Рига 14-Май-2009

# Руководство по настройке Microsoft Windows XP и Microsoft Windows Server 2003 для повышения уровня безопасности и максимально эффективной защиты от вирусов.

Microsoft CERTIFIED Professional
Microsoft CERTIFIED Systems Administrator
Microsoft CERTIFIED Systems Engineer
Microsoft CERTIFIED Trainer
Systems Engineering
Systems Administration

Peter Gubarevich, CIO
Maskavas 261, Riga, Latvia LV-1063
Phone: +371 67188803, +371 29483420
E-mail: peter@optimalsolutions.lv

# Содержание

# 1. Цель документа.

В данном Руководстве рассказывается, как правильно установить операционные системы **Microsoft Windows XP Professional** и **Windows Server 2003** и сконфигурировать их для безопасной работы на одиночных (в т.ч. домашних) компьютерах и в рабочих группах. Эту же методику, но с учётом некоторых особенностей, можно применять и для следующих систем:

- **Microsoft Windows 2000** всех версий;
- **Microsoft Windows XP Home** (некоторые настройки придётся делать в системном реестре вручную, а также применять средства сторонних производителей);
- **Microsoft Windows Vista / Windows Server 2008.**

Главное отличие Руководства от аналогичных документов заключается в том, что оно последовательно описывает точную конфигурацию, которую необходимо выполнить для получения защищённой от вирусного поражения среды. Акцент смещён с «**вы можете** настроить такие-то параметры» на «**вы должны** указать конкретно такие-то значения таких-то параметров».

Несмотря на то, что документ ориентирован в первую очередь на одиночные машины и рабочие группы, данный подход не менее эффективно проявляет себя и в доменах **Active Directory**, где однажды выполненная настройка применяется сразу на большом количестве компьютеров.

# 2. Предисловие автора.

### 2.1. Теория и практика.

Данное Руководство является результатом практических наработок, полученных автором при построении и управлении компьютерными сетями на базе различных версий Microsoft Windows. Все описанные правила на протяжении длительного времени успешно применяются не только самим автором, но и другими системными администраторами, прошедшими соответствующее обучение, на всех подотчётных им коммерческих предприятиях, учебных заведениях и домашних системах.

Каждый пункт этого документа является в равной степени важным для достижения обозначенного в его заголовке результата. Теоретическое обоснование представленных далее методик работы вы можете найти как в официальной литературе Microsoft, так и в документации сторонних производителей.

### 2.2. Для кого предназначен этот документ.

Целевая аудитория Руководства – IT-специалисты начального и среднего уровня, преподаватели информатики школ и других учебных заведений, а также домашние пользователи, работающие с компьютером на уровне Опытного Пользователя. Предполагается, что читатель умеет обращаться с компьютерной аппаратурой, устанавливать Microsoft Windows и бизнес-приложения, но желает научиться обеспечивать надёжную и безопасную работу этих систем.

Употребляемая в тексте терминология предполагает использование англоязычной системы Windows. С целью сохранения небольшого размера документа, не каждое действие описывается во всех подробностях. Также предполагается, что читатель обладает достаточным опытом, чтобы отвечать на вопросы вида «где находится консоль Disk Management?» самостоятельно.

### 2.3. Права и ответственность.

2.3.1. Разрешается использовать данный документ в настройке домашних, учебных и производственных компьютерных систем.
2.3.2. При цитировании или использовании материалов в сторонней документации ссылка на автора обязательна.
2.3.3. Использование данного материала в учебных курсах разрешается только с письменного согласия автора.
2.3.4. Вся информация предоставляется на условиях «КАК ЕСТЬ», без предоставления каких-либо гарантий и прав, кроме оговорённых выше.

# 3. Концепция безопасной работы.

### 3.1. Антивирус – не панацея.

Подавляющее большинство рядовых пользователей, а также большой процент людей из числа системных администраторов полагает, что наличия только антивирусной программы вполне достаточно для защиты компьютера от вирусов; что при этом можно совершенно не заботиться о правах, блокировках и прочих правилах безопасности.

Невозможно отрицать полезность антивирусных средств; однако, сейчас их роль явно преувеличена в сознании людей. Технически, любая антивирусная программа имеет свой процент срабатывания (от 50% до 95%). Вне зависимости от обещаний производителя, 100% на сегодняшний день, равно как и в обозримом будущем, недостижимы. Более того, постоянно появляются угрозы новых типов – не только использующие комбинированные методы проникновения в систему, но и способные задействовать слабые стороны многих антивирусных пакетов.

Практика предъявляет нам более внушительные цифры - по статистике ряда интернет-провайдеров, **не менее 30%** компьютеров (то есть, каждый третий!), принадлежащих домашним пользователям поражены вредоносными программами. При этом практически на всех из них установлены антивирусные пакеты и средства обнаружения шпионских модулей от различных производителей. Пользователи, заявляющие «я всё просканировал, мой антивирус ничего не находит», в принципе, говорят правду – установленный антивирусный продукт действительно **ничего не находит.** Было бы странно, если бы антивирус мог сообщить «я пропустил конкретно такой-то неизвестный мне вирус». В самом деле, угрозы класса **rootkit** чрезвычайно сложны в обнаружении – такова их изначальная природа.

### 3.2. Более эффективные методы защиты.

Опыт показывает, что защита от вирусов только антивирусными программами работает крайне слабо, **является неэффективной.** Однако, уже десятки лет существует и успешно применяется в производственной среде методика защиты от зловредных программ средствами, встроенными в саму операционную систему. В основу защиты положен принцип **предоставления наименьших полномочий,** а также некоторые дополнительные мероприятия, в целом повышающие уровень безопасности компьютерной системы.

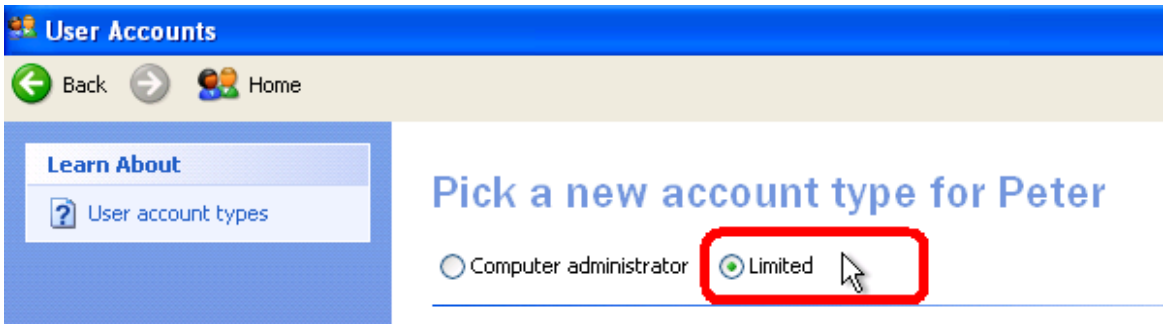



*Рис. 3.1. Фундамент эффективной защиты от вирусов – работа с ограниченными привилегиями*

Максимально эффективная защита от вирусов достигается за счёт соблюдения одновременно нескольких правил:

- **Ограниченные привилегии.** Пользователи допускаются к работе в системе только с ограниченными привилегиями, любое использование привилегий Администратора должно быть жёстко регламентировано;
- **Строгие разрешения NTFS.** Уровень доступа пользователей к исполняемым модулям любых программ ограничивается Чтением. Право Записи допускается только на те папки и файлы, где это действительно необходимо;
- **Политики Software Restriction.** Разрешается запускать программы только из заранее составленного списка, всё остальное должно блокироваться;
- **Security Updates.** Обновления безопасности должны своевременно устанавливаться как для для самой операционной системы, так и связанных с ней компонентов (например, Adobe Flash), а также производственных программ;
- **Политики безопасности**. Параметры системы «по умолчанию» не всегда безопасны. Детальная настройка политик безопасности – важный шаг для повышения уровня защиты компьютера;
- **Блокирование замусоривания системы**. Установка любой новой программы должна быть чётко обоснована техническим персоналом, а инсталляционные файлы проверены антивирусной программой.

### 3.3. Принцип предоставления наименьших полномочий.

Операционная система чётко различает пользователей, предоставляя им различные уровни доступа – например, Административный, Обычного пользователя или Гостевой. **Администратор,** как правило, ничем не ограничен, и человеку с таким уровнем доступа разрешено совершать любые действия – устанавливать новые программы, настраивать параметры системы, регулировать права других пользователей. Постоянная работа с привилегиями Администратора открывает систему для случайного заражения «троянским конём» и других рисков безопасности.

Напротив, привилегий **Обычного пользователя** вполне достаточно для работы с документами, Интернетом, бизнес-приложениями, одновременно оставляя систему и программы «на предохранителе». Ограниченные права не позволяют пользователю (и зловредным программам) вносить ни положительные, ни отрицательные изменения в настройку системы. Таким образом, состояние системы консервируется вне зависимости от того, какие программы запускаются пользователями.

Типовой компьютерный вирус – не мистическая субстанция, а заражение - не магический обряд. То, что мы понимаем под «вирусом» – это просто программа, автор которой заранее нацелил её на выполнение определённых деструктивных действий и дальнейшее распространение.

Будучи случайно или преднамеренно запущенной человеком на исполнение, вирусная программа в дальнейшем оперирует от его лица, обладая тем же уровнем привилегий, что и сам пользователь. Поэтому, вопрос заражения системы и дальнейшего распространения вируса в первую очередь зависит от того, какими правами обладает пользователь, его запустивший. Зловредная программа, выполненная с привилегиями Обычного пользователя, не найдёт путей дальнейшего распространения, будучи физически неспособной проникнуть внутрь системы.

**3.4. Задача непроста, но выполнима.**

Задача, которую мы поставили перед собой и реализуем с помощью Руководства - **законсервировать компьютер** в его первоначально стабильном, незаражённом состоянии и удерживать таковым на протяжении длительного времени. Эта цель последовательно достигается выполнением всех пунктов Руководства, каждый из которых имеет своё существенное значение и должен быть реализован теми или иными средствами на каждом компьютере, будь то производственная или домашняя система.

Кроме устранения вирусных угроз, выполняемые настройки существенно помогут в решении некоторых других вопросов – сохранения производительности системы, организации резервного копирования и повышения общего уровня безопасности сети.

# 4. Правила распределения ресурсов.

Основная задача и смысл работы Администратора - грамотно распоряжаться вычислительными ресурсами, обеспечивая им должную сохранность и предоставляя по необходимости пользователям. Однако, невозможно качественно управлять программами, выполнять резервное копирование и защиту данных, которые беспорядочно разбросаны по дискам и каталогам нескольких компьютеров.

### 4.1. Построение чёткой и понятной структуры ресурсов.

Концентрируйте важные документы и бизнес-программы на главном компьютере (сервере). Разработайте Правила распределения ресурсов, построив их на примере предложенного ниже образца. Направьте Правила на решение следующих задач:

- автоматизированная доступность ресурсов с любой точки сети;
- удобное, понятное и простое разграничение доступа, защита ресурсов;
- резервное копирование, исполняемое с должной частотой и в надлежащем объёме;
- приемлемая производительность компьютера и сети при доступе к ресурсам;
- гибкость и масштабируемость Правил при взаимодействии указанных компонентов.

Любые файловые ресурсы, которыми оперирует ваш компьютер, должны храниться в **заранее определённых** местах - дисках, разделах, папках. От того, насколько точно вы придерживаетесь этого правила, напрямую зависит рассматриваемая нами безопасность системы, а также надёжность и скорость её работы

Организуйте хранение документов в отведённых для этого местах не только программными настройками, но и ознакомьте пользователей с соответствующей письменной инструкцией. Исполнение ими правил хранения данных позволит защитить документы от несанкционированного доступа и обеспечить резервное копирование в должном объёме.

Задокументируйте и чётко соблюдайте принятые вами Правила распределения ресурсов. Это поможет следовать им как в масштабах одного компьютера, так и всей сети, управляемой группой системных администраторов.

### 4.2. Пример Правил для рабочей станции.

Предполагая, что функции компьютера можно описать как "типовая рабочая станция", спланируйте разделение жёсткого диска на две части:

- **C: (System)** для системы и программ, которые вы проинсталлируете дополнительно;
- **D: (Data)** для хранения временных файлов и возможных рабочих директорий пользователей.

В любом случае, пользовательские данные должны быть отделены от системы. Разделённые ресурсы подвергаются раздельному квотированию, фрагментации, резервному копированию. Одновременно, это даёт возможность качественно законсервировать систему.

Обычные бизнес-программы (**Microsoft Office, архиватор**), которые легко восстанавливаются после повреждения, устанавливайте на раздел C: в папку **Program Files.** Других папок в корне системного диска создавать не следует, так как это увеличит число **точек управления** ресурсами.

Исполняемые модули производственных программ, требующих регулярного резервного копирования или ограничения доступа (**1С, SHOP, клиент Интернет-банка** и т.д.), рекомендуется хранить на центральном компьютере и запускать по сети - это упростит операции обслуживания, позволит контролировать доступ в одной точке управления и гарантирует единую версию программ для всех пользователей.

Для случаев, когда это недостижимо, создайте и используйте локальный каталог **D:\Accounting.** Обязательно разделяйте не только различные программы, так и собственно их исполняемые модули от баз данных, например:

```
D:\Accounting\1C
D:\Accounting\1C\Programs
D:\Accounting\1C\Programs\1Cv77
D:\Accounting\1C\Programs\1Cv80
D:\Accounting\1C\Bases
D:\Accounting\1C\Bases\CompanyA
D:\Accounting\1C\Bases\CompanyB
```

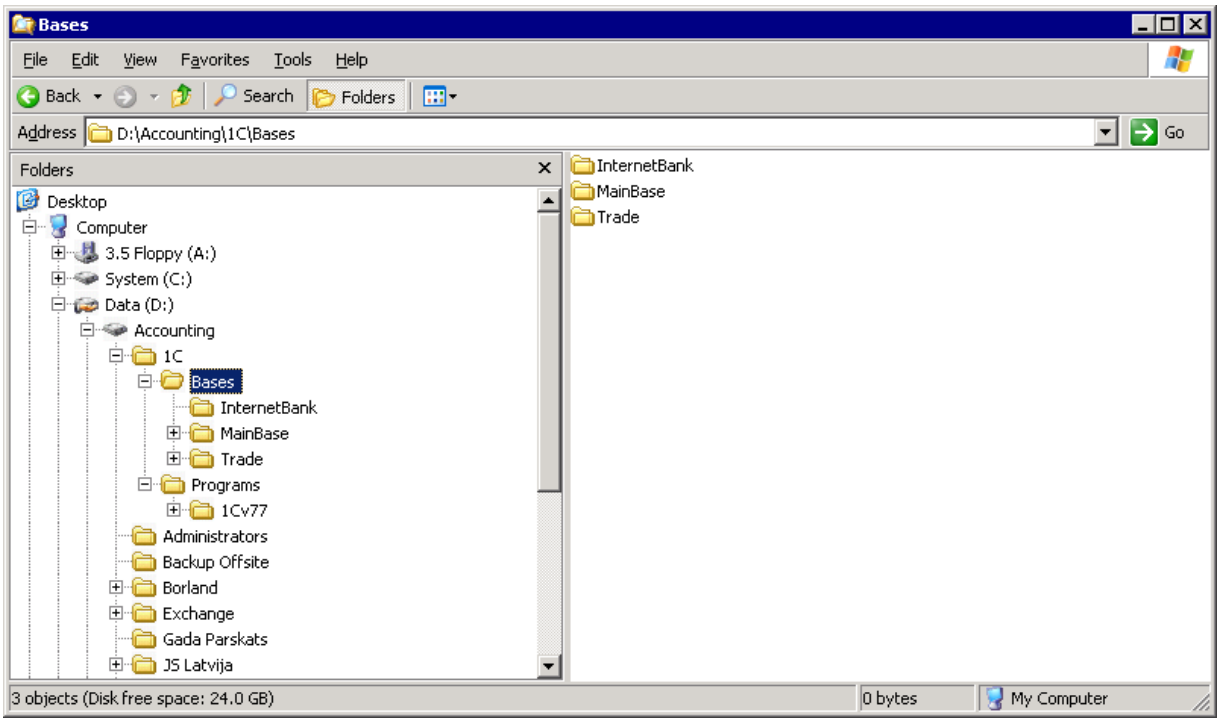



*Рис. 4.1. Пример построения структуры каталогов производственных программ*

Описанная структура упростит резервное копирование и позволит правильно назначить права доступа, закрыв исполняемые модули от несанкционированных изменений и вирусного поражения, а базы данных - от несанкционированного доступа. Для нужд пользовательских программ и записи временных файлов создайте каталог **D:\Users.** Другие папки в корне пользовательского диска создавать не следует, дабы избежать излишней хаотичности структуры каталогов.

### 4.3. Пример Правил для сервера.

При планировании распределения ресурсов на центральном компьютере повышенное внимание уделите дисковой подсистеме. Наиболее медленным компонентом современного компьютера является жёсткий диск – а именно, процесс перемещения головок диска при поиске нужных дорожек. По возможности, не делите диски на разделы, а выделите для хранения документов и бизнес-приложений отдельные физические диски (шпиндели). Это поможет справиться с конкурентными операциями доступа к различным данным, зачастую повышая производительность дисковой подсистемы в десятки раз.

Пример конфигурации типового сервера уровня отдела или малой сети:

- **C: (System)** для системы и программ, которые вы проинсталлируете дополнительно;
- **D: (Data)** для хранения инсталляционных ресурсов и глубинных резервных копий;
- **V: (Accounting)** исполняемые модули бизнес-программ и базы данных;
- **U: (Users)** документы пользователей, файлообмен.

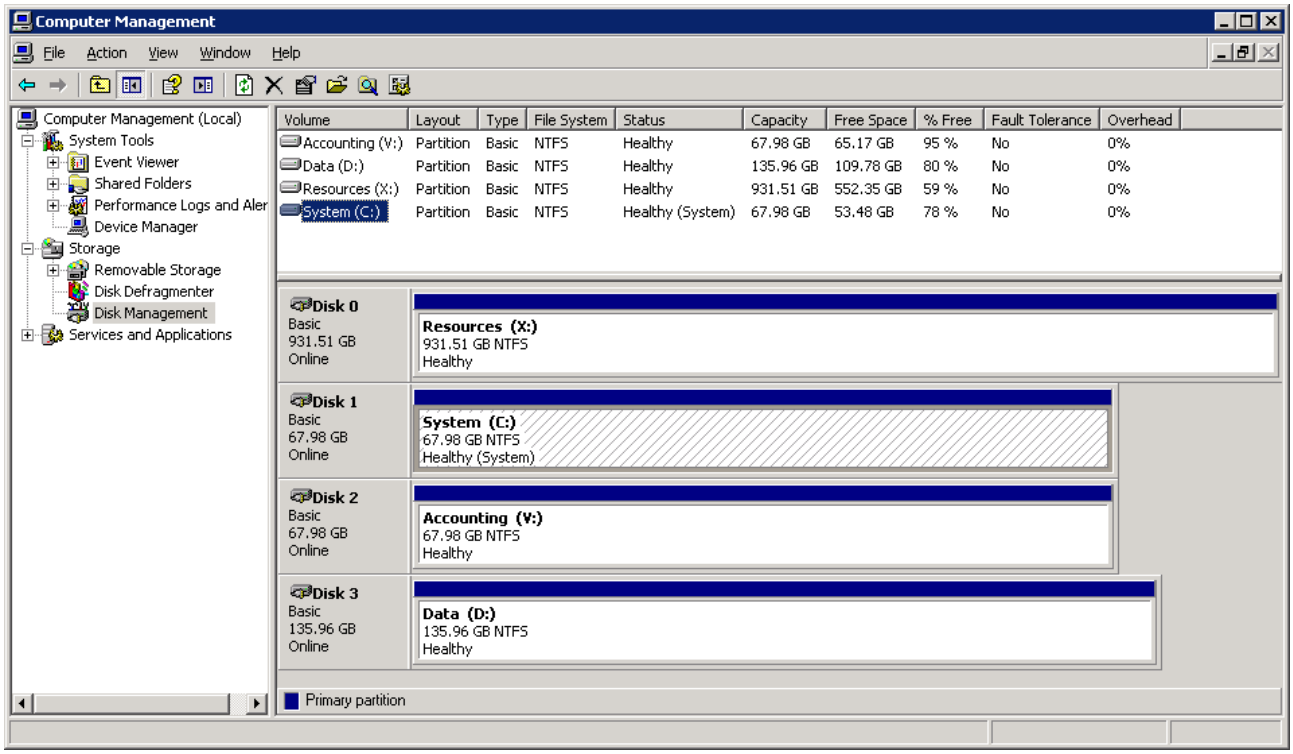



*Рис. 4.2. Пример построения структуры дисковых массивов сервера*

Подмонтировав разделы (или физические диски) V: и U: в папки **D:\Accounting** и **D:\Users** соответственно, вы сможете уменьшить число объектов управления, сузив обзор до системного (C:) и логического ресурсного (D:) разделов. Папку D:\ предоставьте для доступа по сети (**Share "Data"**). Тем самым, вся структура ресурсов будет представлена минимальным числом объектов управления как внутри одного сервера, так и в масштабах целой сети, что позволит обращаться с ними по типовой логике.

Для хранения исполняемых модулей бизнес-приложений и соответствующих данных создайте структуру каталога **D:\Accounting** согласно образцу, описанному в пункте "Пример Правил для рабочей станции". Работа с этой папкой по шаблону позволит вам иметь уверенность, что применяемая защита гарантированно работает на всех компьютерах сети.

Спланируйте размещение документов, электронной почты и других файлов пользователей в следующей структуре папок внутри **D:\Users** :

```
D:\Users\_ Shared Documents
D:\Users\User1
D:\Users\User2
D:\Users\User3
```

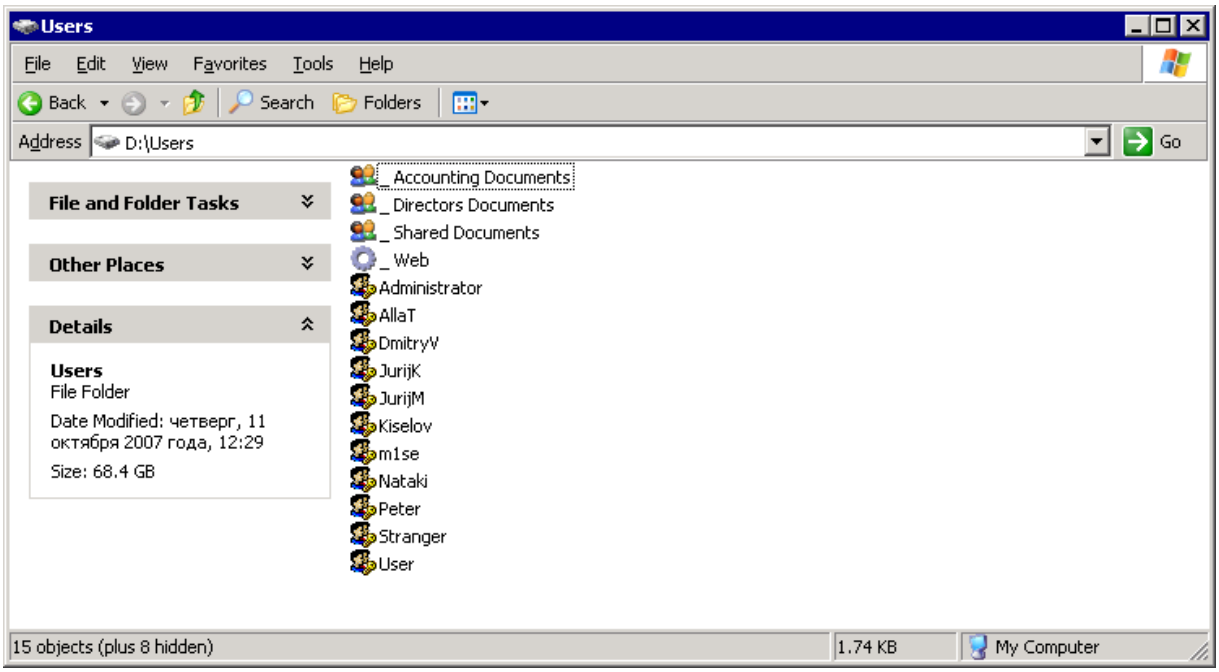



*Рис. 4.3. Пример построения структуры домашних каталогов пользователей*

Любые общие (разделяемые) документы храните внутри каталога **Shared Documents,** при необходимости создавая подкаталоги с ограничениями доступа по группам пользователей. Напротив, **домашние директории** типа D:\Users\Peter предназначены для индивидуальной работы самих пользователей. Подобная системность, поддерживаемая групповой политикой перенаправления папки **My Documents** в путь "\\Server\Data\Users", позволяет пользователям удобно получать доступ к своим документам с любой точки сети и эффективно обмениваться данными друг с другом.

Сохраняйте в **D:\Resources** инсталляционные файлы всех использованных программ и драйверов, серийные номера, а также актуальную копию состояния системы. Это позволит быстро восстановить систему и программы в случае сбоя. Убедитесь, что эта папка доступна только Администраторам, чтобы пользователи не смогли использовать её содержимое в своих целях.

# 5. Первый этап инсталляции системы.

### 5.1. Правильная инсталляция – фундамент стабильной работы.

Заранее проинтегрируйте последний **Service Pack (Пакет Исправлений)** в установочный компакт-диск – это ускорит процесс настройки компьютера, а также будет полезным в дальнейшем – в случае, если придётся восстанавливать повреждённую систему.

Установите Windows, загрузив компьютер с установочного компакт-диска и создав с его помощью только системный раздел. Укажите, чтобы система отформатировала этот раздел в файловой системе NTFS. Остальные разделы и папки вы создадите после инсталляции с помощью консоли **Disk Management** или инструментами командной строки (**diskpart**). Если на момент инсталляции на жёстком диске уже существовали разделы, но нужно изменить их размеры, сначала удалите все разделы. Удаление выполняйте по очереди, начиная с последнего раздела; в противном случае, нумерация в таблице разделов может смениться нежелательным образом. Следует исключить применение любых сторонних средств для операций с дисками:

- встроенные средства Windows способны полностью решить все задачи конфигурации дискового пространства;
- инструментальный набор Windows, обладая полной информацией о возможностях дисковой подсистемы, управляет ею наиболее корректно.

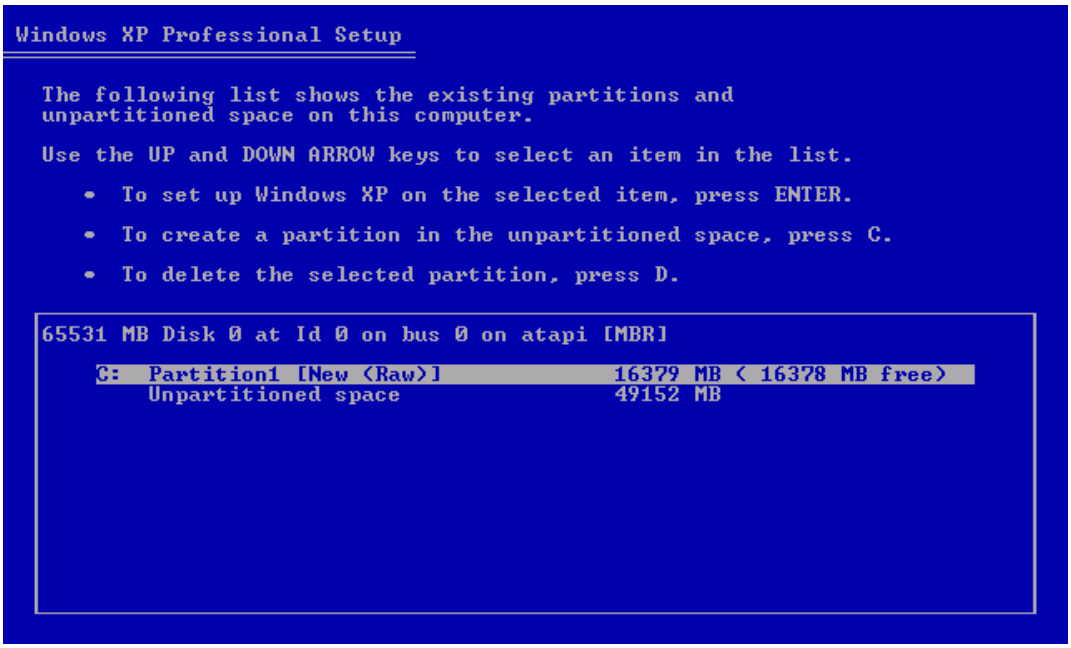



*Рис. 5.1. Создание системного раздела с помощью установочного компакт-диска Windows*

В случае, если установка производится с применением технологий клонирования дисков, убедитесь, что эта процедура выполняется версией программного обеспечения, способной корректно работать со всеми свойствами NTFS, в противном случае существует риск получить частично неисправную систему - например, неработоспособный механизм квотирования (NTFS Quota) при остальных внешне исправных характеристиках.

Также убедитесь, что копия системы получила новый уникальный **Идентификатор Безопасности (SID).** Для этого во время создания образа диска используйте утилиту SysPrep. В случае, если это не было сделано, существует ещё один способ замены SID - утилита NewSID (http://technet.microsoft.com/en-us/sysinternals/bb897418.aspx)

Не подключайте кабель локальной сети до тех пор, пока не закончится инсталляция, и вы не проверите, что **firewall (брандмауэр)** включён. На данном этапе в системе ещё не установлены последние обновления безопасности, и компьютер может быть уязвим к атакам сетевых червей. По окончании процесса инсталляции Windows установите все необходимые драйвера, компоненты системы, после чего выполните процедуру Windows Update. Выполните обновление не только Windows, но и всех других устанавливаемых программ.

### 5.2. Бюрократия – одно из препятствий на пути вирусов.

Зачастую вирусная инфекция приносится вместе с заражёнными файлами устанавливаемых программ. Предлагаемый далее механизм контроля позволяет снизить количество ненужных инсталляций, что также уменьшит вероятность проникновения вирусов и положительно скажется на стабильности работы системы в целом.

Чётко определите функции компьютера. Создайте и поддерживайте в текущем состоянии **Паспорт компьютера,** в котором будут указаны следующие сведения:

- копии чеков, товарно-транспортные накладных и гарантийных талонов приобретённой аппаратуры, программного обеспечения и комплектующих;
- копии лицензий на программное обеспечение и серийные номера;
- список установленного системного и прикладного программного обеспечения;
- контактная информация ответственного персонала.

Убедитесь, что все пользователи с Административными полномочиями ознакомились со списком разрешённых к установке программ и намерены его соблюдать. Строго фильтруйте этот список; не устанавливайте ни единой программы с целью **"просто посмотреть"**, или **"хорошая утилита, друг посоветовал"**. В подавляющем большинстве случаев, система готова к работе и не нуждается ни в каких сторонних утилитах. Любые исключения из этого правила должны иметь техническое обоснование.

Занесите в список тот минимум прикладного программного обеспечения, который **действительно необходим** пользователям для работы. Не допускается инсталляция программ по причинам «на всякий случай», «новый браузер, им сейчас все пользуются» или из-за незнания возможностей уже установленных средств (например, добавление Adobe Photoshop из-за неумения повернуть фотографию в Microsoft Paint).

Инсталляционные ресурсы следует брать только из оригинальных источников (компакт-диск, сайт производителя) или других заведомо чистых носителей. Источники **"сайт одного компьютерного журнала"** или **"мой знакомый дал"** категорически запрещаются! Устанавливайте программы только после антивирусной проверки инсталляционных файлов.

# 6. Регистрация учётных записей пользователей.

Каждому человеку, который будет иметь локальный или удалённый доступ к системе, выдайте **User Account (индивидуальную учётную запись),** обладающую привилегиями **Обычного пользователя.** Во избежание двойных конфигураций и излишней путаницы, убедитесь, что все допущенные люди зарегистрированы только единожды. Исключением являются лишь администраторы, выдайте им по две учётные записи:

- одна с административными привилегиями - для установки программ, настройки системы и конфигурации параметров безопасности;
- одна с правами обычного пользователя, от лица которой администратор будет выполнять остальные свои повседневные задачи (доступ в Интернет и к электронной почте, работа с документами и т.д.).

Убедитесь, что два человека обладают административными учётными записями – в случае, если один из администраторов будет недоступен (недееспособен), ситуация может быть взята под контроль с помощью запасного. Если администратор всего один, пароль запасной административной учётной записи сохраните в сейфе в запечатанном виде.

Создайте отдельную учётную запись **User** с ограниченными привилегиями для тестирования работоспособности системы. Чтобы сохранить пользовательский профиль в неизменном исправном состоянии, не используйте её для реальной работы.

Создайте отдельную учётную запись **Backup** с ограниченными привилегиями для выполнения процедур автоматического резервного копирования. Добавьте её в локальную группу Backup Operators, так как эта группа обладает необходимыми полномочиями для выполнения копирования **System State (состояния системы).**

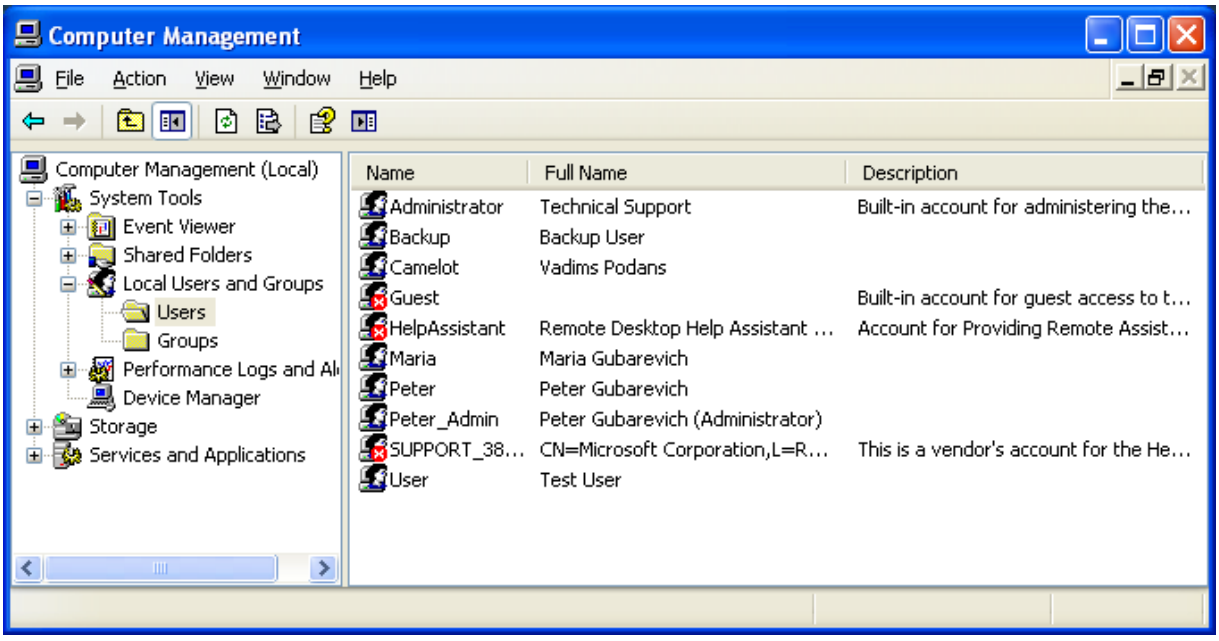



*Рис. 6.1. Каждому пользователю выдана индивидуальная учётная запись*

Создавайте отдельные учётные записи для всех служб, которые способны нормально работать с ограниченными правами (например, **Microsoft SQL Server**). Включайте их в группы безопасности по тому же принципу наименьших привилегий, что и настоящих пользователей. В случае проведения успешной атаки на службу SQL взломщик (или сетевой червь) получит ограниченный уровень доступа, что приведёт к наименьшему ущербу, чем если бы он захватил контроль над всей системой (учётной записью **SYSTEM**, обладающей максимальными привилегиями).

Объедините служебные учётные записи в группе **Service Accounts**. Это поможет назначить общие для них разрешения и запреты – например, запрет на использование Терминальных служб. Также, включите для них параметры **"Password Never Expires" ("Пароль не истекает")** и **"User Cannot Change Password" ("Пользователь не может сменить пароль")**.

Задокументируйте назначение служебных учётных записей и уровень их привилегий. Также опишите процедуры поддержки служб (настройка компонентов, восстановление из резервных копий и т.п.), чтобы ответственный персонал был способен решать проблемы их работоспособности быстро и качественно.

Процесс регистрации новых, а также деактивации неиспользуемых учётных записей обычно состоит из множества сложных шагов и подчиняется определённым правилам. Запротоколируйте все положенные действия, чтобы ответственный персонал выполнял их корректно, не ослабляя уровня безопасности системы.

# 7. Организация работы с группами.

Создавайте отдельные локальные группы для назначения доступа к каждому ресурсу, который будет предоставлен пользователям (цветной лазерный принтер, база данных 1С, папка Shared Documents и т.д.). Добавляйте учётные записи в эти группы только согласно реальной необходимости.

Например, лица, в обязанности которых будет входить работа с программой 1С, должны быть занесены в группу 1С Users. Если на компьютере хранятся несколько баз данных 1С, создайте отдельную локальную группу для каждой из этих баз.

Давайте группам ясные и читабельные названия. Задокументируйте назначение групп, чтобы осуществляющий техническую поддержку персонал не усложнял настройки без надобности и не ослаблял уровня безопасности системы.

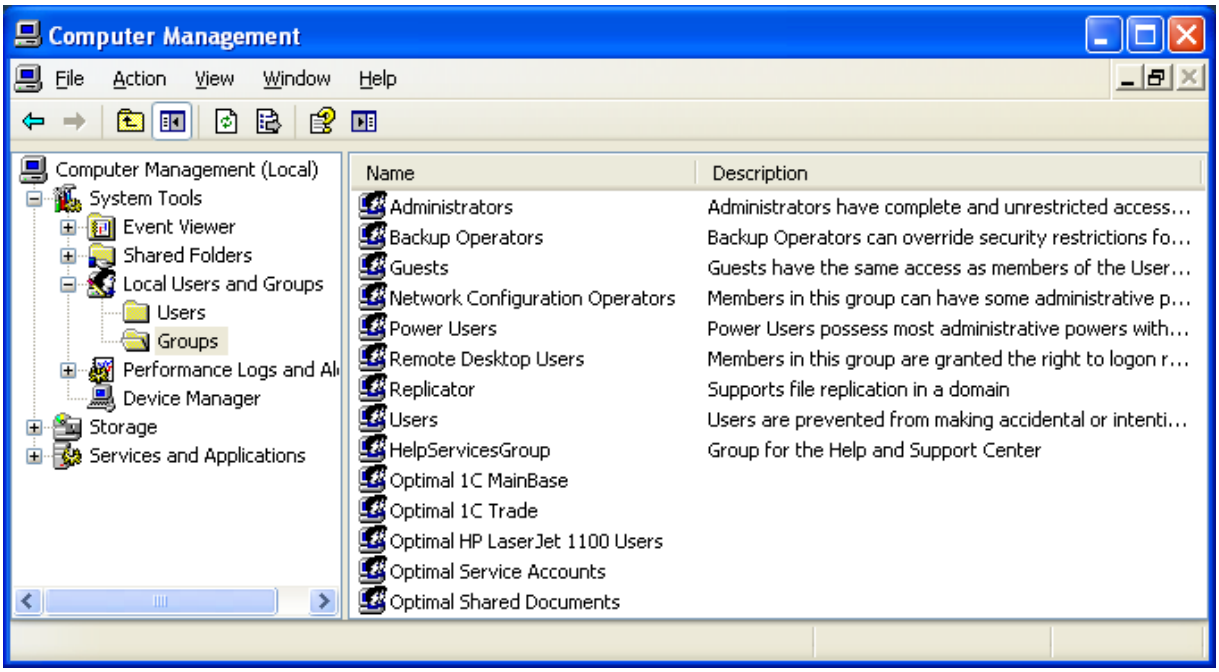



*Рис. 7.1. Для каждого ресурса создана отдельная локальная группа*

Особое внимание следует уделить группам с повышенными полномочиями. Категорически запрещается выдавать административные привилегии рядовым пользователям, в задачи которых не входит обслуживание данной компьютерной системы.

Не добавляйте пользователей в группу **Power Users (Опытные Пользователи)** – права этой группы де-факто являются административными. При её использовании вирусное заражение или захват управления станут столь же вероятными, как при постоянной работе с привилегиями Администратора.

На мобильных компьютерах внесите системную группу **Interactive (Интерактивные пользователи)** в локальную группу **Network Configuration Operators (Операторы сетевой конфигурации)**. Это даст пользователям возможность менять настройки сетевых интерфейсов, не прибегая к привилегиям Администратора.

# 8. Подготовка профилей пользователей.

**User Profile (Профиль пользователя)** – сумма всех личных настроек пользователя, начиная с цвета фона рабочего стола и заканчивая настройками реестра, без которых бизнес-программы не могут работать в нормальном режиме. Работая от лица Администратора, настройте визуальную среду и бизнес-программы. Ниже приведены некоторые настройки, имеющие важное значение для рабочей среды пользователей:

- Установите местоположение папки **My Documents (Мои Документы)** в D:\Users для одиночных машин или \\Company-Server\Data\Users для рабочей группы. Многие программы ориентируются на My Documents, предлагая её по умолчанию при открытии или сохранении документов;

- В Control Panel -> System настройте переменные окружения **%TEMP%** и **%TMP%** пользователя на папку **D:\Users\%UserName%\Temp**. Многие программы создают временные папки и файлы для своей работы. Такие файлы не должны храниться на законсервированном системном разделе. Также, перенацельте системные переменные окружения **%TEMP%** и **%TMP%** в папку **D:\Users\Temp**.

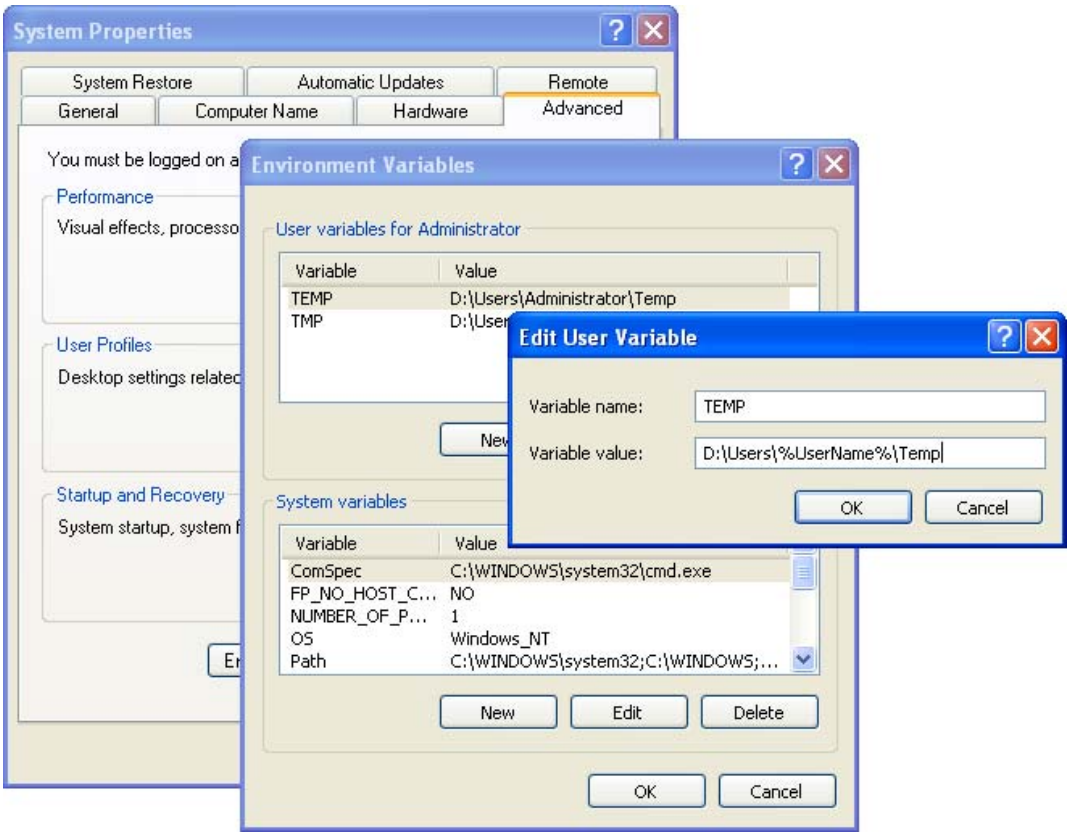



*Рис. 8.1. Настройка переменных окружения %TEMP%, %TMP%*

- Настройте подключения ко всем необходимым **сетевым дискам и принтерам.** Пользователи не должны беспорядочно блуждать по сети, пытаясь найти необходимые им для работы документы;
- Измените размер и местоположение папки **Temporary Internet Files.** Если за компьютером работают несколько человек, суммарный объём этих папок может составлять несколько гигабайт. К сожалению, эта настройка не воспринимает переменные типа %UserName%, поэтому регулируйте её для каждого пользователя отдельно либо вручную, либо в реестре с помощью Logon Script (сценария входа) (см. ключ HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellFolders\). Укажите целевую папку **D:\Users\%UserName%\Temporary Internet Files**;

- Правильно расположите на **Desktop (Рабочем столе)** и в **Start Menu (Меню Пуск)** ярлыки всех необходимых пользователям программ. Ярлыки программ, которые должны быть доступны всем пользователям без исключения, скопируйте в папку C:\Documents and Settings\All Users\Desktop. Ярлыки программ, доступ к которым будет ограничен, скопируйте на личный рабочий стол подготавливаемого профиля (C:\Documents and Settings\Administrator\Desktop). Ярлыки неиспользуемых пользователями программ (например, Command Prompt в Accessories), следует убрать вообще, чтобы не засорять рабочую среду;

- Выполните все частные **настройки бизнес-программ** (например, настройте список баз и шрифты программы 1С). Укажите все необходимые для работы **региональные установки** и раскладки клавиатуры. Как результат, человек должен получить готовую к работе систему, а не пытаться решить множество непонятных ему вопросов при первом входе в компьютер;

- Настройте запрет всех видов **Autorun (автозапуска),** так как некоторые вредоносные программы используют данный механизм для заражения системы и дальнейшего своего распространения. Для этого в групповой политике укажите значение **All Drives** параметра **Turn Off Autoplay** в разделе Administrative Templates, System контейнеров Computer Configuration и User Configuration;

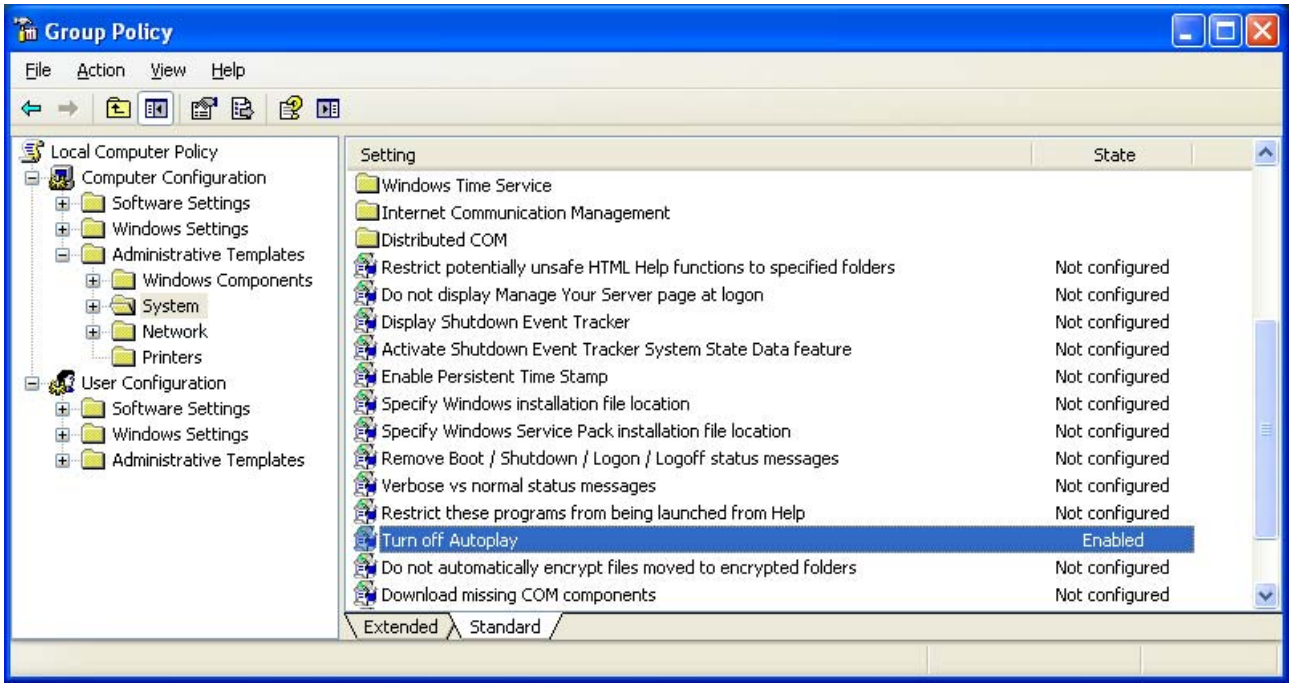



*Рис. 8.2. Запрет Autorun с помощью групповых политик*

- С помощью команды msconfig или утилиты autoruns (http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx) отредактируйте список **запускаемых при входе в компьютер программ.** Следует убрать из автозагрузки программы, не являющиеся необходимыми для работы;

- Настройте включение **Screen Saver (хранителя экрана)** и блокировку системы паролем при бездействии пользователя. Открытый компьютер, оставленный без присмотра, является хорошим плацдармом для нападения злоумышленников. Выберите разумное значение времени бездействия, чтобы не мешать нормальной работе пользователей - например, 1200 секунд (20 минут). Укажите значения параметров **Screen Saver timeout**, **Password protect the screen saver** в разделе Administrative Templates, Control Panel, Display в контейнере User Configuration.

Закончив настройку рабочей среды, освободите текущий профиль от заведомо ненужных остатков инсталляционных пакетов и временных файлов. Объём отлаженного профиля обычно не превышает 5-10 Мб.

Зайдите в систему с учётной записью резервного Администратора. Открыв Control Panel -> System, найдите и скопируйте подготовленный профиль в папку **C:\Documents and Settings\Default User (Пользователя по умолчанию)**. При копировании укажите право пользования профилем группе Authenticated Users. Таким образом, профили всех пользователей, заходящих в компьютер в первый раз, будут сформированы по заготовленному образцу.

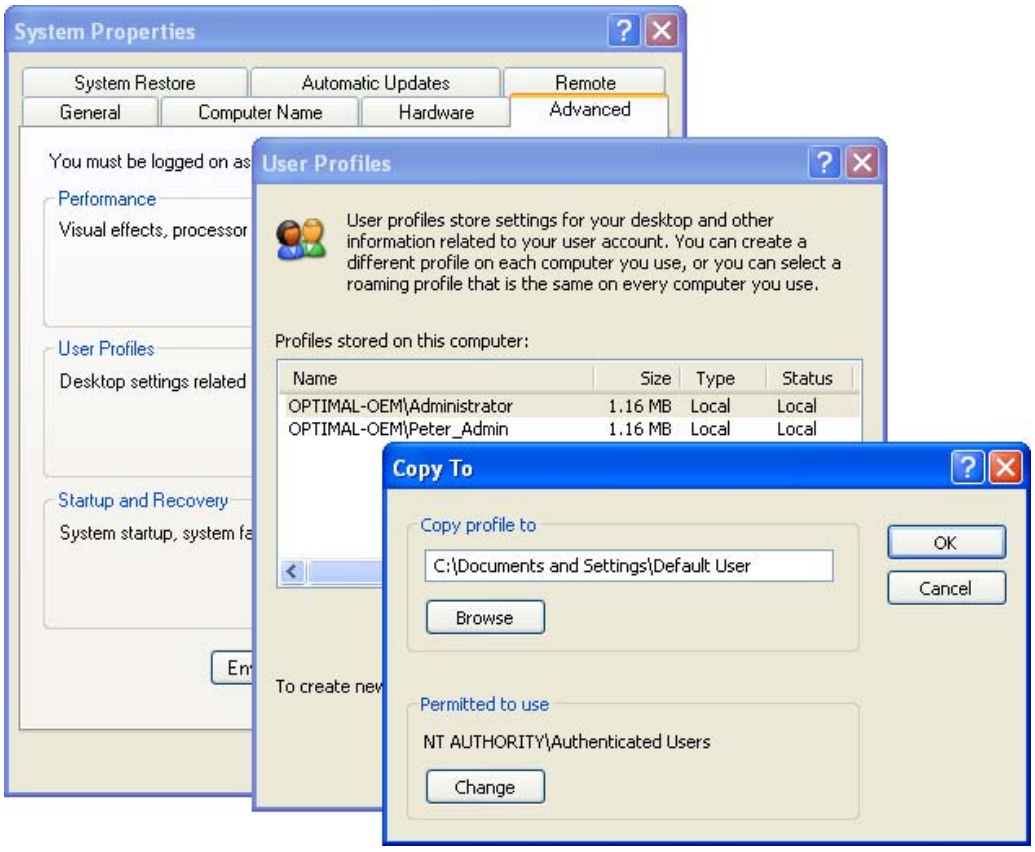



*Рис. 8.3. Создание профиля-образца*

Внимание! После копирования на папку Default User системой будут установлены разрешения NTFS **Full Control** для группы Authenticated Users. Вручную отредактируйте права, сняв с этой группы доступы Modify и Write.

Настройте профиль, который система загружает до входа пользователей в систему (т.е., **Logon Window, Окно входа в Windows**). Для этого в Control Panel -> Accessibility, закладка General, отметьте галочку Apply all settings to logon desktop.

В качестве фонового рисунка экрана входа в систему установите логотип компании – пользователи должны знать, чьим правилам безопасности они подчиняются. Для этого укажите в ключе HKEY_USERS\.Default\Control Panel\Desktop значение REG_SZ Wallpaper: **C:\Windows\Logo.bmp**. Сам файл заранее подготовьте в том разрешении и цветовой гамме, которые будут применены на данном компьютере.

Научите пользователей не оставлять на рабочем столе ничего, кроме ярлыков на часто использующиеся документы и бизнес-программы, а также папки My Documents и Recycler (Корзины). В противном случае, часть важных документов может сохраниться вне определённых Правилами распределения ресурсов мест. Хорошей мерой обеспечения выполнения данного пункта может служить сценарий входа в систему, перемещающий с рабочего стола всё, кроме ярлыков, в домашнюю директорию пользователя.

# 9. Построение иерархии прав доступа.

### 9.1. Права по умолчанию, подлежащие замене.

Из файловых систем, поддерживаемых Windows на локальных жёстких дисках, только NTFS работает с **Access Permissions (Разрешениями доступа)**. На самом деле, безопасностью возможности NTFS не ограничиваются, поэтому следует использовать её везде, где возможно, в том числе на съёмных жёстких дисках.

Если на системе уже существуют разделы, отформатированные в файловой системе FAT, выполните резервное копирование данных и переформатируйте раздел в NTFS, после чего восстановите данные из копии. Не следует делать конвертаций из FAT в NTFS – распределение дисковых структур будет далеко от идеального.

Система по умолчанию достаточно подготовлена к работе пользователей с ограниченными привилегиями, поэтому не меняйте разрешения на папки **Documents and Settings, WINDOWS** и корневые ветви реестра (например, **HKLM\Software**).

Программы, устанавливаемые в **Program Files**, защищены изначально. Пользователи, являющиеся членами группы Users, не имеют прав на изменение содержимого этого каталога. Защита Program Files от вирусного поражения со стороны пользователей в этом случае гарантирована на 100%.

Исключением являются **корневые папки дисков** – сконфигурируйте их таким образом, чтобы пользователи не могли создавать новые файлы и каталоги.

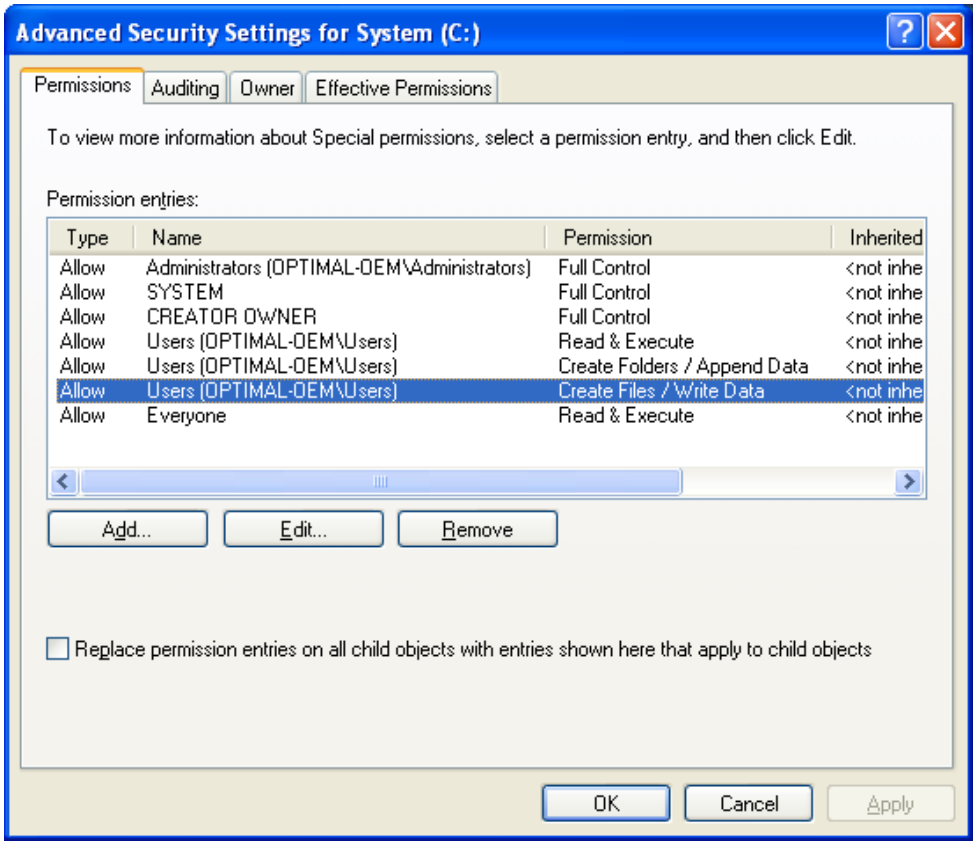



*Рис. 9.1. Права по умолчанию, подлежащие замене*

Рекомендуемая схема прав на указанные каталоги:

```
Administrators, SYSTEM: Full Control
Users: Read
```

Также, на рабочих станциях исправьте права доступа на папку **%SystemRoot%\Tasks** так, чтобы рядовые пользователи не могли добавлять свои задачи в **Scheduled Tasks** (Планировщик задач). Используйте для этого команду **cacls**:

```
cacls %SystemRoot%\Tasks /g Administrators:F SYSTEM:F Users:R
```

В доменной среде этот запрет можно реализовать групповыми политиками, раздел Administrative Templates, Windows Components, Task Scheduler контейнеров User Configuration и/или Computer Configuration.

В случае необходимости, возможно восстановить изначальные разрешения. Для этого примените Шаблон Безопасности (Security Template) **setup security.inf** с помощью консоли MMC Security Configuration and Analysis. Подробнее – в статье MS Knowledge Base http://support.microsoft.com/kb/237399.

### 9.2. Не давайте больше, чем нужно для работы.

Конфигурируя доступ к бизнес-программам, используйте запретительную систему назначения прав – разрешайте пользователям доступ лишь к тем каталогам и ключам реестра, которые им действительно необходимы. По возможности, разрешайте доступ только на **Read (Чтение)** и лишь в необходимых случаях – на **Modify (Изменение).** Исполняемые файлы (.exe, .com, .bat и др.) в любом случае должны остаться закрытыми от изменений – именно это и гарантирует защиту от вирусного поражения со стороны пользователя.

Не допускается применять разрешение **Full Control (Полный доступ)** – это разрешение включает в себя право **Change Permissions (Изменять Права доступа).** Столь мощное право абсолютно не нужно пользователям, зато опасность изменения структуры прав и последующего вирусного поражения возрастает многократно.

Конфигурируя доступ и к бизнес-программам, и к домашним каталогам пользователей, учитывайте потребности резервного копирования. Некоторые решения могут требовать, чтобы группа Backup Operators имела доступ на Чтение этих ресурсов.

Назначайте разрешения только на группы – это существенно сэкономит время перенастройки прав при добавлении новых пользователей или смены должности уже имевших доступ. Не используйте **Access Restrictions (Запреты доступа)** – могут сложиться ситуации, при которых структура прав станет нечитабельной. Как результат, доступ может работать не так, как это задумывалось.

Установите **Auditing (Слежение)** на **Successful Delete (Успешные удаления)** объектов из папок бизнес-программ (D:\Accounting) и папок с общим доступом (Shared Documents). В случае, если пользователи заявят о пропаже документов, с помощью журнала Security можно будет установить, кто и когда удалил эти файлы, после чего восстановить их из ближайшей по времени резервной копии.

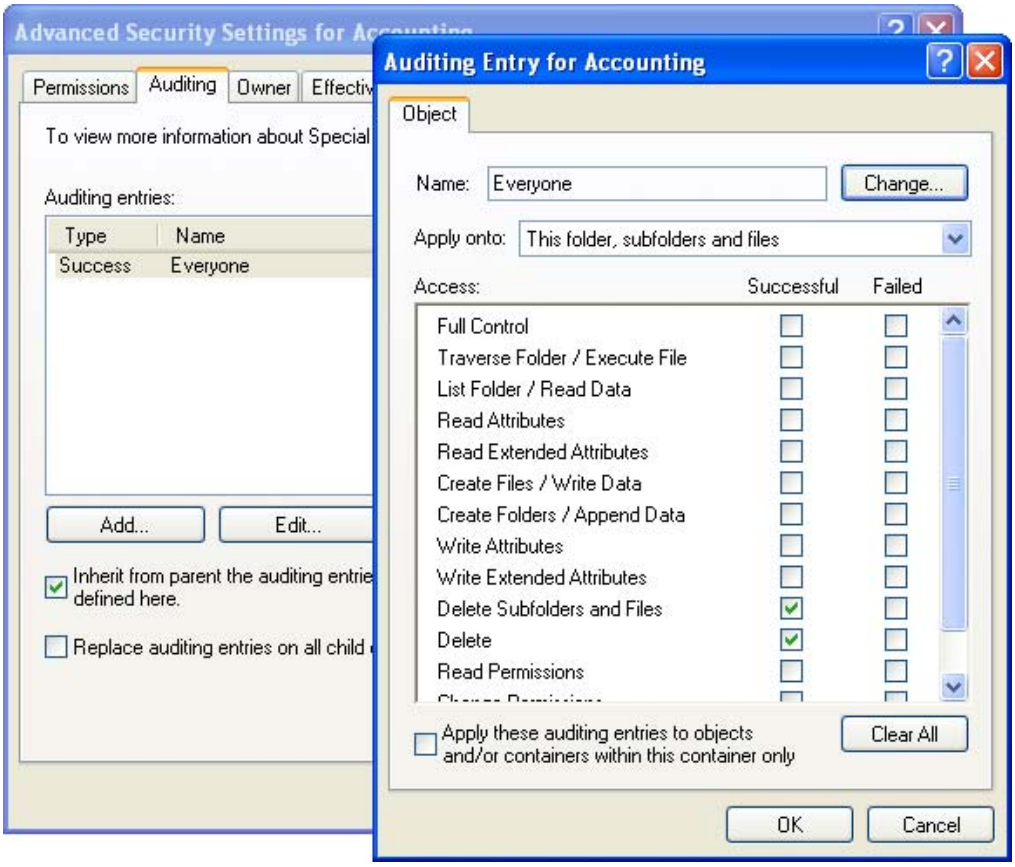



*Рис. 9.2. Установка аудита на папку производственных приложений*

### 9.3. Пример иерархии прав доступа для рабочей станции.

Рассмотрим методику назначения разрешений NTFS для следующего случая:

- функции компьютера можно описать как "типовая рабочая станция";
- на компьютере хранится программа 1С с торговыми базами двух фирм.

```
D:\Accounting\1C\Programs
    Administrators, SYSTEM: Full Control
    Backup Operators, 1C Users: Read
D:\Accounting\1C\Bases\CompanyA
    Administrators, SYSTEM: Full Control
    1C CompanyA Users: Modify
    Backup Operators: Read
D:\Accounting\1C\Bases\CompanyB
    Administrators, SYSTEM: Full Control
    1C CompanyB Users: Modify
    Backup Operators: Read
```

В данном примере группы **Administrators** и **SYSTEM** обладают правом Full Control (Полный Доступ) ко всем каталогам 1С для выполнения обслуживания программы и общего управления ресурсами.

Группе **Backup Operators** предоставлено право Read (Чтение) всех каталогов 1С для выполнения процедур резервного копирования сценариями с применением команды **xcopy**.

Все пользователи, в задачи которых входит работа с 1С, включены в группу **1С Users.** Эта группа имеет доступ на Чтение каталога с программой, что вполне достаточно для её работы и гарантированно защищает исполняемые файлы 1С от вирусного заражения со стороны рядовых сотрудников компании.

Все допущенные пользователи также включены в группы **1С CompanyA Users** и/или **1С CompanyB Users**, что даёт им право на полноценную работу с базой данных соответствующей компании. Предоставленное им право Modify (Изменение) опасно с точки зрения вирусного поражения, но в каталогах баз данных не содержатся исполняемые модули – они хранятся в отдельном каталоге Programs.

Учётные записи персонала, в задачи которого не входит работа с 1С, в соответствующие группы не вносятся и не имеют доступа ни к базам данных, ни к самой программе.

### 9.4. Пример иерархии прав доступа для сервера.

Рассмотрим методику назначения разрешений NTFS для следующего случая:

- функции компьютера можно описать как "файловый сервер";
- на компьютере хранится программа 1С с торговыми базами двух фирм;
- на компьютере хранятся домашние каталоги пользователей и папка-обменник.

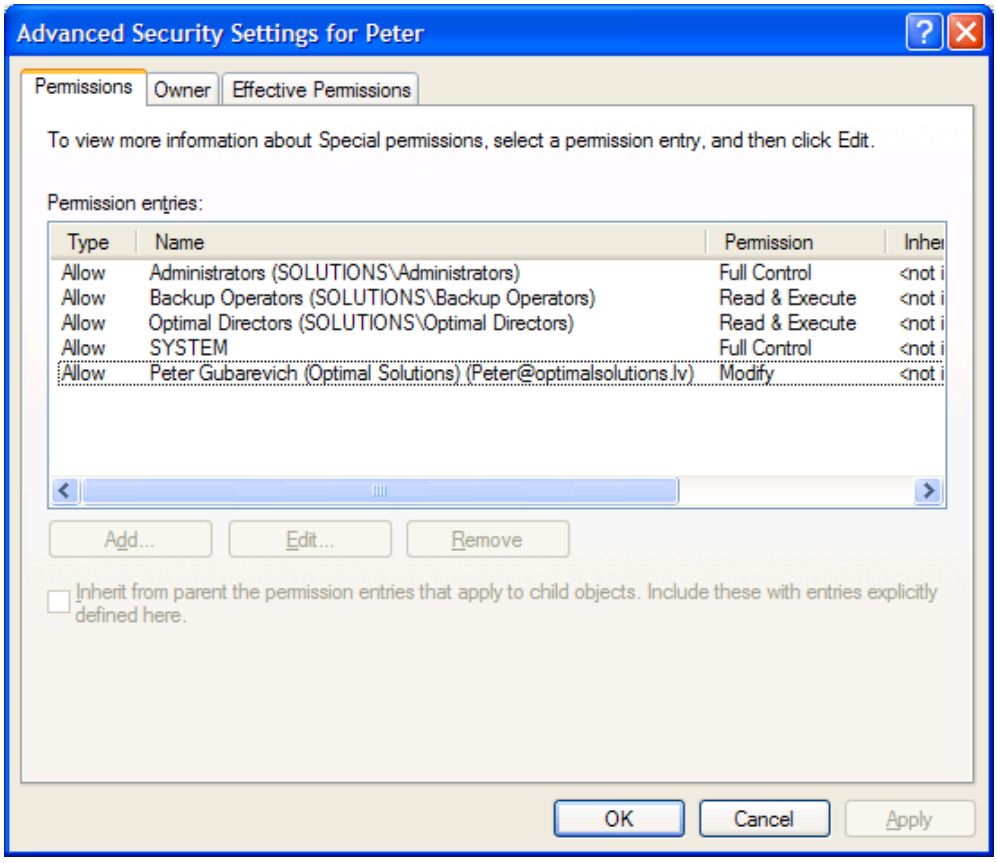



*Рис. 9.3. Пример назначения разрешений NTFS на домашний каталог пользователя*

**D:\Users**
Administrators, SYSTEM: Full Control
CompanyA Directors, Users: Read
**D:\Users_ Shared Documents**
Administrators, SYSTEM: Full Control
CompanyA Directors: Read
CompanyA Shared Documents: Modify
**D:\Users\UserA**
Administrators, SYSTEM: Full Control
CompanyA Directors: Read
UserA: Modify
**D:\Users\UserB**
Administrators, SYSTEM: Full Control
CompanyA Directors: Read
UserB: Modify

В данном примере группы **Administrators** и **SYSTEM** обладают правом Full Control (Полный Доступ) ко всем папкам для выполнения обслуживания системы.

Группе **CompanyA Directors** предоставлено право Read (Чтение) всех папок с целью контроля их содержимого при необходимости. Предполагается, что пользователи осведомлены о контроле со стороны руководства компании, и этому имеется должное юридическое обоснование.

Все пользователи, допущенные к общему каталогу компании CompanyA, включены в группу **CompanyA Shared Documents**. Эта группа имеет доступ Modify (Изменение) содержимого папки-обменника. Учётные записи персонала, в задачи которого не входит работа с общими документами, в соответствующую группу не вносятся.

Доступ к каждому отдельному домашнему каталогу назначается на индивидуальную учётную запись, так как применение групп здесь не имеет смысла. Предоставленного пользователю права на Изменение содержимого папки вполне достаточно для его работы.

Корень диска D:\ предоставлен для **Общего доступа по сети (Shared Folder)** под именем **Data** и доступен на рабочих станциях в качестве диска **F:**. Права общего доступа:

Administrators: Full Control
CompanyA Directors: Read
Users: Change

Полный Доступ для группы Administrators обусловлен технической необходимостью управления ресурсами. Право Change (Менять содержимое), работая в связке с разрешениями NTFS, позволит членам группы Users (рядовым пользователям), выполнять свою работу. Это право определяет максимальный уровень доступа, который пользователи смогут получить внутри диска F: при работе с файлами по сети.

# 10. Настройка общесистемных параметров.

Для обеспечения долговременной стабильной и безопасной работы скорректируйте следующие параметры системы:

- Установите размеры журналов **Application, System** в 16384 Кб. Установите размер журнала **Security** на рабочих станциях 65536 Кб, на серверах – 262144 Кб. Настройте режим перезаписи журналов **As Needed (По необходимости).**

- Журнал безопасности может быстро заполняться событиями аудита при настройке программ или обнаружении попыток взлома системы. Увеличиваясь в размере, evt-файлы становятся сильно фрагментированными. Применив утилиту **SysInternals PageDefrag**, можно их дефрагментировать при следующей перезагрузке системы;

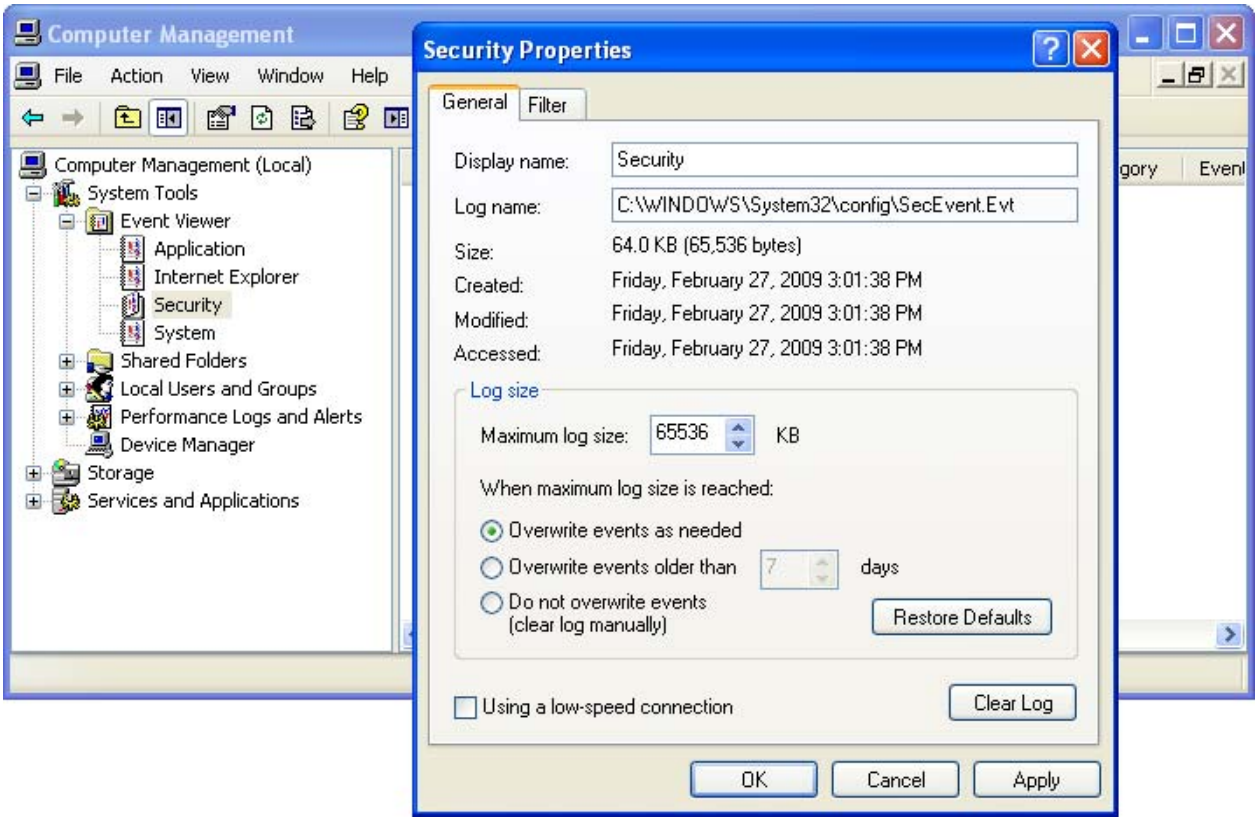



*Рис. 10.1. Ручная настройка размеров системных журналов*

- Установите размер файла виртуальной памяти **фиксированным.** Для типовой рабочей станции он может быть равным двукратному объёму оперативной памяти, для сервера – от одного до трёх объёмов оперативной памяти. Жёстко закрепляя размер файла, можно избежать фрагментации, возникающей при его росте;

  Более детально работа с виртуальной памятью рассматривается в блоге Марка Руссиновича: http://blogs.technet.com/mark_russinovich/archive/2008/11/17/3182311.aspx (ссылка на русский перевод).

- Включите **Data Execution Prevention** для всех программ. В случае, если какая-либо конкретная программа не сможет работать в таком режиме, внесите её в Исключения DEP, но не отключайте защиту вообще. Механизм DEP призван защищать от вирусов (червей), распространяющихся путём сбоев переполнения буфера;

- Запретите пользователям выключать или перезагружать компьютер в случае появления проблем. Системные ошибки (например, нехватка места на диске) таким образом не устраняются, а нештатная перезагрузка может лишь усугубить сбой. Отсоедините провод кнопки **Reset (Аварийной перезагрузки)** от материнской платы компьютера. В управлении электропитанием установите для кнопки PowerOn значение "Do Nothing". Настройте BIOS на выключение компьютера только при длительном удержании кнопки Power;

- На мобильных компьютерах, а также системах, которые положено выключать на ночь, разрешите выключение только с помощью кнопки Shutdown на экране входа в систему. Не назначайте рядовым сотрудникам **User Right (Право Пользователя)** ”Shutdown the system”, чтобы процедуры Log Off (Выход из системы) и Shutdown (Выключение компьютера) воспринимались ими в качестве двух раздельных действий;

- Назначьте группе INTERACTIVE право на перезапуск службы **Print Spooler**, подготовьте скрипт перезапуска и выдайте пользователям инструкцию по последовательности действий в случае отказа принтера (запуск скрипта, физическая перезагрузка печатающего устройства);

- Вынесите рабочую папку службы Print Spooler с системного раздела. Для этого в Control Panel, Printers and Faxes вызовите меню File, Server Properties и на закладке Advanced укажите место для хранения spool-файлов **D:\Users\Spool**. Создайте саму папку и назначьте ей атрибут «hidden» («скрытая»), чтобы не запутывать пользователей.

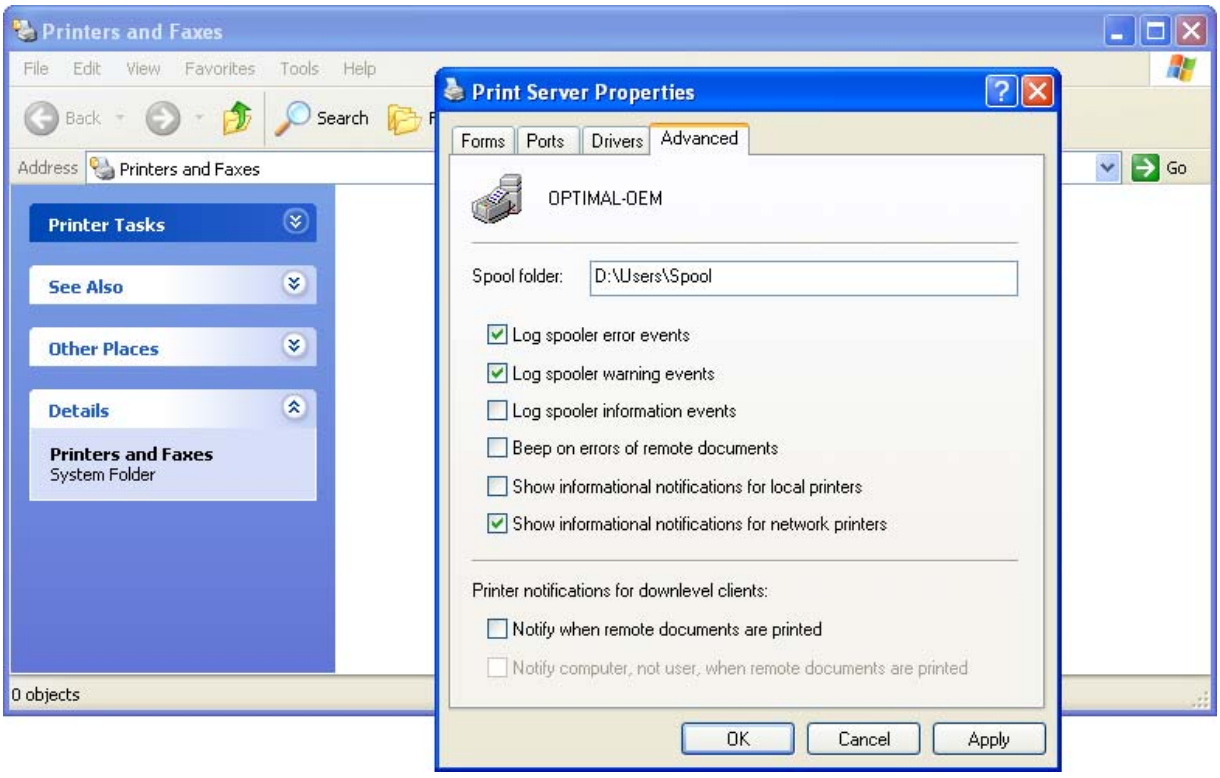



*Рис. 10.2. Перемещение рабочего каталога службы Print Spooler*

# 11. Важнейшие Политики безопасности.

Некоторые версии ОС Windows поставляются в совместимой, но небезопасной конфигурации. Настройте важнейшие параметры безопасности с помощью **Group Policy (Групповых Политик).** Для таких систем, как Windows XP Home, часть этих параметров настраивается только в системном реестре, а часть – сторонними средствами (например, **User Manager for Domains** из комплекта Windows NT Administrative Tools).

### 11.1. Account Policies (Политики Учётных Записей).

11.1.1. **Password Policies (Политика Паролей).** Большое количество взломов и вирусных поражений успешно производится из-за халатного отношения к паролям. Не имеет значения, дома вы работаете с компьютером или в офисе, много пользователей или он всего один – вирусу это безразлично.

- **Enforce password history =24.** Не разрешайте пользователям использовать их старые пароли – возможно, эта информация со временем стала известна кому-либо ещё;
- **Maximum password age = 180..360.** Частота смены паролей пользователей. Не требуйте менять пароли слишком часто, люди начинают записывать их на бумаге. Но годами работать с одним и тем же паролем тоже небезопасно. Для каждого пользователя этот счётчик работает отдельно;
- **Minimum password age = 0.** Как быстро разрешено сменить установленный пароль. Если пароль был назначен и введён администратором, пользователь должен иметь право на незамедлительную смену пароля для сохранения конфиденциальности;
- **Minimum password length = 8.** Чем длиннее пароль, тем сложнее его взломать. Следует установить баланс между удобством работы и безопасностью. В формате LM Hash пароли храниятся блоками по 7 знаков. Если вы используете LM, заставьте взломщика хоть немного напрячься;
- **Passwords must meet complexity requirements = Enabled.** «Сложным» называется пароль, применяющий минимум три категории знаков (например: большие буквы, маленькие буквы, спецсимволы). Для атаки «прямым перебором» на такой пароль взломщик вынужден использовать гораздо большее количество комбинаций, что зачастую делает его работу бессмысленной.

11.1.2. **Account Lockout (Блокировка Учётных Записей).** Блокировка учётных записей при обнаружении попыток угадывания паролей. Эта настройка защищает от проникновения в систему с помощью программ, подбирающих пароли пользователей. Укажите параметры:

- **Account lockout threshold = 10** attempts;
- **Account lockout duration = 5** minutes;
- **Reset account lockout counter after = 5** minutes.

В данном примере проверка осуществляется по формуле ”если в течение 5 минут было отклонено 10 попыток входа с неправильным паролем для пользователя User, заблокировать применение учётной записи User на 5 минут”.

Существуют условия, при которых данная политика не распространяется на членов локальной группы Administrators. Примените **”passprop.exe /adminlockout”** из комплекта Microsoft Windows NT Resource Kit для возможности блокировки учётных записей администраторов (см. статью MS KB http://support.microsoft.com/kb/885119).

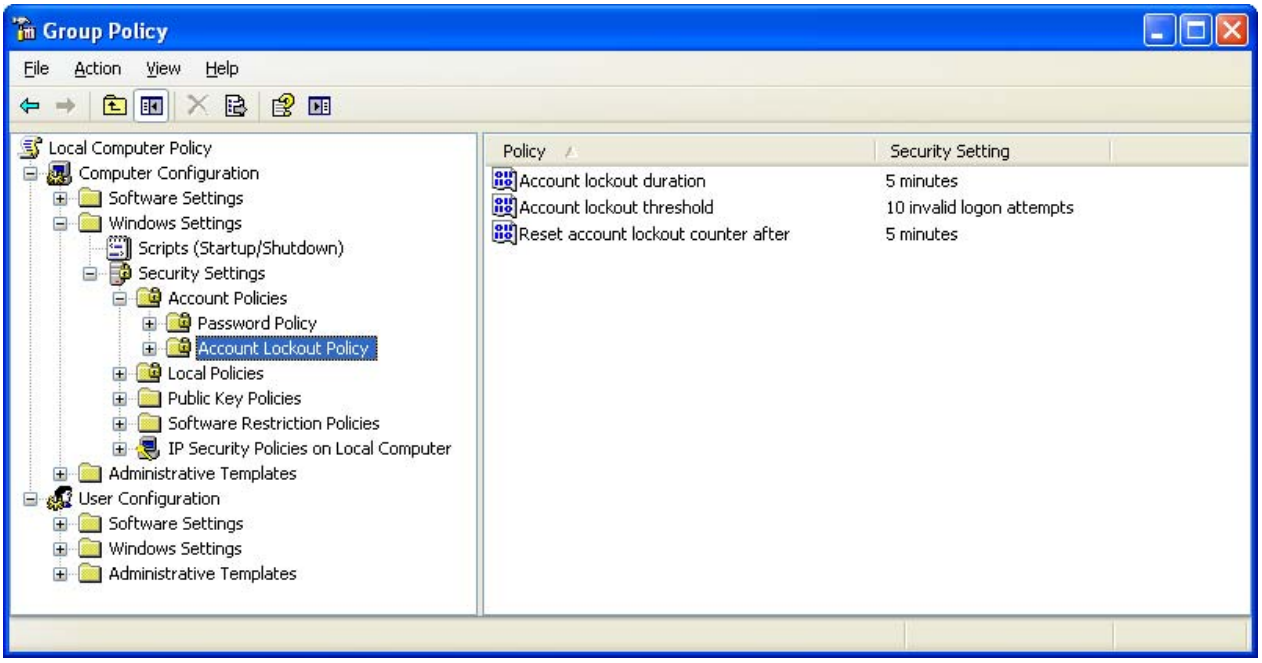



*Рис. 11.1. Включение защиты от угадывания паролей*

**11.2. Local Policies (Общие политики безопасности).**

11.2.1. **Audit Policy (Политика Аудита).** По умолчанию, система не производит полное слежение за действиями пользователей – это не имело бы смысла, было бы излишне расточительно по отношению к вычислительным ресурсам. Но некоторые события всё же следует заносить в **Security Log (Журнал Безопасности):**

- **Account Logon = Failure**, **Logon Events = Failure.** Включите слежение за безуспешными попытками входа в систему. Так вы сможете своевременно отследить попытки взлома паролей учётных записей;
- **Account Management = Success, Failure.** Регистрация учётных записей, смена членства в группах – важные события. Иногда по ним можно быстро найти источник проникновения в систему или нарушения со стороны обслуживающего персонала;
- **Object Access = Success.** Отслеживание успешного доступа к файлам необходимо для разрешения конфликтных ситуаций вида ”Кто удалил мою папку из Shared Documents?”;
- **Policy Change = Success.** Занесение в журнал факта успешной смены настроек политик Прав Пользователей и Аудита;
- **System Events = Success.** Регистрация системных событий, имеющих отношение к безопасности (например, выключение компьютера) или к Журналу Безопасности.

11.2.2. User Rights Assignments (Права Пользователей)**.** Существует ряд прав, который не регулируется разрешениями NTFS или ключами реестра.

- Выдавайте права **Allow Logon Locally** и **Access this computer from the network** только тем группам, которым это необходимо для работы;
- Убедитесь, что группа Backup Operators обладает правами **Backup files and directories** и **Restore files and directories.** Это позволит службе резервного копирования работать с ограниченными привилегиями;

- Назначьте группе **Service Accounts** права **Deny logon through Terminal Services** и **Deny access this computer from the network**. В случае, если злоумышленник захватит управление над служебной учётной записью, он не сможет зайти на компьютер удалённо с помощью Remote Desktop или Microsoft Network;
- Регулировка системного времени должна производиться только доверенным персоналом либо автоматически. От этого зависит работоспособность протоколов безопасности – NTLMv2, Kerberos и других. Убедитесь, что правом **Change the system time** обладают группы LOCAL SERVICE и Administrators (примените SYSTEM, если LOCAL SERVICE недоступен);
- Отрегулируйте право **Shut down the system.** Только Administrators и, при необходимости, Backup Operators должны иметь возможность выключать компьютер непосредственно из своих сессий;
- Уберите группу **Everyone** из списка во всех правах, где она присутствует.

Не стремитесь выдать Администраторам все Права Пользователей, им это просто не нужно. Не используйте **права-запреты** (например, Deny logon locally) для ограничения доступа реальных пользователей – вместо этого, продумайте структуру локальных групп и не выдавайте некоторым группам соответствующие **права-разрешения** (Allow logon locally).

### 11.2.3. Security Options (Дополнительные настройки безопасности).

**Accounts: Guest account status = Disabled.**

Не разрешайте применение учётной записи Guest. Чтобы разделение привилегий было возможным, все пользователи должны иметь свои персональные учётные записи.

**Accounts: Limit local account use of blank passwords.. = Enabled.**

Не разрешайте применять пустые пароли. Если бизнес-задачи требуют упрощённого доступа, ограничьте использование пустого пароля только для интерактивного входа.

**Audit: Shutdown the system immediatelly if unable to log security audits = Disabled.**

В большинстве ситуаций не имеет смысла останавливать систему с сообщением ”Security log is full”, если журнал безопасности переполнен.

**Devices: Prevent users from installing printer drivers = Enabled.**

Не разрешайте пользователям инсталляцию драйверов принтеров – как и любая другая инсталляция, это может быть чревато вирусным поражением.

**Interactive logon: Do not display last user name = Enabled.**

Не следует отображать имя последнего пользователя на экране входа в систему, иначе взломщику останется угадать только пароль. К тому же, пользователи, регулярно работающие за одним компьютером, часто забывают имена своих учётных записей.

**Interactive logon: Do not require Ctrl+Ald+Del = Disabled.**

Требование нажатия Ctrl+Alt+Del при входе в систему позволяет избежать имитации злоумышленником окна входа с целью перехвата паролей.

**Interactive logon: Message text.., Message title..**

Установите информационное сообщение при входе в систему: "Этот компьютер обслуживается таким-то персоналом, в случае проблем свяжитесь с нами так-то".

**Microsoft Network Client: Send unencrypted password to third-party SMB: Disabled.**

Запретите SMB-коммуникации со сторонними SMB-серверами, не поддерживающими шифрование паролей.

**Microsoft Network Client: Digitally sign communications (always + if agrees) = Enabled.**
**Microsoft Network Server: Digitally sign communications (always + if agrees) = Enabled.**

Повысьте уровень безопасности работы с SMB-протоколом, требуя наличия цифровых подписей и для клиентских, и для серверных сессий.

**Network Access: Allow anonymous SID/Name translation = Disabled.**
**Network Access: Do not allow anonymous enumeration of SAM and shares = Enabled.**
**Network Access: Let everyone permissions apply to anonymous users = Disabled.**

Запретите получение SID-ов, информации из базы безопасности SAM, списка общих папок посредством анонимных соединений. Также, запретите причислять анонимные соединения к группе Everyone.

**Network Access: Do not allow storage of credentials or .Net passports.. = Enabled.**

Запретите сохранение паролей и .Net-реквизитов пользователей в системе. Со временем, пользователи забудут свои пароли и не смогут их восстановить.

**Network Access: Sharing and security model for local accounts = Classic.**

Используйте классическую модель безопасности, при которой каждый пользователь идентифицируется согласно своей учётной записи. Использование Guest недопустимо.

**Network Security: Do not store LAN Manager hash value = Enabled.**

Пароли в базе безопасности SAM сохраняются в двух видах: LM Hash и NTLM Hash. LM крайне редко используется в производственной среде, но является крайне уязвимым. Запретите его хранение, после чего смените пароли всех пользователей.

**Network Security: LAN Manager authentication level = NTLMv2 only, refuse LM, NTLM.**

Пароли пользователей передаются в SMB-сессиях, будучи зашифрованными определённым протоколом. Используйте только максимально защищённый NTLMv2, а LM и NTLM запретите.

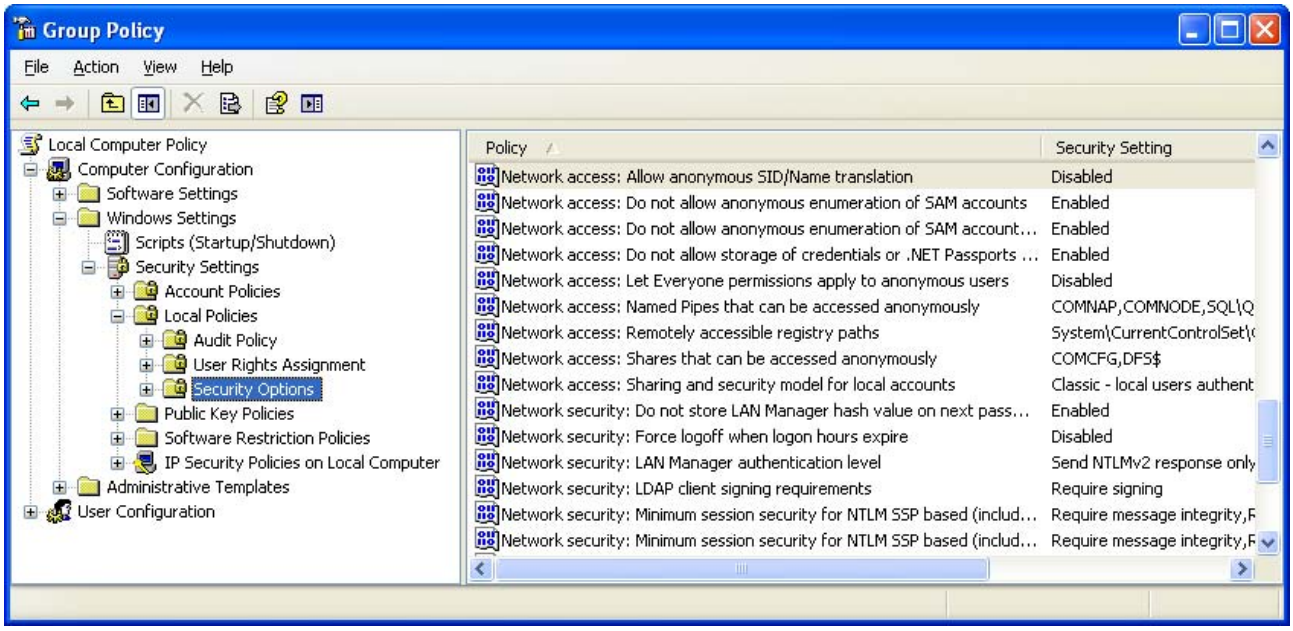



*Рис. 11.2. Настройка параметров безопасности системы*

**Network Security: Minimum session security for NTLM SSP.. clients, servers: All.**

Укрепите безопасность коммуникаций NTLM SSP и Secure RPC-протоколов, потребовав соответствие всем опциям как на серверах, так и на клиентах.

**Shutdown: Allow system to be shut down without having to log on = Enabled.**

Разрешите выключать рабочие станции с экрана входа в систему. Запретите выключать таким методом сервера, а также компьютеры с повышенным уровнем безопасности.

**Shutdown: Clear virtual memory pagefile = Enabled.**

Установите опцию очищения файла виртуальной памяти при выключении компьютера.

**System Objects: Default owner for objects.. = Object creator.**

Если член группы Administrators создаёт файл или папку, в качестве владельца указывать конкретную учётную запись создателя, а не всю группу Администраторов.

**System objects: Strengthen default permissions of internal system objects = Enabled.**

Применять более строгие разрешения по умолчанию на внутренних объектах операционной системы, предоставляя обычным пользователям только права Чтения.

11.2.4. Дополнительные настройки безопасности для доменной среды.

**Domain controller: LDAP Server signing requirements = Require signing.**
**Network Security: LDAP client signing requirements = Require signing.**

Укрепите уровень безопасности протокола LDAP как серверов, так и клиентов, включив требование применения цифровых подписей.

**Domain member: Digitally encrypt or sign secure channel data (always) = Enabled.**
**Domain member: Require strong session key = Enabled.**

Повысьте уровень безопасности коммуникаций членов домена с контроллерами домена, потребовав наличие шифрования трафика Безопасного Канала (Secure Channel), а также применения 128-битного ключа.

**Interactive logon: Number of previous logons to cache = 0.**

Запретите системе запоминать доменные реквизиты последних нескольких пользователей. Исключение - мобильные компьютеры, где это необходимо для работы.

# 12. Корректировка прав доступа для работы с ограниченными привилегиями.

Некоторые производственные программы не запускаются или работают некорректно с ограниченными привилегиями. Подобные продукты могут требовать не только дополнительной настройки своих параметров, но и расширения прав доступа на файловой системе и в **Registry (Системном реестре).**

Для решения проблем запуска такой программы не назначайте разрешение на Изменение (Modify) всего содержимого папки, в которую она установлена. Используйте систему Аудита, чтобы точно узнать, какие именно файлы или ключи реестра нуждаются в расширенных правах. Предпримите для этого следующие действия:

- Убедитесь, что в политиках безопасности системы, **Audit Policy (Политика Аудита)** включён тип аудита **Object Access: Failure (Неуспешный доступ к объектам)**;
- В свойствах системного (C:\) и пользовательского разделов (D:\) на закладке Security (Безопасность) включите слежение за событиями **Access Failed: Full Control (Неуспешный доступ: Полный доступ)** для учётной записи User;
- Вызовите меню **Permissions (Разрешения)** для ключа реестра HKLM\Software и включите слежение за событиями **Access Failed: Full Control (Неуспешный доступ: Полный доступ)** для учётной записи User.

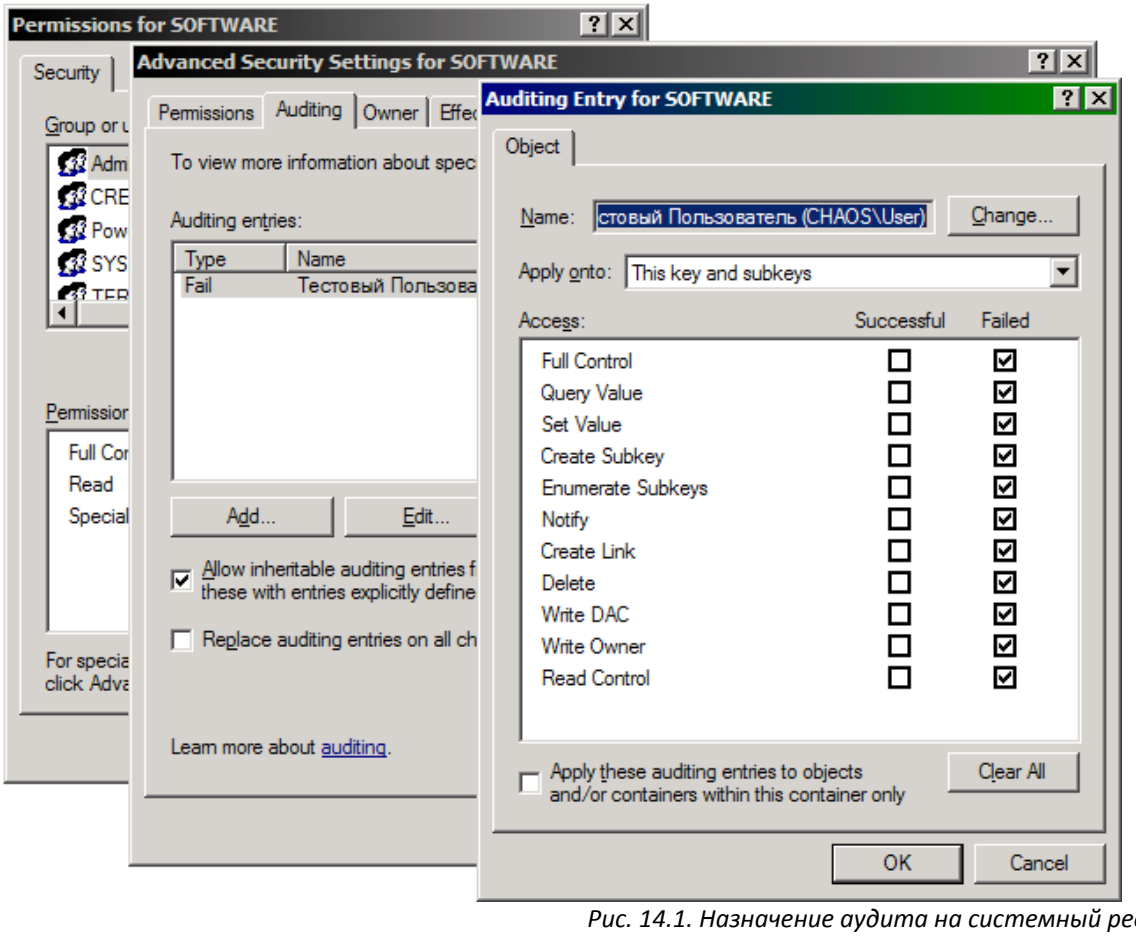



*Рис. 14.1. Назначение аудита на системный реестр*

Запустите проблемную программу от лица User. Это удобно можно сделать, щёлкнув правой кнопкой мыши по ярлыку программы и в появившемся меню выбрав команду **RunAs.**

Выполните все необходимые действия для воспроизведения сбоя программы или появления сообщения об ошибке. В любом случае, прекратите работать с программой при первых же признаках сбоя – это позволит решать все проблемы по мере их возникновения.

Заметив время появления проблемы, запустите **Event Viewer (Просмотрщик событий)** из папки Administrative Tools (Средства администрирования) и отфильтруйте журнал **Security (Безопасность)** по следующим критериям:

- Event Source: Security;
- Category: Object Access;
- Event Types: Failure Audit;
- Event ID: 560.

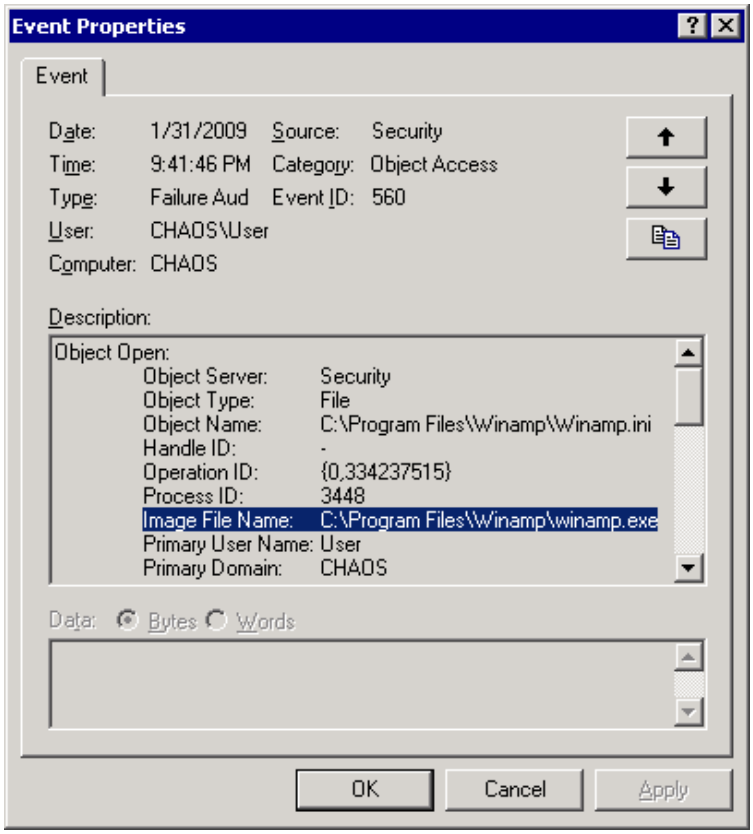



*Рис.14.2. Запись неуспешной попытки доступа в журнале Безопасности*

Расширьте права на файлы и ключи реестра, неудачный доступ к которым отражён в журнале Безопасности. Однако, внимательно отнеситесь к содержимому событий – не каждое из них требует реакции администратора. Обратите внимание на следующие поля:

- **Image File Name.** Должен быть указан исполняемый модуль проблемной программы;
- **Object Name.** Папка, файл или ключ реестра, доступ к которым не удался;
- **Accesses.** Суммарный флаг запрашиваемого доступа.

По окончании процесса регулировки прав Аудит рекомендуется отключить. Задокументируйте внесённые в структуру прав изменения, - возможно, эта информация ещё пригодится другим администраторам.

# 13. Практическое применение Software Restriction Policies.

### 13.1. Технология SRP.

Существуют зловредные программы, успешно работающие с ограниченными привилегиями. Как правило, это – троянские модули, поражающие профили и активирующиеся при входе пользователей в систему.

Источником заражения при этом зачастую служат программы, с которыми работают пользователи – электронная почта, программы мгновенного обмена сообщениями (Skype, ICQ) или съёмные носители (например, flash-диски). Пользователь, открывая в **Outlook Express** приложенный к письму исполняемый файл, невольно копирует его в папку **Temporary Internet Files**, откуда файл запускается, выполняя свою деструктивную задачу.

Технология **Software Restriction Policies (Политика Ограничения Программ)** способна защитить от подобного рода атак, разрешая для выполнения только те программы, что находятся в заранее оговорённом списке. Кроме того, она позволяет заблокировать исполнение других нежелательных программ – игр, чат-программ и торрент-клиентов.

Существуют два подхода к построению политики SRP – составление **«белого списка»** (запрещено всё, но разрешены некоторые программы) и управление **«чёрным списком»** (разрешено всё, но запрещены некоторые программы). Наибольший уровень безопасности обеспечивает «белый список», поэтому мы будем реализовывать только его.

### 13.2. Базовая конфигурация системы.

Создайте в секции Computer Configuration групповых политик новую политику SRP и установите в ней следующие параметры:

- **Security Levels, Set As Default: Disallowed.** По умолчанию, все программы запрещены для запуска. Разрешено запускать только программы из ”белого списка”;
- **Enforcement Properties: All Software except Libraries.** Проверять только основные исполняемые файлы, без динамических библиотек. Если указать режим более строгой проверки, уровень безопасности повысится, но за это придётся расплачиваться сложностью управления и снижением скорости работы системы;
- **Enforcement Properties: All Users.** В системе, защищённой разграничением привилегий, администраторы являются наиболее вероятным источником вирусных заражений. Ни в коем случае не исключайте их из правил SRP;
- **Designated File Types.** Здесь определяются расширения, подлежащие проверке. Уберите из обработки расширение **LNK** (ярлыки Windows Explorer);
- **Trusted Publishers: End Users.** Что бы данный пункт ни значил, придётся выбрать настройку End Users для работоспособности модуля Windows Update.

Некоторые типы файлов, проверяемые политикой Software Restriction Policies по умолчанию (например, **HLP** и **MDB**), являются необходимыми для работы конечных пользователей. Не убирайте нужные расширения из политики, а организуйте хранение этих файлов в определённом месте структуры документов. Отразите такие места в Правилах Распределения Ресурсов и внесите в Разрешённые для запуска пути политики SRP.

### 13.3. Детальные настройки политики.

Приведённые ниже настройки предполагают, что система установлена и настроена согласно Правилам Распределения Ресурсов (см. п. 4). Без правил такого рода служба SRP не имеет смысла – беспорядочную структуру папок было бы практически невозможно охватить «белым списком».

Убедитесь, что в секции **Additional Rules** содержатся следующие пути:
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%**, Unrestricted**
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%**, Unrestricted**
Эта настройка позволяют запускать программы из папок Windows и Program Files. Две другие строки, создаваемые политикой по умолчанию, удалите – они просто не нужны.

Добавьте в Additional Rules следующие параметры:
Path, **D:\Resources, Unrestricted.**
(Папка с инсталляционными ресурсами и скриптом резервного копирования);

Добавьте **hash-значения** каждого исполняемого файла из папки **D:\Accounting.** Такая методика полезна не только основной своей функцией (разрешение запуска лишь определённых версий производственных программ), но и быстрым обнаружением возможного вирусного заражения. В случае распространения вирусной инфекции производственные программы с изменившимися hash-значениями перестанут запускаться, что вызовет необходимость произвести должное расследование проблемы.

Управление hash-значениями может оказаться чрезмерно громоздким или невозможным для некоторых приложений. Но даже в таких случаях будет лучше внести в правила SRP компромиссный Путь (например, ”D:\Accounting\ABC*.bat”), чем открывать полный доступ к папке вообще.

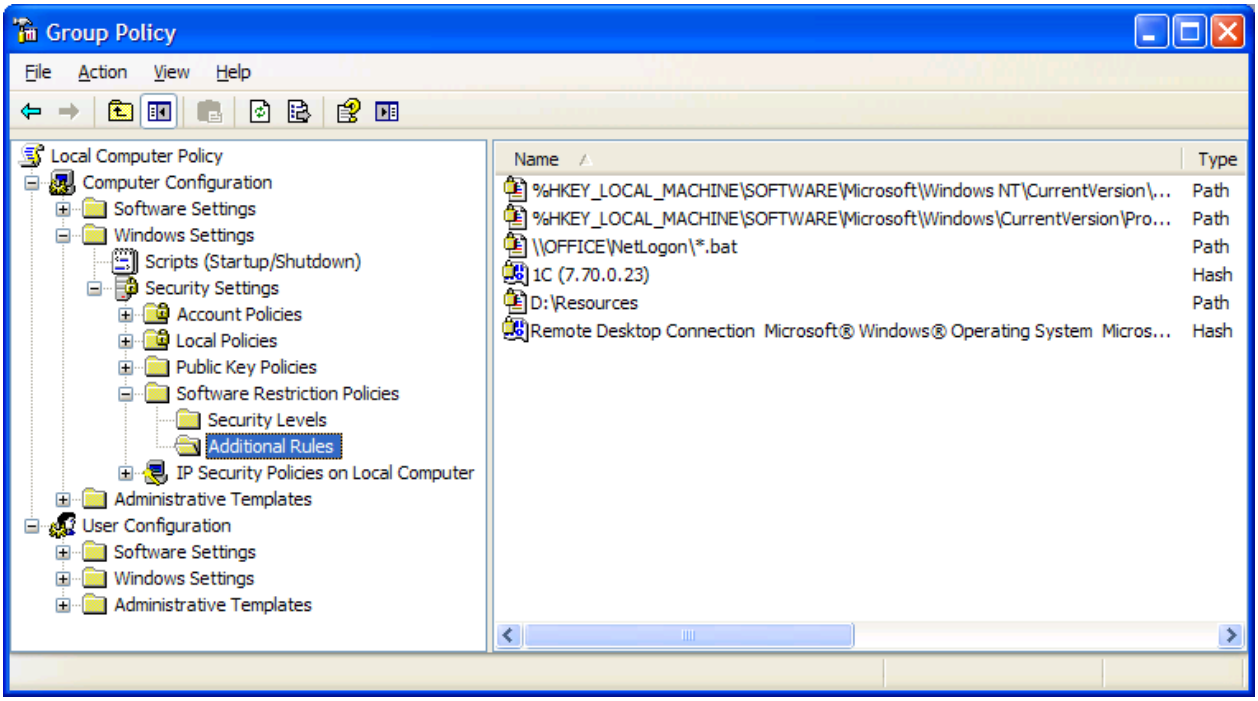



*Рис. 13.1. Пример настроенной политики SRP рабочей станции*

Не вносите в правила SRP пути, к которым пользователи имеют доступ на Запись, в том числе пути к сменным носителям! В противном случае, пользователи получат лёгкий способ обойти запреты и с помощью специальных программ вообще отключить все групповые политики из секции User Configuration.

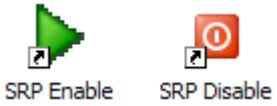
Не следует использовать правила путей с переменными окружения (например, лучше записать путь **\\Company-Server\Netlogon*.bat** вместо **%LogonServer%\Netlogon*.bat)**. Пользователи способны переопределять переменные окружения для своих сессий.

Если используемое программное обеспечение требует наличия избыточных прав на свой каталог, закройте исполняемые модули от изменений со стороны пользователей с помощью детальных разрешений NTFS, затем укажите hash-значения каждого модуля в SRP.

### 13.4. Возможные проблемы и решения.

Если некая программа была заблокирована политиками SRP, запись об этом можно найти в **Application Log (Журнале Приложений).** Просматривайте журнал во время установки или отладки приложений.

Процедуры установки или обновления программного обеспечения можно упростить, разместив на рабочем столе администратора ярлыки на reg-файлы **Включения SRP** и **Отключения SRP:**




**%SystemRoot%\SRP_Enable.reg**

```
Windows Registry Editor Version 5.00
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers]
"DefaultLevel"=dword:00000000
```

**%SystemRoot%\SRP_Disable.reg**

```
Windows Registry Editor Version 5.00
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers]
"DefaultLevel"=dword:00040000
```

Значение **DefaultLevel** = 0x00040000 переводит политику в режим Security Levels: Unrestricted («Чёрного списка»). Настройка вступает в силу незамедлительно.

Отключенная таким образом политика может длительное время оставаться брешью в системе безопасности. Настройте автоматическое включение SRP по истечению некоторого времени или после перезагрузки. Для этого в групповых политиках, секция **Computer Configuration\Administrative Templates\System\Group Policy,** в настройке **Registry Policy Processing** укажите параметр «Process even if the Group Policy objects have not changed» («Применять, даже если политики не изменялись»).

Регулировка периода переприменения политик находится в той же секции, настройки **Group Policy refresh interval for computers** и **domain controllers**. По умолчанию, политики переприменяются на рабочих станциях в течение 90±30 минут, на контроллерах домена – каждые 5 минут. Настройте этот период для контроллеров в пределах 60 минут. Тем самым, отключая SRP, обычно можно будет успевать выполнить все необходимые настройки сервера до момента, когда политика автоматически включится обратно.

# 14. Безопасность резервного копирования.

### 14.1. Задача, осуществляемая с ограниченными привилегиями.

Вне зависимости от способа исполнения, процедуры резервного копирования должны соответствовать ряду условий, от выполнения которых зависит, сможете ли вы доверять сохранённым копиям.

Вопросы контроля качества копий в этой главе не рассматриваются.

Выполняйте процедуры копирования только от лица служебной учётной записи **Backup** с ограниченными привилегиями. Выдайте ей только те права, которые действительно необходимы для считывания резервируемых данных и создания копий.

Убедитесь, что привилегии служебных учётных записей не позволяют использовать их как-то иначе, кроме как для резервного копирования. Например, в случае кражи пароля такой учётной записи взломщик не должен получить доступ к управлению дисками, пользователями или Терминальному Серверу предприятия.

С помощью прав доступа NTFS обеспечьте недоступность резервных копий системы и данных (локальные, сетевые, съёмные) для рядовых пользователей. Убедитесь, что только группы Administrators, SYSTEM и Backup Operators допущены к этим папкам.

Наличие права **Modify (Изменения)** на папку с архивами сделало бы её открытой для вирусного заражения. Пользователи смогут случайно повредить копии, а в некоторых случаях даже сознательно подменить.

Наличие права **Read (Чтения)** копий чревато разглашением информации, доступ к которой должны иметь далеко не все работники предприятия – например, содержимого электронной почты коммерческого директора или документов отдела бухгалтерии.

### 14.2. Безопасность съёмных копий.

В отличие от рядовых автоматизированных процедур, съёмное копирование требует ручных операций по изъятию носителя. Такие операции должны производиться только доверяемым персоналом. Выдайте таким пользователям привилегии, достаточные лишь для чтения нужных архивов.

Съёмные копии сохраняйте на носителе в **зашифрованном** виде. В случае утери диска или ленты информация не должна попасть к случайным людям полностью открытой, даже если вы считаете, что ничего секретного в ней нет. Одной из грубейших ошибок администратора может являться мнение, будто данные предприятия не представляют ценности, либо никому не нужны.

### 14.3. Пример настройки резервного копирования на сервере.

Рассмотрим настройку системы резервного копирования для следующего случая:

- функции компьютера можно описать как "файловый сервер";
- на компьютере хранится программа 1С с торговыми базами;
- на компьютере хранятся домашние каталоги пользователей.

Windows XP Home поставляется без инструмента резервного копирования **NTBackup.** Его можно установить отдельно с оригинального компакт-диска, из папки Valueadd\MSFT.

Согласно имеющейся концепции, резервное копирование самой системы осуществляется встроенной программой **NTBackup,** копирование домашних каталогов и производственных программ - сценарием, использующим команду **xcopy**. Файлы съёмного копирования автоматически подготавливаются в виде зашифрованного **RAR**-архива, который затем вывозится доверенным пользователем за пределы предприятия на USB-диске.

В папке D:\Resources создайте следующую иерархию ресурсов:

- Подпапка Applications для хранения установочных файлов программ, драйверов;
- Подпапка Backup Data для хранения регулярных копий системы и данных;
- Подпапка Backup Offsite с архивом съёмных копий;
- Подпапка Backup Script для сценариев архивирования.

**D:\Resources**
```
Administrators, Backup Operators: Read
SYSTEM: Full Control
Company Backup Offsite: Read (This Folder Only)
```
**D:\Resources\Backup Data**
```
Все унаследованные разрешения
Backup Operators: Modify
```
**D:\Resources\Backup Offsite**
```
Все унаследованные разрешения
Backup Operators: Modify
Company Backup Offsite: Read and Execute
```
**D:\Resources\Backup Script**
```
Все унаследованные разрешения
```

Приведённым выше набором разрешений достигаются следующие цели:

- Существует большая вероятность, что установочные файлы программ и резервные копии данных могут быть повреждены в результате вирусного заражения или неосторожный действий администратора. Ограничение доступа к этим ресурсам повышает их защищённость. При необходимости обновить содержимое папки Applications права можно временно расширять.
- Доверенные пользователи, выполняющие съёмное копирование, имеют доступ только к подготовленным архивам, содержимое которых зашифровано. Разрешений на чтение «живых», незащищённых данных или их копий нет.
- Разрешения удобно назначаются и контролируются лишь в трёх точках иерархии, вне зависимости от сложности и глубины резервного копирования.
- Членам группы Backup Operators доступны только необходимые для работы каталоги. Исполняемые модули защищены от изменений с их стороны.


*Рис. 14.1. Выбор объектов копирования в программе NTBackup*

Программа NTBackup способна сохранять не только выбранные папки и файлы, но и **System State (Состояние Системы).** Для того, чтобы все эти данные были успешно сохранены, учётная запись, от лица которой выполняется копирование, должна обладать привилегиями Backup Files and Directories и Restore Files and Directories. Убедитесь, что группа Backup Operators обладает указанными привилегиями.

NTBackup использует отдельную папку для создания и хранения каталогов архивов: **%AllUsersProfile%\Application Data\Microsoft\Windows NT\NTBackup.** Со временем, каталоги накапливаются и могут занять существенное дисковое пространство. Регулярно очищайте содержимое указанной папки. Также, настройте для неё следующие разрешения:

```
Administrators: Full Control
Backup Operators: Full Control
SYSTEM: Full Control
```

Эта папка может отсутствовать, если вы ещё ни разу не запускали NTBackup на данном компьютере. В таком случае, создайте её вручную.

Выполняя копирование сценарием, создавайте bkf-файл во временной папке; затем, по окончании процесса архивации, проверяйте журнал операций, после чего копируйте архив в конечную папку внутри D:\Resources\Backup. Смысл усложнения заключается в том, что NTBackup, как и любой другой архиватор, создаёт архивы жёстко фрагментированными. Копирование уже готового файла позволяет роста фрагментации избежать.

Если сценарий резервного копирования является пакетным файлом (.bat), убедитесь, что члены группы Backup Operators обладают привилегией **Logon as a Batch Job**. Более того, на системах Windows Server 2003 отредактируйте права доступа к файлу **%SystemRoot%\System32\cmd.exe**, разрешив системной группе **BATCH** Чтение и Запуск.

В случае, если NTBackup зависает в оперативной памяти в начале процедур копирования, генерируя в журнале System ошибку **DCOM 10016**, настройте службу **COM+**. Запустите консоль **Component Services** из папки Control Panel, Administrative Tools, откройте контейнер Component Services, Computers. В свойствах My Computer, на закладке **COM Security** отредактируйте права по умолчанию **Launch and Activation Permissions**, предоставив группе Backup Operators разрешения **Local Launch** и **Local Activation**.

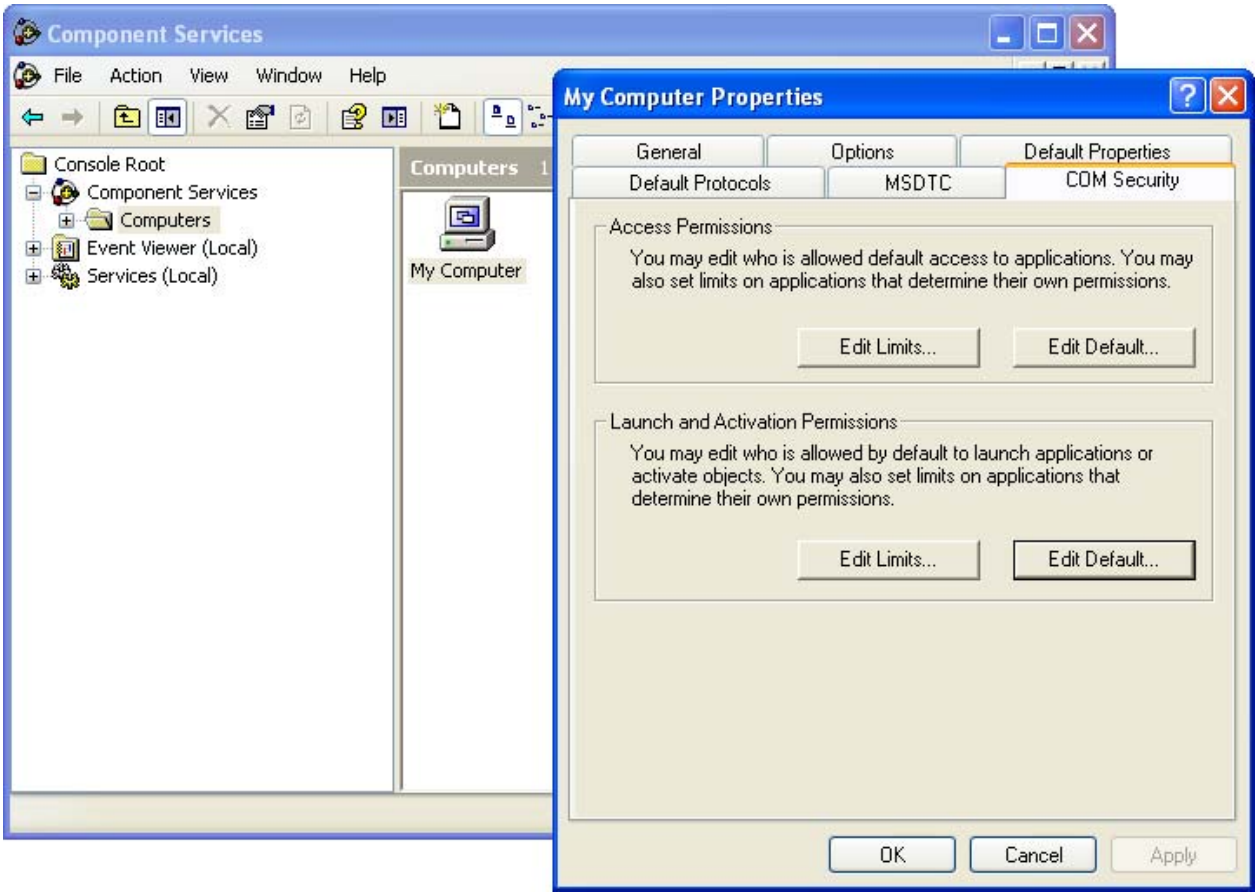



*Рис. 14.2. Настройка службы COM+*

Данная настройка также регулируется средствами локальных и доменных групповых политик в контейнере Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options. Осторожно применяйте её в доменной среде, так как это может привести к отказу системы.

### 14.4. Планировщик задач.

В Control Panel, Scheduled Tasks (Панель Управления, Запланированные Задачи) настройте запуск сценариев автоматического резервного копирования:

- еженедельно со Вторника по Субботу в 01:00, Backup Daily (тома Accounting, Users)
- еженедельно по Воскресеньям в 01:00, Backup Weekly (том C:\ и SystemState)
- еженедельно по Понедельникам в 01:00, Backup Offsite (архивирование последних копий Daily и Weekly с паролем)

Укажите исполнение сценариев от лица служебной учётной записи **Backup**. Убедитесь, что и на сетевом компьютере, используемом для хранения сетевых копий, и в локальном томе Resources достаточно места для указанной в скрипте глубины копирования.

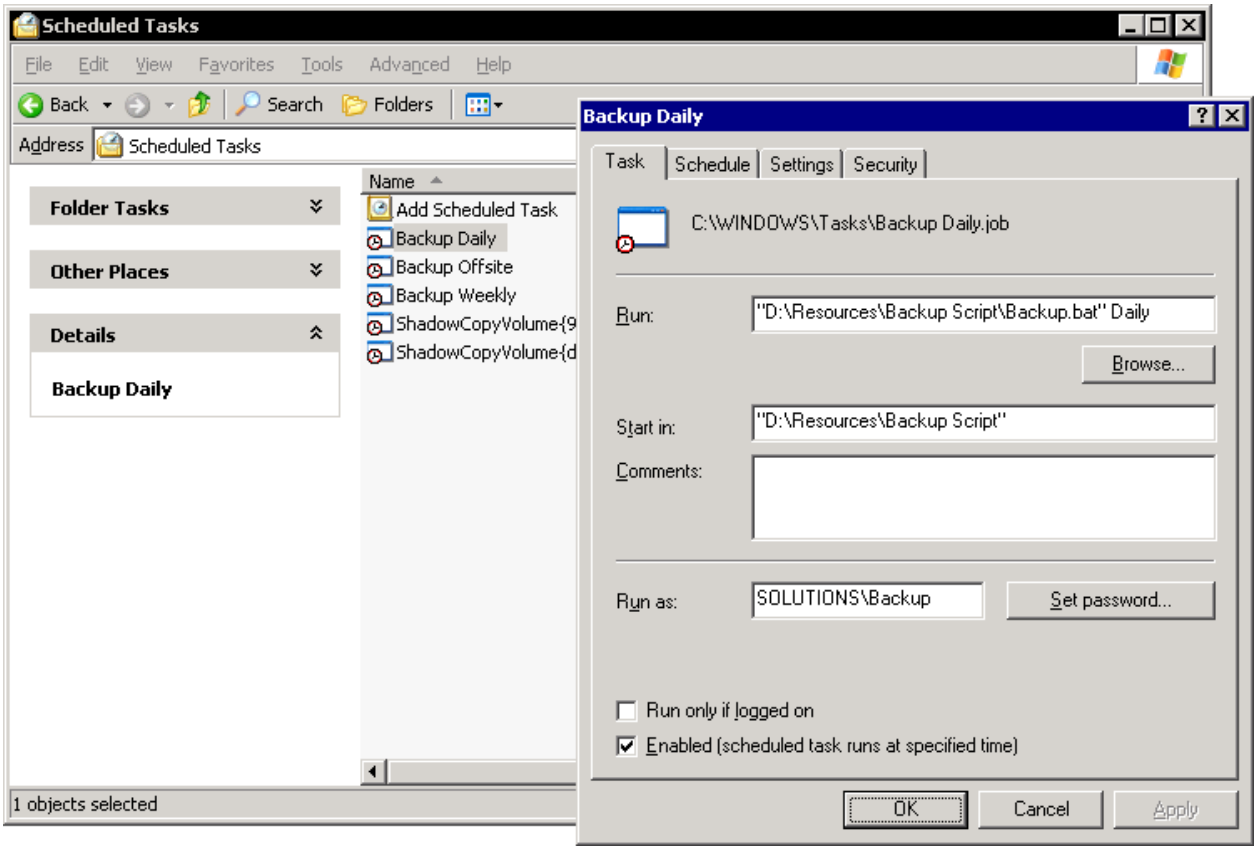



*Рис. 14.3. Исполнение запланированных задач от лица пользователя с ограниченными привилегиями*

Для компьютеров, поддерживающих технологию **Shadow Copies**, включите теневое копирование томов Accounting и Users каждые два часа в рабочее время. Укажите следующие параметры:

- ёмкость хранилища Shadow Copies в размере 20% от копируемых томов;
- местоположение копий – том Resources, если тот хранится на отдельном жёстком диске. Следует учесть, что данная настройка отражается только на производительности системы, но не позволит вам восстановить данные в случае отказа копируемого диска.

# 15. Регулярное обслуживание системы.

### 15.1. Использование административных привилегий.

Фундамент надёжной защиты от вирусов – разграничение привилегий, в результате которого состояние системы консервируется, и она не подвергается нежелательным изменениям со стороны пользователей. Выполняйте повседневные задачи только от лица учётной записи с ограниченными привилегиями – вкупе со всеми другими упомянутыми в данном Руководстве мерами безопасности, это защитит систему от вирусной инфекции или случайного повреждения.

Никогда не выдавайте рядовым пользователям членство в группах **Administrators** или **Power Users**. Исключительные ситуации могут быть решены отдельно:

- для тестирования работоспособности программ используйте соответствующую служебную учётную запись **User**. Можете добавлять её в группу Administrators по мере необходимости и убирать по окончании проверки.
- пользователи мобильных компьютеров могут обладать запасной локальной учётной записью с повышенными привилегиями, но не должны использовать её для обычной работы. Учтите, что ряд проблем не требует наличия прав Администратора лля своего решения. Например, для смены IP-адреса сетевого интерфейса достаточно быть членом группы **Network Configuration Operators**.

Если какая-то производственная программа не запускается с привилегиями рядового пользователя, выполните настройку системы согласно главе «Корректировка прав доступа для работы с ограниченными привилегиями». Выдавать вместо этого пользователям права Администратора или назначать полный доступ на весь диск или на весь реестр недопустимо!

Регулярно сверяйте список зарегистрированных пользователей и уровень их привилегий с фактическим положением дел. Это поможет в выявлении деятельности некоторых троянских программ, а также наличия неправомерного доступа у уволенного или сменившего занимаемую должность персонала.

### 15.2. Установка новых программ, настройка системы.

Однако, система не мертва, и повышенные привилегии необходимо использовать – например, при настройке рабочих параметров, а также для установки или обновления программ. Этот процесс необходимо строго регламентировать, так как компьютер, даже будучи защищённым от заражения со стороны рядовых пользователей, всё равно остаётся уязвимым к действиям лиц, обладающих административным доступом.

Никогда не устанавливайте и даже не пытайтесь запускать новые программы, не требующие инсталляции, **без должного технического обоснования**, ради «только посмотрю и уберу» или «мне сказали, полезная вещь». Приятная внешне и интересная на первый взгляд бесплатная программа, скачанная из Интернета или принесённая на диске от знакомых, может оказаться опасной ловушкой для людей, наивно полагающих «я сто раз такое делал, и ничего не случалось».

В случаях, когда тестирование действительно необходимо, производите эксперименты на **выделенном компьютере** или в **виртуальной среде**.

Если для установки производственных программ обоснование может быть достаточно кратким – «эта программа будет применена на складе для учёта товара», то разрешение на установку программ системного уровня должно опираться на технические характеристики, исключающие некомпетентную оценку ситуации. Например, недопустимо мотивировать установку firewall-модуля стороннего производителя следующим образом – «мне сказали, этот firewall хороший, а встроенный всё равно не работает, это все знают».

Помните, что система целостна и не нуждается в «полезных чистильщиках» или «оптимизаторах памяти». Не бывает версий Windows, которые самостоятельно замусориваются – это всегда происходит по вине и при ручном вмешательстве администратора. Компьютер не должен подвергаться воздействию подобных программ - эффект их применения в лучшем случае равняется нулю, а зачастую даже приравнивается к последствиям игры в **русскую рулетку**.

Настраивая систему, гораздо удобнее и безопаснее запускать от лица Администратора лишь отдельные программы, нежели прерывать работу пользователя, закрывая все его приложения с целью зайти в компьютер с другой учётной записью.

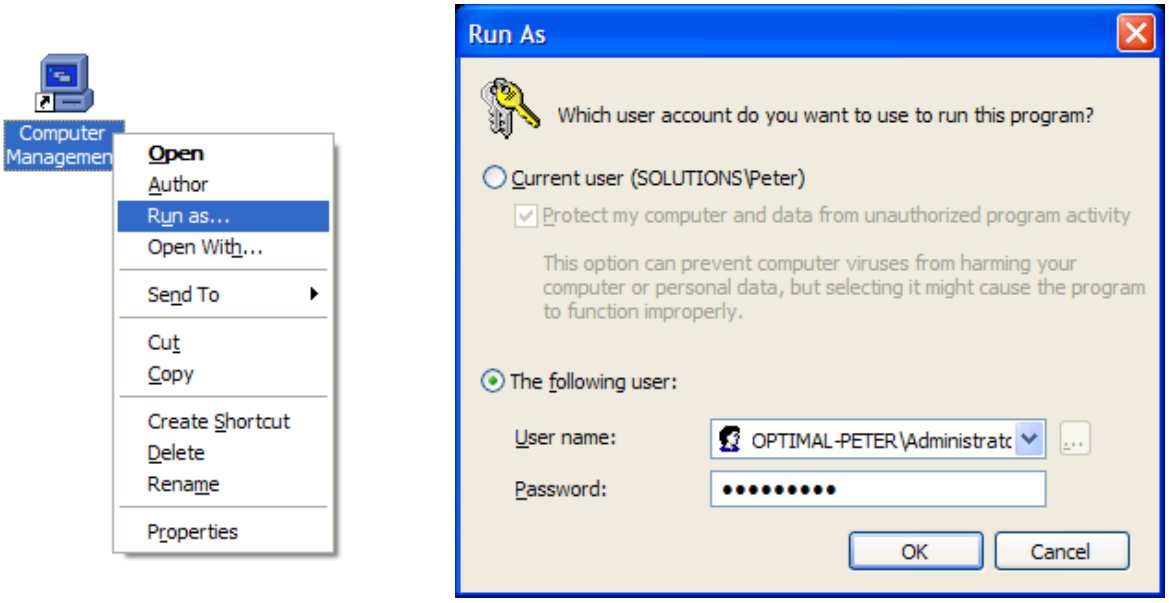



*Рис. 15.1. Запуск программы с альтернативными привилегиями*

Приняв решение установить ту или иную программу, инсталляционные файлы берите **только в оригинальном источнике** (компакт-диске или web-сайте)! Например, категорически запрещается скачивать Windows Service Pack в peer-to-peer сетях или «с сайта известного компьютерного журнала», в то время как он доступен для свободного скачивания на сайте производителя (http://download.microsoft.com).

Установите **антивирусную программу** для проверки полученных инсталляционных файлов, а также обычных регулярных сканирований дисков. Но помните, что существуют угрозы, не распознаваемые антивирусными приложениями!

Перед установкой новых программ или внесением серьёзных изменений в конфигурацию компьютера рекомендуется создать резервную копию состояния системы (C:\ и SystemState единым блоком).

Устанавливая программы, соблюдайте Правила распределения ресурсов. Все изменения программной конфигурации системы отражайте в Паспорте компьютера. Это поможет выяснить источник проблемы в случае сбоя.

Убедитесь, что документация, регламентирующая порядок работы с административными привилегиями, доступна всем ответственным лицам; что она им понятна, и каждый умеет произвести восстановление системы из резервной копии.

### 15.3. Установка обновлений.

Своевременно устанавливайте обновления безопасности. Все громкие эпидемии сетевых червей **CodeRed, Slammer, MSBlast, Kido** (и многих других) произошли из-за халатности системных администраторов и беспечности домашних пользователей, не устанавливавших обновления для Windows, SQL Server и других служб от полугода и более. Как результат, черви удалённо атаковали обнаруженные ранее уязвимости, проникали в систему и продолжали распространяться с захваченных компьютеров далее.

Уязвимости обнаруживаются не только в Windows или SQL, но и во всех других системах, служебных и производственных приложениях. Для инсталляции обновлений Windows настройте компонент **Automatic Updates** или еженедельно посещайте сайт **Windows Update** вручную. На производственных предприятиях для централизованной установки обновлений примените более удобную и эффективную службу **WSUS** (Windows Software Update Services) под управлением Microsoft Windows Server.

Обновления требуются также и для производственных программ. Например, понятие **Service Pack** существует не только для Microsoft Office, но и для программ сторонних производителей. Регулярно устанавливайте обновления также и для вспомогательных модулей – например, **Adobe Flash** или **Sun Java**.

Никогда не берите эти обновления в сторонних источниках, всегда используйте только оригинальные носители или веб-сайты!

### 15.4. Другие рекомендации.

Не реже, чем раз в полгода, **меняйте пароли** административных и служебных учётных записей. Не используйте эти же пароли для доступа к другим системам (веб-сайтам, электронной почте). Помните, что пароли доступа к обычным FTP- и HTTP-сайтам, а также к почтовым POP3-серверам передаются через Интернет в полностью открытом виде!

Регулярно просматривайте журналы системы с целью обнаружения деятельности зловредных программ или попыток взлома. Журнал **Application (Приложений)** может содержать события службы Software Restriction Policies, журнал **Security (Безопасности)** – следы попыток взлома паролей учётных записей, журнал **System (Системы)** – события аварийных перезагрузок компьютера.

# 16. Действия при обнаружении заражения.

Не все виды угроз могут быть успешно распознаны антивирусными программами. Приведённые ниже методики могут помочь обнаружить заражение в ситуациях, когда система ведёт себя неадекватно, а антивирус сообщает, что ничего опасного не найдено.

## 16.1. Анализ признаков проблемы.

- **заметно упала скорость связи с Интернетом**
  Интернет-черви не ограничиваются захватом контроля над одним компьютером. Они стараются активно распространяться далее, максимально используя пропускную способность Интернет-канала, отнимая тем самым её у других программ. Закройте все программы, выполните команду **netstat** в командной строке и оцените статистику сетевых соединений – каково их количество, какие порты используются. Задействуйте утилиту Sysinternals **TCPView** для получения более детальной информации в реальном времени.

- **постоянно блокируются учётные записи пользователей**
  Некоторые модификации Интернет-червей, а также специализированные программы взлома атакуют базу учётных записей пользователей, пытаясь подобрать их пароли. Настроенные политики безопасности блокируют попытки взлома паролей, тем самым обнаруживая подозрительную деятельность в сети. В консоли **Event Viewer** откройте журнал **Security** и изучите содержимое событий неудачного входа в систему. В них могут быть указаны имя или IP-адрес атакующего компьютера.

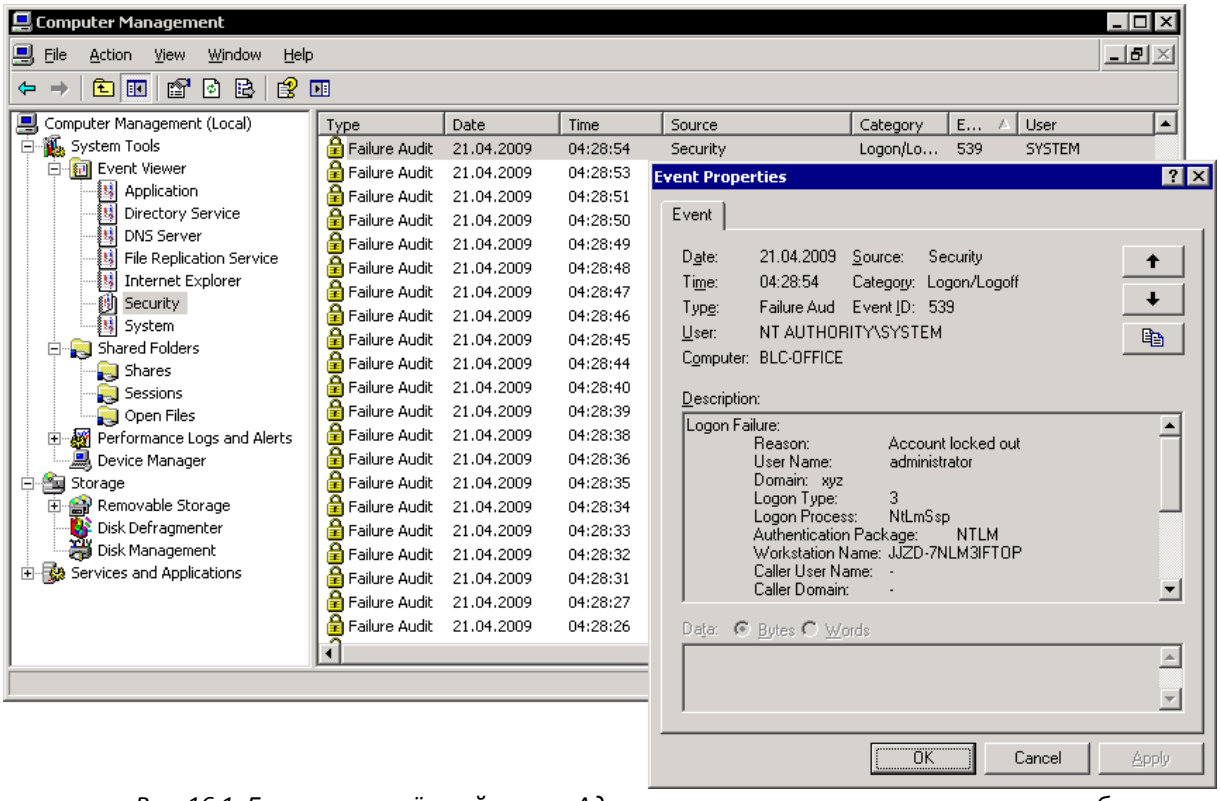



*Рис. 16.1. Блокировка учётной записи Администратора в результате атаки перебора паролей*

- **существенно снизилась скорость работы системы и прикладных программ**
  Вирус или процесс, запущенный хакером, могут отнимать большой объём системных ресурсов (оперативная память, процессор, жёсткий диск) для своей деятельности, тем самым «заглушая» работу остальных программ. Запустите программу **Task Manager**, осмотрите список запущенных процессов и даваемую ими нагрузку. Обычно пользователи работают с одними и теми же известными приложениями. Неожиданное появление новых процессов в оперативной памяти является поводом для проведения расследования, что они из себя представляют. Задействуйте утилиту Sysinternals **Autoruns** для просмотра списка всех программ, запускающихся при загрузке или входе пользователя в систему.

- **неожиданно перестали запускаться производственные программы**
  Политики SRP описывают hash-значения разрешённых для запуска производственых программ. Вирус, заражая исполняемые модули этих программ, изменяет их контрольные суммы. Испорченные файлы более не попадают в зону действия «белого списка» SRP и заражение может быть легко обнаружено. В консоли **Event Viewer** откройте журнал **Application** и выполните поиск событий от источника SRP.

- **появление новых файлов в местах, для этого не предназначенных**
  Типовым примером является наличие скрытого файл **autorun.inf** в корневых каталогах дисков. Его появление однозначно указывает на вирусную деятельность. Следите за чётким исполнением **Правил распределения ресурсов** со стороны административного персонала. При появлении файлов неизвестного происхождения установите их владельца (в свойствах файла закладка Security, Advanced, Owner);

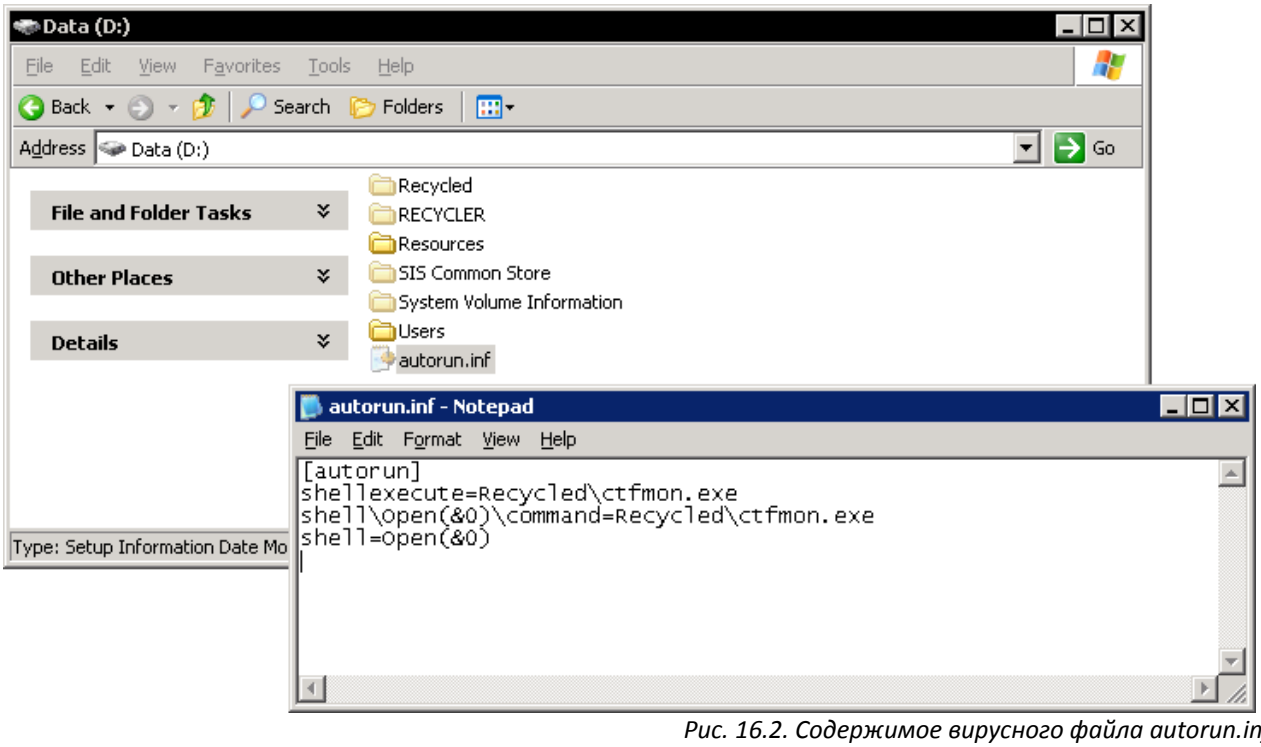



*Рис. 16.2. Содержимое вирусного файла autorun.inf*

- **невозможность зайти на сайты, связанные с безопасностью**
  Некоторые вирусы пытаются сорвать попытки пользователя устранить заражение, в том числе блокируя доступ к Windows Update и сайтам антивирусных производителей. Проверьте наличие установленных обновлений, открыв сайт **Windows Update** вручную.

Выполняя плановое сканирование содержимого жёсткого диска, антивирусная программа может обнаружить тело известного ей вируса и выдать сообщение об этом на экране. Однако, это вовсе необязательно свидетельствуют о заражении – возможно, файл вируса просто хранится в папке Интернет-кэша, но запуститься не может, будучи блокируемым политиками безопасности. Внимательно читайте сообщения антивирусной программы – возможно, никаких действий предпринимать не требуется вообще.

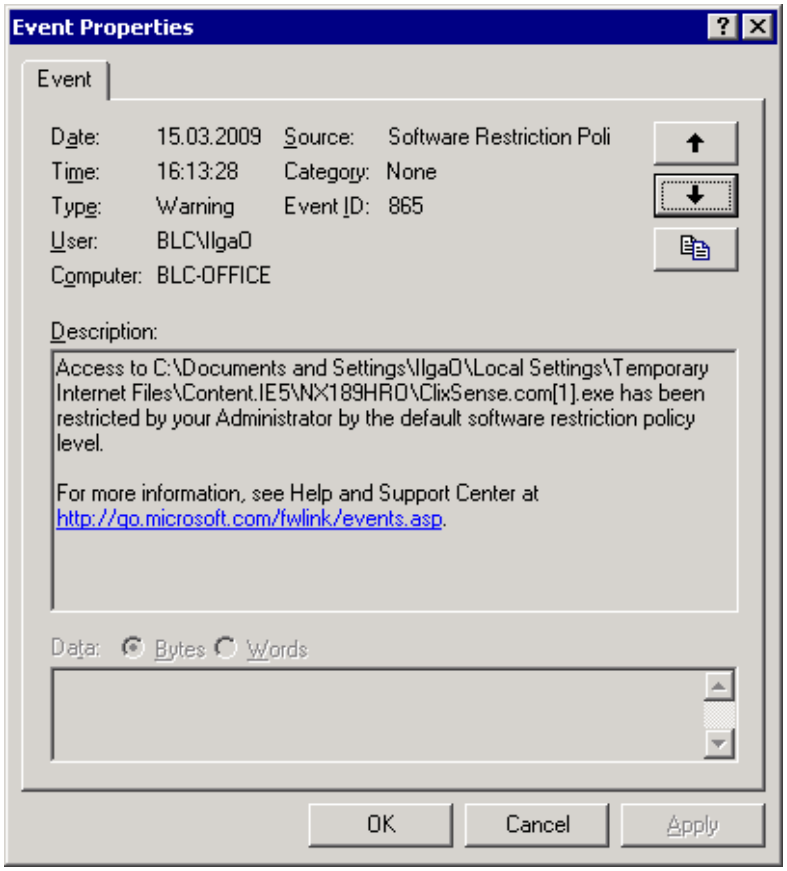



*Рис. 16.3. Политика SRP успешно заблокировала запуск вирусной программы. Реакция не требуется*

### 16.2. Действия при обнаружении заражения.

Доказав наличие заражения, попытайтесь оценить его масштаб. Решающим фактором может оказаться, удалось ли зловредной программе выполниться с привилегиями администратора или системного пользователя SYSTEM.

В большинстве случаев, когда вирусная программа смогла запуститься только от лица пользователя с ограниченными привилегиями, вполне достаточным может оказаться очистить или пересоздать с нуля пользовательский профиль.

Получив повышенные привилегии, зловредная программа может встроить в систему rootkit-модуль, обнаружить который крайне сложно либо **не стоит затраченных усилий**. Как вариант, само вирусное заражение могло быть получено с помощью rootkit-модуля, уже имевшегося в системе задолго до возникновения проблемы.

В этом случае, для **гарантированного** уничтожения угрозы придётся отформатировать диски и выполнить полную переинсталляцию скомпрометированной системы и прикладных программ. Облегчить процесс переустановки могут как различные средства автоматизации установки, так и восстановление системы из последней заведомо чистой копии.

Существуют вирусы, способные проникать в **Master Boot Record** (MBR) жёстких дисков. Выполните перезапись MBR непосредственно перед переустановкой системы. Это можно сделать как с помощью **Recovery Console**, загрузившись с инсталляционного компакт-диска Windows, так и сторонними средствами (LiveCD).

Приняв решение о полной переинсталляции, демонтируйте жёсткий диск заражённого компьютера, скопируйте все критически важные документы на отдельный носитель и выполните полную переустановку Windows с нуля. Не разрешается подключать к работающей поражённой системе любые съёмные носители. Также, не разрешается переносить с поражённой системы любые исполняемые модули, драйвера или инсталляционные файлы. Эти ресурсы придётся взять в заведомо чистом источнике.

### 16.3. Анализ происшествия.

Не спешите сразу устранять все следы взлома или вирусного заражения. Сделайте копию системы для дальнейшего анализа ситуации, поиска слабых мест и изучения возможностей повышения уровня безопасности.

Наиболее грубую ошибку допускает тот, кто обвиняет в заражении системы вирусами пользователей или антивирусную программу. Как правило, вина в такого рода происшествиях целиком и полностью лежит на администраторе, нарушившим один или несколько принципов безопасной работы.

Соберите сведения о всех последних действиях пользователей и администраторов до наступления проблемы. Попытайтесь выяснить вид и источник поражения. Выясните и устраните пробел в защите системы.

# 17. Заключение.

Согласно проведённым ранее исследованиям, не более 10% пользователей практикуют взвешенный подход к безопасности своих компьютеров. Ещё около 80% полагают, что наличия антивирусной программы вполне достаточно; остальные 10% не предпринимают вообще ничего. Закономерным итогом подобного отношения являются все громкие эпидемии интернет-червей, вирусов и регулярно обнаруживаемые ботнеты.

Приведённые в данном Руководстве методики не смогут обеспечить стопроцентную защиту от вирусов – как и все идеалы, 100% недостижимы в принципе. Однако, если бы большинство системных администраторов практиковало предлагаемый подход к безопасности, а пользователи обращались бы к ним за настройкой в том числе своих домашних систем, компьютерные вирусы однозначно перестали бы быть столь значимой угрозой, каковой они являются сейчас.

Помните: не существует безвредных вирусов – есть вирусы, о которых мы мало знаем.

В сравнении с обычным заблуждением сегодняшнего дня «я нажму одну кнопку в антивирусе, и он решит все мои проблемы», эффективность предлагаемых методов такова, что позволяет говорить о практически **гарантированной** защите от вирусов.