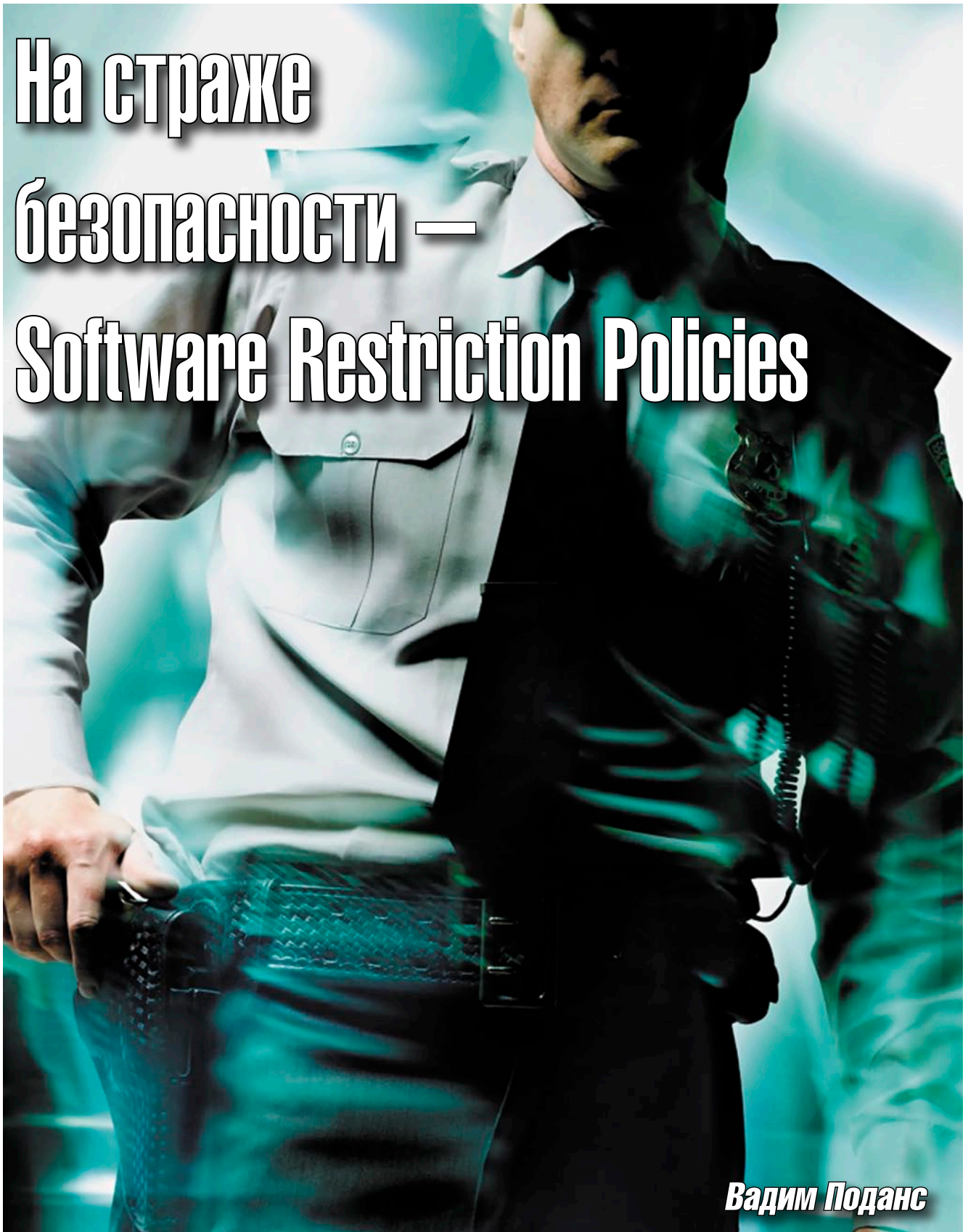


# На страже безопасности — Software Restriction Policies



*Вадим Поданс*

Заботитесь о безопасности сети? Для этого необязательно покупать новые дорогостоящие продукты, поскольку зачастую высокоэффективные средства уже вами куплены, но не используются. Научитесь эффективно применять их.

Задачей каждого системного администратора является поддержание в безопасности IT-инфраструктуры своего предприятия, а также ограничивать запуск ненужных пользователю для работы приложений.

Microsoft предлагает интегрированное в линейку Windows Server и линейку корпоративных настольных систем Windows XP/Windows Vista решение, которое называется Software Restriction Policies (сокращённо SRP) – политики ограниченного использования программ.

Данная технология предлагается ещё с линейки Windows 2000 и развивается до сих пор. Тем не менее многие системные администраторы не знают даже о существовании этой политики или избегают её использования из-за сложности настройки. В широком смысле данная политика определяет, какие приложения можно запускать пользователю, а какие запрещено, тем самым снижая риск, что пользователь запустит недозволенное программное обеспечение, скачанное из Интернета, принесённое на флешке или полученное другими противоречащими корпоративной политике способами.

Самый простой способ назначить политику – запустить Group Policy Management Console. Затем перейти в узел: «Computer/User Configuration → Windows Settings → Security Settings → Software Restriction Policies».

При создании политики (кликнуть правой кнопкой мыши и выбрать Create New Policy) она переходит в состояние Unrestricted, то есть не запрещает ничего. Внутри консоли будет 5 объектов (см. **рис. 1**):

- **Security Levels** – определяет основной уровень безопасности политики по умолчанию.
- **Additional Rules** – здесь задаются исключения для уровня по умолчанию.
- **Enforcement** – окно для выбора степени действия политики.
- **Designated File Types** – окно управления списком расширений файлов, которые проверяются правилом по умолчанию.
- **Trusted Publishers** – представляет настройки управления списками доверенных подписчиков для приложений и скриптов.

Политики SRP имеют 3 уровня безопасности, которые отображены в Security Levels:

- **Disallowed** – запрещено всё, кроме исключений в Additional Rules.
- **Unrestricted** – разрешено всё, кроме исключений в Additional Rules.
- **Basic User** – то же самое, что и Unrestricted, только дополнительно включает запрет запуска приложений с повышенными привилегиями.

Далее следует объект Enforcement (см. **рис. 2**). В этом окне можно форсировать применение политики не только к исполняемым файлам, но и к связанным с ними библиотекам DLL. Включение данной опции может значительно повысить нагрузку на систему, так как при запуске приложения через политику проходят и все файлы библиотек, из-за чего расходуются и время, и процессорные мощности. Но при этом данная опция позволяет программе при старте подгружать библиотеки только из разрешенных мест. Например, если при запуске программы последняя пытается загрузить библиотеки из профиля пользователя и путь размещения библиотек не указан в исключениях, то политика блокирует их загрузку в память.

Чуть ниже предлагается выбор применения политики для всех пользователей без исключения или для всех пользователей, кроме членов группы Administrators.

Здесь хочу отметить, что при включенном UAC (User Account Control) локальные администраторы не выводятся из-под действия политики SRP и освобождаются от фильтрации только приложения, которые запущены с использованием повышенных привилегий. Также в доменной среде данная опция доступна только в секции Computer Configuration редактора групповых политик.

И последняя опция – Enforce Certificate Rule. На практике правила сертификатов редко используются, и зачастую есть смысл отключить их проверку, что приведет к ускорению обработки политики.

Следом идёт элемент Designated File Type. Здесь перечислен список расширений файлов, которые контро-

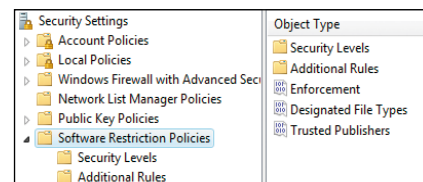


Рисунок 1. Внешний вид консоли управления политикой Software Restriction Policies

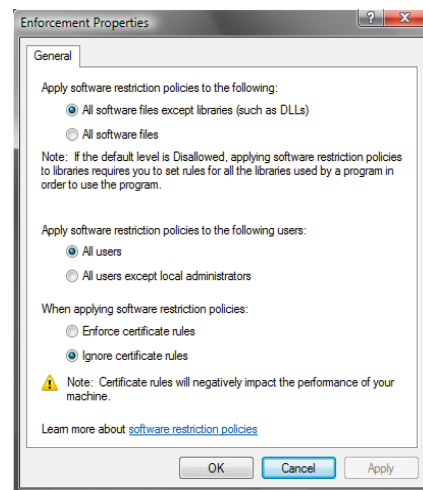


Рисунок 2. Окно выбора степени воздействия политики SRP. Настройки этого окна влияют на глобальную эффективность политик SRP

лируются Software Restriction Policies. Если пользователям необходимо запускать (или запрещено запускать) файлы с указанными в этом списке расширениями, то для них нужно составлять исключения для уровня безопасности по умолчанию (об этом подробнее чуть дальше). Данный список можно редактировать под свои условия.

И последний элемент – Trusted Publishers (см. **рис. 3**). В этом окне регулируются настройки доверенных издателей сертификатов, которыми подписываются приложения. Данное окно актуально, только если используются правила для сертификатов. В остальных случаях оно не используется. Однако для корректной работы некоторых программ (например, Windows Update в Windows XP/Windows Server 2003) необходимо разрешить управление списком Trusted Publishers для End users (самая верхняя опция).

И, наконец, рабочая область – раздел Additional Rules (см. **рис. 4**). В этом разделе составляются все исключения для действия политики по умолчанию. Можно использовать следующие типы исключений (дополнительных правил) с учётом порядка их применения:

- **Certificate Rule** – правило для сертификатов. Данный тип правила используется только для подписанных приложений и скриптов. Например, можно разрешить запуск всех приложений, которые подписаны сертификатом Microsoft Corporation, вне зависимости от их расположения и запретить запуск приложений, которые подписаны Adobe Systems. При этом нужно указать сертификаты соответствующих издателей, которые должны быть загружены либо локально, либо на сетевую папку.
- **Hash Rule** – правило хэша. Для каждого приложения требуется создание отдельного правила. Данный тип правил очень полезен для приложений и файлов, которые находятся в открытых для записи пользователями папках. Например, можно разрешить запуск приложения из папки My Documents (куда пользователь имеет права записи) по хэшу. В таком случае гарантируется защита от подмены файла (с таким же именем) или при инфицировании файла вирусом, так как в обоих случаях хэш самого файла изменится и не подпадёт под правило хэша политики SRP и запуск его будет невозможен. В Windows Vista/Windows Server 2008 хранится 2 хэша – MD5 для совместимости с клиентами Windows XP и SHA256, как «родной» алгоритм хэширования новых систем.
- **Network Zone Rule** – правило зоны сети. В Windows реализовано несколько зон сети, как Интернет, Trusted Sites, Restricted Sites, Local Intranet и Local Computer. Данный тип правил регулирует, какие установочные пакеты разрешены для скачивания исходя из условия их размещения. Для корректной работы правил на основе зон сети установочные пакеты должны быть основаны на Windows Installer (иметь расширение .MSI). Например, можно разрешить скачивание пакетов Windows Installer из зоны Trusted Sites и запретить скачивание из зоны Restricted Sites. Однако следует учесть, что данная политика не влияет на скачивание файлов из браузера Internet Explorer. На практике правила зон сети используются достаточно редко.
- **Path Rule** – правило пути. Правила данного типа позволяют указывать размещение приложений и файлов, которые не будут проверяться политикой и будут разрешены для запуска. По умолчанию уже созданы два разрешающих правила для системных папок Windows и Program Files. Благодаря этому приложения из данных папок будут разрешены для запуска, если, конечно, не удалить правила вручную (чего делать не рекомендуется). Правила для путей могут настраиваться очень гибко, так как позволяют использовать системные и пользовательские переменные окружения (например, %windir%) и знаки подстановок (например, «?» и «\*»). Кроме того, можно указать ключ реестра, из которого будет получен путь.

## Практическая реализация на примерах

Итак, мы рассмотрели все необходимые опции, которые присутствуют в консоли MMC – Software Restriction Policies. Изучив вышеизложенный материал, можно начинать создавать свои правила политики SRP, но для полноты картины я расскажу о некоторых принципах построения надёжных политик и важных вещах при работе с SRP.

Наиболее эффективным применением политик Software Restriction Policies будет разрешение запуска файлов из папок, куда пользователи не имеют права записи, и запрещение запуска файлов из папок, куда пользователи имеют право записи. В таком случае пользователь гарантированно не сможет запустить файл с рабочего стола (куда он имеет права на запись), но может запустить файл из системной папки Windows (куда обычный пользователь не имеет права записи). Этой схеме наиболее полно отвечает уровень безопасности по умолчанию – Disallowed, которое имеет значение – запретить всё, кроме правил, которые указаны в Additional Rules.

Если применить уровень безопасности по умолчанию Disallowed, то для запуска файлов придётся запускать непосредственно сами файлы в папках, в которых они размещены, так как запуск ярлыков из пользовательского окружения запрещён. Поэтому в Additional Rules необходимо будет создать разрешительные правила, которые позволят запускать ярлыки из Start Menu (это ярлыки, которые отображаются в меню Start и «Start → All Programs»). Для этого в Additional Rules необходимо создать правила для пути, которые будут указывать на:

```
C:\Users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\*.lnk
C:\Users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\*\*.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\*.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\*\*.lnk
```

Здесь используется системная переменная %username%, вместо которой при работе автоматически будет подставляться имя текущего пользователя. Однако следует учесть, что разрешение запуска ярлыка ещё не значит, что разре-

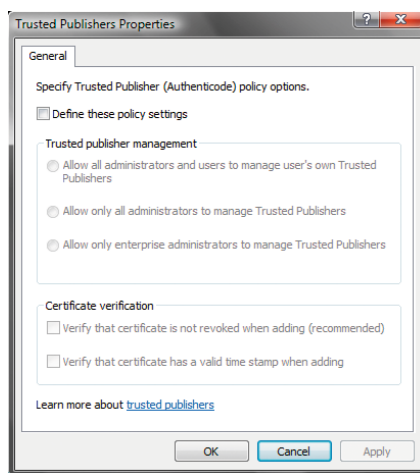


Рисунок 3. Окно с настройкой прав пользователей для редактирования списка доверенных издателей сертификатов и поведения системы при проверке сертификатов

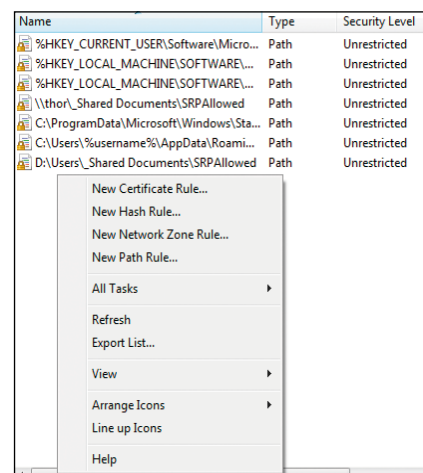


Рисунок 4. Основное окно, в котором администратор создаёт правила исключений. Правила создаются нажатием правой кнопки мыши и выбором нужного типа исключения

шено запускать программу, на которую указывает сам ярлык, еще должно быть разрешающее правило и для самой программы. То есть пользователь не сможет просто изменить путь, на который указывает ярлык для программы в меню «Пуск».

Для этих двух правил необходимо выставить уровень Unrestricted, в результате чего пользователи смогут спокойно запускать ярлыки из меню Start и из вложенных папок первого уровня (например, «Accessories → Paint.Ink»). Однако для систем Windows XP/Windows Server 2003 и систем с локализацией на других языках эти пути могут изменяться в зависимости от языка системы.

Для унификации работы с папками профилей пользователей политика SRP предлагает возможность чтения значений из реестра. Ветка реестра: HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\ содержит пути для большинства пользовательских папок профиля. Для указания пути к Start Menu рекомендуется использовать значения реестра для каждой локальной машины. Чтобы использовать значения реестра, его ключ нужно заключить в знаки процента «%», как это показано на примерах:

```
%HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\Shell Folders\Programs*.lnk
%HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Explorer\Shell Folders\
Start Menu%*.lnk
```

Для того чтобы разрешить запуск ярлыков из меню быстрого запуска (Quick Launch), нужно добавить правило для пути:

```
%userprofile%\AppData\Roaming\Microsoft\
Internet Explorer\Quick Launch*.lnk
```

Таким образом, пользователям уже разрешается запускать ярлыки из меню Start и Programs, при этом абсолютное местоположение меню Start будет определяться каждой машиной индивидуально. Если необходимо разрешить запуск ярлыков или программ из других локаций, то это достигается добавлением правил пути или хэша, как это показано ниже.

Если у вас на диске D: установлено приложение, которое в силу своих особенностей требует разрешения записи в папку с программой для пользователей (увы, но такие приложения до сих пор встречаются, и с ними приходится считаться), то правило пути типа: D:\Programs\SpecProgram\\*.exe. Или указание имени программы не будет эффективным решением, поскольку пользователю не составит труда переименовать программу и замаскировать под это имя свою любимую игру или зараженный файл. В таких случаях разумнее использовать правила хэша. Если по такому правилу разрешить только необходимые исполняемые (или скриптовые) файлы программы, то при подмене файлов пользователю не удастся запустить ложное приложение, так как хэш нового файла не будет совпадать и файл не подпадёт ни под одно исключение, в следствие чего запуск будет предотвращён уровнем безопасности по умолчанию, то есть Disallowed.

Вот таким комбинированием типов правил в итоге можно получить достаточно гибкую и эффективную политику

ограниченного использования программ, которая позволит контролировать, что пользователи могут запускать только те файлы, которые разрешены политикой компании.

## Полезные приёмы

Как правило, при реализованных политиках SRP используется общий уровень безопасности Disallowed, который позволяет достаточно комфортно и безопасно работать в системе, но вносит ограничение на некоторые операции, такие как установка новых приложений. На время процесса инсталляции приложений или других административных операций требуется временно отключать действие политики по умолчанию. Делать это в редакторе политик не очень удобно. Но есть и другое решение – временная деактивизация через реестр. Для этого можно воспользоваться тремя .REG-файлами, которые временно изменяют уровень безопасности (только для Windows Vista/Windows Server 2008):

- **SRP\_Enable** – включает уровень политики в Disallowed:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\
Windows\safer\codeidentifiers]
"DefaultLevel"=dword:00000000
```

- **SRP\_Disable** – включает уровень политики в Unrestricted:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\
Windows\safer\codeidentifiers]
"DefaultLevel"=dword:00040000
```

**Самый удобный способ приобретения ПО**

Интернет-супермаркет программного обеспечения

**SOFTKEY**

открыто 24 часа

Круглосуточный интернет-супермаркет программного обеспечения

[www.softkey.ru](http://www.softkey.ru)

Реклама

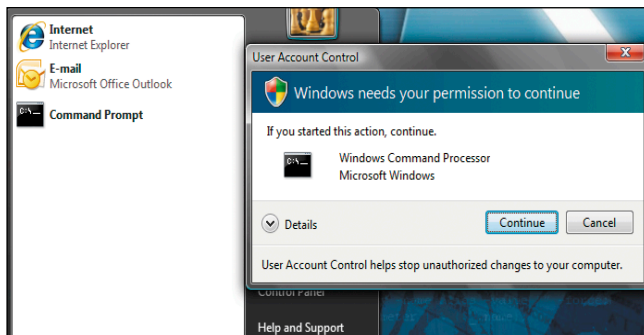


Рисунок 5. Окно UAC, которое требует подтвердить использование повышенных привилегий или отменить эту операцию

#### ■ SRP\_Basic – включает уровень политики в Basic User:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\
  Windows\Safer\CodeIdentifiers]
"DefaultLevel"=dword:00020000
```

И .REG-файлы для Windows XP /Windows Server 2003:

#### ■ SRP\_Enable – включает уровень политики в Disallowed:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\
  Windows\safer\codeidentifiers]
"authenticodeenabled"=dword:00000000
```

#### ■ SRP\_Disable – включает уровень политики в Unrestricted:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\
  Windows\safer\codeidentifiers]
"authenticodeenabled"=dword:00040000
```

Для администраторов рекомендуется использовать логон-скрипт, который будет копировать эти файлы в системную папку и заодно будет копировать ярлыки на рабочий стол администратора при входе на любую рабочую станцию домена. И при необходимости администратор этими ярлыками может временно изменить состояние политики на локальной машине. После перезагрузки системы или очередного обновления групповых политик восстановятся исходные настройки политик.

## Что нового в Windows Vista/Server 2008?

Пользователей и администраторов, использующих Windows Vista и/или Windows Server 2008, может заинтересовать уро-

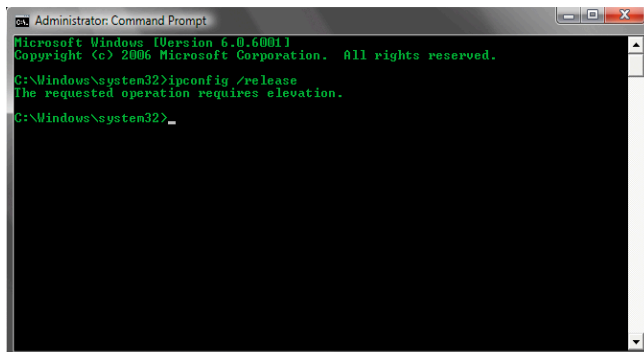


Рисунок 7. Результат выполнения команды «ipconfig /release» в консоли CMD.EXE с отфильтрованными привилегиями уровнем Basic User

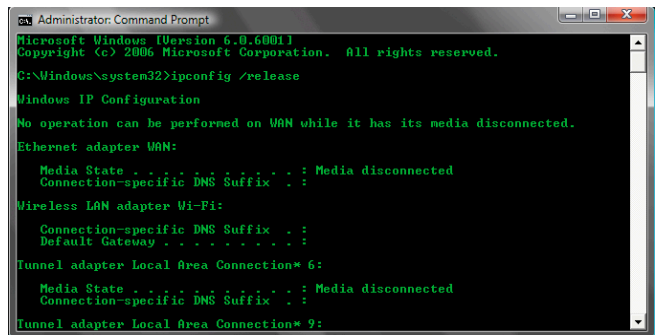


Рисунок 6. Результат выполнения команды «ipconfig /release» в консоли CMD.EXE с использованием повышенных привилегий

вень безопасности Basic User, который является расширением UAC (User Account Control). В начале статьи ему было дано только определение, а теперь рассмотрим его на практических примерах.

Для начала стоит внести ясность в модель User Account Control. Данный механизм позволяет пользователям с административными учётными записями работать в системе в режиме простого пользователя без использования административных привилегий. То есть локальный администратор в обычном режиме по сути не отличается от обычного пользователя, что обеспечивает защиту от случайных действий администратора.

Когда требуется выполнить административное действие, UAC запрашивает подтверждение на использование административных привилегий, и после подтверждения права администратора значительно повышаются, позволяя изменять настройки системы.

Также UAC позволяет и рядовым пользователям при необходимости повышать свои полномочия до административных путём ввода пароля администратора в окно UAC. Подробнее про UAC можно почитать тут – <http://technet.microsoft.com/ru-ru/magazine/cc138019.aspx>.

Уровень политики SRP – Basic User позволяет пользователям и/или администраторам запускать приложения в обычном режиме (без использования административных привилегий), но запрещает запуск того же приложения с использованием повышенных привилегий.

Для понимания Basic User приведу два наглядных примера.

### Пример 1. Запуск консоли CMD для сброса настроек IP всех сетевых интерфейсов

Данное действие из консоли командной строки требует использование повышенных привилегий. Как это выглядит в действительности? Для этого нужно войти в систему под административной учётной записью, кликнуть правой кнопкой мыши на ярлык Command Prompt и выбрать Run As Administrator. После чего UAC попросит подтвердить применение административных привилегий (см. рис. 5).

Подтверждаем эту операцию (нажимаем Continue) и выполняем команду IPCONFIG /RELEASE, которая сбрасывает настройки IP для всех сетевых интерфейсов (см. рис. 6). Команда успешно выполнена, и настройки обнулились.

Для реализации уровня Basic User в Additional Rules создадим хэш-правило для файла CMD.EXE и в качестве Security Level укажем Basic User (см. рис. 8).

Теперь повторяем операцию, подтверждаем использование повышенных привилегий и повторяем команду (см. рис. 7). Как видно из картинки, данная операция не удалась. Хотя мы и запросили повышенные привилегии, уровень Basic User не позволил их получить и и запустил консоль в обычном пользовательском режиме.

## Пример 2. Запуск System Configuration

Запуск инструментов для диагностирования проблем с запуском системы и автозапуском программ требует использования повышенных привилегий, и без них запустить приложение невозможно. Чтобы продемонстрировать действие Basic User на приложение, которое требует повышенных привилегий, создадим в Additional Rules хэш-правило для этой утилиты, которая находится по адресу: %SystemRoot%\system32\msconfig.exe.

И в Security Level укажем Basic User (см. рис. 9).

Теперь запускаем утилиту из папки Administrative Tools, и снова появляется окно UAC, которое требует подтвердить повышенные привилегии. При подтверждении политика SRP снова по хэш-правилу отменяет эти привилегии и пытается запустить приложение в обычном пользовательском режиме (см. рис. 10).

Однако данное приложение не поддерживает такую работу, в результате чего запуск приложения блокируется полностью действием по умолчанию, как это продемонстрировано на скриншоте.

Таким образом, уровень Basic User позволяет создавать менее жёсткие правила запуска приложений. Например, можно разрешить запуск приложений из любых мест, не опасаясь, что они нанесут ущерб системе, поскольку для деструктивных действий требуются повышенные привилегии.

## Заключение

Из вышеизложенного материала следует, что политики ограниченного использования программ – Software Restriction Policies являются гибким и эффективным инструментом в управлении решением контроля запуска приложений пользователями. Однако политики SRP должны быть не един-

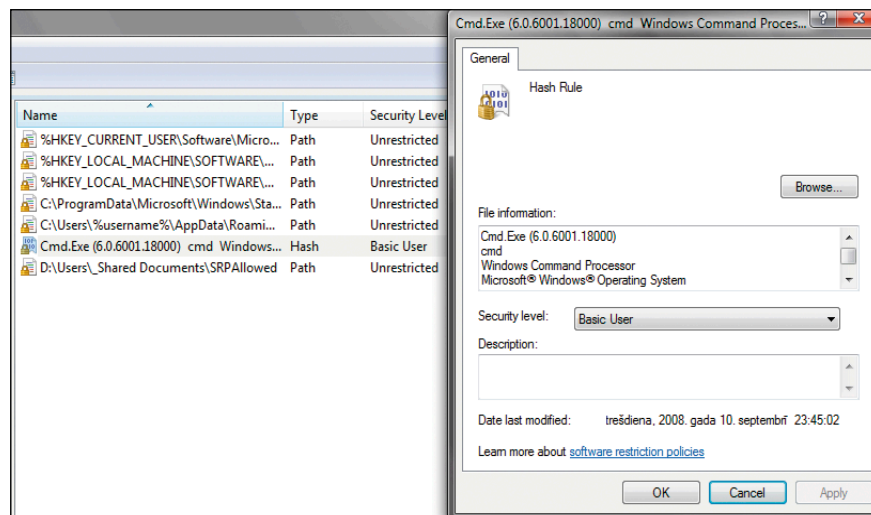


Рисунок 8. Свойства созданного хэш-правила для программы CMD.EXE

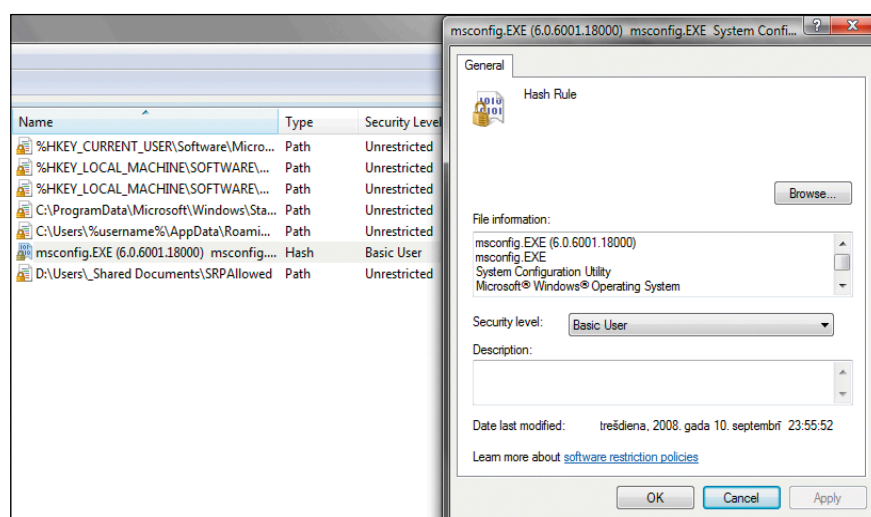


Рисунок 9. Настроенный уровень Basic User хэш-правила для утилиты MSCONFIG.EXE

ственным средством обеспечения безопасности, а являться частью общего комплекса мер безопасности, и только тогда политики SRP будут по-настоящему эффективны. Фундаментальной частью системы безопасности является работа в системе с минимальными необходимыми привилегиями. Если все пользователи в системе работают под учётной записью с административными привилегиями, то польза от применения политик SRP будет минимальна. Также советую более ответственно относиться к планированию реализации политик SRP. Чем больше внимания вы уделите стадии планирования, тем меньше времени потребуется для конечной реализации. Кроме того, план поможет избежать ошибок.

1. Software restriction policies overview – <http://technet.microsoft.com/en-us/library/cc759106.aspx>.

2. Using Software Restriction Policies to Protect Against Unauthorized Software (Windows XP/Windows Server 2003) – <http://technet.microsoft.com/en-us/library/bb457006.aspx>.
3. Using Software Restriction Policies to Protect Against Unauthorized Software (Windows Vista/Windows Server 2008) – <http://technet.microsoft.com/en-us/appcompat/aa940985.aspx>.
4. Explore the features: User Account Control – <http://www.microsoft.com/windows/windows-vista/features/user-account-control.aspx>.

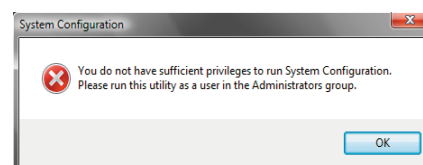


Рисунок 10. Такое сообщение будет получено при попытке запустить системную утилиту без использования повышенных привилегий