МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

ОТЧЕТ

по лабораторной работе №2

«Администрирование и управление ресурсами Windows Server»

по дисциплине

«Программное обеспечение вычислительных сетей»

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_ Кочешков А. А.\_\_

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Игнаков К. М.\_\_\_

(подпись) (фамилия, и.,о.)

\_\_\_\_\_\_19-ВМ\_\_\_\_\_\_\_\_

(шифр группы)

Работа защищена «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород 2022

Цель работы

Ознакомиться с основными задачами управления доступом к ресурсам, составом и назначением встроенных субъектов безопасности Windows. Изучить смысл и примене-ние разрешений доступа файловой системы NTFS, сетевых ресурсов и других объектов безопасности. Опробовать методы управления доступом в различных модельных задачах администрирования пользователей и ресурсов в домене Active Directory.

Ход работы

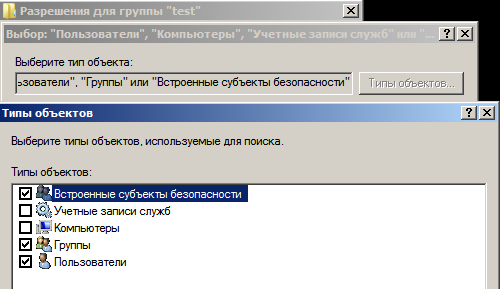
1. Система управления доступа к ресурсам Windows

Субъект безопасности — это любая сущность, которая может быть проверена операционной системой, например учетной записью пользователя, учетной записью компьютера или потоком или процессом, который выполняется в контексте безопасности учетной записи пользователя или компьютера или групп безопасности для этих учетных записей. Субъекты безопасности уже давно являются основой для управления доступом к защищаемым ресурсам на компьютерах Windows. Каждый субъект безопасности представлен в операционной системе уникальным идентификатором безопасности (SID).

Субъекты безопасности, созданные в домене Active Directory, — это объекты Active Directory, которые можно использовать для управления доступом к ресурсам домена. Каждому субъекту безопасности присваивается уникальный идентификатор, который сохраняется в течение всего времени существования. Учетные записи локальных пользователей и группы безопасности создаются на локальном компьютере, и их можно использовать для управления доступом к ресурсам на этом компьютере. Локальные учетные записи пользователей и группы безопасности управляются диспетчером учетных записей безопасности (SAM) на локальном компьютере.

Способы, которые позволяют диспетчерам ресурсов управлять доступом:

* Отказ в доступе неавторизованным пользователям и группам;
* Установка четко определенных ограничений на доступ, предоставляемый авторизованным пользователям и группам.



Вынесем в таблицу состав субъектов безопасности для узла домена.

|  |  |  |
| --- | --- | --- |
| **Имя субъекта** | **Тип субъекта** | **SID субъекта** |
| Администратор | Учетная запись пользователя | S-1-5-21-2306…569-500 |
| Гость | Учетная запись пользователя | S-1-5-21-2306…569-501 |
| Poly | Добавленная учетная запись пользователя | S-1-5-21-2306…569-1001 |
| Администраторы | Предопределенная локальная группа | S-1-5-32-544 |
| Гости | Предопределенная локальная группа | S-1-5-32-546 |
| Операторы архива | Предопределенная локальная группа | S-1-5-32-551 |
| Операторы печати | Предопределенная локальная группа | S-1-5-32-550 |
| Операторы настройки сети | Предопределенная локальная группа | S-1-5-32-556 |
| Опытные пользователи | Предопределенная локальная группа | S-1-5-32-547 |
| Пользователи | Предопределенная локальная группа | S-1-5-32-545 |
| Пользователи DCOM | Предопределенная локальная группа | S-1-5-32-562 |
| Пользователи Журналов производительности | Предопределенная локальная группа | S-1-5-32-559 |
| Пользователи системного монитора | Предопределенная локальная группа | S-1-5-32-558 |
| Репликатор | Предопределенная локальная группа | S-1-5-32-552 |
| Читатели журнала событий | Предопределенная локальная группа | S-1-5-32-573 |
| Local Service | Предопределенная учетная запись службы | S-1-5-19 |
| Network Service | Предопределенная учетная запись службы | S-1-5-20 |
| Remote interactive logon | Предопределенная учетная запись службы | S-1-5-14 |
| Анонимный вход | Предопределенная учетная запись службы | S-1-5-7 |
| Сеть | Предопределенная учетная запись службы | S-1-5-2 |
| Служба | Предопределенная учетная запись службы | S-1-5-6 |
| Все | Предопределенная специальная группа | S-1-1-0 |
| Группа-создатель | Предопределенная специальная группа | S-1-3-1 |
| Интерактивные | Предопределенная специальная группа | S-1-5-4 |
| Прошедшие проверку | Предопределенная специальная группа | S-1-5-11 |
| Создатель-владелец | Предопределенная специальная группа | S-1-3-0 |

На контроллере домена локальные пользователи заблокированы для безопасности, для того чтобы восстановить их необходимо это сделать через “Безопасную загрузку”.

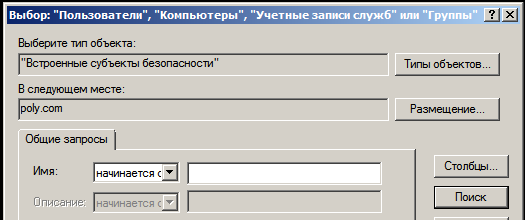




Таблица субъектов безопасности для члена домена. Как видим: учетные записи служб и специальные группы совпадают.

|  |  |  |
| --- | --- | --- |
| **Имя субъекта** | **Тип субъекта** | **SID субъекта** |
| Администратор | Встроенная учетная запись пользователя домена | S-1-5-21-4675…024-500 |
| Гость | Встроенная учетная запись пользователя домена | S-1-5-21-4675…024-501 |
| Даня | Добавленная учетная запись пользователя домена | S-1-5-21-4675…024-1009 |
| DNSadmins | Встроенная локальная группа домена | S-1-5-21-4675…024-1101 |
| Издатели сертификатов | Встроенная локальная группа домена | S-1-5-21-4675…024-517 |
| Серверы RAS и IAS | Встроенная локальная группа домена | S-1-5-21-4675…024-553 |
| DnsUpdateProxy | Встроенная глобальная группа домена | S-1-5-21-4675…024-1102 |
| Администраторы домена | Встроенная глобальная группа домена | S-1-5-21-4675…024-512 |
| Администраторы предприятия | Встроенная глобальная группа домена | S-1-5-21-4675…024-519 |
| Администраторы схемы | Встроенная глобальная группа домена | S-1-5-21-4675…024-518 |
| Владельцы-создатели групповой политики | Встроенная глобальная группа домена | S-1-5-21-4675…024-520 |
| Гости домена | Встроенная глобальная группа домена | S-1-5-21-4675…024-514 |
| Пользователи домена | Встроенная глобальная группа домена | S-1-5-21-4675…024-513 |
| Разработчики | Добавленная глобальная группа домена | S-1-5-21-4675…024-1116 |

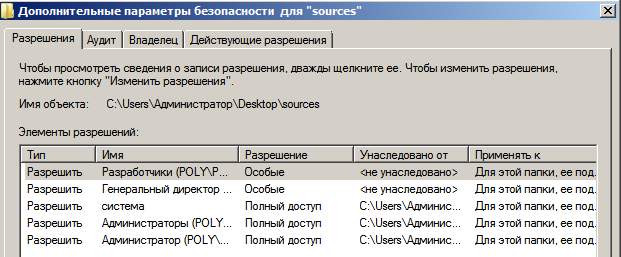
На контроллере домена «встроенные субъекты безопасности» дополняются субъектами из контейнера Builtin, который образованы из встроенных субъектов безопасности сервера (Администраторы, гости, операторы…). SID элементов Builtin совпадает с локальными субъектами безопасности компьютера-члена домена.

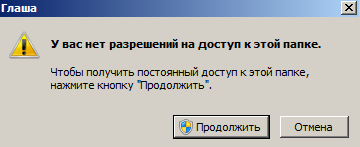
Анализ:

* Локальные субъекты безопасности (группы и учетные записи) создаются на локальном компьютере, и использовать их можно для управления доступом к ресурсам, находящимся только на этом компьютере. Данные субъекты доступны только на компьютере-члене домена. Предопределённые субъекты имеют короткий well-known SID, добавленные имеют длинный SID, связанный с конкретным компьютером.
* Встроенные субъекты безопасности из контейнера Builtin заменяют локальные субъекты рядового сервера и могут быть использованы для управления доступа только на данном контроллере домена. Предоставление доступа к сетевому ресурсу данным субъектам недоступно из-за их области действия.
* Доменные субъекты безопасности могут быть использованы для ограничения/разрешения доступа к ресурсам по сети, поскольку они имеют уникальные SID’ы.

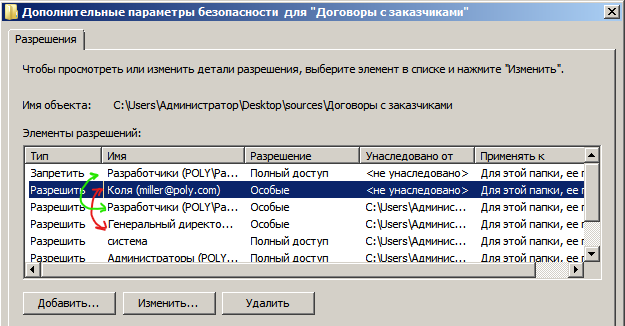
1. Доступ к файлам и каталогам
   1. Назначение разрешений

В корне диска создадим папку «Исходники» и разрешим доступ группам: «Разработчики» и «Начальство». Для каждого участника можно определить соответствующие права: «Полный доступ», «Чтение и выполнение», «Особые» и др. Если пользователь попробует открыть или запустить без советующих разрешений, то будет выведено сообщение об ошибке.

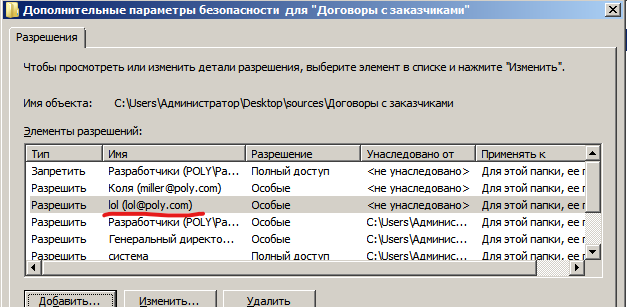




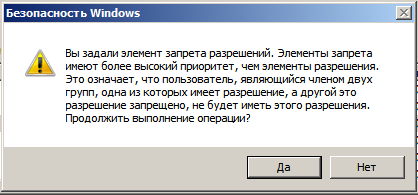
Внутри создадим каталог для начальства, выдадим права для конкретного пользователя, однако запретим доступ для группы разработчиков. Однако,



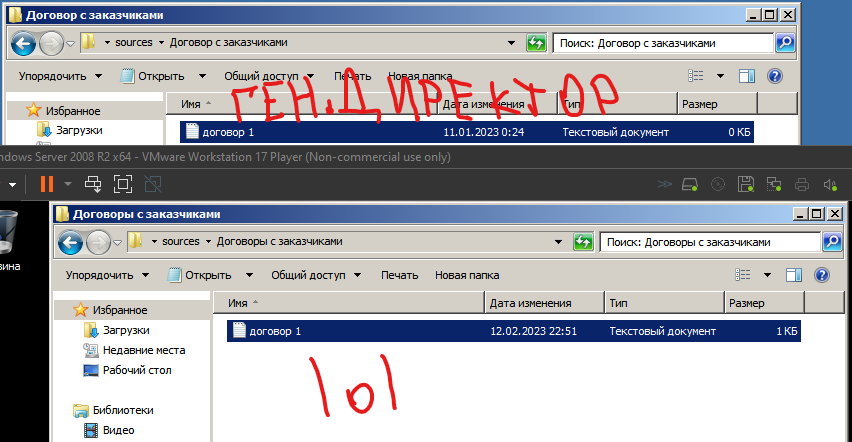
Ради эксперимента добавим разрешение для конкретного пользователя из группы «Разработчики» к каталогу «Договоры с заказчиками», условно это будет старший разработчик и попробуем зайти в эту папку:



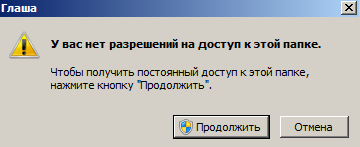
Перед сохранением получим такое предупреждение:



Как видим пользователь из группы, у которой стоит запрет на доступ к этому каталогу имеет доступ, это значит явное разрешение выше указанного:



Чтобы это проверить зайдем под другим любым пользователем из группы «Разработчики»:



* 1. Использование команды icacls

Управление доступом к объектам файловой системы NTFS реализуется с использованием специальных записей в таблице MFT (Master File Table). Каждому файлу или папке файловой системы NTFS соответствует запись в таблице MFT, содержащая специальный дескриптор безопасности SD (Security Descriptor). Каждый дескриптор безопасности содержит два списка контроля доступа:

System Access-Control List (SACL) и Discretionary Access-Control List (DACL) - это два типа Access Control List (ACL), используемых в операционных системах Windows, для управления доступом к файлам, папкам и другим ресурсам.

DACL - это список контроля доступа, который содержит правила, контролирующие доступ к ресурсу. Он определяет, кто может выполнять определенные действия, такие как чтение, запись или выполнение, с определенным ресурсом. Владелец ресурса может настроить DACL, чтобы указать, какие права имеют другие пользователи или группы.

SACL - это список контроля доступа, который контролирует отслеживание событий, связанных с ресурсом, таких как попытки доступа или изменения. Он может быть использован для отслеживания и аудита действий, происходящих с ресурсом. Обычно SACL настроен администратором системы. События, которые отслеживаются с помощью SACL, могут включать в себя попытки доступа к ресурсу, изменения или удаление ресурса. Эти события могут быть записаны в журнале событий системы или в другой журнал, где они могут быть проанализированы для определения необходимых действий.

Команда icacls в Windows позволяет вам управлять и изменять ACL файлов и папок. С помощью команды icacls можно просматривать, добавлять, изменять или удалять права доступа для пользователей или групп. Также с помощью команды icacls можно настраивать SACL для отслеживания и аудита событий, связанных с файлом или папкой.

Практическое использование:

icacls – это командная утилита, которая может использоваться для изменения прав доступа к файлам и папкам в Microsoft Windows.

Примеры использования:

Назначение чтения и выполнение для всех пользователей:

icacls folder\_name /grant "Everyone:(RX)"

Отображение текущих прав доступа для файла:

icacls file\_name

Удаление права доступа у пользователя:

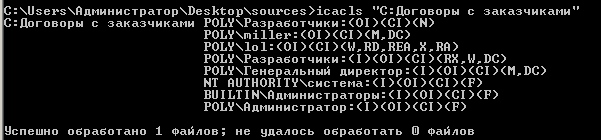
icacls file\_name /remove username

Обновление прав доступа, наследуемых от родительской папки:

icacls folder\_name /inheritance:r

Для получения дополнительной информации и полного списка параметров можно выполнить команду icacls /?.

Проверим доступ к каталогу «Договоры с заказчиками»:

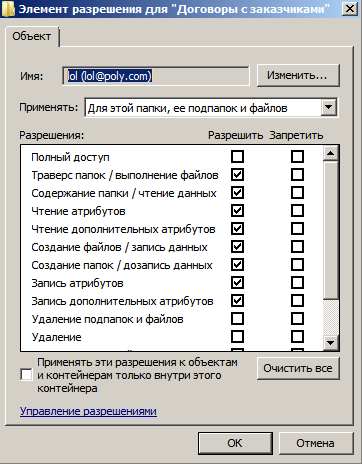


Как видим:

* Разработчики:
  + (OI) — объект наследуется. Объекты в этом контейнере наследуют этот ACE. Применяется только к каталогам.
  + (CI) — контейнер наследуется. Контейнеры в этом родительском контейнере наследуют этот ACE. Применяется только к каталогам.
  + (N) – нет доступа, это значит, если есть права на доступ к этому каталогу, то приоритет запрета будет выше.
* Miller:
  + M— изменение доступа
  + DC – удаление дочерних файлов и каталогов
* Lol:
  + RX — доступ для чтения и выполнения
  + W — доступ только для записи
* Администраторы:
  + F — полный доступ

1. Варианты разрешений доступа к каталогам и файлам

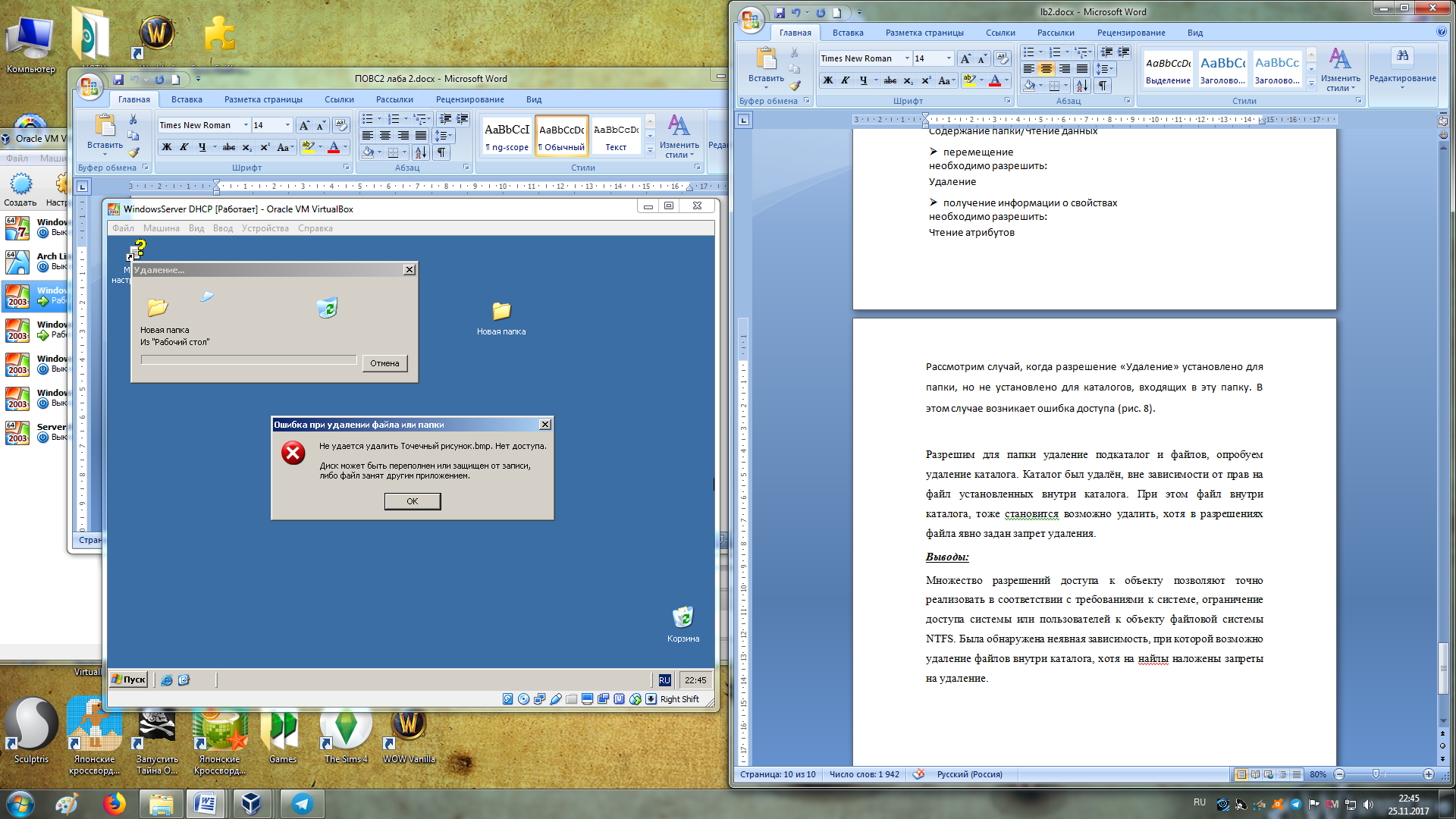
Для установки «специальных» разрешений необходимо перейти в свойства файла или каталога→ «Безопасность» → «Дополнительно» → «Изменить разрешения» → «Изменить».



Соотношение действий файлов и каталогов с разрешениями, необходимы для этих действий.

* Создание файлов и папок.
  + Содержание папки/Чтение данных
  + файлов/Запись данных
  + Создание папок/Дозапись данных
* Удаление не пустой папки.
  + Содержание папки/Чтение данных
  + Удаление подпапок и файлов
  + Удаление
* Копирование файла.
  + Чтение атрибутов
  + Чтение дополнительных атрибутов
  + Содержание папки/Чтение данных
* Перемещение.
  + Удаление
* Получение информации о свойствах.
  + Чтение атрибутов

Если установить разрешение на удаление папки, но не установить разрешение на удаление файлов входящих в эту папку, то возникнет ошибка.



Соотношение NTFS разрешения для каталогов с возможными действиями над ним:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Действие** | **FC** | **M** | **R&E** | **L** | **R** | **W** |
| Просмотр содержимого папки | + | + | + | + | + | + |
| Создание подкаталогов | + | + | + | + | + | + |
| Создание файлов | + | + | - | - | - | + |
| Переход в подкаталоги | + | + | + | + | + | + |
| Удаление подкаталогов и файлов | + | + | - | - | - | - |
| Чтение разрешений | + | + | + | + | + | + |
| Чтение владельца | + | + | + | + | + | + |
| Изменение разрешений | + | - | - | - | - | - |
| Смена владельца | - | - | - | - | - | - |
| Удаление каталога | + | + | - | - | - | - |

Соотношение NTFS разрешения для файлов с возможными действиями над каталогами:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Действие** | **FC** | **M** | **R&E** | **R** | **W** |
| Чтение содержимого файла | + | + | + | + | + |
| Чтение владельца | + | + | + | + | + |
| Выполнение файла | + | + | + | - | - |
| Изменение файла | + | + | - | - | + |
| Изменение разрешений | + | - | - | - | - |
| Удаление файла | + | + | - | - | - |
| Смена владельца | - | - | - | - | - |

**Вывод:**

Настройка доступа для каталогов и файлов очень гибка, поэтому комбинируя различные стандартные разрешения можно получить необходимый результат.

1. Наследование решений

Наследование разрешений доступа заключается в том, что разрешения доступа для объекта (файла или каталога) – родителя будут распространяться на дочерние каталоги. Данное свойство позволяет задавать настройки только у корневого каталога дерева каталогов и наследовать их для всех объектов в этом дереве, а не задавать разрешения каждому объекту в отдельности. По умолчанию наследование разрешений доступа включено.

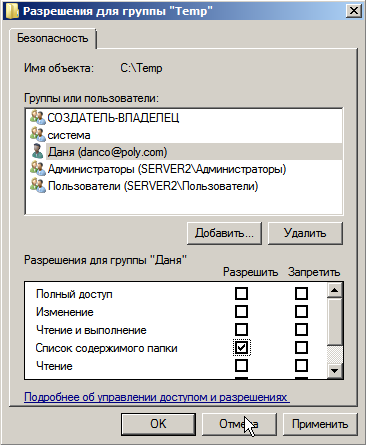
Существует два основных преимущества использования унаследованных разрешений для управления тем, кто из пользователей может просматривать папки в пространстве имен DFS:

* Можно быстро применить унаследованные разрешения к множеству папок, не прибегая к использованию сценариев.
* Можно применять унаследованные разрешения к корням пространства имен и папкам без конечных объектов.

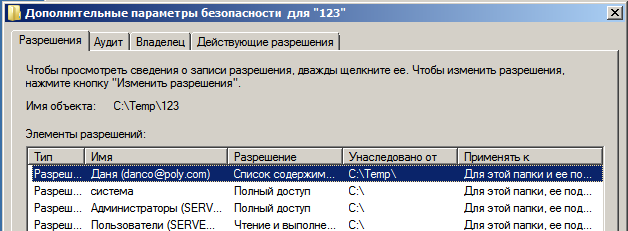
Несмотря на преимущества, с унаследованными разрешениями в пространствах имен DFS связан ряд ограничений, которые делают их неприменимыми для большинства сред:

* Изменения унаследованных разрешений не реплицируются на другие серверы пространства имен. Таким образом, использовать унаследованные разрешения имеет смысл только применительно к изолированным пространствам имен или в средах, где можно реализовать стороннюю систему репликации для обеспечения синхронизации списков управления доступом (ACL) на всех серверах пространства имен.
* Оснастка "Управление DFS" и команда Dfsutil не позволяют просматривать или изменять унаследованные разрешения. Таким образом, для управления пространством имен в дополнение к оснастке "Управление DFS" или команде Dfsutil необходимо использовать проводник или команду Icacls.
* При использовании унаследованных разрешений невозможно изменить разрешения папки с конечными объектами, кроме как с помощью команды Dfsutil. Пространства имен DFS автоматически удаляют разрешения с папок с конечными объектами, заданные с использованием других средств или методов.
* При задании разрешений для папки с конечными объектами, когда вы используете унаследованные разрешения, список управления доступом, который вы установили для папки с конечными объектами, объединяется с разрешениями, наследуемыми от родителя папки в файловой системе. Необходимо изучить оба набора разрешений, чтобы определить, каковы будут результирующие разрешения.
  1. Использование наследования

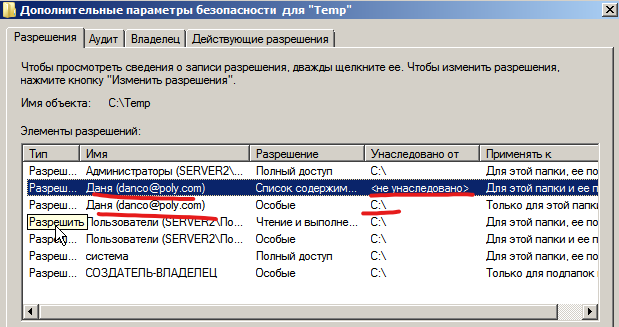
Реализуем пример наследования разрешений. Добавим пользователя Даня в ACL каталога Temp. И установим для него разрешение L.



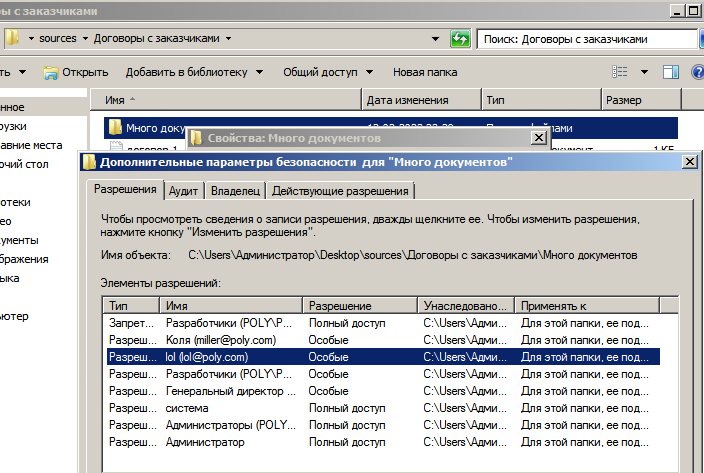
Далее создадим вложенный каталог и проверим его разрешения, как видим каталог 123 унаследовал разрешение L от каталога Temp.



Если указать явно разрешения вложенного каталога, то появится еще одно разрешение, которое не будет унаследовано.



Для примера в каталоге с договорами создадим подкаталог «Много документов» и посмотрим параметры безопасности у этого каталога:



Как видим разрешения унаследовались от родительского каталога, в котором есть полный доступ для «Ген. директора», он же «Коля», полный запрет для группы «Разработчики», однако явный доступ для чтения есть у пользователя «lol», пример доступа был рассмотрен выше.

**Вывод:**

Для того чтобы пользователю был или не был доступен какой-либо файл или каталог, достаточно явно прописать это правило, т.к явное разрешение выше унаследованного.

* 1. Целесообразное и нецелесообразное применение наследование.

Наследование является целесообразным в том случае, когда в одном каталоге содержится очень много подкаталогов или файлов. Тогда определение вручную разрешений для объектов заняло бы очень продолжительное время. В этом случае нам следует только для родительского объекта определить разрешения и выбрать применение разрешений ко всем вложенным объектам. Также если будет необходимость для какого-либо определенного объекта сделать дополнительное разрешение, мы сможем это сделать явно и разрешение будет активно, так как явно указанное разрешение преобладает над унаследованным (даже если это запрет).

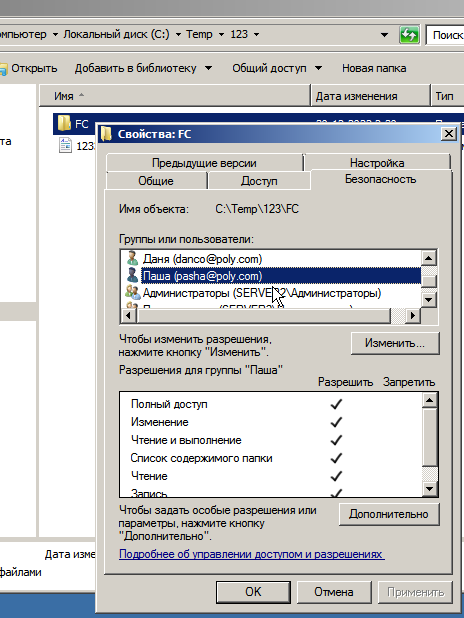
Нецелесообразным является наследование, когда существует несколько пользователей, у которых имеются свои рабочие каталоги в одном общем. В таком случаем мы не можем применить наследование для группы этих пользователей. Нам нужно назначить для группы пользователей разрешение просмотра списка содержимого общего каталога и не указывать применение к дочерним объектам, чтобы пользователи не могли просматривать всё дерево каталогов. А для личного каталога добавить соответствующую учетную запись и назначить для нее явно свои разрешения (к дочерним каталогам этого личного каталога уже можно применить наследование).

На примере «Обход перекрестной проверки» показать преобладание привилегий над разрешениями.

Обход перекрестной проверки – это право пользователя производить обзор дерева каталога, даже если у этого пользователя нет разрешения на каталог. Пользователь не сможет просматривать содержимое каталогов, а сможет только выполнять обзор.

По умолчанию обход перекрестной проверки разрешен для всех пользователей. Создадим в каталоге Temp каталог 123, а в каталоге 123 создадим каталог FC.

На каталог 123 оставим только полный доступ администратору, а на каталог FC предоставим полный доступ пользователю Паша.



Если зайти под пользователем Паша и открыть директорию C:\Temp\123, то появится ошибка доступа, однако если указать путь до каталога с полными правами полностью, то такой проблемы не будет.

**Вывод**:

В дополнительных настройках безопасности NTFS имеется возможность устанавливать наследование разрешений отдельных субъектов. При этом в дочерних объектах можно преобразовать наследуемые разрешения в явные для ручной настройки.

Наследование упрощает работу для администраторов, если требуется назначить разрешения для множества объектов. Если у каждого объекта необходимо установить индивидуальный доступ, то данную функцию будет нецелесообразно использовать.

«Обход перекрестной проверки» позволяет, указав абсолютный или относительный путь, иметь доступ к внутреннему каталогу, не имея доступа на каталог выше. Таким образом, данная привилегия преобладает над разрешением.

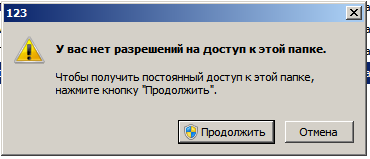
1. Владение объектом.

Главным назначением владельца объекта является то, что только владелец может управлять разрешениями доступа к этому объекту. То есть, чтобы иметь возможность изменять разрешения доступа к объекту, надо быть владельцем этого объекта. По умолчанию Администраторы всегда могут стать владельцами объектов.

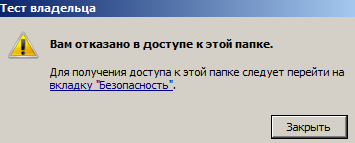
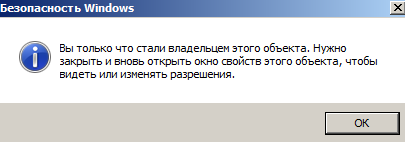
Это очень важное свойство, так как при отсутствии всех разрешений на объект Администратор может назначить себя владельцем данного объекта и изменить разрешения доступа.

* 1. Опробовать смену владельца объекта

Для каталога “123”, который был создан в предыдущих пунктах, поменяем владельца на “Даня” – удалив всем остальным пользователям доступ к этому каталогу, то есть сделаем его недоступным другим пользователям, кроме пользователя “Даня”.



Теперь зайдем, используя Администратора и попробуем открыть данный каталог. При попытке открытия возникла ошибка доступа. При попытке открытия возникла ошибка доступа. Теперь сменим владельца на Администратора.

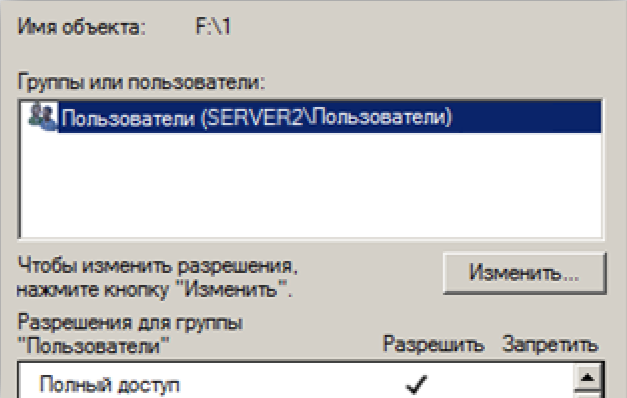
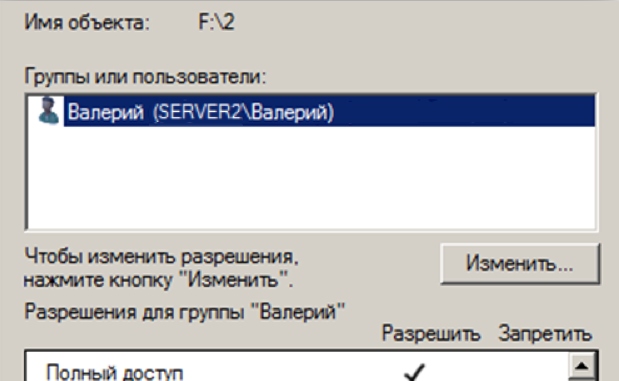
 

У него по-прежнему нет доступа к папке, но так как он стал её владельцем, он может добавить себя в список разрешений доступа к данному объекту. Теперь ему открылся полный доступ к данной папке, хотя изначально создатель этой папки запретил доступ к ней кому-либо.

* 1. Применить смену владельца для восстановления доступа к данным на съемном носителе.

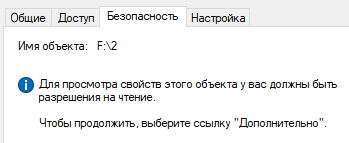
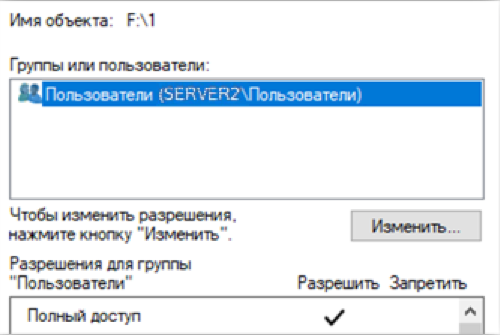
Отформатировать сменный флэш-носитель в файловую систему NTFS, создать два каталога, на один назначить доступ локальной группе Пользователи, на другой – конкретной локальной учетной записи. Проверить и обосновать возможность доступа к каталогам носителя на другом компьютере, на котором есть группы и локальные пользователи с теми же именами. Применить смену владельца для восстановления доступа.

После форматирования флэш-носителя создадим 2 каталога с именами 1 и 2. Первый каталог будет иметь в качестве субъекта группу «Пользователи» с полным доступом. Второй каталог будет иметь в качестве субъекта конкретного локального пользователя с полным доступом.

Перейдем к основной машине, на которой есть локальная учетная запись с таким же именем и подключим флеш-носитель.

Первый каталог мы можем без проблем открыть. Также мы можем открыть свойства безопасности и увидеть, что в субъектах безопасности стоит группа «Пользователи». SID этой встроенной группы одинаков на всех системах.



Доступа ко второму каталогу нет. Это происходит потому, что эти 2 пользователя с одинаковыми именами имеют разные SIDы.

Решение: используя привилегию администратора, установить владельцем каталога группу «Пользователи».

**Вывод:**

Администратор вправе завладеть любым объектом. Важное свойство владельца: владелец всегда имеет разрешение на изменение разрешений.

1. Разрешение системных каталогов.
   1. Разрешение доступа к каталогам системного диска у разных групп, установленные по умолчанию

Разрешения доступа к системному диску:

|  |  |  |  |
| --- | --- | --- | --- |
| **Владелец** | **Разрешение** | **Субъекты безопасности** | **Применять для** |
| TrustedInstaller | Полный доступ | Система | Этой папки, её подпапок и файлов |
| Полный доступ | Администраторы | Этой папки, её подпапок и файлов |
| Полный доступ | Создатель-владелец | Только для подпапок и файлов |
| Чтение и выполнение | Пользователи | Этой папки, её подпапок и файлов |
| Создание папок | Пользователи | Этой папки и её подпапок |
| Создание файлов | Пользователи | Только для подпапок |

Разрешения доступа к каталогам “Windows”, “Windows/system32”, “Program files”:

|  |  |  |  |
| --- | --- | --- | --- |
| **Владелец** | **Разрешение** | **Субъекты безопасности** | **Применять для** |
| TrustedInstaller | Полный доступ  кроме удаления подпапок и файлов, смены разрешений и смены владельца | Система | Этой папки |
| Полный доступ | Система | Подпапок и файлов |
| Полный доступ  кроме удаления подпапок и файлов, смены разрешений и смены владельца | Администраторы | Этой папки |
| Полный доступ | Администраторы | Подпапок и файлов |
| Полный доступ | Создатель-владелец | Только для подпапок и файлов |
| Чтение и выполнение | Пользователи | Этой папки, её подпапок и файлов |
| Полный доступ | TrustedInstaller | Этой папки и её подпапок |

Для каталога “Program files”:

|  |  |  |  |
| --- | --- | --- | --- |
| **Владелец** | **Разрешение** | **Субъекты безопасности** | **Применять для** |
| Администраторы | Полный доступ | Система | Этой папки, её подпапок и файлов |
| Полный доступ | Администраторы | Этой папки, её подпапок и файлов |
| Полный доступ | Создатель-владелец | Только для подпапок и файлов |
| Чтение и выполнение  +  Создание файлов, создание папок | Пользователи | Этой папки и её подпапок |

Для каталога “Users”:

|  |  |  |  |
| --- | --- | --- | --- |
| **Владелец** | **Разрешение** | **Субъекты безопасности** | **Применять для** |
| Администраторы | Полный доступ | Система | Этой папки, её подпапок и файлов |
| Полный доступ | Администраторы | Этой папки, её подпапок и файлов |
| Чтение и выполнение | Пользователи | Этой папки, её подпапок и файлов |
| Чтение и выполнение | Все | Этой папки, её подпапок и файлов |

Для каталога “Users\poly”:

|  |  |  |  |
| --- | --- | --- | --- |
| **Владелец** | **Разрешение** | **Субъекты безопасности** | **Применять для** |
| Система | Полный доступ | Система | Этой папки, её подпапок и файлов |
| Полный доступ | Администраторы | Этой папки, её подпапок и файлов |
| Полный доступ | poly | Этой папки, её подпапок и файлов |

Для Junction point “Users\poly\AppData”:

|  |  |  |  |
| --- | --- | --- | --- |
| **Владелец** | **Разрешение** | **Субъекты безопасности** | **Применять для** |
| poly | Полный доступ | Система | Этой папки, её подпапок и файлов |
| Полный доступ | Администраторы | Этой папки, её подпапок и файлов |
| Полный доступ | poly | Этой папки, её подпапок и файлов |

Вывод:

Группа пользователи имеет доступ на чтение и выполнение к системным файлам, так как без этого доступа для них система не смогла бы корректно работать. Но тем не менее пользователи не имеют полного доступа к системным файлам, что обеспечивает защиту системы.

TrustedInstaller.exe – важная служба и часть «Установщика модулей Windows». Он предназначен для проверки обновлений операционной системы. Он позволяет устанавливать, изменять и удалять обновления Windows и дополнительные компоненты. Исполняемый файл находится в подпапке C:\Window\servicing\. TrustedInstaller является владельцем системных каталогов и имеет большие разрешения, чем Администраторы.

* 1. Действующие разрешения к каталогам системного диска.

Рассмотрел разрешения, их наследование, применение и владельца у каталогов Windows

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Имя** | **Разрешение** | **Унаследовано от** | | **Применять к** | | |
| **C:\ (Владелец TrustedInstaller)** | | | | | | |
| система | FC | не унаследовано | | Для этой папки, ее подпапок и файлов | | |
| Администраторы | FC | не унаследовано | | Для этой папки, ее подпапок и файлов | | |
| Пользователи | RX | не унаследовано | | Для этой папки и подпапок | | |
| Пользователи | Создание папок/дозапись данных | не унаследовано | | Для этой папки и её подпапок | | |
| Пользователи | Создание файлов/запись данных | не унаследовано | | Только для подпапок | | |
| Создатель-  владелец | FC | не унаследовано | | Только для подпапок и файлов | | |
| **C:\Windows (Владелец TrustedInstaller)** | | | | | | |
| система | Все, кроме удаления подпапок и файлов, смены разрешений и владельца | не унаследовано | | Только для этой папки | | |
| система | Полный доступ | не унаследовано | | Только для подпапок и файлов | | |
| Администраторы | Все, кроме удаления подпапок и файлов, смены разрешений и владельца | не унаследовано | | Только для этой папки | | |
| Администраторы | Полный доступ | не унаследовано | | Только для подпапок и файлов | | |
| Пользователи | RX | не унаследовано | | Для этой папки, ее подпапок и файлов | | |
| TrustedInstaller | Полный доступ | не унаследовано | | Для этой папки и ее подпапок | | |
| **C:\Windows\Boot (Владелец TrustedInstaller)** | | | | | | |
| система | RX | | не унаследовано | | Только для этой папки | |
| Администраторы | RX | | не унаследовано | | Только для этой папки | |
| Пользователи | RX | | не унаследовано | | Для этой папки, ее подпапок и файлов | |
| TrustedInstaller | FC | | не унаследовано | | Для этой папки и ее подпапок | |
| **C:\Windows\Logs (Владелец Администраторы)** | | | | | | |
| TrustedInstaller | Полный доступ | | С:\Windows\ | | Для этой папки и ее подпапок | |
| система | FC | | С:\Windows\ | | Для этой папки, ее подпапок и файлов | |
| Администраторы | FC | | С:\Windows\ | | Для этой папки, ее подпапок и файлов | |
| Пользователи | RX | | С:\Windows\ | | Для этой папки, ее подпапок и файлов | |
| Создатель-владелец | Полный доступ | | С:\Windows\ | | Только для подпапок и файлов | |
| **C:\Program Files (Владелец TrustedInstaller)** | | | | | | |
| система | Все, кроме удаления подпапок и файлов, смены разрешений и владельца | не унаследовано | | Только для этой папки | | |
| система | Полный доступ | не унаследовано | | Только для подпапок и файлов | | |
| Администраторы | Все, кроме удаления подпапок и файлов, смены разрешений и владельца | не унаследовано | | Только для этой папки | | |
| Администраторы | Полный доступ | не унаследовано | | Только для подпапок и файлов | | |
| Пользователи | RX | не унаследовано | | Для этой папки, ее подпапок и файлов | | |
| TrustedInstaller | Полный доступ | не унаследовано | | Для этой папки и ее подпапок | | |
| Создатель-  владелец | FC | не унаследовано | | Только для подпапок и файлов | | |
| **C:\Program Data (Владелец Администраторы)** | | | | | | |
| система | FC | | не унаследовано | | Для этой папки, ее подпапок и файлов |
| Администраторы | FC | | не унаследовано | | Для этой папки, ее подпапок и файлов |
| Пользователи | RX | | не унаследовано | | Для этой папки, ее подпапок и файлов |
| Пользователи | Создание файлов/запись данных  Создание папок/дозапись данных  Запись атрибутов  Запись доп. атрибутов | | не унаследовано | | Для этой папки и ее подпапок |
| Создатель-  владелец | Полный  доступ | | не унаследовано | | Только для подпапок и файлов |
| **C:\Users (Владелец Администраторы)** | | | | | | |
| система | FC | | не унаследовано | | Для этой папки, ее подпапок и файлов |
| Администраторы | FC | | не унаследовано | | Для этой папки, ее подпапок и файлов |
| Пользователи | RX | | не унаследовано | | Для этой папки, ее подпапок и файлов |
| Все | RX | | не унаследовано | | Для этой папки, ее подпапок и файлов |

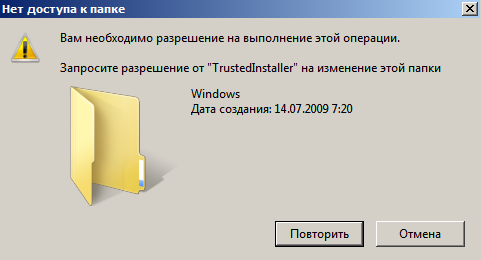
Рассмотрел junction point Application Data в каталоге пользователя poly:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **C:\Users\poly\Application Data (Владелец система)** | | | | |
| система | | FC | C:\Users\poly\ | Для этой папки, ее подпапок и файлов |
| Администраторы | | FC | C:\Users\poly \ | Для этой папки, ее подпапок и файлов |
| poly | | FC | C:\Users\poly \ | Для этой папки, ее подпапок и файлов |
| Запрет | Все | Содержание папки/  чтение данных | не унаследовано | Только для этой папки |

Аналогичные разрешения, кроме запрета, имеет папка AppData. Аналогичные разрешения содержат и другие junction points в папке пользователя.

Пользователи имеют разрешения на чтение и выполнение системных файлов. Иначе бы система могла работать не корректно. Но при этом им не предоставляется полный доступ для защиты данных файлов и целостности структуры системы.

TrustedInstaller — служба установки программных модулей. У этого компонента основная задача – инсталляция обновлений. TrustedInstaller является владельцем системных каталогов. При этом администратор ограничен в изменении системных файлов. Изменение защищенных частей реестра доступно процессам обновления.



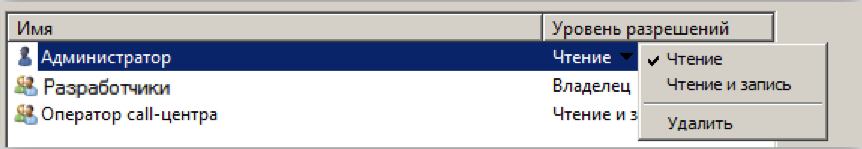
**Вывод:**

Локальная учетная запись, не входящая в группу «Администраторы», имеет ограниченные разрешения доступа на системном диске – только чтение. В личном каталоге пользователя учетная запись имеет полный доступ. Пользователи имеют разрешения на чтение и выполнение системных файлов.

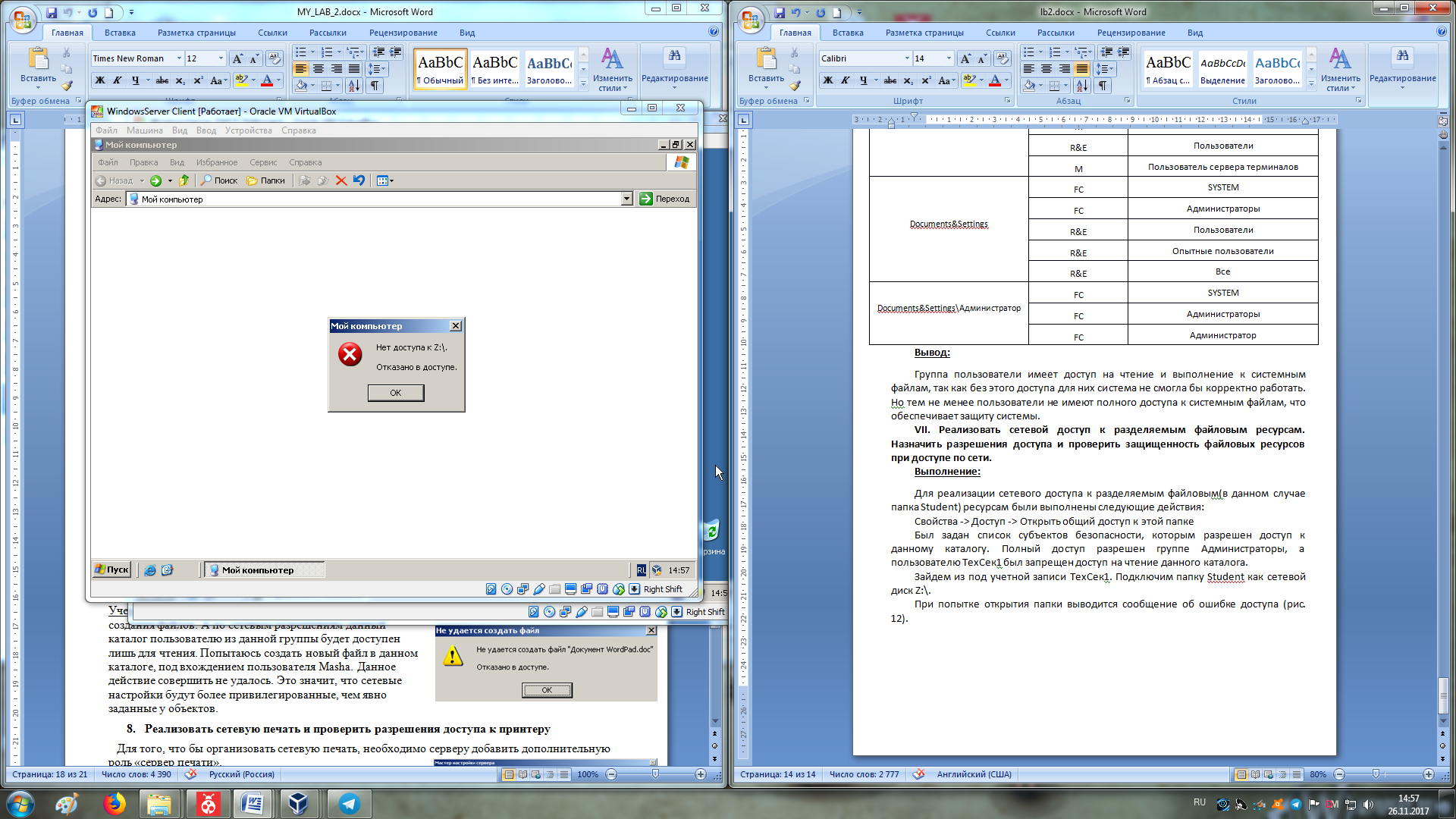
1. Сетевой доступ к общим файловым ресурсам.

Для реализации сетевого доступа к каталогу «Сетевая\_папка» были выполнены следующие действия: Свойства -> Доступ -> Открыть общий доступ к этой папке.

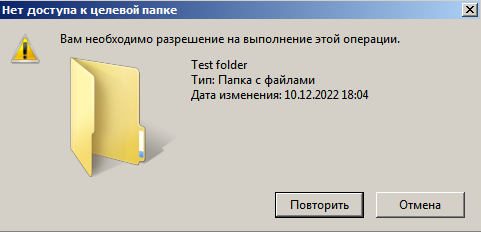
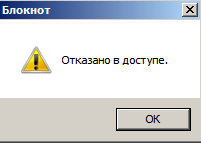
Для субъектов безопасности можно установить 2 уровня разрешений «Чтение» и «Чтение и выполнение». Для группы пользователей «Разработчики» были прописаны явные разрешения для файлов и каталогов на полный доступ. *Владельцем каталога устанавливается группа «Администраторы».*



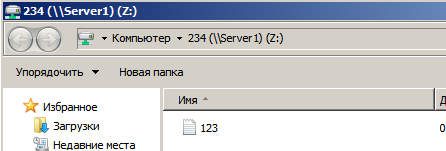
При попытке подключения сетевого диска с другого компьютера с учетной записи, которая не имеет доступ к этому ресурсу получим следующую ошибку доступа:



Например, при разрешении только «Чтение» есть возможность открыть файлы и каталоги, но внести изменения не получится. Будут выведены ошибки при создании каталога или сохранении изменений в текстовом файле:

Под учетной записью администратора подключение и открытие каталога прошло успешно.



Разрешение для сетевых ресурсов на типичные действия:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Создание подкаталогов и файлов | Просмотр содержимого каталога | Удаление подкаталогов и файлов | Смена  владельца | Смена разрешений | Копирование каталога |
| FC | + | + | + | - | + | + |
| C | + | + | + | - | - | + |
| R | - | + | - | - | - | + |

1. Реализовать сетевую печать и проверить разрешения доступа к принтеру
   1. Разрешения доступа

Настройки безопасности расположены в оснастке “Устройства и принтеры” – “Свойства принтера” -> “Безопасность”.

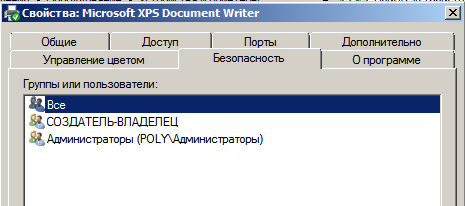


Таблица разрешений:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Субъект** | **Разрешения** | | | | | |
| Печать | Управление эти принтером | Управление документами | Смена разрешений | Смена владельца | Чтение разрешений |
| Все | + | - | - | - | - | + |
| Создатель-владелец | + | - | + | - | - | + |
| Администраторы | + | + | + | + | + | + |

Вывод:

Доступ к принтеру на печать может получить любой пользователь. Управление принтером доступно только группе Администраторы. Для того, чтобы разрешить управление принтером менее квалифицированным пользователям Администратор может назначить разрешения доступа для группы встроенной группы «Операторы печати».

* 1. Сетевая печать

«Стандартный» принтер Microsoft XPS Document Writer нельзя выделить в общий доступ. Создадим новый виртуальный принтер HP Tank H540. Далее откроем принтер для общего доступа.

Выберем виртуальный принтер -> Свойства -> Доступ -> Общий доступ к данному принтеру. Так же отметим галочку «Внести в Active Directory».

Попробуем распечатать документ. В окне печати присутствует только что установленный принтер HP Tank H540. Файл появился в очереди на печать на машине Server2.

Проверим возможность печати с другого сервера, для чего установим сетевой принтер на удалённой машине.

Вывод:

Функция печати посредством разрешения принтеру общего доступа очень удобна для организаций с множеством работников и небольшим числом принтеров. При предоставлении принтеру общего доступа необходимо задать разрешения для его работы. Их можно задавать как для принтера, так и для документов.

1. Реализовать сетевую структуру совместного использования данных
   1. Создание структуры

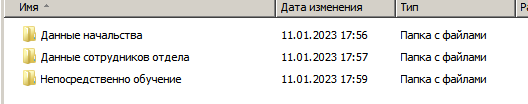
Для данного пункта берутся сведения из 1 лабораторной работы. Мною была рассмотрена модель IT-отдела, занимающегося разработкой ПО.

В её состав вошли такие глобальные доменные группы, как:

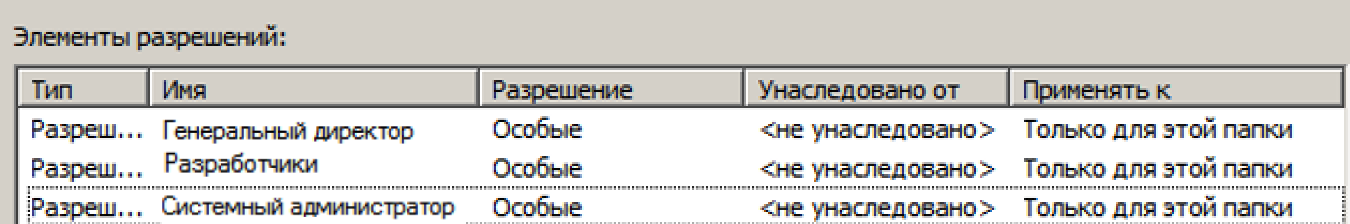
* Генеральный директор
* Разработчики
* Администраторы

Реализуем сетевую структуру для совместного использования данных разными пользователями, использующие разные компьютеры. На контроллере домена создадим каталог «Данные отдела», который будет хранить данные, необходимые для работы отдела.

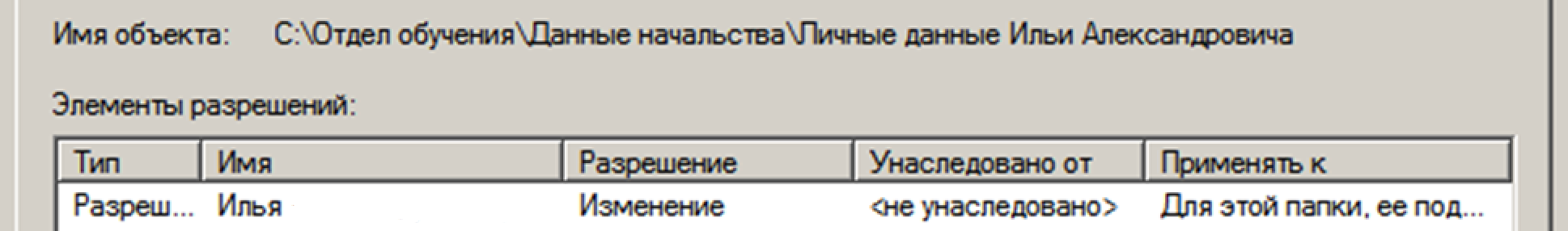
Первый созданный каталог – в нём будут храниться материалы для повышения квалификации сотрудников.



Для беспрепятственного доступа настроим разрешения для каталога «Отдел обучения». Для разработчиков и системных администраторов настроил разрешение «Чтение» с применением только для данного каталога, для генеральных директоров возможна еще запись для добавления нового материала для обучения:



К папке «Данные начальства» применил подобные настройки, но только для группы «Генеральный директор». Для личной папки Ильи настроил доступ «Изменение» с применением для этой папки, её подпапок и файлов.



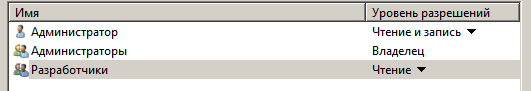
В итоге получаем следующую схему:



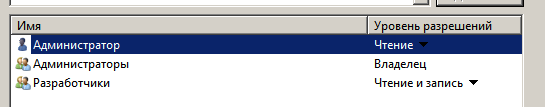
* 1. Установление разрешений и выведение каталога в общий доступ.

Для выделения каталога в общий доступ, в свойствах каталога перейдем на вкладку «Доступ» и выберем группы, которым хотим предоставить доступ.

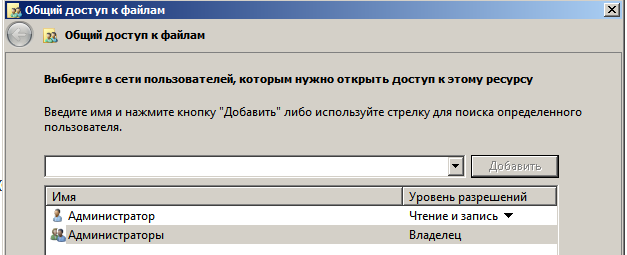
Установим разрешения доступа к каталогу «Данные отдела». Для групп, являющихся сотрудниками отдела.



Для разработчиков укажем полный доступ к папке с исходным кодом

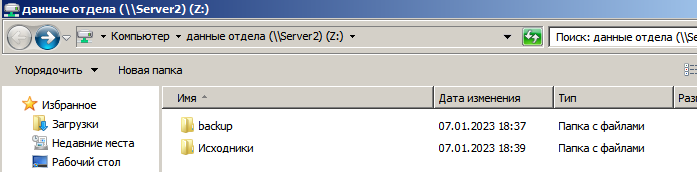


Для каталога с бэкапами дадим доступ только администраторам:

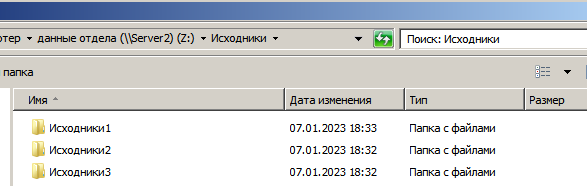


* 1. Подключение каталога, как сетевого диска

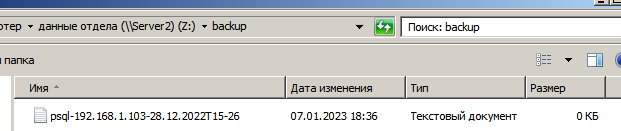
При подключении каталога у нас имеется 2 каталога, для разработчиков с исходным кодом и для администраторов, где хранятся бэкапы.



Разработчики имеют полный доступ к каталогу «Исходники» и всем подкатегориям и файлам, но не имеют доступ к каталогу «backup».



Каталог для администраторов, недоступный для разработчиков:



Вывод:

С помощью общего доступа можно реализовать структуру данных, доступную по сети для всех компьютеров в домене. Благодаря настройке разрешений можно точно установить доступные внутренние каталоги данной структуры для разных групп пользователей и учетных записей.