

Методические рекомендации по администрированию локальных сетей под управлением операционной системы Microsoft Windows Server

Туманов Иван Анатольевич
методист ГБУ ДПО “СПбЦОКОиИТ”
tumanov.i78@gmail.com

Санкт-Петербург
2020г

Содержание:

1. [Windows Server](#)
2. [Управление элементами Active Directory](#)
3. [Групповые политики](#)
4. [Профили пользователей](#)
5. [Общий профиль в Windows 10](#)
6. [Делегирование полномочий в домене Active Directory](#)
7. [Файловый сервер](#)

Windows Server

[К содержанию](#)

Windows Server

Windows Server предназначена для организаций, в нее включены различные программные модули, в числе которых роли сервера, позволяющие выполнять следующие функции:

- **Active Directory** – служба управления учетными записями пользователей, предназначенная для организации внутреннего контроллера домена.
- **DHCP** – сетевой протокол динамического распределения хостов, позволяющий назначать автоматически IP-адреса всем компьютерам внутри локальной сети или домена. В домашних условиях эту функцию обычно выполняет роутер, но на предприятиях с большим количеством рабочих станций потребуется использовать различные дополнительные настройки этой службы.
- **Файловый сервер**, позволяющий хранить файлы с применением отказоустойчивых RAID-массивов, а также ограничивать доступ к определенной информации для некоторых рабочих станций или пользовательских профилей.
- **Сервер обновлений** устанавливает обновления на все компьютеры внутри домена по определенному расписанию.
- и др.

Домен Windows

Домен Windows является формой компьютерной сети, в которой все учетные записи пользователей, компьютеры, принтеры и другие участники безопасности регистрируются в центральной базе данных, расположенной на одном или нескольких центральных компьютерах, называемых **контроллеры домена**.

Аутентификация происходит на контроллерах домена, т.е. централизовано. Каждый человек получает уникальную учетную запись пользователя, которой затем может быть назначен доступ к ресурсам в домене.

Начиная с Windows 2003, компонентом Windows, отвечающим за поддержание этой центральной базы данных является **Active Directory** или служба каталогов.

Роль контроллера домена настраивается только на серверных версиях ОС Windows.

Скачивание Windows Server

[Скачать Windows Server 2019 для ЛВС](#)

Windows Server 2019
Оценки | 180 дн.

В дополнение к пробной версии Windows Server 2019 содержит дополнительные возможности рабочего стола, устранения неполадок и отладки. Компоненты Windows с помощью команды DISM. Узнайте больше о компонентах сведения о компонентах по требованию (FOD) и компонентах.

Начать ознакомление

Выберите тип файла для ознакомления:

- ISO
- Azure
- VHD

Продолжить

Начать ознакомление

Выберите язык:

Русский

Назад Загрузка

Установка Windows Server 2019

| Операционная система | Архитектура | Дата измене... |
|---|-------------|-------------------|
| Windows Server 2019 Standard Evaluation | x64 | 07.09.2019 |
| Windows Server 2019 Standard Evaluation (возможности ра... | x64 | 07.09.2019 |
| Windows Server 2019 Datacenter Evaluation | x64 | 07.09.2019 |
| Windows Server 2019 Datacenter Evaluation (возможности ... | x64 | 07.09.2019 |

Общие
Имя: WinServer2019
ОС: Windows 2019 (64-bit)

Система
Оперативная память: 1024 МБ
Порядок загрузки: Гибкий диск, Оптический диск, Жёсткий диск
Ускорение: VT-x/AMD-V, Nested Paging

Дисплей
Видеопамять: 128 МБ
Графический контроллер: VBoxSVGA
Сервер удалённого дисплея: Выключен
Запись: Выключена

Носители
Контроллер: SATA
SATA порт 0: WinServer2019.vdi (Обычный, 50,00 ГБ)
SATA порт 1: [Оптический привод] Пусто

Аудио
Аудиодрайвер: Windows DirectSound
Аудиоконтроллер: Intel HD Audio

Сеть
Адаптер 1: Intel PRO/1000 MT Desktop (Внутренняя сеть,

При установке лучше выделить больше ресурсов (особенно оперативной памяти), после установки и первичной настройки можно уменьшить...

Пароль администратора имеет ограничения - можно использовать 123qweASD, этого достаточно для выполнения условий по СЛОЖНОСТИ.

Первым делом устанавливаем драйверы от VirtualBox, потом не забываем изменить имя ОС, после рекомендуется отключить блокировку экрана в виртуальной машине.

Клиентские ОС в домене

Клиентом домена в семействе Microsoft Windows могут быть версии с названиями Business, Professional, Enterprise...

В версиях Home функционал доменной интеграции отсутствует.

Клиентом домена могут быть также ОС Linux. Они могут использовать централизованную аутентификацию, но не управляются групповыми политиками.

Контроллер домена можно также развернуть на ОС Linux. Для этих целей используется свободное ПО SAMBA.

Управление элементами Active Directory

Способы управления Active Directory (AD)

Типичные задачи контроллера домена:

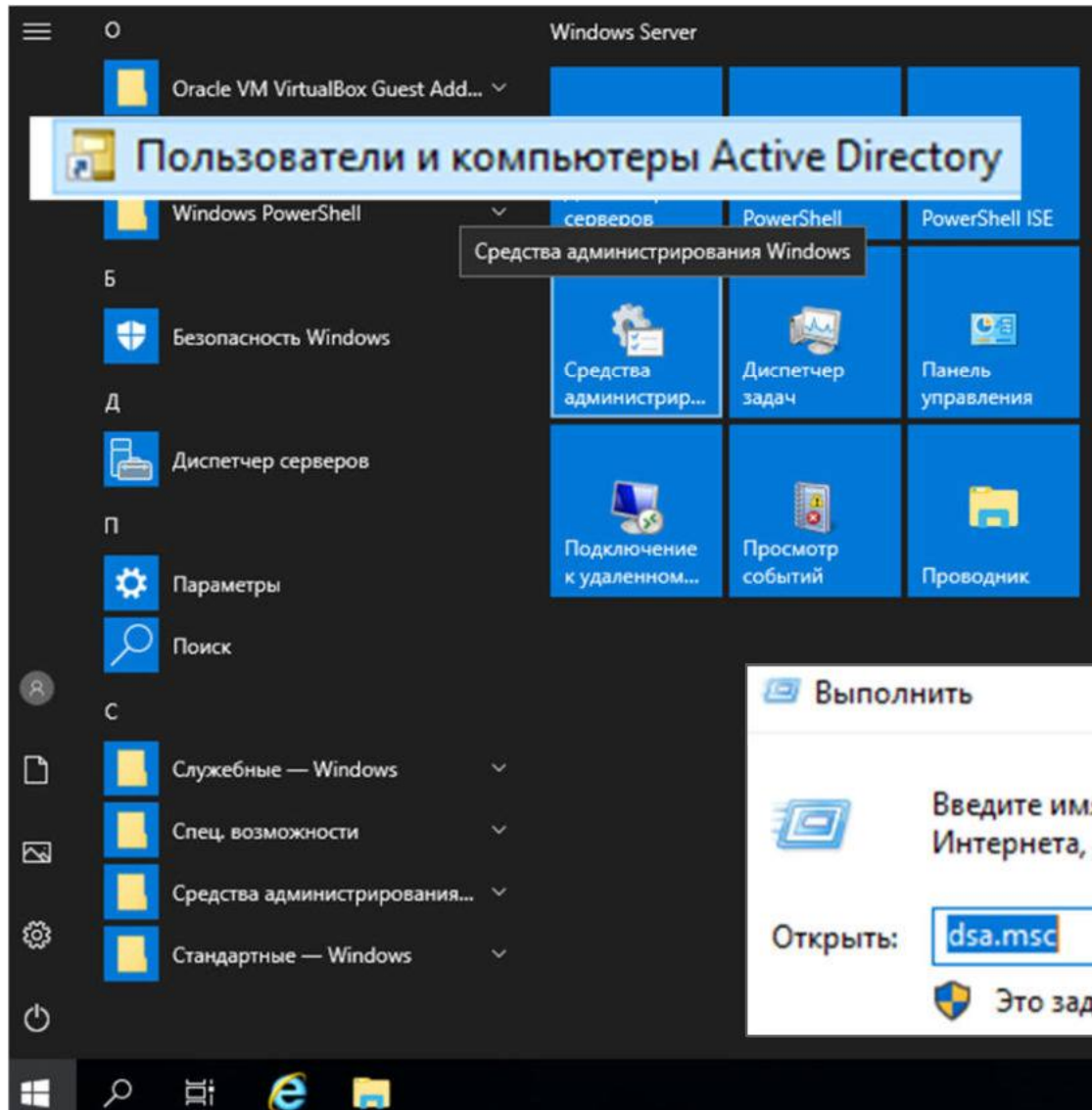
1. Управление пользователями и группами
2. Управление групповыми политиками домена
3. Управление ресурсами файлового сервера

Стандартно эти элементы доступны после установки роли контроллера домена на серверной версии Windows. Работать с ними можно на рабочем столе непосредственно или через удаленный рабочий стол.

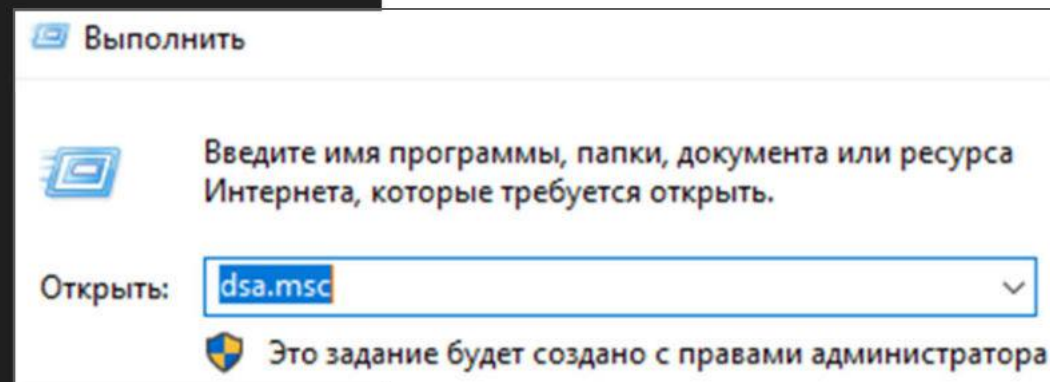
Другой вариант - установить на рабочую станцию средства управления доменом. Это позволит управлять настройками AD пользователям, не имеющим прав администратора домена (а только эти пользователи могут удаленно подключаться к серверу без приобретения дополнительных лицензий терминального доступа).

В AD можно **делегировать** часть прав “не администраторам”, так, например, можно позволить учителям сбрасывать пароли ученикам или включать\выключать их из группы, отвечающей за доступ к Интернет.

Запуск оснастки управления пользователями AD



Выполнить “dsa.msc”
или в меню “пуск”:



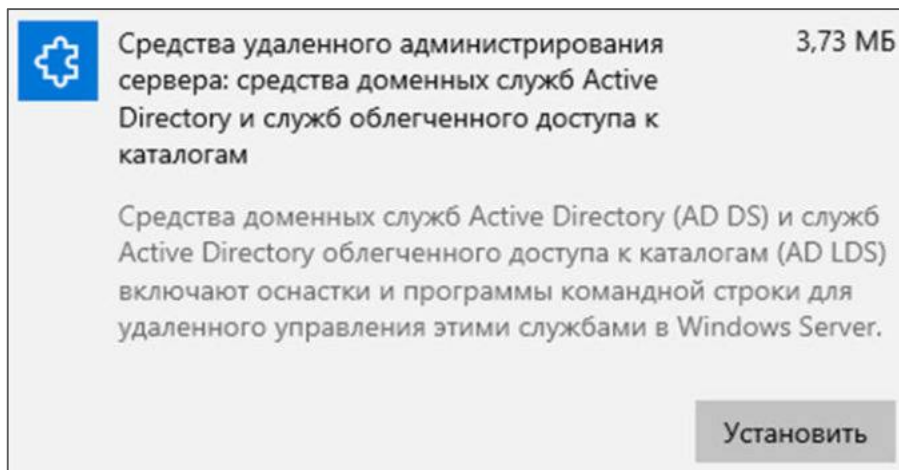
Средства управления доменом

Чтобы управлять AD с клиентского компьютера с Windows (7-10), необходимо установить компонент Microsoft Remote Server Administration Tools (RSAT).

Скачать нужную версию RSAT можно бесплатно с официального сайта microsoft.ru указав в поиске RSAT и выбрав файл для нужной версии Windows и разрядность.

Возможно управление AD в PowerShell - оболочке с интерфейсом командной строки.

Начиная с версии Windows 10 1809 RSAT включены в ОС, необходимо



ы, они скачаются сами:

“Параметры - Приложения и возможности - Управление дополнительными компонентами - Добавить компонент”

Подразделение (OU, Organizational Unit)

Организационное **подразделение** (OU) представляет собой контейнер в домене Active Directory, который может содержать различные объекты из того же самого домена AD: другие контейнеры, группы, аккаунты пользователей и компьютеров.

Две основные задачи OU, кроме хранения объектов Active Directory:

1. **Делегирование управления** и административных задач внутри домена другим администраторам и обычным пользователям без предоставления им прав администратора домена;
2. **Назначение групповых политик** на все объекты (пользователей и компьютеры), которые находятся в данном подразделении (OU).

Подразделение

Active Directory - пользователи и компьютеры

Файл Действие Вид Справка

Пользователи и компьютеры

| Имя | Тип | Описание |
|------------|---------------|------------------------------|
| Builtin | builtinDomain | |
| school.lan | | |
| Builti | | Default container for up... |
| Compu | | Default container for do... |
| Domai | | Default container for sec... |
| Foreig | | Default container for ma... |
| Manag | | Default container for up... |
| Users | | |

- Делегирование управления...
- Найти...
- Сменить домен...
- Сменить контроллер домена...
- Повысить режим работы домена... Хозяева операций...
- Создать**
- Все задачи
- Вид
- Обновить
- Экспортировать список...
- Свойства
- Справка

- Компьютер
- Контакт
- Группа
- InetOrgPerson
- msDS-ShadowPrincipalContainer
- msImaging-PSPs
- Псевдоним очереди MSMQ
- Подразделение**
- Принтер
- Пользователь
- Общая папка

Новый объект - Подразделение

Создать в: school.lan/

Имя:
TEACHERS

Защитить контейнер от случайного удаления

OK Отмена Справка

Группа Active Directory

Группа Active Directory – это совокупность объектов в Active Directory. В группу могут входить пользователи, компьютеры, другие группы и другие объекты AD. Администратор управляет группой как одним объектом.

В AD существует два типа групп:

1. **Группа безопасности** – этот тип группы используется для предоставления доступа к ресурсам, например, к сетевым каталогам.
2. **Группа распространения** – данный тип групп используется для создания групп почтовых рассылок, нельзя использовать для доступа к ресурсам домена.

Для каждого типа группы существует три области действия:

1. **Локальная в домене** — используется для управления разрешениями доступа к ресурсам (файлам, папкам и другим типам ресурсов) только того домена, где она была создана.
2. **Глобальная группа** – данная группа может использоваться для предоставления доступа к ресурсам другого домена. В эту группу можно добавить только учетные записи из того же домена, в котором создана группа.
3. **Универсальная группа** — рекомендуется использовать в лесах из множества доменов.

Так как обычно в школах нет леса и почтовых доменов, то достаточно создавать все группы с настройками по умолчанию как глобальные группы безопасности.

The image shows a screenshot of the Active Directory console and a dialog box for creating a new group.

Active Directory Console:

- Title: Active Directory - пользователи и компьютеры
- Menu: Файл, Действие, Вид, Справка
- Tree view: Пользователи и компьютеры > Сохраненные запросы > school.lan > TEACHERS
- Table columns: Имя, Тип
- Context menu for TEACHERS:
 - Делегирование управления...
 - Переместить...
 - Найти...
 - Создать >
 - Компьютер
 - Контакт
 - Группа
 - Все задачи >
 - Вид >

Dialog Box: Новый объект - Группа

- Close button: X
- Header: Создать в: school.lan/TEACHERS
- Имя группы: teachers
- Имя группы (пред-Windows 2000): teachers
- Область действия группы:
 - Локальная в домене
 - Глобальная
 - Универсальная
- Тип группы:
 - Группа безопасности
 - Группа распространения
- Buttons: OK, Отмена

Пользователь

The image shows a sequence of steps for creating a user in Active Directory:

- Active Directory - пользователи и компьютеры:** The left pane shows the tree structure with 'TEACHERS' selected under 'Users'.
- Context Menu:** A right-click menu is open over 'TEACHERS', with 'Создать' (Create) selected. A sub-menu is open, showing 'Пользователь' (User) as the selected option.
- Новый объект - Пользователь (Step 1):** A dialog box titled 'Новый объект - Пользователь' with 'Создать в: school.lan/TEACHERS'. Fields include: 'Имя: teacher', 'Инициалы: [empty]', 'Фамилия: [empty]', 'Полное имя: teacher', 'Имя входа пользователя: teacher@school.lan', and 'Имя входа пользователя (пред-Windows 2000): SCHOOL\teacher'. Buttons: '< Назад', 'Далее >'. A close button 'X' is in the top right.
- Новый объект - Пользователь (Step 2):** A second dialog box titled 'Новый объект - Пользователь' with 'Создать в: school.lan/TEACHERS'. Fields include: 'Пароль: [masked]', 'Подтверждение: [masked]', and four checkboxes: 'Требовать смены пароля при следующем входе в систему', 'Запретить смену пароля пользователем', 'Срок действия пароля не ограничен', and 'Отключить учетную запись'. Buttons: '< Назад', 'Далее >', 'Отмена'. A close button 'X' is in the top right.

Добавление пользователя в группу

The image illustrates the steps to add a user to a group in Windows Active Directory. It consists of three main components:

- User List:** A table showing users. The 'teacher' user is selected, and a context menu is open with 'Добавить в группу...' (Add to group...) highlighted.
- 'Выбор: Группы' (Select: Groups) Dialog:** A dialog box for selecting a group. It shows the object type as 'Группы' (Groups) and the location as 'school.lan'. The 'Введите имена выбираемых объектов' (Enter the names of the objects to be selected) field contains 'teachers' (marked with a red circle and '1'). The 'Проверить имена' (Check names) button is also circled in red and marked with '2'.
- 'Свойства: teacher' (Properties: teacher) Dialog:** A dialog box showing the properties of the 'teacher' user. The 'Член групп' (Group memberships) tab is active, showing a list of groups. The 'teachers' group in the 'school.lan/TEACHERS' folder is highlighted (marked with a red circle and '3').

| Имя | Тип | Описание |
|----------|-----|----------|
| teacher | | |
| teachers | | |

Выбор: "Группы"

Выберите тип объекта:
"Группы" или "Встроенные субъекты безопасности" Типы объектов...

В следующем месте:
school.lan Размещение...

Введите имена выбираемых объектов (примеры):
teachers Проверить имена

Свойства: teacher

Член групп:

| Имя | Папка доменных служб Active Directory |
|-------------------|---------------------------------------|
| teachers | school.lan/TEACHERS |
| Пользователи д... | school.lan/Users |

Групповые политики

[К содержанию](#)

Групповые политики

Групповая политика (Group Policy Object, GPO) - механизм, позволяющий изменять различные параметры, связанные с операционной системой, пользователями и различными приложениями в графическом режиме при помощи **редактора** групповых политик.

Большинство настроек Windows возможны через реестр, редактор GPO это фактически и делает, но наглядным способом.

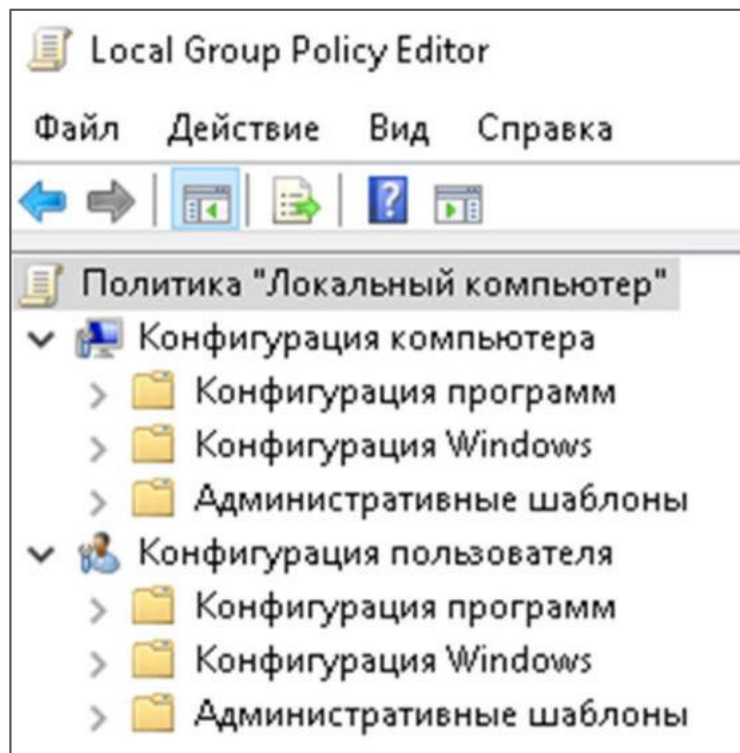
GPO представляет собой файлы в определенном формате, связанные (назначенные) определенным объектам.

Групповые политики подразделяются на:

- локальные (выполнить gpedit.msc)
- доменне (выполнить gpmc.msc)

Структура групповых политик

Групповая политика делится на две категории:



- **Конфигурация компьютера.** Политики этой категории применяются ко всему компьютеру независимо от пользователя. Например, если вы хотите применить политику надежности пароля для всех пользователей на компьютере или в домене, измените соответствующую политику в этой категории.
- **Конфигурация пользователя.** Политики этой категории применяются к пользователям, а не ко всему компьютеру, независимо от того, с какого компьютера пользователь входит в систему. Это, например, ограничения на доступ к отдельному ПО или скрипты при входе в систему.

Групповые политики в домене

В домене групповая GPO является объектом, который можно связать с сайтом, доменом и подразделением (в том числе с вложенными (дочерними) подразделениями).

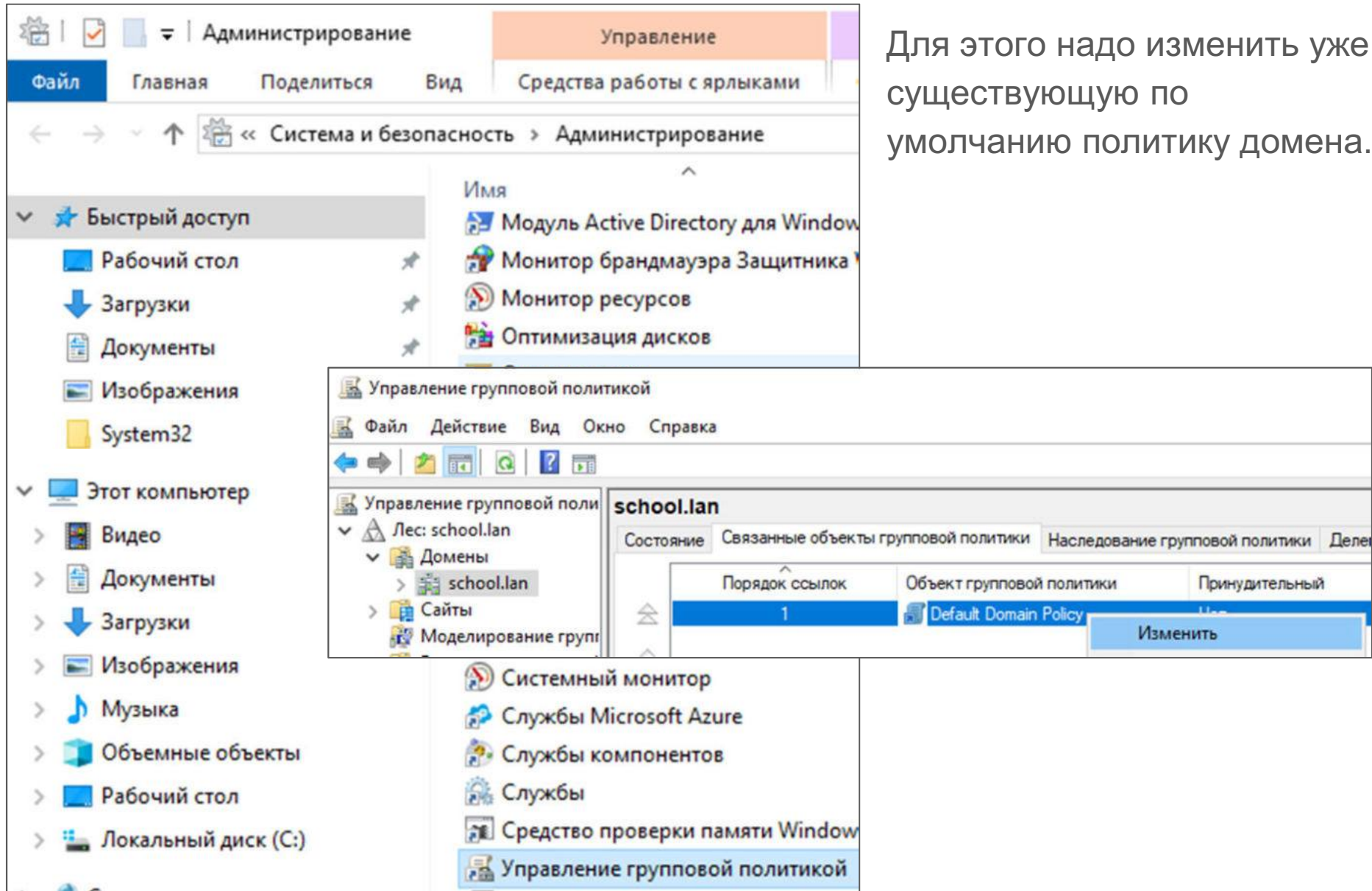
В случае наличия нескольких групповых политик сразу, порядок применения будет следующий:

1. Локальная групповая политика.
2. Групповая политика сайта.
3. Групповая политика домена.
4. Групповая политика верхнего подразделения.
5. Групповая политика дочернего подразделения.

Это надо учитывать и, при необходимости, отключать наследование GPO.

Политика сложности паролей в домене

Для этого надо изменить уже существующую по умолчанию политику домена.

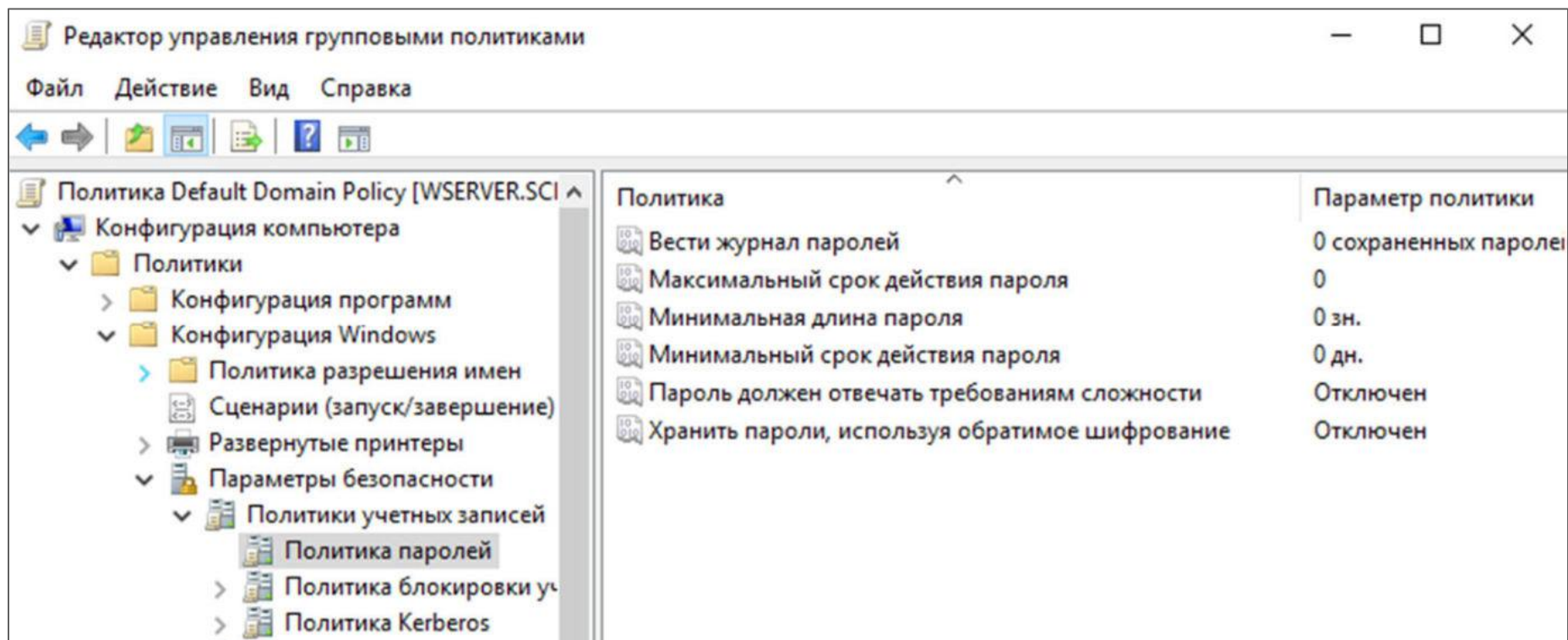


Политика сложности паролей в домене

Нужно привести параметры доменной групповой политики в вид, как на рис.

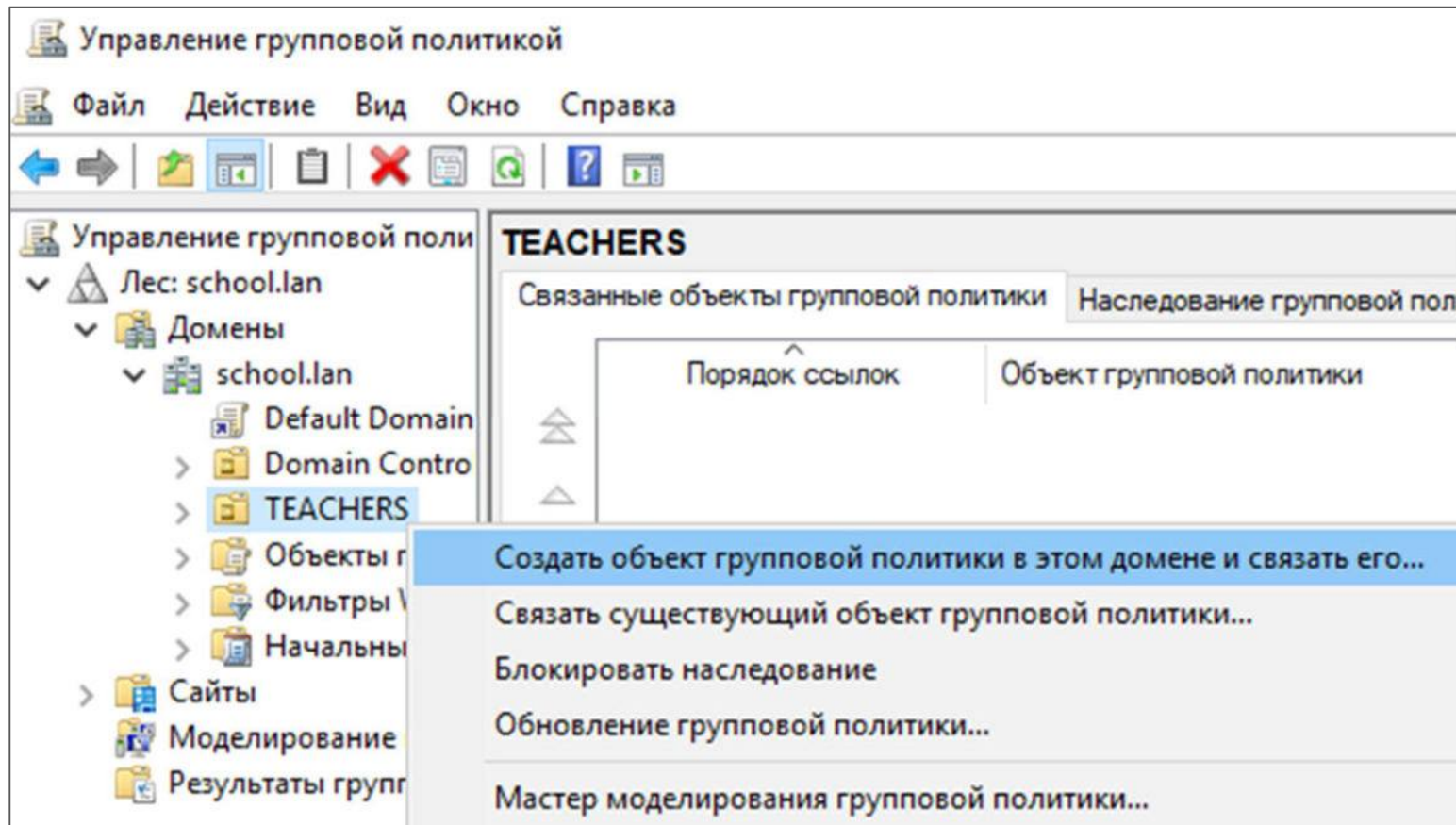
Политики из категории “Конфигурация компьютера” применяются только при загрузке ПК (поэтому лучше перезагрузить сервер).

Политики из категории “Конфигурация пользователя” применяются при логине ПК (достаточно “выйти и зайти”).



Создание объектов GPO

Чтобы не забивать настройками общую доменную политику, часто лучше создать несколько отдельных политик для определенных подразделений.

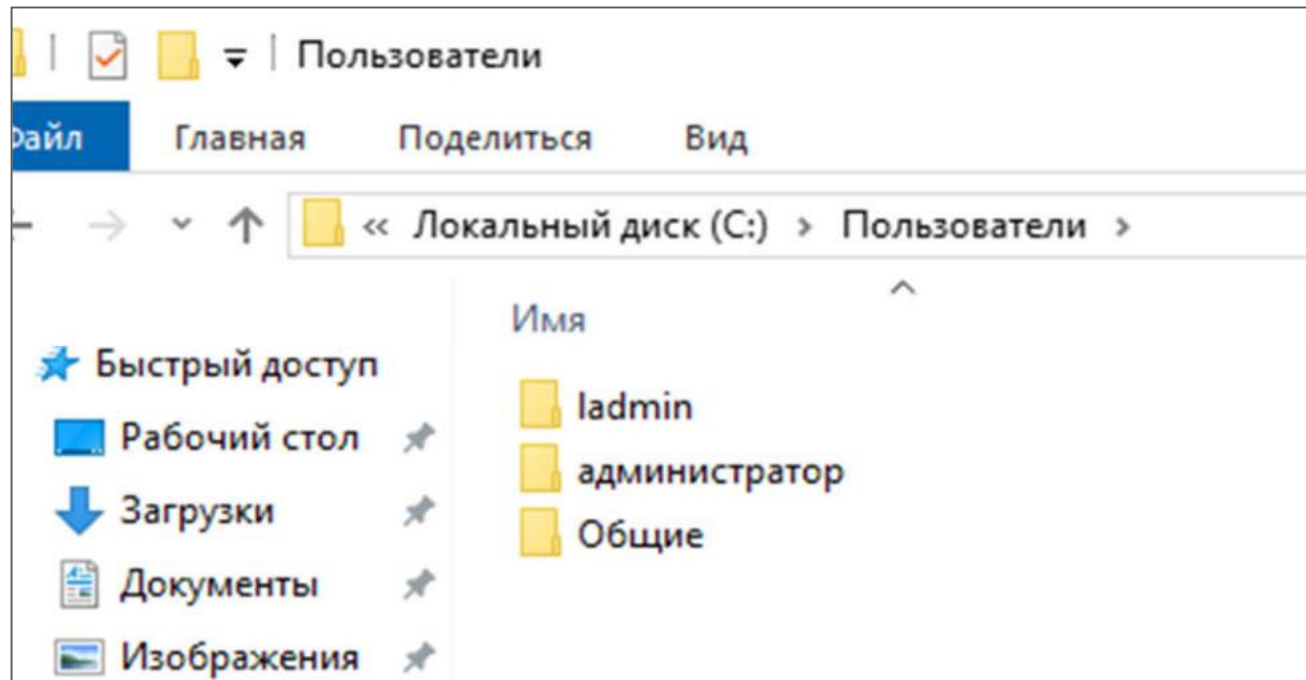


Профили пользователей

[К содержанию](#)

Профиль пользователя

Профиль пользователя Windows – это набор файлов и папок, которые закреплены за конкретной учетной записью. В профиле пользователя Windows находятся файлы, содержащие информацию об индивидуальных настройках операционной системы, о ярлыках программ и файлов, размещенных в меню Пуск, на панели задач или Рабочем столе.



Типы профилей

Профили подразделяются на:

- **локальные** (привязаны к локальному ПК)
- **перемещаемые** (за счет хранения в сети, синхронизируются и копируются пользователю при входе на любую доменную машину)

Перемещаемые профили могут быть также:

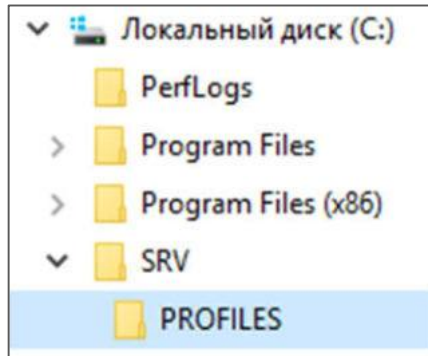
- **общими** (едиными для нескольких пользователей)
- **обязательными** (не сохраняющими изменения)

В домене при большом количестве однотипных пользователей удобно создать один перемещаемый общий обязательный профиль, тогда не надо “переживать” за изменение внешнего вида рабочего стола учениками.

Персональные данные хранятся на индивидуальных сетевых каталогах.

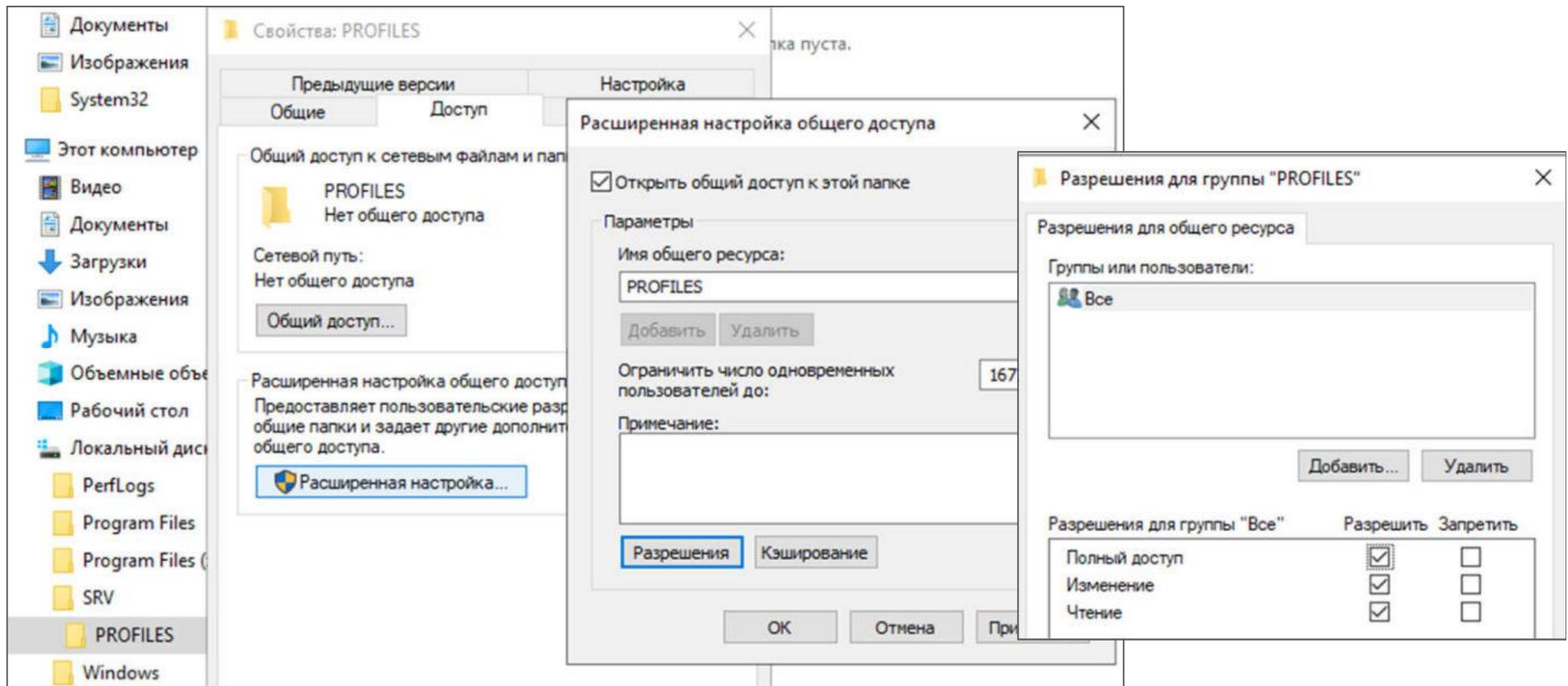
[Документация на сайте microsoft.](#)

Подготовка каталогов на сервере



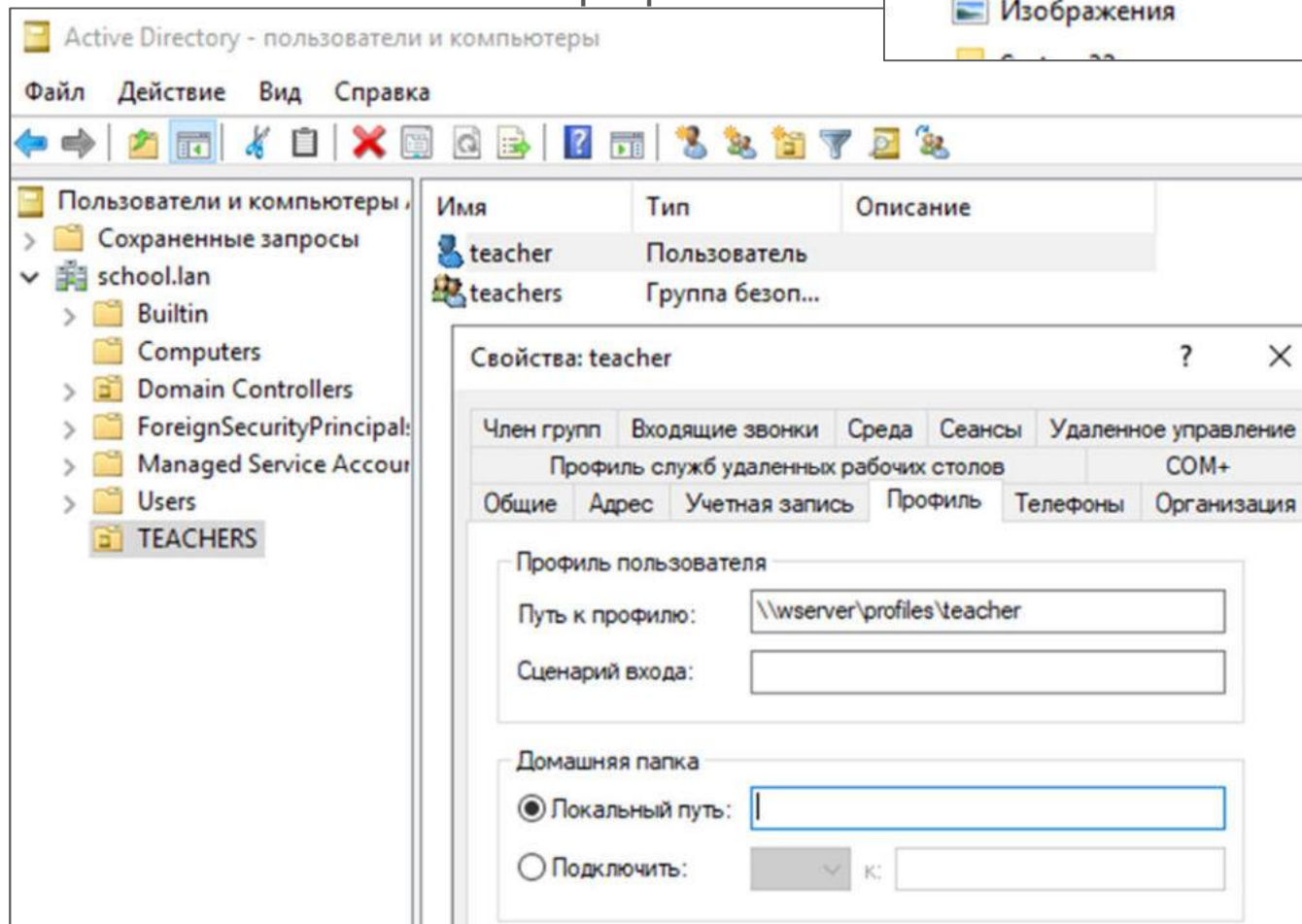
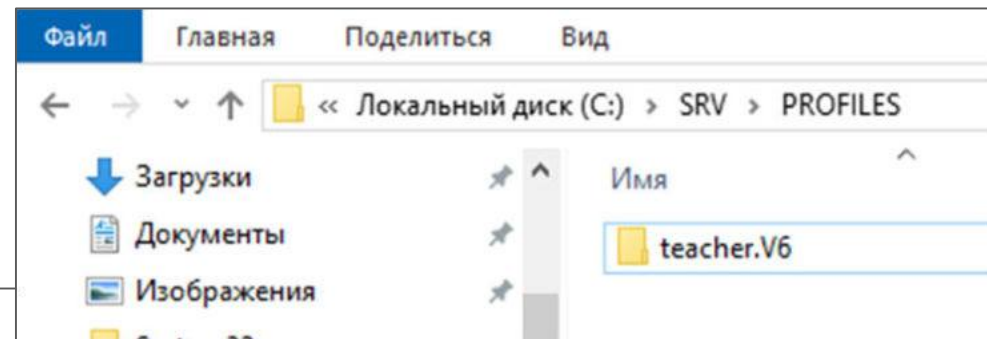
Создаём на сервере каталоги SRV и внутри PROFILES.

PROFILES делаем доступным всем как сетевую папку.



Перемещаемый профиль в AD

Указываем в AD путь к профилю.
После первого входа пользователя на рабочую станцию на сервере появится каталог с его профилем.

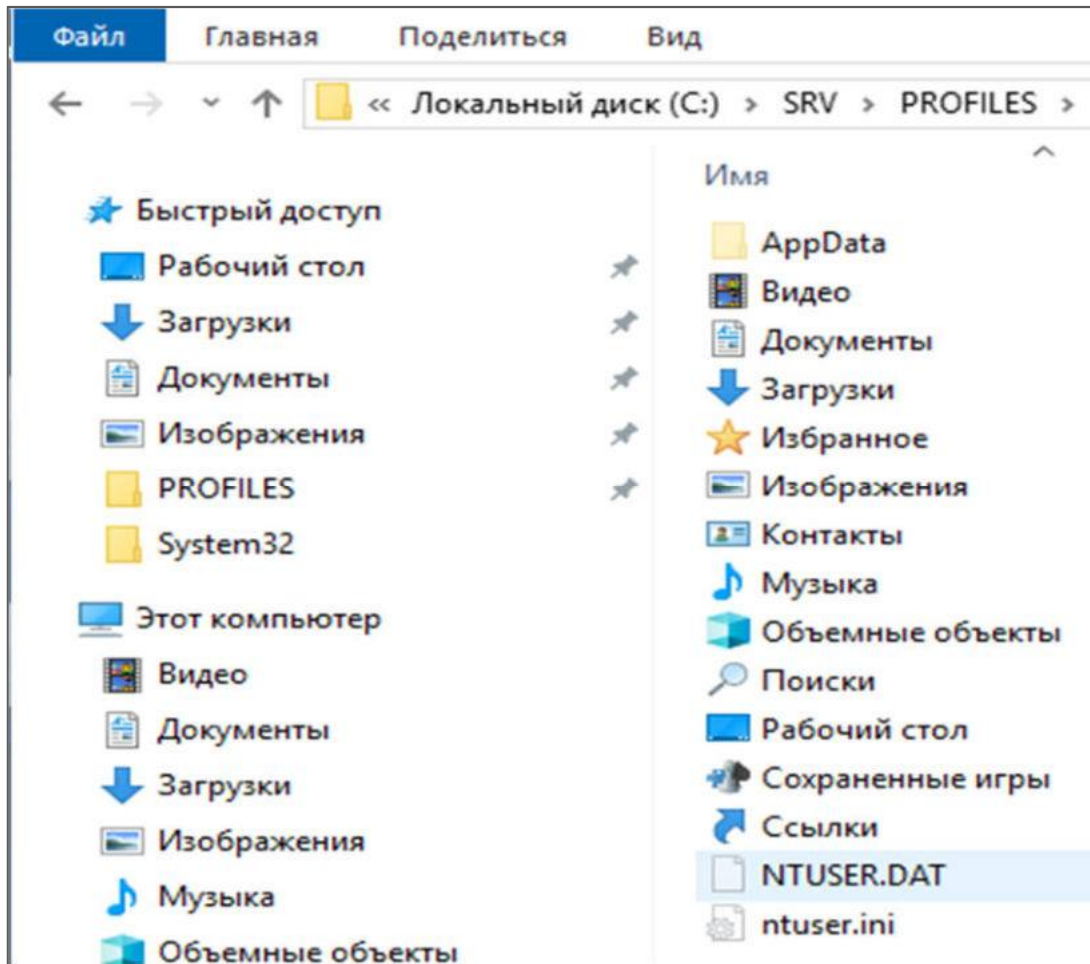


Профиль доступен только данному пользователю.

При входе он будет подгружаться, при выходе - выгружаться на сервер.

На локальных машинах будут оставаться копии профиля для ускорения загрузки.

Обязательный профиль



Для “обязательности” надо изменить расширение файла NTUSER.DAT на NTUSER.MAN

После этого профиль будет при входе копироваться на локальную машину, а потом НЕ копироваться обратно на сервер, откидывая, соответственно, все изменения и файлы.

Локальную копию профиля можно удалять через групповые политики.

Разрешения на каталог с обязательным профилем можно сделать так:

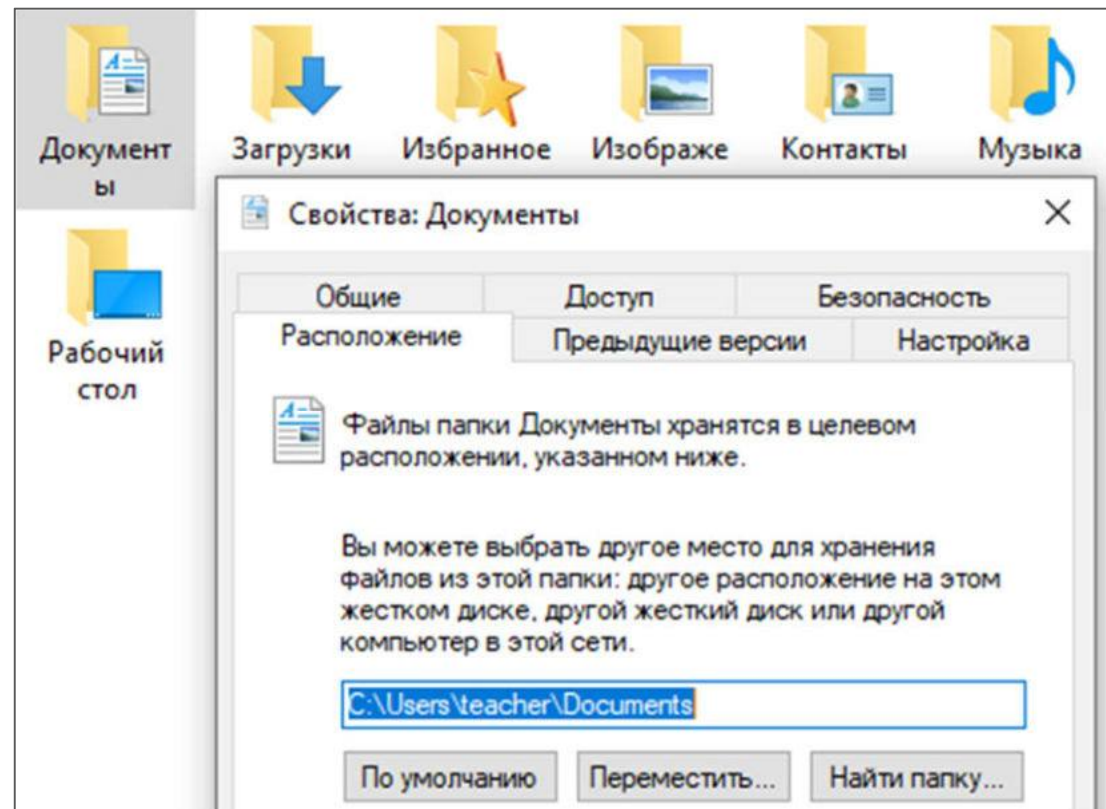
| Элементы разрешений: | | | |
|----------------------|------------------------------|---------------------|--|
| Тип | Субъект | Доступ | |
| Разр... | СИСТЕМА | Полный доступ | |
| Разр... | teacher (teacher@school.lan) | Чтение и выполнение | |
| Разр... | Администраторы (SCHOOL\... | Полный доступ | |

Управление обязательным профилем

При необходимости внесения изменений в профиль, можно переименовать MAN в DAT, настроить разрешения пользователю на “полный доступ”, войти пользователем, внести изменения, выйти и переименовать обратно, выставив разрешения “на чтение”..

Так как из “загрузок” и “рабочего стола” всё будет удаляться, пользователям надо привыкнуть...

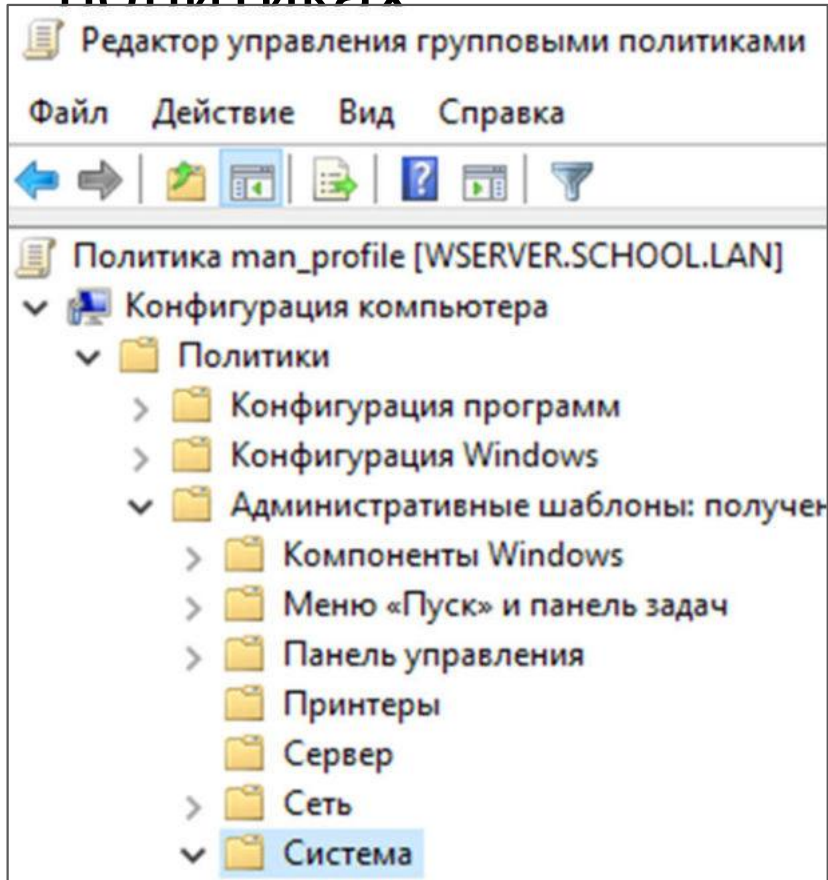
Для сохранения файлов можно в профиле настроить ярлыки на локальные или сетевые каталоги с доступом пользователю на чтение или перенаправить на такие расположения некоторые каталоги из профиля (например, “документы”).



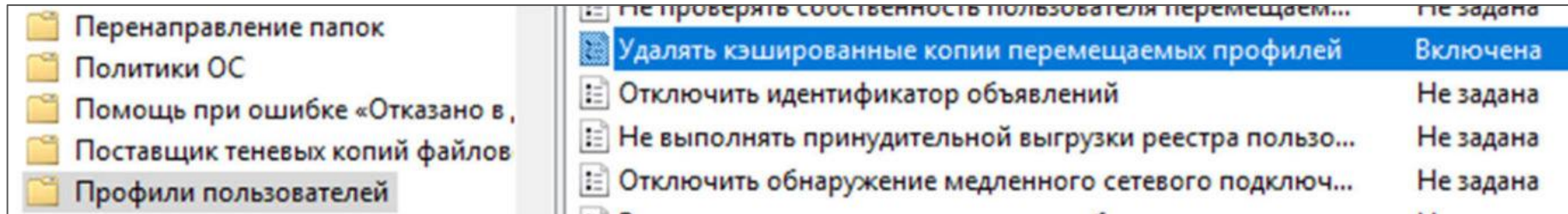
Неудобства перемещаемого профиля

1. Если не делать профиль обязательным, то, по опыту, пользователи хранят очень много данных на рабочем столе и в загрузках (загрузки, фильмы, например), что сильно замедляет вход-выход из системы из-за синхронизации с сервером. Начинаются жалобы + “забивается” сеть.
2. Т.к. на ПК остаются локальные копии, то несколько перемещаемых профилей могут “съесть” все пространство на диске “С”.
3. Настройки групповой политики по удалению локальных кэшированных профилей не всегда срабатывают корректно, иногда приходится это делать вручную.
4. Если профиль обязательный, то можно сделать его **общим** сразу для всех пользователей.

Удаление копий профилей в групповых политиках



Надо в групповых политиках включить следующий параметр (действует после перезагрузки клиентов):



Общий профиль в Windows 10

[К содержанию](#)

Создание общего обязательного профиля

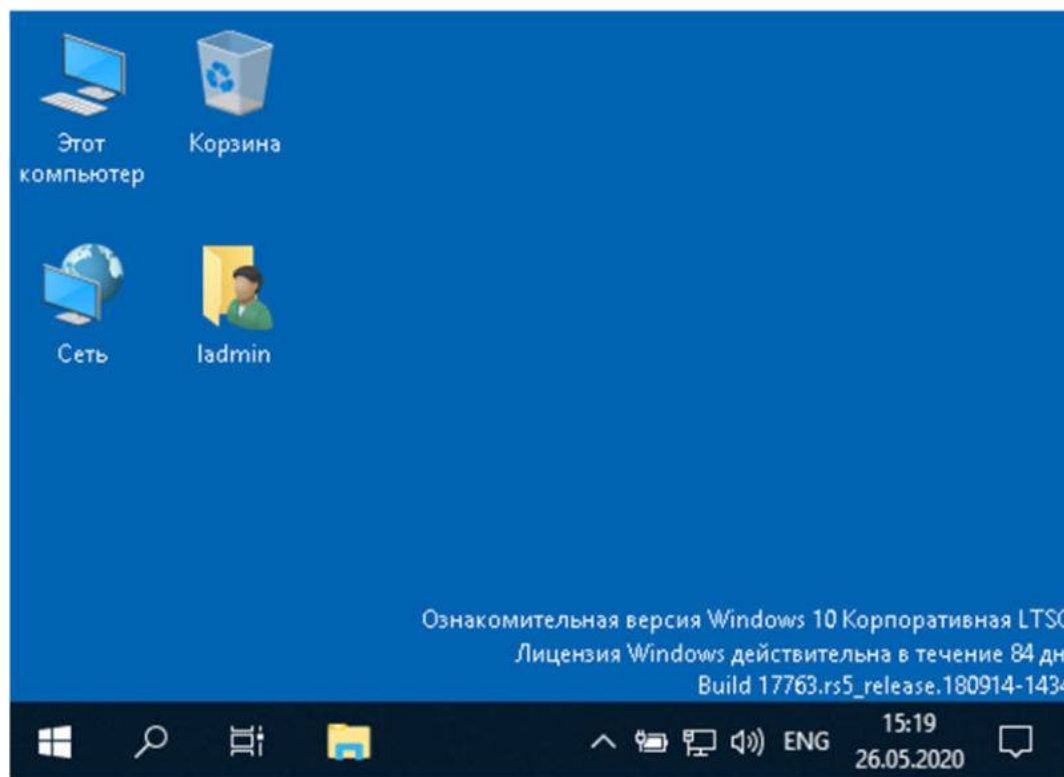
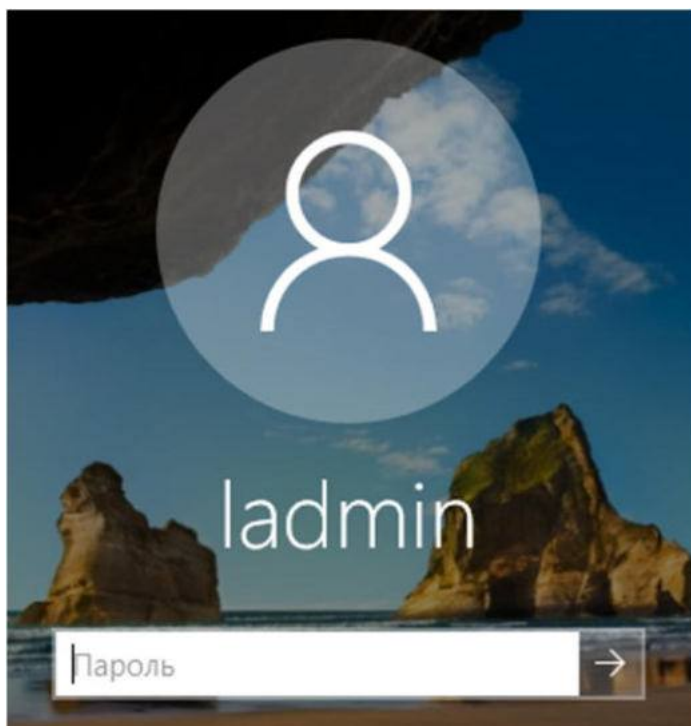
Этапность:

1. Настройка профиля на тестовой машине
2. Перенос профиля в “профиль по умолчанию”
3. Копирование профиля “по умолчанию” на сервер
4. Назначение профиля как перемещаемого

В Windows 10 процедура не самая явная, в ранних версиях п1 и 2 не было..

Настройка профиля на тестовой машине

Входим на тестовую машину под администратором и настраиваем внешний вид на свой вкус. На самом деле неважно, после можно будет донастроить.



Перенос профиля в “профиль по умолчанию”

1. Создаём файл unattend.xml следующего содержания (“amd64” поменять на “x86”, если версия 32 бита) и сохраняем на диск C:

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
  <settings pass="specialize">
    <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <CopyProfile>true</CopyProfile>
    </component>
  </settings>
</unattend>
```

Параметр CopyProfile указывает, что программа Sysprep (утилита системной подготовки Microsoft Windows к развертыванию) копирует папку профиля пользователя, выполнившего вход в настоящее время, в профиль пользователя по умолчанию.

2. Запускаем команду

```
C:\Windows\System32\Sysprep\sysprep.exe /oobe /reboot /generalize /unattend:c:\unattend.xml
```

Ошибки sysprep

В случае ошибки sysprep указывает файл, где указаны проблемы с запуском.

В случае Windows 10 LTSC 1809, используемой в данном курсе, ошибка вызвана наличием пакета локализации (русификации). Для дальнейшей работы в данной версии его придется удалить (потом поставим обратно).

Штатными средствами подобный пакет не удалить. Придется использовать средства PowerShell (“продвинутая” командная строка Windows).

Запускаем PowerShell (можно в поиске) и выполняем команду:

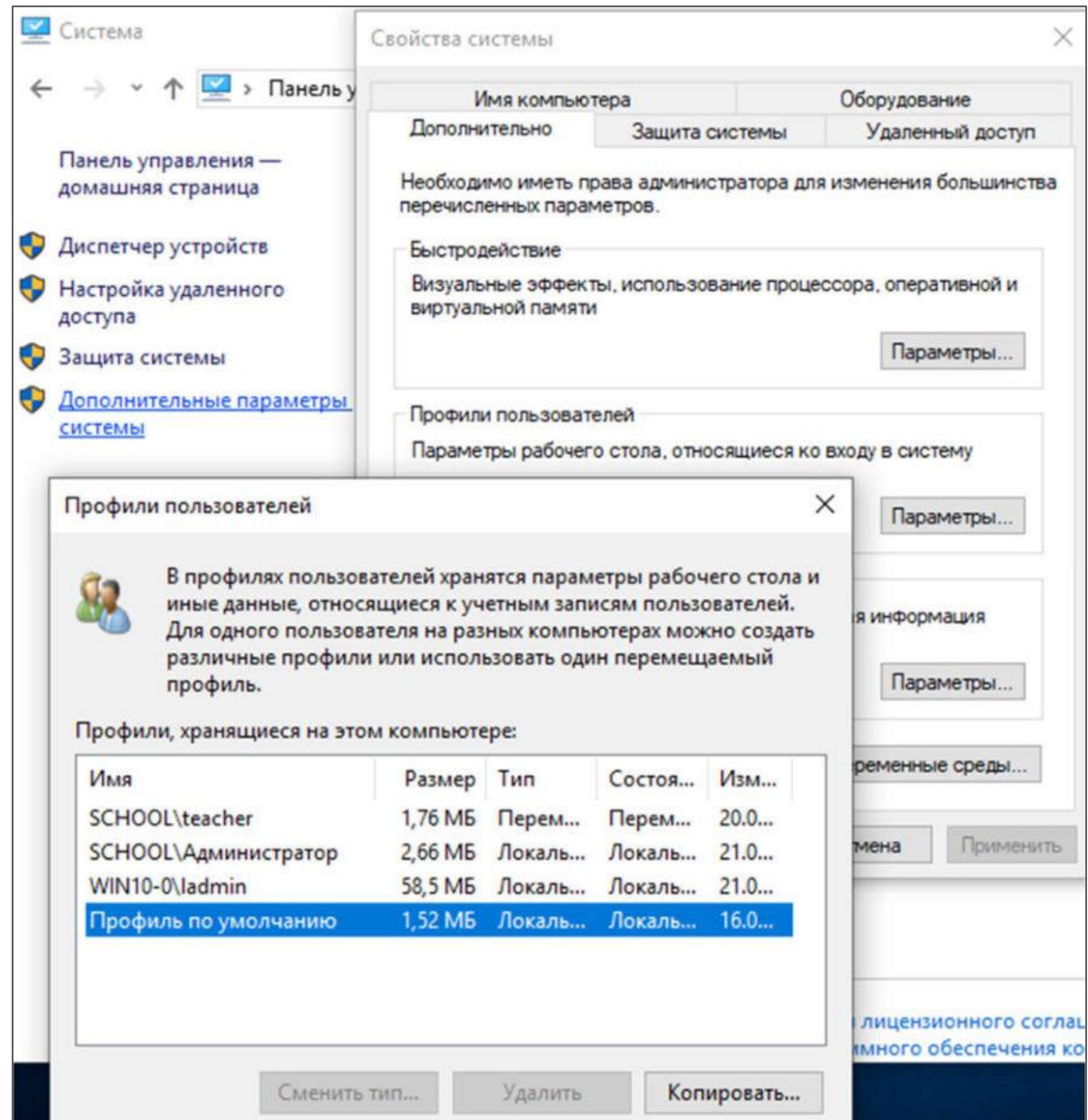
```
Get-AppxPackage Microsoft.LanguageExperiencePackru-RU | Remove-AppxPackage
```

Если всё верно, то Windows станет “английским”, зато sysprep запустится и отработает.

Sysprep возвращает образ ОС в начальное состояние, сбрасывает имя ПК, отключает от домена и т.п., поэтому лучше делать на свежестановленном образе в виртуальной машине.

Копирование профиля “по умолчанию” на сервер

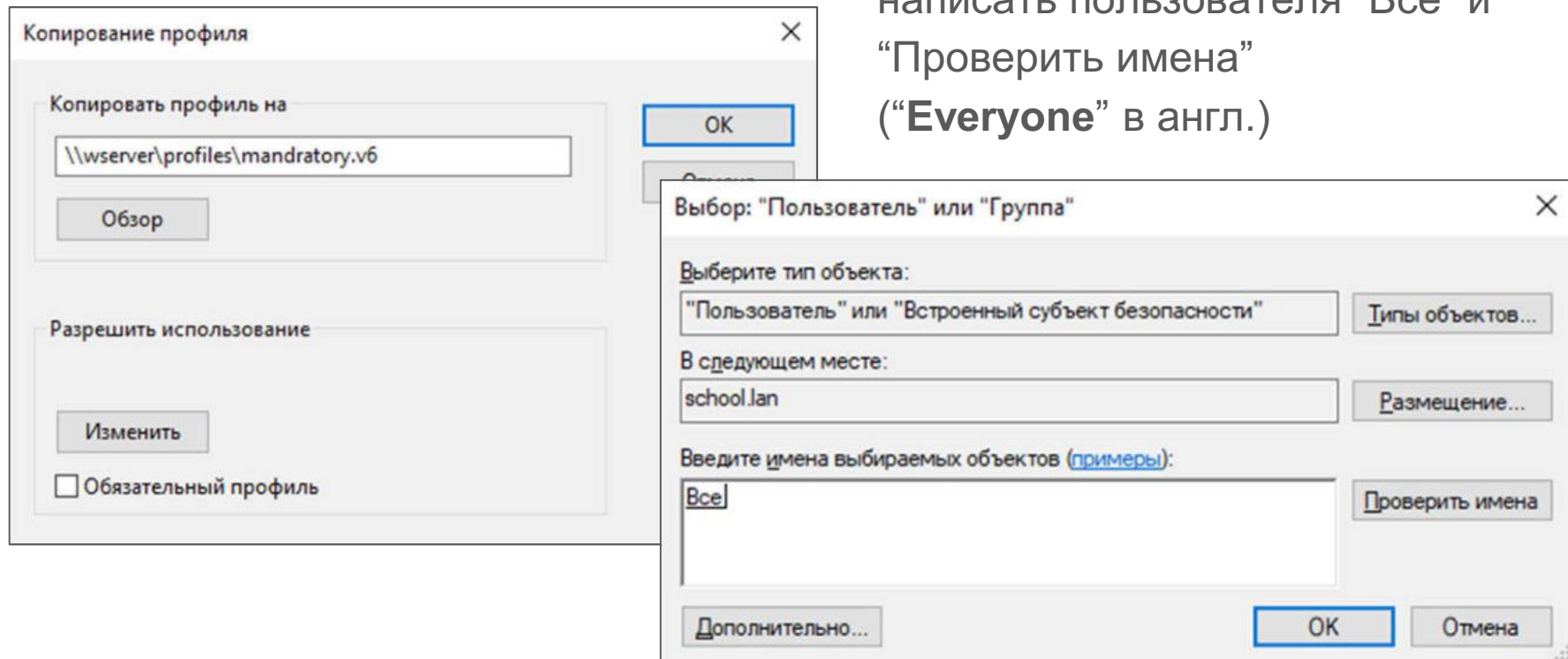
1. Заходим на клиентскую машину под администратором.
2. Копируем “Профиль по умолчанию” на сервер.



Копирование профиля “по умолчанию” на сервер

Копируем в папку с расширением .v6
(для Win10). Обязательно!

!!! В “Разрешить использование”
написать пользователя “Все” и
“Проверить имена”
(“**Everyone**” в англ.)



Только потом нажимаем “OK” для копирования.

Можно скопировать профиль в папку на локальном диске, а потом перенести на сервер.

Назначение профиля как перемещаемого

1. Назначаем в AD пользователю созданный ему перемещаемый профиль.
2. Даём полный доступ пользователю.
3. Заходим на клиенте, настраиваем профиль. (Русифицируем). Выходим.
4. На сервере переименовываем NTUSER.DAT в NTUSER.MAN.

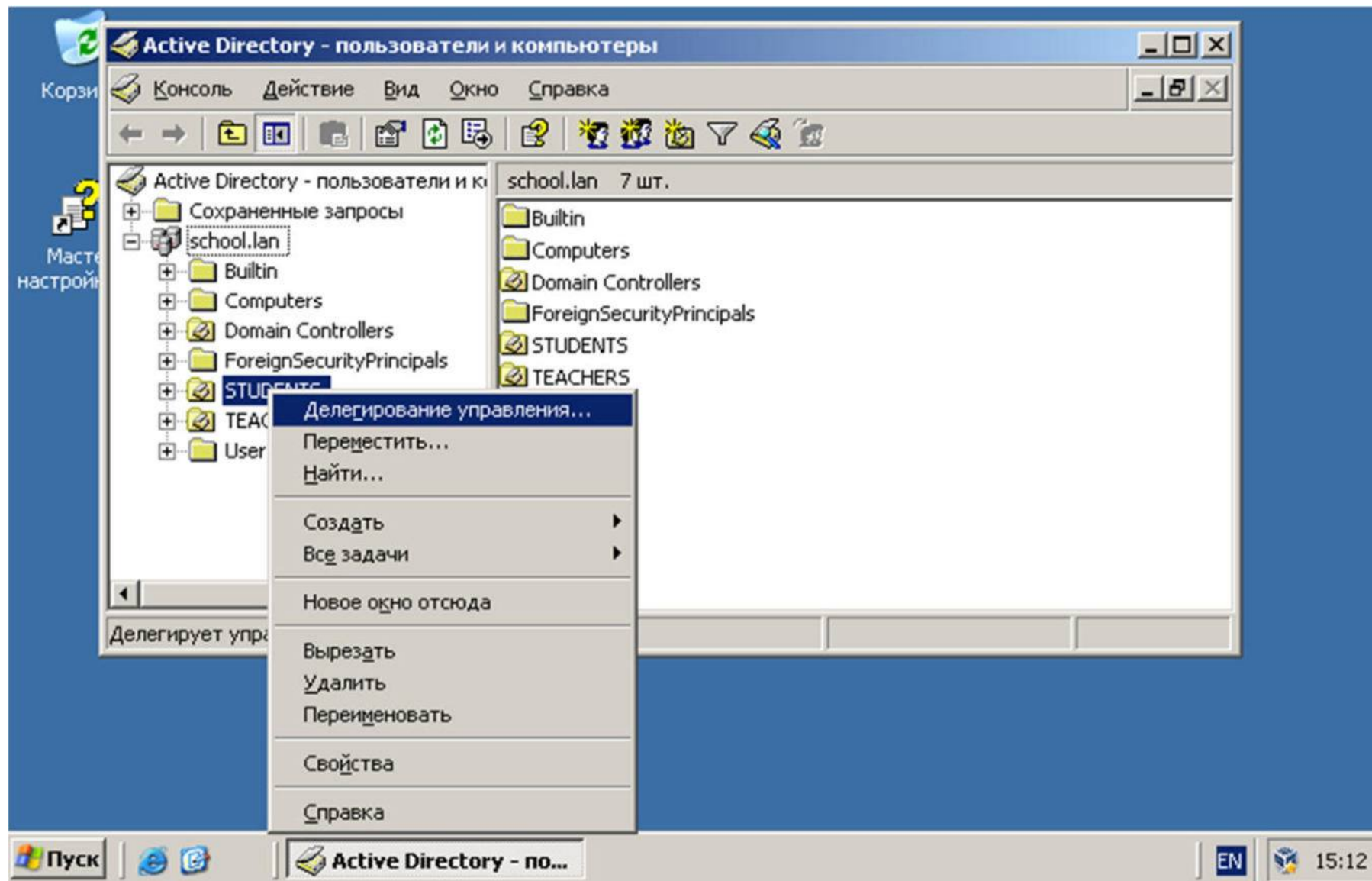
Делаем всё как с обычным перемещаемым профилем, только теперь он еще и общий, соответственно, его можно назначать любому количеству пользователей.

Для внесения изменений рекомендую разрешить полный доступ к профилю на сервере только 1 пользователю (“дежурному”). Переименовывая MAN в DAT и входя под этим пользователем, можно вносить изменения в общий профиль - настраивать ярлыки, внешний вид, стартовую страницу и т.п.

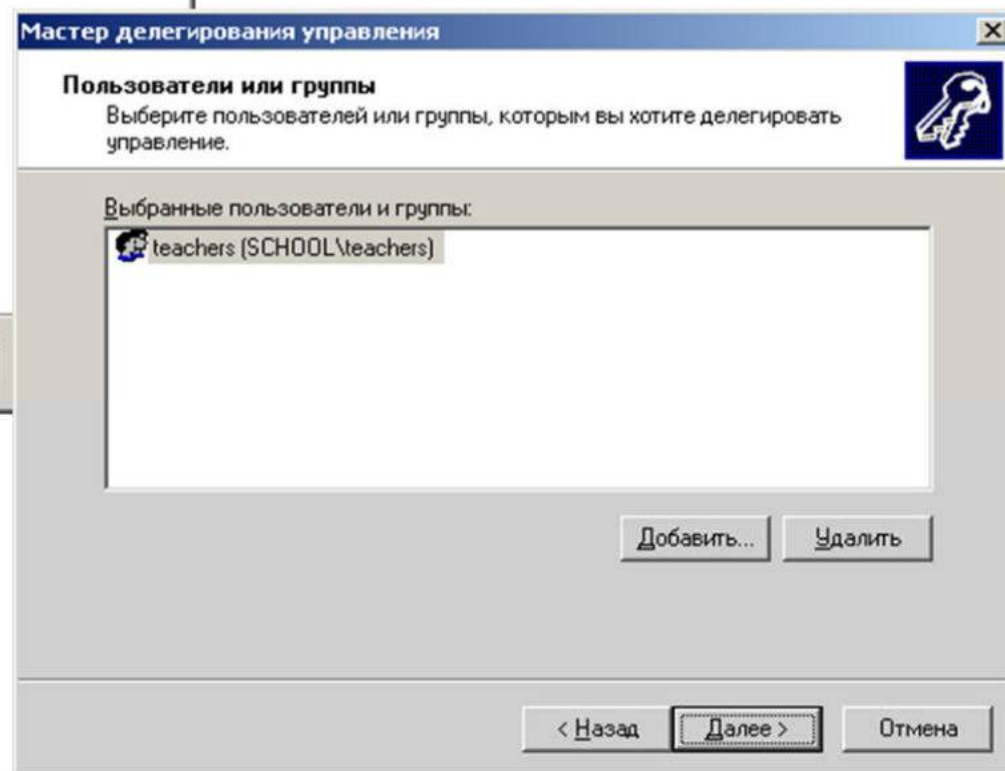
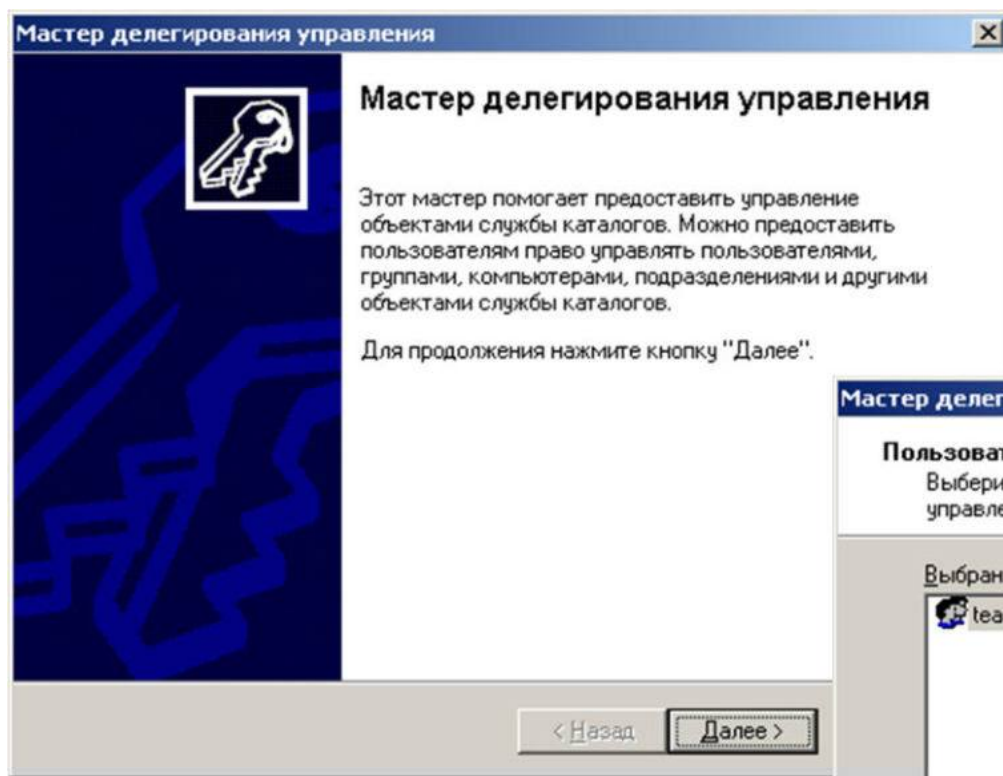
По [данной ссылке](#) выложен файл unattend.xml и уже готовый профиль.

Делегирование полномочий в домене Active Directory

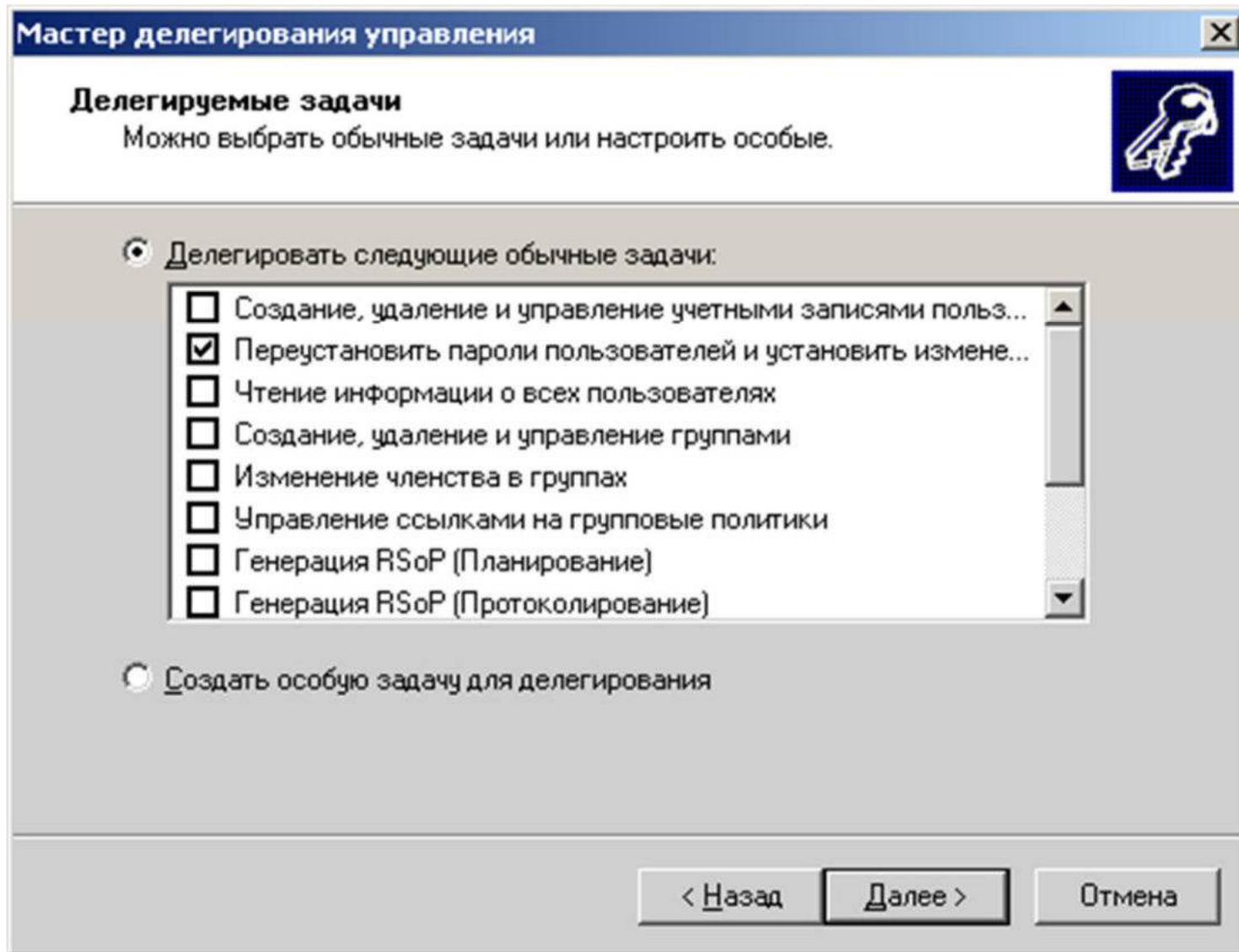
Предоставление прав



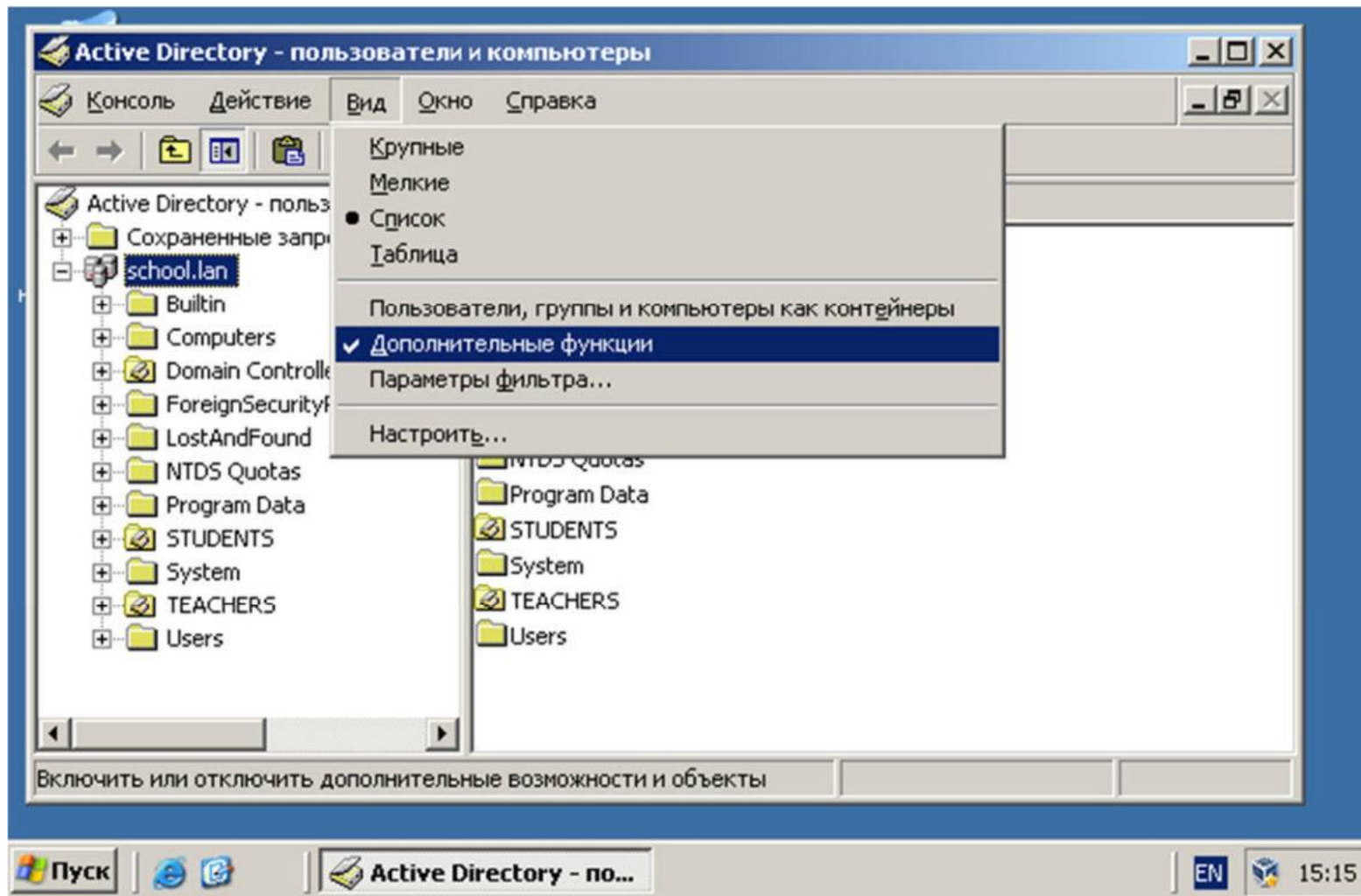
Кому делегируем



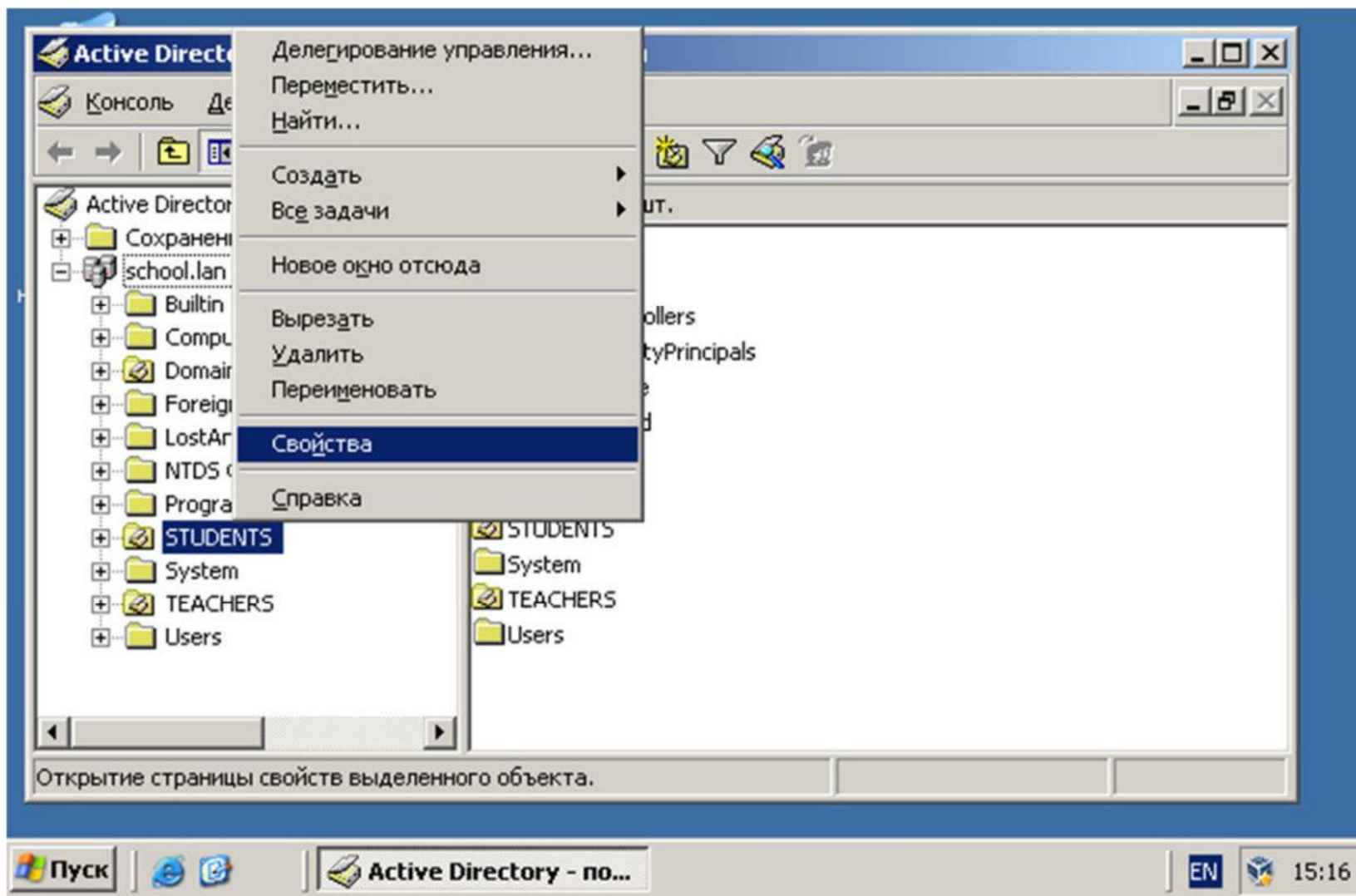
Что делегируем



Просмотр делегированных прав.
Включаем “дополнительные функции”:



Просмотр делегированных прав.



Просмотр делегированных прав.

Свойства: STUDENTS

Общие | Управляется | Об...
Безопасность | COM+ | Групповая п...

Группы или пользователи:

- SYSTEM
- teachers (SCHOOL\teachers)
- Администраторы (SCHOOL\Администраторы)
- Администраторы домена (SCHOOL\Администраторы домена)
- Администраторы предприятия (SCHOOL\Администраторы предприятия)

Разрешения для teachers

| | |
|---------------------------------|--------------------------|
| Полный доступ | <input type="checkbox"/> |
| Чтение | <input type="checkbox"/> |
| Запись | <input type="checkbox"/> |
| Создание всех дочерних объектов | <input type="checkbox"/> |
| Удаление всех дочерних объектов | <input type="checkbox"/> |
| Генерация RSoP (Планирование) | <input type="checkbox"/> |

Дополнительно

ОК | Отмена | Применить

Дополнительные параметры безопасности для STUDENTS

Разрешения | Аудит | Владелец | Действующие разрешения

Для просмотра сведений об особых разрешениях выберите элемент разрешения и нажмите кнопку "Изменить".

Элементы разрешений:

| Тип | Имя | Разрешение | Унаследовано... | Применять к |
|----------|-----------------------|------------------|------------------|---------------------|
| Разре... | teachers (SCHOOL\... | Чтение и запи... | <не унаследов... | Пользователь объ... |
| Разре... | teachers (SCHOOL\... | Сброс пароля | <не унаследов... | Пользователь объ... |
| Разре... | SYSTEM | Полный доступ | <не унаследов... | Только этот объект |
| Разре... | Администраторы д... | Полный доступ | <не унаследов... | Только этот объект |
| Разре... | Операторы учета (...) | Создание/уда... | <не унаследов... | Только этот объект |
| Разре... | Операторы учета (...) | Создание/уда... | <не унаследов... | Только этот объект |
| Разре... | Операторы учета (...) | Создание/уда... | <не унаследов... | Только этот объект |
| Разре... | Операторы печати ... | Создание/уда... | <не унаследов... | Только этот объект |

Добавить... | Изменить... | Удалить

Разрешить наследование разрешений от родительского объекта к этому объекту и его дочерним объектам, добавляя их к разрешениям, явно заданным в этом окне.

Чтобы заменить все элементы разрешений значениями по умолчанию, нажмите кнопку "По умолчанию".
Подробнее об [управлении доступом](#).

По умолчанию

ОК | Отмена | Применить

Файловый сервер

[К содержанию](#)

Сетевой каталог

При создании сетевых каталогов можно руководствоваться следующим:

1. Права безопасности устанавливаются для каталога и на SMB (протокол сетевого доступа-сетевая файловая система) и на NTFS (дисконвая файловая система), но NTFS позволяет изменять права для подкаталогов. Поэтому для SMB делаем полный доступ всем, а ограничения - на уровне NTFS.
2. Имя каталога SMB может отличаться от NTFS, добавление символа \$ к имени SMB делает каталог скрытым (для Windows-машин).
3. На NTFS-уровне не забываем следить за наследованием прав безопасности - оставляйте только нужные.
4. Пользователям "СИСТЕМА" и "Администраторы" всегда делайте полный доступ.
5. Сетевые каталоги создавайте на отдельном диске или разделе.





Создание общего каталога

Сделать каталог, доступный учителям на запись, ученикам только для чтения.

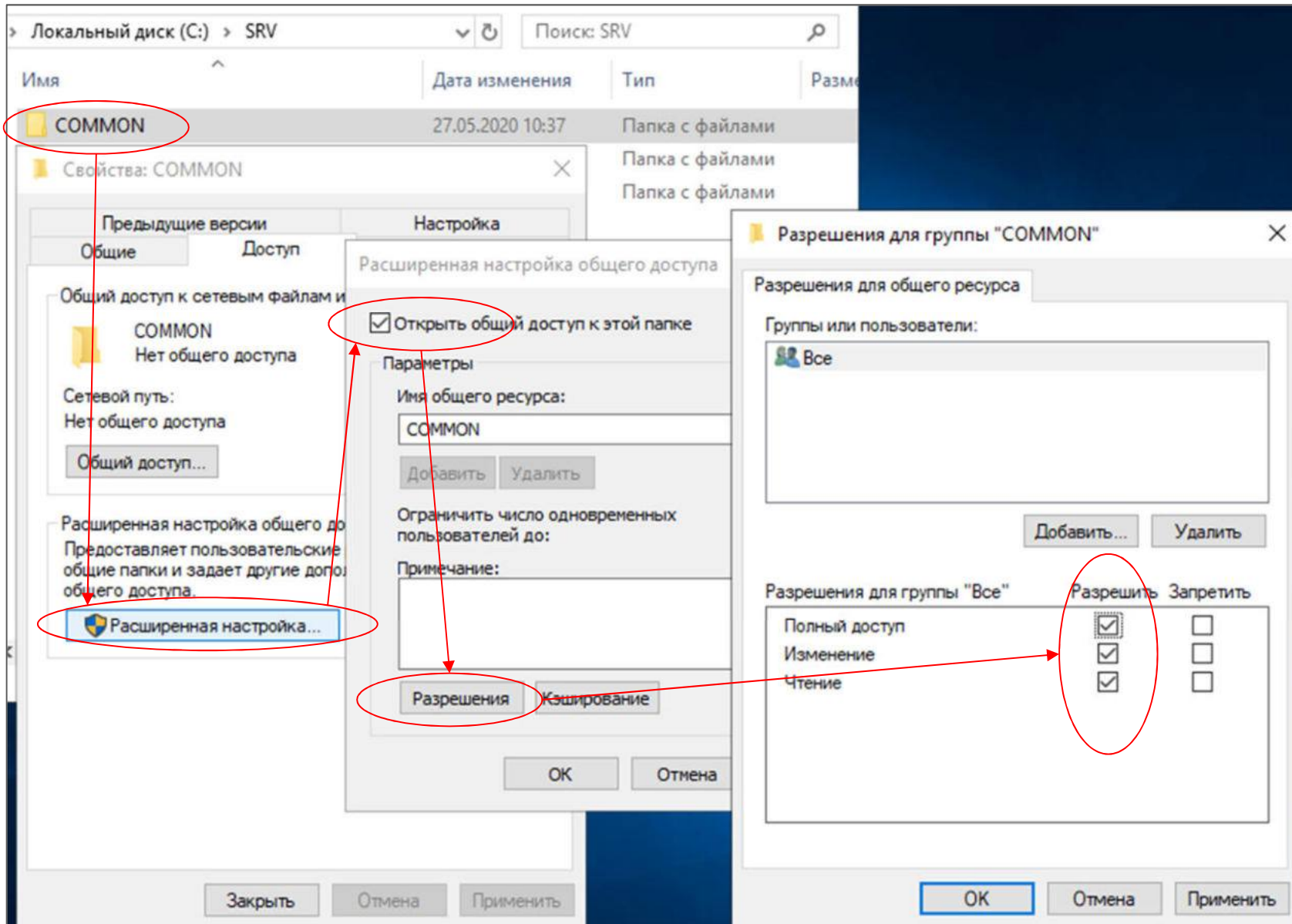
1. Создать каталог COMMON в C:\SRV.
2. Создать в AD группы безопасности “teachers” и “students”
3. Настроить сетевую (SMB) доступность
4. Настроить NTFS-безопасность

Итоговые права безопасности должны выглядеть следующим образом (но сначала отключить наследование):

Элементы разрешений:

| | Тип | Субъект | Доступ | Унаследовано от | Применяется к |
|---|---------|----------------------------|---------------------|-----------------|---------------------------------|
|  | Разр... | students (SCHOOL\students) | Чтение и выполнение | Нет | Для этой папки, ее подпапок ... |
|  | Разр... | teachers (SCHOOL\teachers) | Полный доступ | Нет | Для этой папки, ее подпапок ... |
|  | Разр... | СИСТЕМА | Полный доступ | Нет | Для этой папки, ее подпапок ... |
|  | Разр... | Администраторы (SCHOOL\... | Полный доступ | Нет | Для этой папки, ее подпапок ... |

Уровень SMB



Уровень NTFS. Отключение наследования

Свойства: COMMON

Настройка Безопасность

Имя объекта: C:\SRV\COMMON

Группы или пользователи:

- СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ
- СИСТЕМА
- Администраторы (SCHOOL\Администраторы)
- Пользователи (SCHOOL\Пользователи)

Разрешения для группы "СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ"

| Разрешение | Разрешить | Запретить |
|--------------------------|--------------------------|--------------------------|
| Полный доступ | <input type="checkbox"/> | <input type="checkbox"/> |
| Изменение | <input type="checkbox"/> | <input type="checkbox"/> |
| Чтение и выполнение | <input type="checkbox"/> | <input type="checkbox"/> |
| Список содержимого папки | <input type="checkbox"/> | <input type="checkbox"/> |
| Чтение | <input type="checkbox"/> | <input type="checkbox"/> |
| Запись | <input type="checkbox"/> | <input type="checkbox"/> |

Дополнительно

Отключение наследования

Замени все записи разрешений дочернего объекта наследуемыми от этого объекта

Блокировать наследование

Что вы хотите сделать с текущими унаследованными разрешениями?

Наследование для данного объекта будет заблокировано. В результате разрешения, унаследованные от родительского объекта, больше не будут применимы к данному объекту.

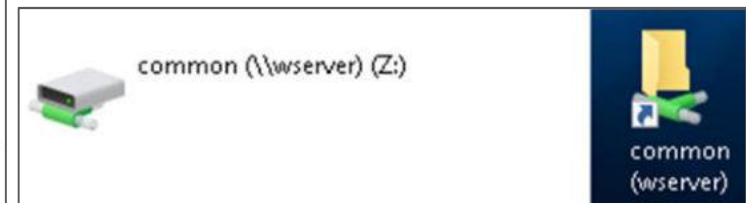
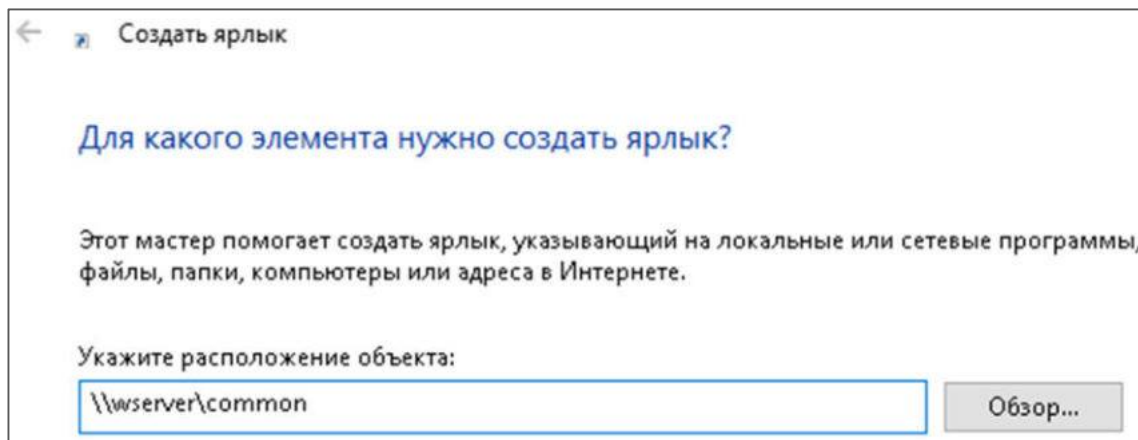
- Преобразовать унаследованные разрешения в явные разрешения этого объекта.
- Удалить все унаследованные разрешения из этого объекта.

Подключение общего каталога пользователям

Подключить общий каталог можно

1. **К букве диска.** (Настроить шаблонный профиль, или в групповых политиках, или скриптом\командой при старте (`net use z: \\wserver\common`) в настройках пользователя, или в автозагрузке).
2. **Ярлыком** на рабочем столе (можно через общий профиль).

Из опыта, с точки зрения безопасности, ярлык намного предпочтительней, т.к. к буквам диска часто пытаются прицепиться вирусы с файлом “autorun”, который стартует при двойном клике именно на букве диска, один неаккуратный пользователь заразит всю сеть. С ярлыками таких проблем нет...



Домашние персональные каталоги через AD

Персональные каталоги - способ хранения данных пользователя в сетевой папке, доступной только этому пользователю (иногда группе). Способ очень важен при использовании общих профилей, там все данные в профиле удаляются.

Создание ресурса для хранения персональных каталогов учителей (C:\SRV\THOMES, отключаем наследование, права как на рисунке):

Имя: C:\SRV\THOMES
Владелец: Администраторы (SCHOOL\Администраторы) Изменить

Разрешения | Аудит | Д

Для получения дополнительных сведений дважды щелкните элемент и нажмите кнопку "Изменить" (если она доступна).

Элементы разрешений:

| Тип | Субъект | Доступ | |
|-----|---------|----------------------------|---------------|
| | Разр... | СИСТЕМА | Полный доступ |
| | Разр... | Администраторы (SCHOOL\... | Полный доступ |

Свойства: THOMES | Расширенная настройка

Общие

Общий доступ к сетевым папкам

THOMES
Нет общего доступа

Сетевой путь:
Нет общего доступа

Общий доступ...

Расширенная настройка

Предоставляет пользователям возможность открывать общие папки и задавать параметры общего доступа.

Расширенная настройка

Расширенная настройка

Открыть общий доступ

Параметры

Имя общего ресурса:
THOMES

Добавить... Удалить...

Ограничить число пользователей, имеющих доступ к папке

Примечание:

Разрешения

Разрешения для группы "THOMES"

Разрешения для общего ресурса

Группы или пользователи:

Все

Добавить...

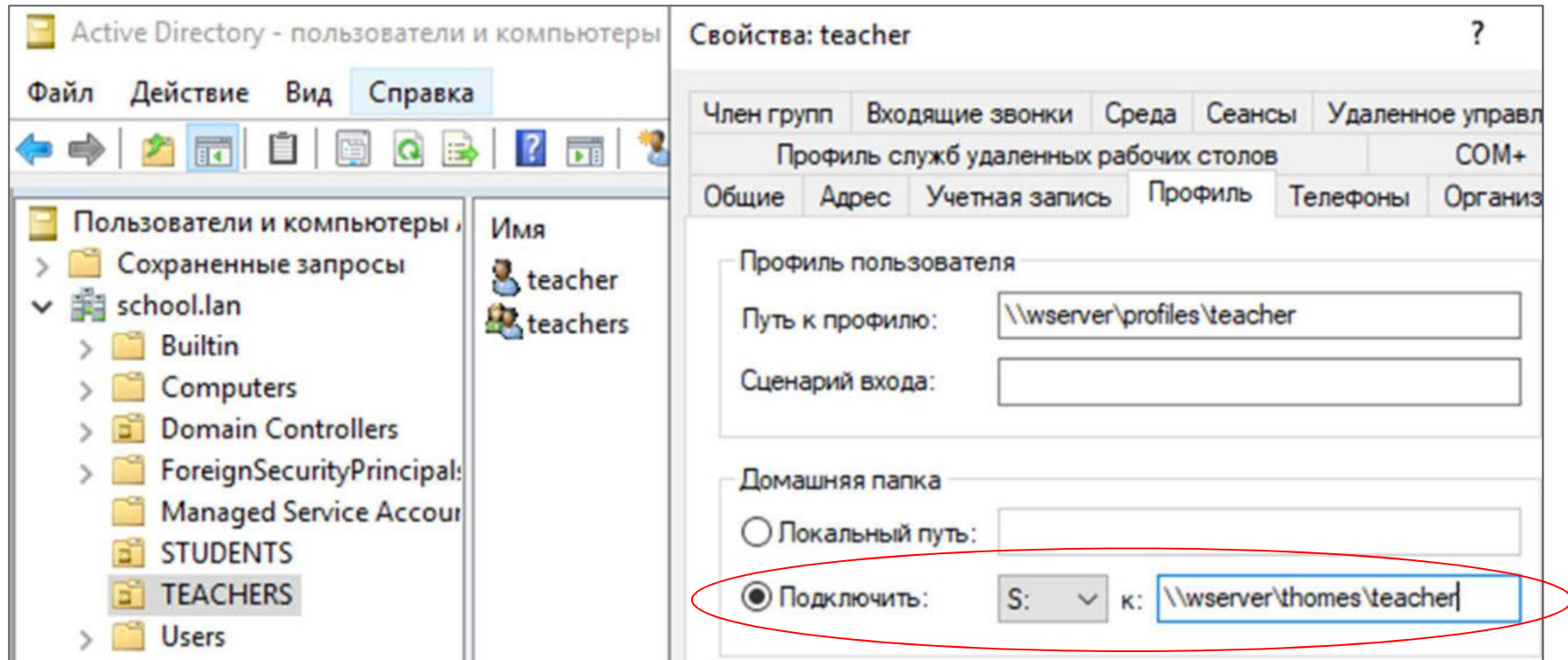
Разрешения для группы "Все"

| Разрешения | Разрешить |
|---------------|-------------------------------------|
| Полный доступ | <input checked="" type="checkbox"/> |
| Изменение | <input checked="" type="checkbox"/> |
| Чтение | <input checked="" type="checkbox"/> |

Домашние персональные каталоги через AD

Назначаем путь к домашнему каталогу в AD.

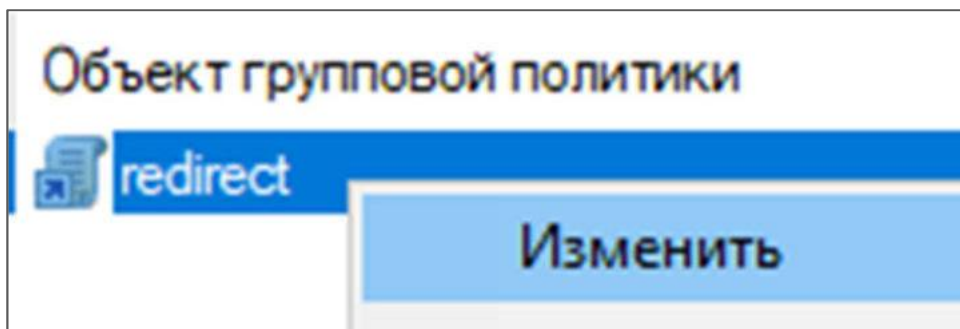
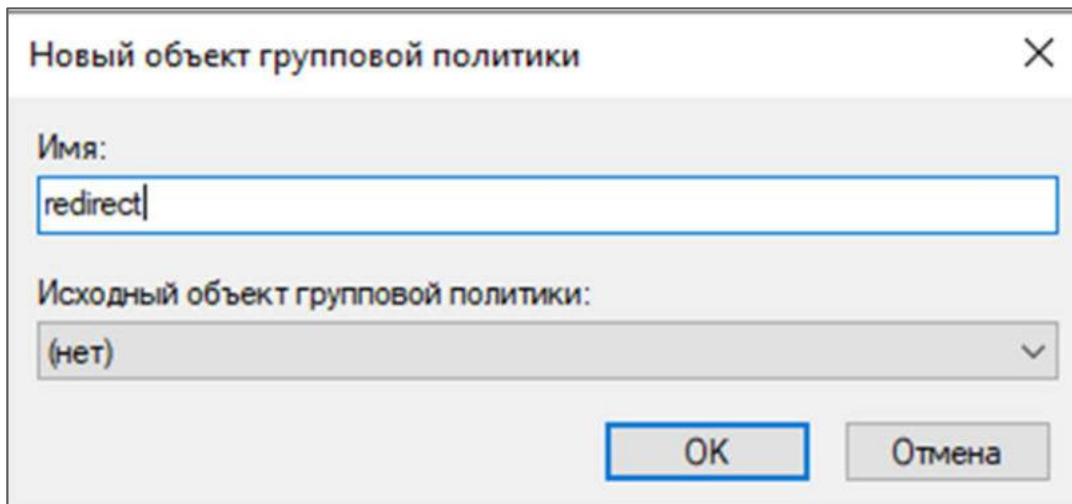
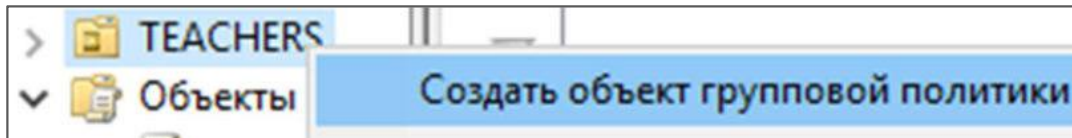
!!! Каталог в NTFS создается автоматически!!!.



Права доступа только для teacher (+наследованные).

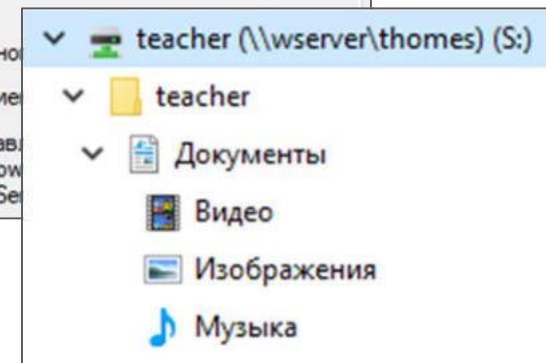
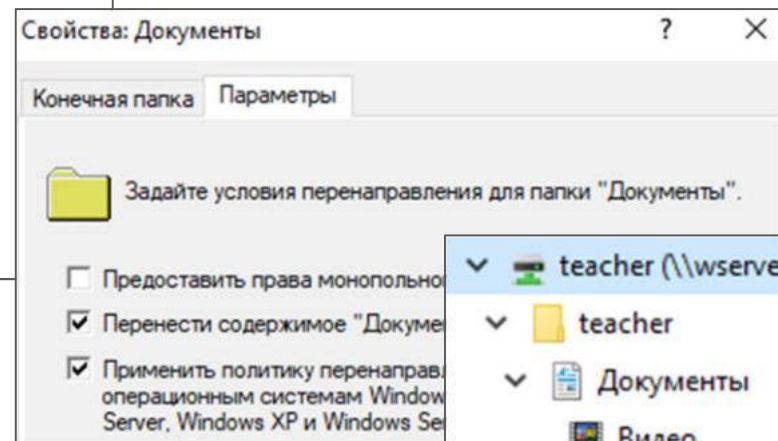
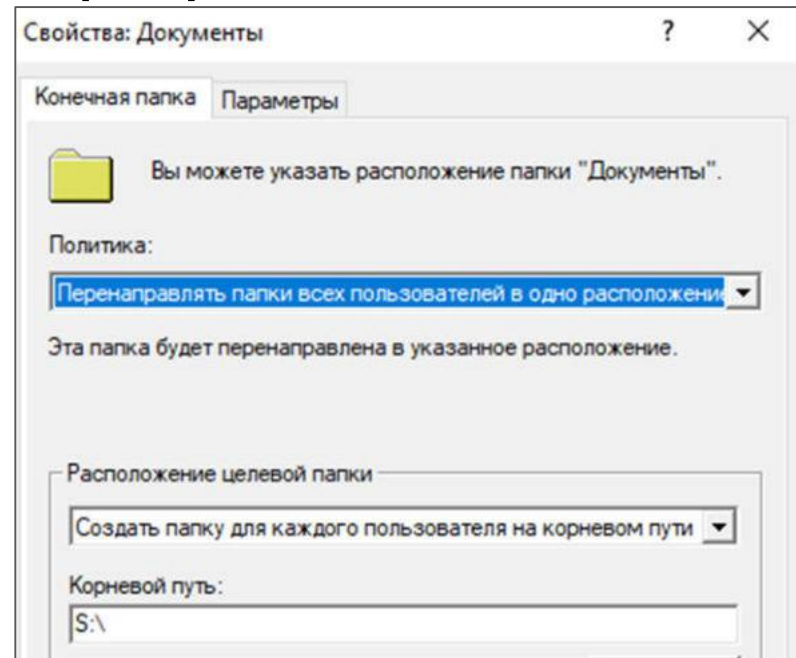
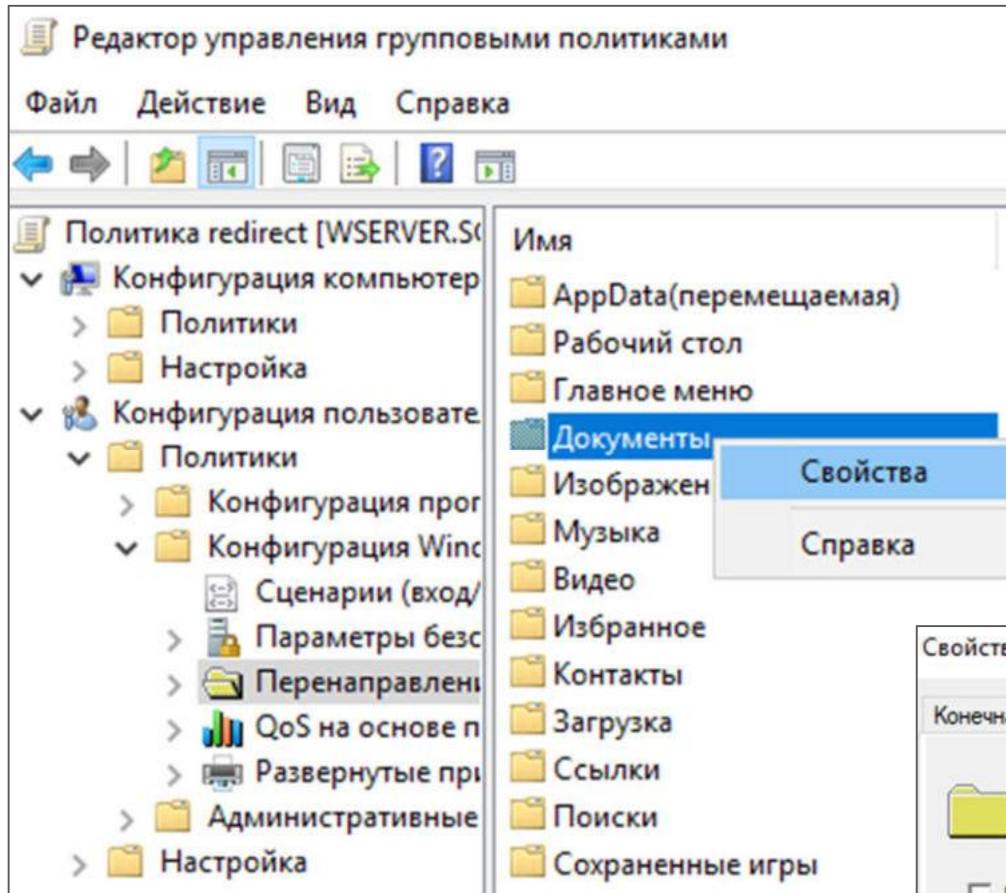
При следующем входе к букве S: подключится каталог.

Перенаправление каталогов профиля



Лучше не трогать доменную политику, которая действует на всех, а создать отдельный объект GPO для OU, которая будет действовать на всех пользователей, размещенных в данном подразделении.

Перенаправление каталогов профиля



После входа пользователя проверяйте редирект на каталогах пользователя!

Копирование пользователей

Если создавать нового пользователя в оснастке AD в режиме копирования, то перенесутся не только параметры принадлежности к группам, но и ссылка на профиль и домашний каталог.

Причем, если домашний каталог у шаблонного пользователя совпадал с его именем, то для нового сгенерируется каталог с его созданным именем!!!

