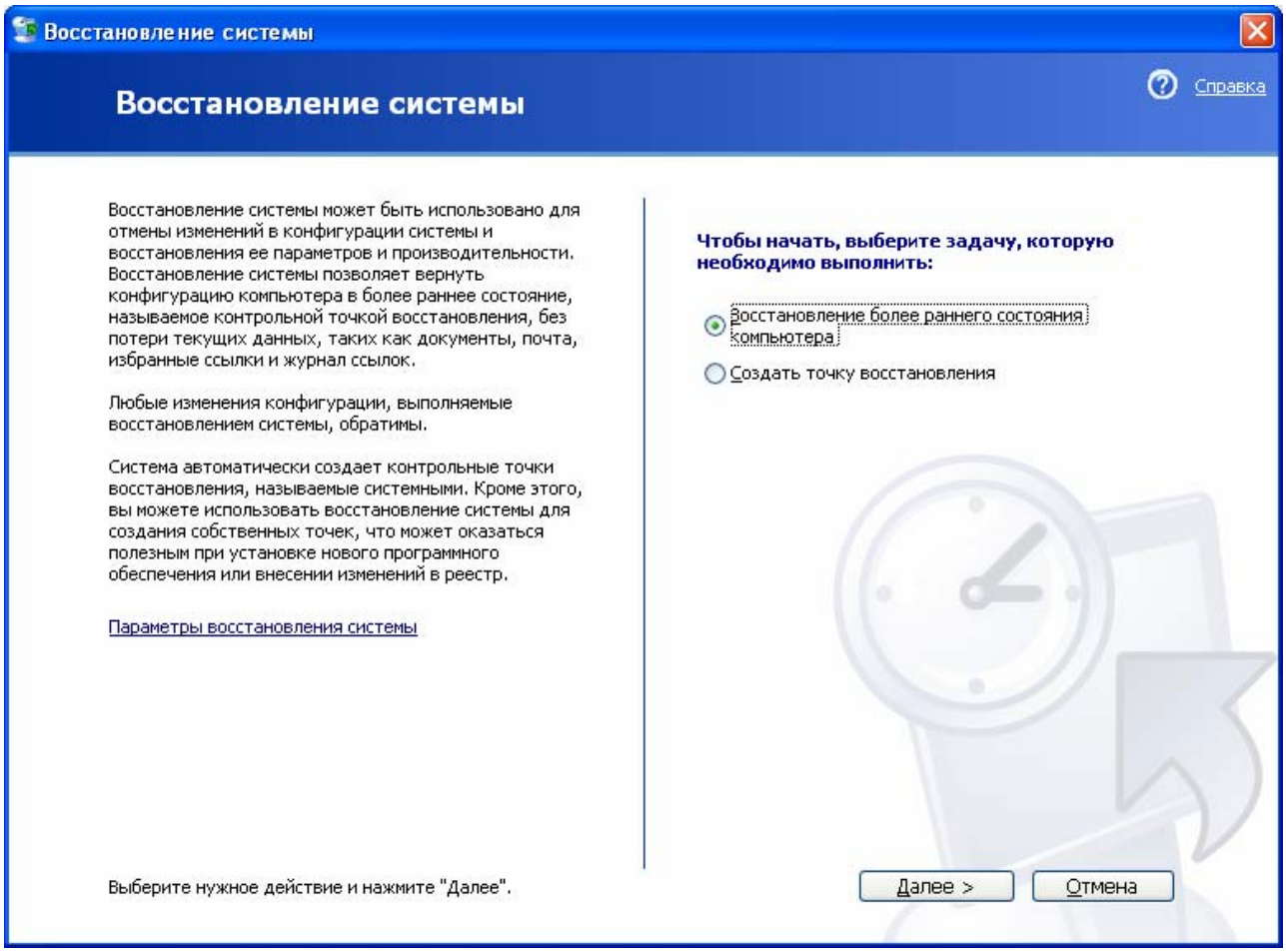

Рис.4 Восстановление системы

Восстановление системных файлов опирается на фоновую службу, которая минимально сказывается на быстродействии и записывает снимки, отнимающие часть дискового пространства. Вы можете вручную отвести максимальный объем дискового пространства для данной службы. Вы также можете полностью отключить службу для всех дисков.

Отключить можно, поставив галочку "Отключить службу восстановления". Поскольку служба восстановления системных файлов может влиять на результаты тестовых программ, ее обычно отключают перед тестированием.

Автоматическая очистка диска

Для проведения очистки жесткого диска от ненужных файлов используется программа cleanmgr.exe
Ключи программы:
/d driveletter: - указывает букву диска, которая будет очищаться
/sageset: n – эта команда запускает мастер очистки диска, и создает ключ в реестре для сохранения параметров. Параметр **n** может принимать значения от 0 до 65535.
/sagerun: n – используется для запуска мастера очистки диска с определенными параметрами, которые были заданы заранее с помощью предыдущего ключа.
Для автоматизации этого процесса можно воспользоваться планировщиком заданий.

Регулярно производите дефрагментацию.

DOS и не-NT версии Windows мало заботились об оптимизации своих файловых систем. Когда вы устанавливаете и удаляете программы, то в различных областях дискового пространства создаются "дыры". В результате свободное место представляет собой не сплошной блок, оно разбросанно по всему диску. При заполнении свободного пространства файлы также оказываются разбросанными по нескольким секторам, что сильно снижает производительность – при обращении к файлу диску приходится читать не один последовательный участок, а несколько произвольно разбросанных.

В NT-версиях Windows, использующих файловую систему NTFS, применяются особые меры для сохранения целостности дискового пространства – но фрагментация все равно

происходит. Поэтому вы должны регулярно дефрагментировать ваш жесткий диск, причем регулярность зависит от характера вашей деятельности на компьютере.

В случае использования файловой системы FAT32 дефрагментация еще более необходима!

Если вы часто устанавливаете и удаляете программы, или вы постоянно создаете, перемещаете или удаляете файлы, то вы должны выполнять дефрагментацию раз в неделю. Если же вы долгое время используете одни и те же приложения, при этом вы не слишком часто перемещаете файлы, то вы можете увеличить промежуток между дефрагментациями до одного месяца.

Если вы достаточно часто выполняете дефрагментацию, то вы не заметите ощутимого прироста в производительности после дефрагментации. Это совершенно нормально. Если же прирост явно ощутим, то вы слишком долго не выполняли дефрагментацию.

Автоматизируем процесс дефрагментации диска

Создаем bat-файл, который, к примеру, назовем **defrag.bat** следующего содержания:
Rem **This batch file is defragmenting your hard drive.**
Rem **To cancel Press Ctrl+C on the keyboard.**
Defrag.exe C: -F
Формат команды **Defrag:**
defrag <том> [-a] [-f] [-v] [-?]
том – Буква диска, или точка подключения (например, c: или d:\vol\mpoint)
-a – Только анализ
-f – Дефрагментация даже при ограниченном месте на диске
-v – Подробные результаты
-? – Вывод справки о команде
Теперь в Планировщике заданий указываем этот файл и ставим его в расписание. Рекомендуется установить запуск каждую неделю (но не меньше 1 раза в месяц). Теперь Дефрагментация диска будет автоматически запускаться в Windows XP.
Вы также можете установить дефрагментацию в расписание и без создания bat-файла, делается это так:

- Заходим в **Панель управления -> Назначенные задания -> Добавить задание**
- Нажмите Обзор и выберите программу **Defrag.exe**, находится она в каталоге **C:\Windows\System32**
- Во время последнего экрана не забудьте поставить галочку около пункта **Установить дополнительные параметры после нажатия кнопки Готово**
- В строке выполнить после адреса файла добавьте ключ **-f**

Как удалить "скрытые" компоненты Windows XP?

В отличие от Windows 9*/NT, в процессе установки Windows XP нет возможности выбирать необходимые компоненты. На мой взгляд, это правильное решение Microsoft - сначала следует установить операционную систему со всеми ее причудами, а уж затем, поработав, можно решать, что следует оставить, а что нет.

Однако при этом в окне "Add/Remove Windows Components", что присутствует в апплете "Add or Remove Programs" Контрольной панели, удалять-то практически нечего, потому что многие из составляющих Windows скрыты от шаловливых ручек не слишком опытных пользователей. Для решения этой проблемы открываем системную папку Inf (по умолчанию - C:\Windows\Inf), находим в ней файл sysoc.inf, открываем его и удаляем во всех строках слово HIDE. Главное при этом - оставить неизменным формат файла, то есть следует удалять только HIDE, оставляя запятые до и после этого слова.

Для примера - исходная строка и та, что должна получиться:

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

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

Сохраняем файл sysoc.inf, открываем "Add/Remove Windows Components" и видим значительно более длинный список, чем тот, что был на этой страничке до проведения описанной выше операции. (Рис. 5) Правда, и в этом случае много удалить не получится.

Кстати, точно также можно поступить и в случае с Windows 2000...

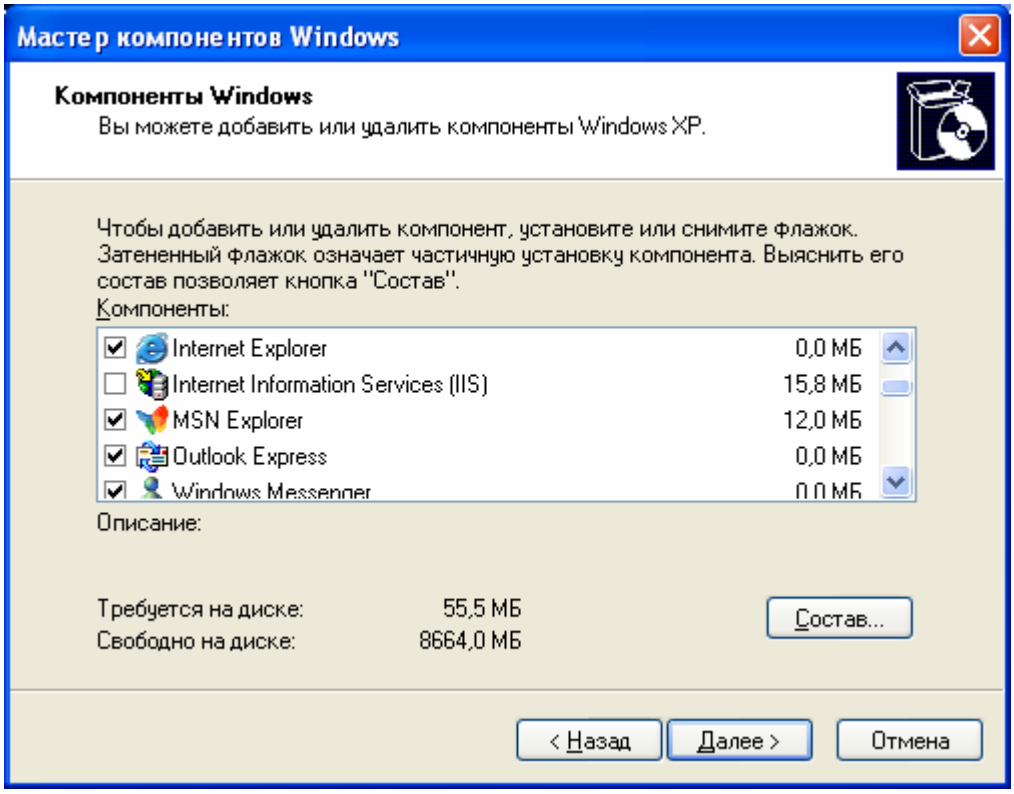

Рис 5 Окно компонентов Windows XP

Вы можете задать резонный вопрос, а какое это отношение имеет к безопасности?

Во-первых, если в вашей организации существует корпоративная политика в области использования программного обеспечения и в ней в качестве почтового клиента выбран, например, The Bat! или почтовый клиент Mozilla (Opera), то не стоит оставлять на компьютере насквозь дырявый Outlook Express и вводить пользователя в искушение пользоваться им.

Во-вторых, если у вас не принято использовать службу мгновенных сообщений, то удалите Windows Messenger.

И, наконец, просто избавьтесь от ненужных вам компонент. Меньше неиспользуемого ПО, меньше возможностей использовать его не по назначению, а, следовательно, вольно или невольно нанести вред вашей организации.

Настройка автоматически выполняемых программ

Одна из типичных проблем, связанных с безопасностью, это запуск программ типа «троянский конь» в процессе загрузки Windows XP.

В программа может быть запущена автоматически следующими способами:

1. Добавление в папку **Автозагрузка** для данного пользователя
2. Добавление в папку **Автозагрузка**[5] для всех пользователей
3. Ключ **Run** (компьютера) Ключ реестра **HKLM\Software\Microsoft\Windows\CurrentVersion\Run**
4. Ключ **Run** (пользователя) Ключ реестра **HKCU\Software\Microsoft\Windows\CurrentVersion\Run**
5. Ключ **RunServices**. Разница между RunServices и просто Run в том, что при запуске программы в ключе RunServices она будет запущена как обслуживающий процесс и

[5] Следует помнить, о том, что папку автозагрузки можно подменять с помощью ключа реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Ключ: Common Startup="ПУТЬ_К_ПАПКЕ_АВТОЗАГРУЗКИ"

ей будет выделено меньше приоритетного процессорного времени при работе. При запуске же в ключе Run, программа запуститься как обычно с нормальным приоритетом.

6. Папки **Планировщика задач**
7. **Win.ini.** Программы, предназначенные для 16-разрядных версий Windows могут добавить строки типа **Load=** и **Run=** этого файла
8. Ключи **RunOnce** и **RunOnceEx.** Группа ключей реестра, содержащая список программ, выполняемых однократно в момент запуска компьютера. Эти ключи могут относиться и к конкретной учетной записи данного компьютера[6]
   HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
   HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
   HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
   HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
9. **Групповая политика**. Содержит две политики (с именами **Запуск программ при входе пользователя в систему**). Находятся в папках **Конфигурация компьютера ►Конфигурация Windows ► Административные шаблоны ► Система ► Вход в систему (Computer configuration ► Administrative Templates ►System ►Logon) и Конфигурация пользователя ►Конфигурация Windows ► Административные шаблоны ► Система ► Вход в систему (User configuration ► Administrative Templates ►System ►Logon)**
10. Сценарии входа в систему. Настраиваются **Групповая политика: Конфигурация компьютера ►Конфигурация Windows ► Сценарии и Конфигурация пользователя►Конфигурация Windows ►Сценарии (входа в систему** и **выхода из системы)**
11. Файл AUTOEXEC.BAT в корневом каталоге загрузочного диска. Все программы, которые вы хотите запустить из него, должны выполняться в реальном режиме DOS, так как выполнение этого командного файла происходит до загрузки графической оболочки. Используется для того, чтобы снова и снова копировать в "автозапуск" из скрытой папки рекламные модули, которые пользователь удалил

Для настройки списка автоматически вызываемых программ в состав Windows XP входит утилита **Настройка системы (System Configuration Utility) Msconfig.exe**, которая позволяет вывести список всех автоматически загружаемых программ. Рабочее окно программы приведено на рис. 6

[6] Сюда же относятся иключи указанных разделов **RunServices** и **RunServicesOnce**

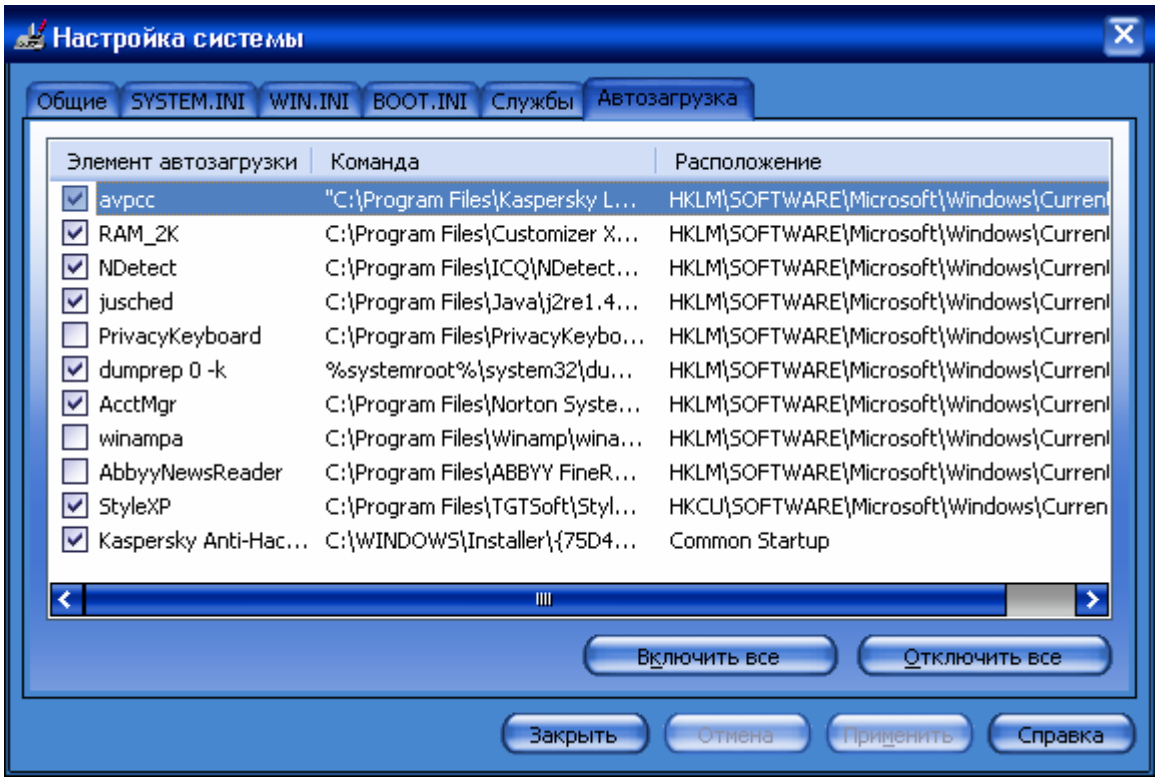

Рис.6 Рабочее окно программы Msconfig

Настройка системы безопасности Windows XP

Операционная система Windows XP обладает развитой системой безопасности, которая, тем не менее, нуждается в настройке.[7] Мы надеемся, что вы понимаете, что система Windows XP должна устанавливаться на разделах NTFS, что применение файловой системы FAT32 не рекомендуется, исходя из принципов безопасности (встроенные средства безопасности просто не могут быть реализованы при условии применения FAT32). В случае применения файловой системы FAT 32 почти все утверждения данного раздела теряют для вас всякое значение. Единственный способ включить все разрешения файловой системы – преобразовать диск в формат NTFS.

После чистой установки Windows XP предлагаемые по умолчанию параметры безопасности работают как переключатели типа «включить-выключить». Такой интерфейс носит по умолчанию название **Простой общий доступ (Simple File Sharing).**

Такая конфигурация обладает низким уровнем безопасности, практически совпадающей со стандартной конфигурацией Windows 95/98/Me.

Если вас не устраивает такая конфигурация, вы можете воспользоваться всей мощью разрешений для файлов в стиле Windows 2000. Для этого откройте произвольную папку в **Проводнике** и выберите **Сервис → Свойства папки** (**Tools → Folder options**). Перейдите на вкладку **Вид** найдите в списке флажок **Использовать простой общий доступ к файлам (рекомендуется) (Use File Sharing (recommended)** и снимите его.[8]

[7] По умолчанию Windows XP Professional предоставляют пользователю весьма упрощенный интерфейс безопасности, позволяющий устанавливать значения весьма ограниченного числа параметров доступа на основе членства во встроенных группах.

[8] Чтобы изменить этот параметр вы должны быть членом группы **Администраторы**.

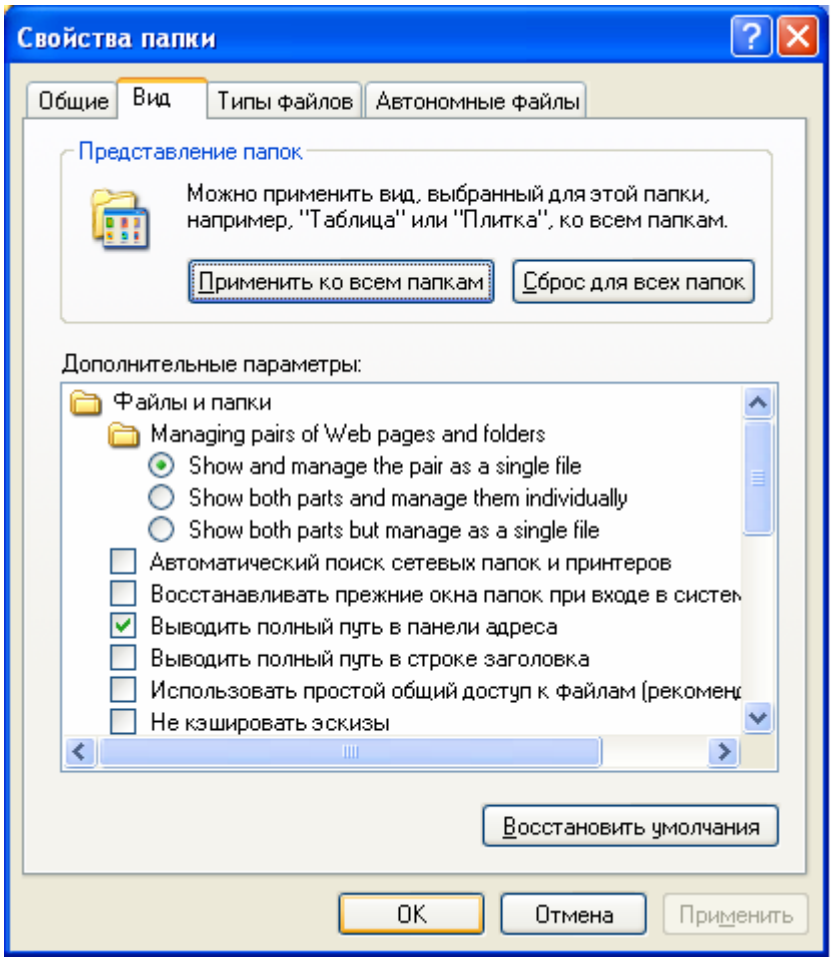

Рис. 7 Свойства папки

Когда вы выключаете простой общий доступ, в диалоговом окне свойств любой папки появляется вкладка **Безопасность**.

Аналогично осуществляется выдача разрешений на файлы. Все разрешения хранятся в списках управления доступом (Access Control List – ACL).

При установке и удалении разрешений руководствуйтесь следующими основными принципами:

1. **Работайте по схеме «сверху-вниз»**.
2. **Храните общие файлы данных вместе.**
3. **Работайте с группами везде, где это только возможно.**
4. **Не пользуйтесь особыми разрешениями.**
5. **Не давайте пользователям большего уровня полномочий, чем это абсолютно необходимо (принцип минимизации полномочий).**

Установка разрешения из командной строки

Утилита командной строки cacls.exe доступна в Windows XP Professional позволяет просматривать и изменять разрешения файлов и папок. Cacls – сокращение от Control ACLs – управление списками управления доступом.

Ключи командной строки утилиты cacls

Таблица 1

Ключ	Действие

/T	Смена разрешений доступа к указанным файлам в текущей папке и всех подпапках
/E	Изменение списка управления доступом (а не полная его замена)
/C	Продолжить при возникновении ошибки «отказано в доступе»
/G пользователь:разрешение	Выделение пользователю указанного разрешения. Без ключа /E полностью заменяет текущие разрешения
/R пользователь	Отменяет права доступа для текущего пользователя (используется только с ключом /E)
/P пользователь:разрешение	Замена указанных разрешений пользователя
/D пользователь	Запрещает пользователю доступ к объекту

С ключами /G и /P нужно использовать одну их перечисленных ниже букв (вместо слова разрешение):

- F (полный доступ) – эквивалентно установке флажка *Разрешить полный доступ (Full Control)* на вкладке *Безопасность*.
- C (изменить) – тождественно установке флажка *Разрешить Изменить (Modify)*
- R (чтение) – эквивалентно установке флажка *Разрешить Чтение и выполнение (Read & Execute)*
- W (запись) – равнозначно установке флажка *Разрешить запись (Write)*

Microsoft Windows XP позволяет предотвратить попадание конфиденциальных данных в чужие руки. Шифрующая файловая система (Encrypting File System - EFS) шифрует файлы на диске. Однако, следует иметь ввиду, что если вы утеряете ключ для расшифровки, данные можно считать утерянными. Поэтому если вы решите воспользоваться преимуществами EFS необходимо создать учетную запись агента восстановления, резервную копию собственного сертификата и сертификата агента восстановления.

Если вы предпочитаете работать с командной строкой, то можете воспользоваться программой cipher.exe.

Команда cipher без параметров выводит информацию о текущей папке и размещенных в ней файлах (зашифрованы они или нет). В таблице 2 приведен список наиболее часто используемых ключей команды cipher

Таблица 2

Ключ	Описание
/E	Шифрование указанных папок
/D	Расшифровка указанных папок
/S:папка	Операция применяется к папке и всем вложенным подпапкам (но не файлам)
/A	Операция применяется к указанным файлам и файлам в указанных папках
/K	Создание нового ключа шифрования для пользователя, запустившего программу. Если этот ключ задан, все остальные игнорируются
/R	Создание ключа и сертификата агента восстановления файлов. Ключ и сертификат помещаются в файл .CFX, а копия сертификата в файле .CER
/U	Обновление ключа шифрования пользователя или агента восстановления для всех файлов на всех локальных дисках

/U /N	Вывод списка всех зашифрованных файлов на локальных дисках без каких-либо других действий

Агент восстановления данных

Агентом восстановления данных (Data Recovery Agent) назначается обычно администратор. Для создания агента восстановления нужно сначала создать сертификат восстановления данных, а затем назначить одного из пользователей таким агентом.

Чтобы создать сертификат нужно сделать следующее:

1. Нужно войти в систему под именем Администратор
2. Ввести в командной строке cipher /R: имя файла
3. Введите пароль для вновь создаваемых файлов

Файлы сертификата имеют расширение .PFX и .CER и указанное вами имя.[9]

Для назначения агента восстановления:

1. Войти в систему под учетной записью, которая должна стать агентом восстановления данных
2. В консоли **Сертификаты** перейдите в раздел Сертификаты – Текущий пользователь → Личные (Current User → Personal)
3. Действие → Все задачи → Импорт (Actions → All Tasks → Import) для запуска мастера импорта сертификатов
4. Проведите импорт сертификата восстановления

При неправильном использования средств шифрования вы можете получить больше вреда, чем пользы.

Краткие рекомендации по шифрованию:

1. Зашифруйте все папки, в которых вы храните документы
2. Зашифруйте папки %Temp% и %Tmp%. Это обеспечит шифрование всех временных файлов
3. Всегда включайте шифрование для папок, а не для файлов. Тогда шифруются и все создаваемые в ней впоследствии файлы, что оказывается важным при работе с программами, создающими свои копии файлов при редактировании, а затем перезаписывающими копии поверх оригинала
4. Экспортируйте и защитите личные ключи учетной записи агента восстановления, после чего удалите их с компьютера
5. Экспортируйте личные сертификаты шифрования всех учетных записей
6. Не удаляйте сертификаты восстановления при смене политик агентов восстановления. Храните их до тех пор, пока не будете уверены, что все файлы, защищенные с учетом этих сертификатов, не будут обновлены.
7. При печати не создавайте временных файлов или зашифруйте папку, в которой они будут создаваться
8. Защитите файл подкачки. Он должен автоматически удаляться при выходе из Windows

Конструктор шаблонов безопасности

Шаблоны безопасности представляют собой текстовые файлы. Для изменения таких файлов используется оснастка шаблонов безопасности из состава MMC или текстовый редактор (например, программа «Блокнот»). Некоторые разделы файлов шаблона содержат списки управления доступом (ACL), определенные на языке Security Descriptor

---

[9] эти файлы позволяют любому пользователю системы стать агентом восстановления. Обязательно скопируйте их на дискету и храните в защищенном месте. После копирования удалите файлы сертификата с жесткого диска.

Definition Language (SDDL). Для получения дополнительной информации о внесении изменений в шаблоны безопасности и языке SDDL воспользуйтесь указанными в разделе «Дополнительные сведения» источниками.
Однако лучше воспользоваться оснасткой Security Templates консоли Microsoft Management Console (MMC). Для этого в командной строке нужно ввести **mmc /a** в этой консоли выбрать меню **File – Add/Remove**. В диалоговом окне **Add Standalone Snap-in** выбрать **Security Templates** – **Add.**

Управление оснасткой

Шаблоны безопасности расположены в папке \%systemroot%\security\templates. Количество встроенных шаблонов изменяется в зависимости от версии операционной системы и установленных пакетов обновлений.
Если раскрыть любую папку в Security Templates, то в правой панели будут показаны папки, которые соответствуют контролируемым элементам:

- **Account Policies** – управление паролями, блокировками и политиками Kerberos
- **Local Policies** – управление параметрами аудита, пользовательскими правами и настройками безопасности
- **Event Log –** управление параметрами системного журнала
- **Restricted Groups –** определение элементов различных локальных групп
- **System Services –** включение и отключение служб и присвоение права модификации системных служб
- **Registry –** назначение разрешений на изменение и просмотр разделов реестра
- **File System –** управление разрешениями NTFS для папок и файлов

Управление шаблонами безопасности

Используемые шаблоны безопасности должны храниться в защищенном месте. Доступ к ним предоставляется только администраторам, которые отвечают за реализацию групповой политики. По умолчанию на компьютерах под управлением Windows XP и Windows Server 2003 для хранения шаблонов безопасности используется папка %SystemRoot%\security\templates.
Эта папка не реплицируется между контроллерами домена. Таким образом, во избежание возникновения проблем с управлением версиями шаблонов безопасности, необходимо определить контроллер домена для хранения оригинала шаблонов. Оптимальной является практика, когда изменения всегда вносятся в одну и ту же копию шаблонов.

Импорт шаблона безопасности

Для импорта шаблона безопасности необходимо выполнить следующие действия.

1. В окне редактора групповой политики найдите папку Конфигурация Windows.
2. Откройте ее и выделите папку Параметры безопасности.
3. Щелкните ее правой кнопкой мыши и выберите пункт Импорт политики.
4. Выберите шаблон безопасности, который требуется импортировать, и нажмите кнопку Открыть. Параметры импортируются из выбранного файла в объект групповой политики.

Административные шаблоны

С помощью административных шаблонов (файлы в формате Unicode) могут быть установлены дополнительные параметры безопасности. Такие шаблоны содержат параметры реестра, которые влияют на поведение Windows XP и установленных приложений (например Microsoft Office XP). Это могут быть как параметры для компьютеров, так и параметры для пользователей. Для хранения параметров компьютера используется куст реестра HKEY_LOCAL_MACHINE. Для хранения параметров пользователя — куст реестра HKEY_CURRENT_USER.

Управление административными шаблонами

Используемые административные шаблоны, как и шаблоны безопасности, должны храниться в защищенном месте. Доступ к ним предоставляется только администраторам, которые отвечают за реализацию групповой политики. Административные шаблоны, которые поставляются в составе Windows XP и Windows 2003 Server, хранятся в папке %systemroot%\inf. В состав Office XP Resource Kit входят дополнительные шаблоны для Office XP. Поскольку при выходе пакетов обновления в такие шаблоны могут быть внесены изменения, модифицировать их самостоятельно не следует.

Добавление административного шаблона к политике

К объектам групповой политики, которые используются для настройки Office XP, помимо административных шаблонов из состава Windows XP, необходимо применить специальные шаблоны Office XP. Для добавления шаблона к объекту групповой политики необходимо выполнить следующие действия.

1. В окне редактора групповой политики найдите папку Административные шаблоны.
2. Щелкните папку правой кнопкой мыши и выберите пункт Добавление и удаление шаблонов.
3. В диалоговом окне Добавление и удаление шаблонов нажмите кнопку Добавить.
4. Перейдите в папку, которая содержит файлы административных шаблонов.
5. Выберите шаблон, нажмите кнопку Открыть, а затем — Закрыть.

Групповая политика на уровне домена

В состав групповой политики на уровне домена входят параметры, которые относятся ко всем компьютерам и пользователям в рамках домена. Подробное описание групповой политики на уровне домена можно найти в главе 2 «Configuring the Domain Infrastructure» руководства по безопасности **Windows Server 2003 Security Guide**, которое находится на веб-узле по адресу: http://go.microsoft.com/fwlink/?LinkId=14845.

Политика паролей

Использование регулярно изменяемых, сложных паролей снижает вероятность их взлома. Параметры политики паролей служат для определения уровня сложности и длительности использования паролей. В этом разделе описаны все параметры политики безопасности для окружений «ПК на предприятии» и «Система с высоким уровнем безопасности».

С помощью редактора групповой политики по указанному ниже адресу настраиваются соответствующие параметры групповой политики домена.

Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей

Таблица содержит рекомендованные[10] значения параметров политики паролей для двух типов безопасной среды, которые были определены в этой статье.

Таблица 3

Наименование политики	Значение по умолчанию для	ПК на предприятии[11]	Высокий уровень безопасности[12]

[10] Параметры рекомендованы корпорацией Microsoft

[11] Рабочая среда на предприятии состоит из домена Microsoft Active Directory® на базе Windows 2000 или Windows Server 2003. Для управления клиентскими компьютерами в такой среде используется групповая политика, которая применяется к контейнерам, узлам, доменам и организационным подразделениям (ОП). Групповая политика служит для централизованного управления безопасностью всей рабочей среды.

[12] Высокий уровень безопасности среды обеспечивается установкой более жестких значений параметров безопасности для клиентских компьютеров. При этом функциональные возможности

	контроллера домена		
Требовать неповторяемости паролей[13]	24 хранимых пароля	24 хранимых пароля	24 хранимых пароля
Максимальный срок действия пароля	42 дня	42 дня	42 дня
Минимальный срок действия пароля	1 день	2 дня	2 дня
Минимальная длина пароля	7 символов	8 символов	12 символов
Пароль должен отвечать требованиям сложности	Включен	Включен	Включен
Хранить пароли всех пользователей в домене, используя обратимое шифрование[14]	Отключен	Отключен	Отключен

Изменение пароля только по запросу операционной системы

В некоторых организациях описанные выше политики должны дополняться централизованным контролем над всеми пользователями. Выполнение описанных в этом разделе действий предотвращает произвольное изменение пароля пользователями (кроме случаев соответствующего требования со стороны операционной системы).

Централизованный контроль над паролями пользователей — это краеугольный камень профессионально составленной схемы безопасности Windows XP. С помощью групповой политики устанавливаются минимальный и максимальный сроки действия пароля. Однако необходимость слишком часто менять пароль позволяет пользователям нейтрализовать действие параметра Требовать неповторяемости паролей. Кроме того, использование слишком длинных паролей может привести к росту количества обращений в службу поддержки со стороны забывчивых пользователей.

Пользователь имеет право менять пароль на протяжении периода, который определяется установленными значениями параметров минимального и максимального срока действия пароля. С другой стороны, в среде «Система с высоким уровнем безопасности» пароль должен изменяться только по запросу операционной системы, после истечения максимального срока действия (42 дня). Чтобы разрешить пользователям менять пароль только по требованию операционной системы, администратор должен соответствующим образом настроить Windows. Для этого в диалоговом окне Безопасность Windows, которое появляется после нажатия комбинации клавиш CTRL+ALT+DELETE, необходимо деактивировать кнопку Смена пароля.

В рамках всего домена данная конфигурация реализуется с помощью групповой политики, а для отдельных пользователей — внесением изменений в системный реестр. Для получения дополнительных сведений об этой конфигурации обратитесь к статье **Microsoft Knowledge Base 324744 «How To: Prevent Users from Changing a Password Except**

пользователей ограничиваются выполнением определенных заданий. Доступ возможен только к санкционированным приложениям, службам и компонентам инфраструктуры.

[13] Параметр безопасности **Требовать неповторяемости паролей** определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Эффективность данного параметра обеспечивается использованием параметра **Минимальный срок действия пароля**, который предотвращает попытки слишком частого изменения пароля пользователем

[14] Параметром **Хранить пароли всех пользователей в домене, используя обратимое шифрование** определяется использование операционной системой обратимого шифрования при сохранении паролей.. Хранить пароли, зашифрованные обратимым методом, — это все равно что хранить их открытым текстом. Данную политику следует использовать лишь в исключительных случаях, если потребности приложения важнее, чем защита пароля. По умолчанию параметр имеет значение **Отключен**

When Required in Windows Server 2003», которая расположена на веб-узле корпорации Майкрософт по адресу: http://support.microsoft.com/default.aspx?scid=324744. Необходимые сведения для домена на основе Windows 2000 содержатся в статье **Microsoft Knowledge Base 309799 «How To: Prevent Users from Changing a Password Except When Required in Windows 2000»**, которая расположена на веб-узле корпорации Майкрософт по адресу: http://support.microsoft.com/default.aspx?scid=309799.

Политика блокировки учетной записи

Политика блокировки учетной записи — это компонент Active Directory, который используется для блокировки учетной записи, если в течение заданного промежутка времени регистрируется определенное количество неудачных попыток входа в систему. Количество попыток и интервал времени устанавливаются с помощью параметров политики блокировки учетной записи. Пользователь не сможет войти в систему, если его учетная запись заблокирована. Попытки входа в систему отслеживаются контроллерами домена, а соответствующим образом настроенное ПО на сервере реагирует на потенциальные атаки такого вида, блокируя учетную запись на заданный интервал времени.

В процессе настройки политики блокировки учетной записи администратор может установить любые значения разрешенного количества попыток и периода времени. Однако если значение параметра **Сброс счетчика блокировки через** больше значения параметра **Блокировка учетной записи на**, контроллер домена автоматически присваивает последнему значение параметра **Сброс счетчика блокировки через**.

Кроме того, если значение параметра **Блокировка учетной записи на** меньше значения параметра **Сброс счетчика блокировки через**, контроллер домена автоматически присваивает последнему значение параметра **Блокировка учетной записи на**. Таким образом, если значение параметра **Блокировка учетной записи на** уже установлено, значение параметра **Сброс счетчика блокировки через** не должно превышать его.

Такая оптимизация направлена на предотвращение установки конфликтующих значений параметров при настройке политики безопасности. Если значение параметра **Сброс счетчика блокировки через** больше значения параметра **Блокировка учетной записи на**, срок действия параметра **Блокировка учетной записи на** истечет раньше и пользователь получит возможность войти в сеть. С другой стороны, обратный отсчет для параметра **Сброс счетчика блокировки через** будет продолжаться. По этой причине параметр **Пороговое значение блокировки** не допустит больше трех неудачных попыток и пользователь не сможет войти в систему.

Для недопущения возникновения такой ситуации контроллер домена автоматически присваивает параметру **Сброс счетчика блокировки через** значение параметра **Блокировка учетной записи на**.

Данные параметры политики безопасности помогают предотвратить возможность подбора пароля злоумышленником и снижают вероятность получения несанкционированного доступа к сети. С помощью редактора групповой политики по указанному ниже адресу настраиваются приведенные в таблице параметры групповой политики домена.

Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика блокировки учетной записи

Таблица 4 содержит рекомендованные значения параметров политики блокировки учетных записей для двух типов безопасной среды, которые были определены выше.

Таблица 4

Наименование политики	Значение по умолчанию для контроллера домена	ПК на предприятии	Высокий уровень безопасности
Блокировка учетной записи на	Не определено	30 минут	30 минут
Пороговое значение блокировки	0 ошибок входа в систему	5 ошибок входа в систему	5 ошибок входа в систему
Сброс счетчика блокировки через	Не определено	30 минут	30 минут

Назначение прав пользователя

В системе Windows XP параметры назначения прав пользователей настраиваются в разделе редактора групповой политики, расположенном по следующему адресу:
Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Назначение прав пользователей

Таблица 5. Параметры назначения прав пользователей, используемые для обеспечения безопасности компьютеров под управлением Windows XP.

Название параметра	**ПК на предприятии (настольная система)**	**ПК на предприятии (портативная система)**	**Высокий уровень безопасности (настольная система)**	**Высокий уровень безопасности (портативная система)**
Сетевой доступ к этому компьютеру	Администраторы, пользователи	Администраторы, пользователи	Администраторы, пользователи	Администраторы, пользователи
Разрешение входа в систему через службы терминалов	Администраторы	Администраторы	Никто	Никто
Архивирование файлов и каталогов	Не определено	Не определено	Администраторы	Администраторы
Обход перекрестной проверки	Пользователи	Пользователи	Пользователи	Пользователи
Изменение системного времени	Не определено	Не определено	Администраторы	Администраторы
Отладка программ	Никто	Никто	Никто	Никто
Запрещение входа в систему через службы терминалов	Не определено	Не определено	Все	Все
Принудительное удаленное завершение работы	Не определено	Не определено	Администраторы	Администраторы
Локальный вход в систему	Администраторы, пользователи	Администраторы, пользователи	Администраторы, пользователи	Администраторы, пользователи
Конфигурация отдельного процесса	Не определено	Не определено	Администраторы	Администраторы
Восстановление файлов и каталогов	Не определено	Не определено	Администраторы	Администраторы, пользователи
Завершение работы системы	Не определено	Не определено	Администраторы, пользователи	Администраторы, пользователи

Параметры безопасности

С помощью редактора групповой политики по указанному ниже адресу настраиваются приведенные в таблице параметры политики.
Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности

Таблица 6. Параметры безопасности, используемые для обеспечения безопасности компьютеров под управлением Windows XP.

Название параметра	ПК на предприятии (настольная система)	ПК на предприятии (портативная система)	Высокий уровень безопасности (настольная система)	Высокий уровень безопасности (портативная система)
Учетные записи: разрешить использование пустых паролей в локальной учетной записи только при входе с консоли	Включено	Включено	Включено	Включено
Учетные записи:	Рекомендуется	Рекомендуется	Рекомендуетс	Рекомендуется

переименование учетной записи администратора			я	
Учетные записи: переименование учетной записи гостя	Рекомендуется	Рекомендуется	Рекомендуется	Рекомендуется
Устройства: разрешать отстыковку без входа в систему	Отключено	Включено	Отключено	Отключено
Устройства: разрешено форматировать и извлекать съемные носители	Администраторы, интерактивные пользователи	Администраторы, интерактивные пользователи	Администраторы	Администраторы
Устройства: запретить пользователям установку драйверов принтера	Включено	Отключено	Включено	Отключено
Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям	Отключено	Отключено	Включено	Включено
Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям	Включено	Включено	Включено	Включено
Устройства: поведение при установке неподписанного драйвера	Предупреждать, но разрешать установку	Предупреждать, но разрешать установку	Не разрешать установку	Не разрешать установку
Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL	Отключено	Отключено	Отключено	Отключено
Интерактивный вход в систему: текст сообщения для пользователей при входе в систему	Вход только для авторизованных пользователей. Лица, осуществляющие попытки несанкционированного доступа, будут преследоваться по закону.	Вход только для авторизованных пользователей. Лица, осуществляющие попытки несанкционированного доступа, будут преследоваться по закону.	Вход только для авторизованных пользователей. Лица, осуществляющие попытки несанкционированного доступа, будут преследоваться по закону.	Вход только для авторизованных пользователей. Лица, осуществляющие попытки несанкционированного доступа, будут преследоваться по закону.
Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему	ПРОДОЛЖЕНИЕ ПОПЫТОК БЕЗ НАДЛЕЖАЩЕЙ АВТОРИЗАЦИИ ЯВЛЯЕТСЯ ПРЕСТУПЛЕНИЕМ.	ПРОДОЛЖЕНИЕ ПОПЫТОК БЕЗ НАДЛЕЖАЩЕЙ АВТОРИЗАЦИИ ЯВЛЯЕТСЯ ПРЕСТУПЛЕНИЕМ.	ПРОДОЛЖЕНИЕ ПОПЫТОК БЕЗ НАДЛЕЖАЩЕЙ АВТОРИЗАЦИИ ЯВЛЯЕТСЯ ПРЕСТУПЛЕНИЕМ.	ПРОДОЛЖЕНИЕ ПОПЫТОК БЕЗ НАДЛЕЖАЩЕЙ АВТОРИЗАЦИИ ЯВЛЯЕТСЯ ПРЕСТУПЛЕНИЕМ.
Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена)	2	2	0	1

Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее	14 дней	14 дней	14 дней	14 дней
Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки рабочей станции	Отключено	Отключено	Включено	Отключено
Интерактивный вход в систему: поведение при извлечении смарт-карты	Блокировка рабочей станции	Блокировка рабочей станции	Блокировка рабочей станции	Блокировка рабочей станции
Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера)	Включено	Включено	Включено	Включено
Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам	Отключено	Отключено	Отключено	Отключено
Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа	Включено	Отключено	Включено	Отключено
Доступ к сети: Разрешить трансляцию анонимного SID в имя	Отключено	Отключено	Отключено	Отключено
Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями	Включено	Включено	Включено	Включено
Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями	Включено	Включено	Включено	Включено
Сетевой доступ: не разрешать сохранение учетных данных или цифровых паспортов .NET для сетевой проверки подлинности пользователя	Включено	Включено	Включено	Включено
Сетевой доступ: запретить анонимный доступ к именованным каналам и общим ресурсам	Включено	Включено	Включено	Включено
Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей	Обычная - локальные пользователи удостоверяются как они сами	Обычная - локальные пользователи удостоверяются как они сами	Обычная - локальные пользователи удостоверяются как они сами	Обычная - локальные пользователи удостоверяются как они сами
Сетевая безопасность: не хранить хеш-значений LAN Manager при следующей смене пароля	Включено	Включено	Включено	Включено
Сетевая безопасность: принудительный вывод из сеанса по истечении допустимых часов работы	Включено	Отключено	Включено	Отключено
Сетевая безопасность: уровень проверки подлинности LAN Manager	Отправлять только NTLMv2 ответы	Отправлять только NTLMv2 ответы	Отправлять только NTLMv2	Отправлять только NTLMv2 ответ, отказывать

			ответ, отказывать LM и NTLM	LM и NTLM
Сетевая безопасность: минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC)	Минимума нет	Минимума нет	Требовать сеансовую безопасность NTLMv2, требовать 128-битное шифрование	Требовать сеансовую безопасность NTLMv2, требовать 128-битное шифрование
Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC)	Минимума нет	Минимума нет	Требовать сеансовую безопасность NTLMv2, требовать 128-битное шифрование	Требовать сеансовую безопасность NTLMv2, требовать 128-битное шифрование
Консоль восстановления: разрешить автоматический вход администратора	Отключено	Отключено	Отключено	Отключено
Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам	Включено	Включено	Отключено	Отключено
Завершение работы: разрешить завершение работы системы без выполнения входа в систему	Отключено	Отключено	Отключено	Отключено
Завершение работы: очистка страничного файла виртуальной памяти	Отключено	Отключено	Включено	Включено
Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хеширования и подписывания	Отключено	Отключено	Отключено	Отключено
Системные объекты: владелец по умолчанию для объектов, созданных членами группы администраторов	Создатель объекта	Создатель объекта	Создатель объекта	Создатель объекта
Параметры системы: использовать правила сертификатов для исполняемых файлов Windows для политик ограниченного использования программ	Отключено	Отключено	Отключено	Отключено

Параметры политики аудита

С помощью политики аудита определяются события безопасности, которые включаются в отчет для администратора. В результате этого создается журнал регистрации определенных действий системы и пользователей. Администратор получает возможность следить за действиями, имеющими отношение к безопасности, например за тем, кто получает доступ к объекту, когда пользователь входит и выходит из системы, а также за изменением параметров политики аудита.

Перед внедрением политики аудита необходимо определить категории событий, которые будут отслеживаться с ее помощью. Политика аудита определяется выбранными для каждой категории событий параметрами. Путем определения параметров для различных категорий событий можно создавать политику аудита, удовлетворяющую всем требованиям безопасности организации.

Если политика аудита не настроена, то в случае возникновения проблемы с безопасностью, будет очень сложно (или вообще не возможно) определить, что

произошло в действительности. С другой стороны, если настройками аудита назначено отслеживание большого количества разрешенных действий, журнал событий безопасности будет переполнен бесполезной информацией.
С помощью редактора политики настраиваются параметры политики аудита в Windows XP. Они расположены по следующему адресу:
Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Политика аудита

Таблица 7. Параметры политики аудита, которые используются для обеспечения безопасности компьютеров под управлением Windows XP

Название параметра	**ПК на предприятии (настольная система)**	**ПК на предприятии (портативная система)**	**Высокий уровень безопасности (настольная система)**	**Высокий уровень безопасности (портативная система)**
Аудит событий входа в систему	Успех, отказ	Успех, отказ	Успех, отказ	Успех, отказ
Аудит управления учетными записями	Успех, отказ	Успех, отказ	Успех, отказ	Успех, отказ
Аудит доступа к службе каталогов	Нет аудита	Нет аудита	Нет аудита	Нет аудита
Аудит входа в систему	Успех, отказ	Успех, отказ	Успех, отказ	Успех, отказ
Аудит доступа к объектам	Успех, отказ	Успех, отказ	Успех, отказ	Успех, отказ
Аудит изменения политики	Успех	Успех	Успех	Успех
Аудит использования привилегий	Нет аудита	Нет аудита	Отказ	Отказ
Аудит отслеживания процессов	Нет аудита	Нет аудита	Нет аудита	Нет аудита
Аудит системных событий	Успех	Успех	Успех, отказ	Успех, отказ

Параметры Internet Explorer

Настройте рекомендованные параметры пользователя для Internet Explorer в административном шаблоне по указанному адресу с помощью редактора объектов групповой политики.
Конфигурация пользователя\Административные шаблоны\Компоненты Windows
Таблица 8. Параметры пользователя для Internet Explorer.

Название параметра	**ПК на предприятии**	**Высокий уровень безопасности**
Меню обозревателя\Отключить параметр «Сохранить эту программу на диске»	Включен	Включен
Панель управления обозревателем\Отключить страницу «Дополнительно»	Включен	Включен
Панель управления обозревателем\Отключить страницу «Безопасность»	Включен	Включен
Автономные страницы\Отключить добавление каналов	Включен	Включен
Автономные страницы\Отключить добавление расписаний для автономных страниц	Включен	Включен
Автономные страницы\Отключить все расписания для автономных страниц	Включен	Включен
Автономные страницы\Полное отключение пользовательского интерфейса каналов	Включен	Включен
Автономные страницы\Отключить загрузку содержимого подписки	Включен	Включен
Автономные страницы\Отключить редактирование и создание новых групп расписаний	Включен	Включен
Автономные страницы\Отключить изменение	Включен	Включен

расписаний для автономных страниц		
Автономные страницы\Отключить протоколирование обращений к автономным страницам	Включен	Включен
Автономные страницы\Отключить удаление каналов	Включен	Включен
Автономные страницы\Отключить удаление расписаний для автономных страниц	Включен	Включен
Настройка Outlook Express	Включен	Включен
Отключить изменение параметров страницы «Дополнительно»	Включен	Включен
Отключить изменение параметров автонастройки	Включен	Включен
Отключить изменение параметров сертификатов	Включен	Включен
Отключить изменение параметров подключений	Включен	Включен
Отключить изменение параметров прокси	Включен	Включен
Отключить мастер подключения к Интернету	Включен	Включен
Запретить автозаполнению сохранение паролей	Включен	Включен

Хотелось бы рекомендовать размер Кеша Internet Explorer выставлять в минимум. В случае если у вас в кеше порядка ста тысяч мелких файлов размером в два-три килобайта, любой антивирус при сканировании данной папки будет работать очень медленно

Для защиты Internet Explorer от «изобретательных» пользователей можно воспользоваться следующим:

IExplorer: Hide General Page from Internet Properties
Чтобы спрятать вкладку Общие в параметрах Internet Explorer'a, добавьте в реестр:
[HKEY_CURRENT_USER\Software\Policies\Microsoft\ Internet Explorer\Control Panel]
"GeneralTab"=dword:1

IExplorer: Hide Securiry Page from Internet Properties
Чтобы спрятать вкладку Безопасность в параметрах Internet Explorer'a, добавьте в реестр:
[HKEY_CURRENT_USER\Software\Policies\Microsoft\ Internet Explorer\Control Panel]
"SecurityTab"=dword:1

IExplorer: Hide Programs Page from Internet Properties
Чтобы спрятать вкладку Программы в параметрах Internet Explorer'a:
[HKEY_CURRENT_USER\Software\Policies\Microsoft\ Internet Explorer\Control Panel]
"ProgramsTab"=dword:1

IExplorer: Hide Advanced Page from Internet Properties
Чтобы спрятать вкладку Дополнительно в параметрах Internet Explorer'a, добавьте в реестр:
[HKEY_CURRENT_USER\Software\Policies\Microsoft\ Internet Explorer\Control Panel]
"AdvancedTab"=dword:1

IExplorer: Hide Connections Page from Internet Properties
Чтобы спрятать вкладку Подключения в параметрах Internet Explorer'a, добавьте в реестр:
[HKEY_CURRENT_USER\Software\Policies\Microsoft\ Internet Explorer\Control Panel]
"ConnectionsTab"=dword:1

Защита подключения к Интернет

Для обеспечения безопасности при подключении к Интернет необходимо:

- Активизировать брандмауэр[15] подключения к Интернет (Internet Connection Firewall) или установить брандмауэр третьих фирм
- Отключить **Службу доступа к файлам** и принтерам сетей Microsoft

[15] Брандмауэром подключения к Интернет называется программный компонент, блокирующий нежелательный трафик.

Активация Брандмауэра подключения к Интернет.

- Откройте **Панель управления** – **Сетевые подключения**
- Щелкните **правой** кнопкой мыши на соединении, которое вы хотите защитить и выберите из меню пункт **Свойства**
- Перейдите на вкладку **Дополнительно**, поставьте галочку **Защитить мое подключение к Интернет**

Проводник

Проводник используется для навигации по файловой системе на клиентских ПК под управлением Windows XP Professional.
Настройте рекомендованные параметры проводника в административном шаблоне по указанному адресу с помощью редактора объектов групповой политики.
Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Проводник

Таблица 9. Параметры пользователя для Проводника.

Название параметра	ПК на предприятии	Высокий уровень безопасности
Удалить возможности записи компакт-дисков[16]	Не задан	Включен
Удалить вкладку «Безопасность»	Не задан	Включен

Иначе предотвратить запись компакт-дисков можно с помощью замены устройств с возможностью записи на обычные (read-only) или полного отказа от использования лазерных приводов.

Политика ограниченного использования программ для клиентских ПК под управлением Windows XP

Политика ограниченного использования программ позволяет администратору определить программы, которые могут быть запущены на локальном компьютере. Политика защищает компьютеры под управлением Microsoft® Windows® XP Professional от известных конфликтов и предотвращает запуск нежелательных программ, вирусов и «троянских коней». Политика ограниченного использования программ полностью интегрирована с Microsoft Active Directory® и групповой политикой. Ее также можно использовать на автономных компьютерах.
Администратор вначале определяет набор приложений, которые разрешается запускать на клиентских компьютерах, а затем устанавливает ограничения, которые будут применяться политикой к клиентским компьютерам.
Политика ограниченного использования программ в исходном виде состоит из заданного по умолчанию уровня безопасности для неограниченных или запрещенных параметров и правил, определенных для объекта групповой политики. Политика может применяться в домене, для локальных компьютеров или пользователей. Политика ограниченного использования программ предусматривает несколько способов определения программы, а также инфраструктуру на основе политики, обеспечивающую применение правил выполнения определенной программы. Пользователи, запускающие программы, должны руководствоваться принципами, установленными администратором в политике ограниченного использования программ.
Политики ограниченного использования программ применяются для выполнения следующих действий:

1. определения программ, разрешенных для запуска на клиентских компьютерах;
2. ограничения доступа пользователей к конкретным файлам на компьютерах, имеющих несколько пользователей;
3. определения круга лиц, имеющих право добавлять к клиентским компьютерам доверенных издателей;

[16] Данный параметр не запрещает запись компакт-дисков с помощью приложений сторонних производителей. В этом руководстве рекомендуется воспользоваться политиками ограниченного использования программ, чтобы не допустить использования приложений сторонних производителей для записи компакт-дисков.

4. определения влияния политики на всех пользователей или только пользователей на клиентских компьютерах;
5. запрещения запуска исполняемых файлов на локальном компьютере, в подразделении, узле или домене.

Архитектура политики ограниченного использования программ обеспечивает целый спектр возможностей.[17]

Политика ограниченного использования программ позволяет администратору определять и контролировать программы, запускаемые на компьютерах под управлением Windows XP Professional в рамках домена. Возможно создание политик, блокирующих выполнение несанкционированных сценариев, дополнительно изолирующих компьютеры или препятствующих запуску приложений. Оптимальным вариантом для управления политикой ограниченного использования программ на предприятии является использование объектов групповой политики и адаптирование каждой созданной политики к требованиям групп пользователей и компьютеров организации.

Не рекомендуется пытаться управлять группами пользователей в автономной среде[18]. Результатом правильного применения политики ограниченного использования программ будет улучшение целостности, управляемости и, в конечном счете, снижение совокупной стоимости владения и поддержки операционных систем на компьютерах организации.[19]

---

[17] Подробное рассмотрение этой политики выходит за рамки данной статьи

[18] Автономная среда встречается в организациях, компьютеры которых не могут быть включены в домен, или компьютеры, которые входят в домен под управлением Windows NT 4.0. Такие компьютеры настраиваются с помощью параметров локальной политики. Управление автономными компьютерами может представлять значительно больше сложностей по сравнению с организацией учетных записей пользователей и политик при помощи домена на базе Active Directory.

[19] Дополнительные сведения о политике ограниченного использования программ см. в статье «Using Software Restriction Policies to Protect Against Unauthorized Software» по адресу: http://www.microsoft.com/windowsxp/pro/techinfo/administration/restrictionpolicies/default.asp. Дополнительные сведения о службах, обеспечивающих безопасность среды, можно найти в документе «Technical Overview of Windows Server 2003 Security Services» по адресу: http://www.microsoft.com/windows.netserver/techinfo/overview/security.mspx. Дополнительные сведения о групповой политике см. в статье «Windows 2000 Group Policy» по адресу: http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp. Дополнительные сведения о безопасности переносных компьютеров можно найти в статье «Securing Mobile Computers with Windows XP Professional» по адресу: http://www.microsoft.com/windowsxp/pro/techinfo/administration/mobile/default.asp.

Заключение

Изложенные выше рекомендации не являются исчерпывающим материалом по настройке операционной системы Windows XP Professional, однако надеюсь, они смогут помочь вам в этом нелегком процессе