Стандарт управления правами доступа к корпоративным файловым информационным ресурсам

Что может быть проще, чем разграничить права на папку в NTFS? Но эта простая задача может превратиться в настоящий кошмар, когда подобных папок сотни, если не тысячи, а изменение прав к одной папке «ломает» права на другие. Чтобы эффективно работать в подобных условиях, требуется определенная договоренность, или стандарт, который бы описывал, как решать подобные задачи. В данной статье мы как раз и рассмотрим один из вариантов подобного стандарта.

Сфера действия

Стандарт управления правами доступа к корпоративным файловым информационным ресурсам (далее – Стандарт) регламентирует процессы предоставления доступа к файловым информационным ресурсам, размещенным на компьютерах, работающих под управлением операционных систем семейства Microsoft Windows. Стандарт распространяется на случаи, когда в качестве файловой системы используется NTFS, а в качестве сетевого протокола для совместного доступа к файлам SMB/CIFS.

Термины и определения

Информационный ресурс – поименованная совокупность данных, к которой применяются методы и средства обеспечения информационной безопасности (например, разграничение доступа).
Файловый информационный ресурс – совокупность файлов и папок, хранящихся в каталоге файловой системы (который называется корневым каталогом файлового информационного ресурса), доступ к которой разграничивается.
Составной файловый информационный ресурс – это файловый информационный ресурс, содержащий в себе один или несколько вложенных файловых информационных ресурсов, отличающихся от данного ресурса правами доступа.
Вложенный файловый информационный ресурс – это файловый информационный ресурс, входящий в составной информационный ресурс.
Точка входа в файловый информационный ресурс – каталог файловой системы, к которому предоставляется сетевой доступ (shared folder) и который используется для обеспечения доступа к файловому информационному ресурсу. Данный каталог обычно совпадает с корневым каталогом файлового информационного ресурса, но может быть и вышестоящим.
Промежуточный каталог – каталог файловой системы, находящийся на пути от точки входа в файловый информационной ресурс к корневому каталогу файлового информационного ресурса. Если точка входа в файловый информационный ресурс является вышестоящим каталогом по отношению к корневому каталогу файлового информационного ресурса, то она также будет являться промежуточным каталогом.
Группа доступа пользователей – локальная или доменная группа безопасности, содержащая в конечном счете учетные записи пользователей, наделенные одним из вариантов полномочий доступа к файловому информационному ресурсу.

Основные принципы

1. Доступ разграничивается только на уровне каталогов. Ограничение доступа к отдельным файлам не проводится.
2. Назначение прав доступа выполняется на базе групп безопасности. Назначение прав доступа на отдельные учетные записи пользователей не проводится.
3. Явно запрещающие полномочия доступа (deny permissions) не применяются.
4. Разграничение прав доступа проводится только на уровне файловой системы. На уровне сетевых протоколов SMB/CIFS права не разграничиваются (Группа «Все» – полномочия «Чтение/Запись» / Everyone – Change).
5. При настройке сетевого доступа к файловому информационному ресурсу в настройках SMB/CIFS устанавливается опция «Перечисление на основе доступа (Access based enumeration)».
6. Создание файловых информационных ресурсов на рабочих станциях пользователей недопустимо.
7. Не рекомендуется размещать файловые информационные ресурсы на системных разделах серверов.

8. Не рекомендуется создавать несколько точек входа в файловый информационный ресурс.
9. Следует по возможности избегать создание вложенных файловых информационных ресурсов, а в случаях, когда имена файлов или каталогов содержат конфиденциальную информацию, это вовсе недопустимо

Модель разграничения доступа

Доступ пользователей к файловому информационному ресурсу предоставляется путем наделения их одним из вариантов полномочий:

- Доступ «Только на чтение (**R**ead **O**nly)».
- Доступ «Чтение и запись (**R**ead & **W**rite)».

В подавляющем количестве задач разграничения доступа подобных вариантов полномочий доступа будет достаточно, но при необходимости возможно формирование новых вариантов полномочий, например, «Чтение и запись, кроме удаления (Read & Write without Remove)». Для реализаций новый полномочий необходимо будет уточнить пункт В.3 Таблицы 1, в остальном применение Стандарта останется неизменным.

Правила именования групп доступа пользователей

Имена групп доступа пользователей формируются по шаблону:

FILE-Имя файлового информационного ресурса–аббревиатура полномочий

Имя файлового информационного ресурса должно совпадать с UNC именем ресурса или состоять из имени сервера и локального пути (если сетевой доступ к ресурсу не предоставляется). При необходимости в данном поле допускаются сокращения. Символы «\\» опускаются, а «\» и «:» заменяются на «-».

Аббревиатуры полномочий:

- RO — для варианта доступа «Только на чтение (Read Only)»
- RW — для варианта доступа «Чтение и запись (Read & Write)».

Пример 1
Имя группы доступа пользователей, имеющих полномочия «Только чтение» для файлового информационного ресурса с UNC именем \\FILESRV\Report, будет: FILE-FILESRV-Report-RO

Пример 2
Имя группы доступа пользователей, имеющих полномочия «Чтение и запись» для файлового информационного ресурса, размещенного на сервере TERMSRV по пути D:\UsersData, будет:
FILE-TERMSRV-D-UsersData-RW

Шаблон прав доступа к каталогам файлового информационного ресурса

Таблица 1 – Шаблон NTFS-прав доступа для корневого каталога файлового информационного ресурса.

Субъекты	**Права**	**Режим наследования**
Наследование прав доступа от вышестоящих каталогов отключено		
А) Обязательные права		
Специальная учетная запись: «СИСТЕМА (SYSTEM)»	Полный доступ (Full access)	Для этой папки, ее подпапок и файлов (This folder, subfolders and files)
Локальная группа безопасности: «Администраторы (Administrators)»	Полный доступ (Full access)	Для этой папки, ее подпапок и файлов (This folder, subfolders and files)
*Б.1) Полномочия «Только чтение (**R**ead **O**nly)»*		
Группа доступа пользователей: «FILE-Имя ресурса-RO»	Базовые права: а) чтение и выполнение (read & execute); б) список содержимого папки (list folder contents); в) чтение (read);	Для этой папки, ее подпапок и файлов (This folder, subfolders and files)
*Б.2) Полномочия «Чтение и запись (**R**ead & **W**rite)»*		
Группа доступа пользователей: «FILE-Имя ресурса-RW»	Базовые права: а) изменение (modify); б) чтение и выполнение (read & execute); в) список содержимого папки (list folder contents); г) чтение (read); д) запись (write);	Для этой папки, ее подпапок и файлов (This folder, subfolders and files)

Субъекты	Права	Режим наследования
Б.3) Другие полномочия при их наличии		
Группа доступа пользователей: «FILE-Имя ресурса-аббревиатура полномочий»	Согласно полномочиям	Для этой папки, ее подпапок и файлов (This folder, subfolders and files)

Таблица 2 – Шаблон NTFS-прав доступа для промежуточных каталогов файлового информационного ресурса.

Субъекты	Права	Режим наследования
Наследование прав доступа от вышестоящих каталогов включено, но если данный каталог является вышестоящим по отношению к файловым информационным ресурсам и не входит ни в один другой файловый информационный ресурс, то наследование отключено		
А) Обязательные права		
Специальная учетная запись: «СИСТЕМА (SYSTEM)»	Полный доступ (Full access)	Для этой папки, ее подпапок и файлов (This folder, subfolders and files)
Локальная группа безопасности: «Администраторы»	Полный доступ (Full access)	Для этой папки, ее подпапок и файлов (This folder, subfolders and files)
Б.1) Полномочия «Проход через каталог (TRAVERSE)»		
Группы доступа пользователей информационных ресурсов, для которых этот каталог является промежуточным	Дополнительные параметры безопасности: а) траверс папок / выполнение файлов (travers folder / execute files); б) содержимое папки / чтение данных (list folder / read data); в) чтение атрибутов (read attributes); в) чтение дополнительных атрибутов (read extended attributes); г) чтение разрешений	Только для этой папки (This folder only)

Субъекты	Права	Режим наследования
	(read permissions);	

Бизнес процессы управления доступом к файловым информационным ресурсам

А. Создание файлового информационного ресурса
При создании файлового информационного ресурса выполняются следующие действия:

1. Создаются группы доступа пользователей. Если сервер, на котором размещен файловый информационный ресурс, является членом домена, то создаются доменные группы. Если нет, то группы создаются локально на сервере.
2. На корневой каталог и промежуточные каталоги файлового информационного ресурса назначаются права доступа согласно шаблонам прав доступа.
3. В группы доступа пользователей добавляются учетные записи пользователей в соответствии с их полномочиями.
4. При необходимости для файлового информационного ресурса создается сетевая папка (shared folder).

Б. Предоставление пользователю доступа к файловому информационному ресурсу
Учетная запись пользователя помещается в соответствующую группу доступа пользователя в зависимости от его полномочий.

В. Изменение доступа пользователя к файловому информационному ресурсу
Учетная запись пользователя перемещается в другую группу доступа пользователей в зависимости от указанных полномочий.

Г. Блокирование доступа пользователя к файловому информационному ресурсу
Учетная запись пользователя удаляется из групп доступа пользователей файлового информационного ресурса. Если работник увольняется, то членство в группах не меняется, а блокируется учетная запись целиком.

Д1. Создание вложенного файлового информационного ресурса. Расширение доступа
Данная задача возникает, когда к некоторому каталогу файлового информационного ресурса необходимо предоставить доступ дополнительной группе лиц (расширить доступ). При этом выполняются следующие мероприятия:

1. Регистрируется вложенный файловый информационный ресурс (согласно процессу А)

2. В группы доступа пользователей, вложенного файлового информационного ресурса, добавляются группы доступа пользователей вышестоящего составного файлового информационного ресурса.

Д2. Создание вложенного файлового информационного ресурса. Сужение доступа

Данная задача возникает, когда к некоторому каталогу файлового информационного ресурса необходимо ограничить доступ и предоставить его только ограниченной группе лиц:

1. Регистрируется вложенный файловый информационный ресурс (согласно процессу А)
2. В группы доступа пользователей создаваемого информационного ресурса помещаются те учетные записи пользователей, которым требуется предоставить доступ.

Е. Изменение модели предоставления доступа к файловому информационному ресурсу

В случаях, когда к стандартным вариантам полномочий «Только чтение (Read only)» или «Чтение и запись (Read & Write)» необходимо добавить новые типы полномочий, например, «Чтение и запись, кроме удаления (Read & Write without Remove)» выполняют следующие действия:

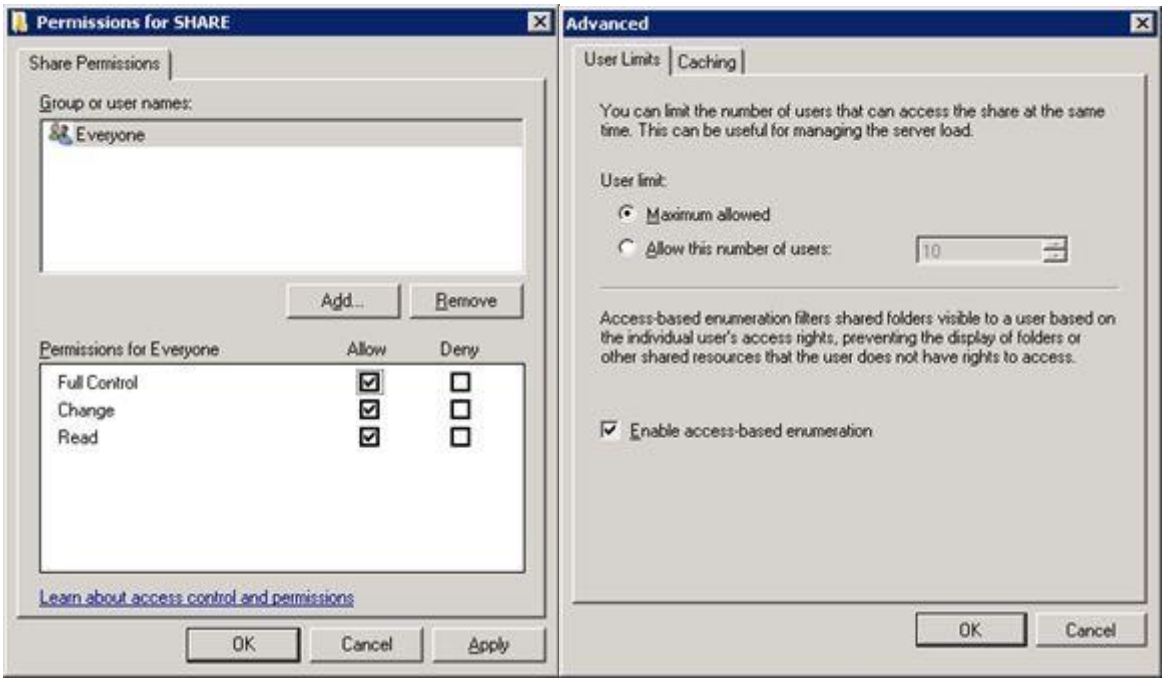
1. Организационными (или техническими, но не связанными с изменением прав доступа к каталогам файловой системы) мерами блокируется доступ пользователей к данному и всем вложенным файловым информационным ресурсам.
2. К корневому каталогу файлового информационного ресурса назначаются новые права доступа, при этом заменяются права доступа для всех дочерних объектов (активируется наследие).
3. Перенастраиваются права доступа для всех вложенных информационных ресурсов.
4. Настраиваются промежуточные каталоги для данного и вложенных информационных ресурсов.

Примеры

Рассмотрим применение данного стандарта на примере гипотетической организации ООО «ИнфоКриптоСервис», где для централизованного хранения файловых информационных ресурсов выделен сервер с именем «FILESRV». Сервер работает под управлением операционной системы Microsoft Windows Server 2008 R2 и является членом домена Active Directory с FQDN именем «domain.ics» и NetBIOS именем «ICS».

Подготовка файлового сервера

На диске «D:» сервера «FILESRV» создаем каталог «D:\SHARE\». Этот каталог будет единой точкой входа во все файловые информационные ресурсы, размещенные на данном сервере. Организуем сетевой доступ к данной папке (используем апплет «Share and Storage Management»):



Создание файлового информационного ресурса

Постановка задачи.

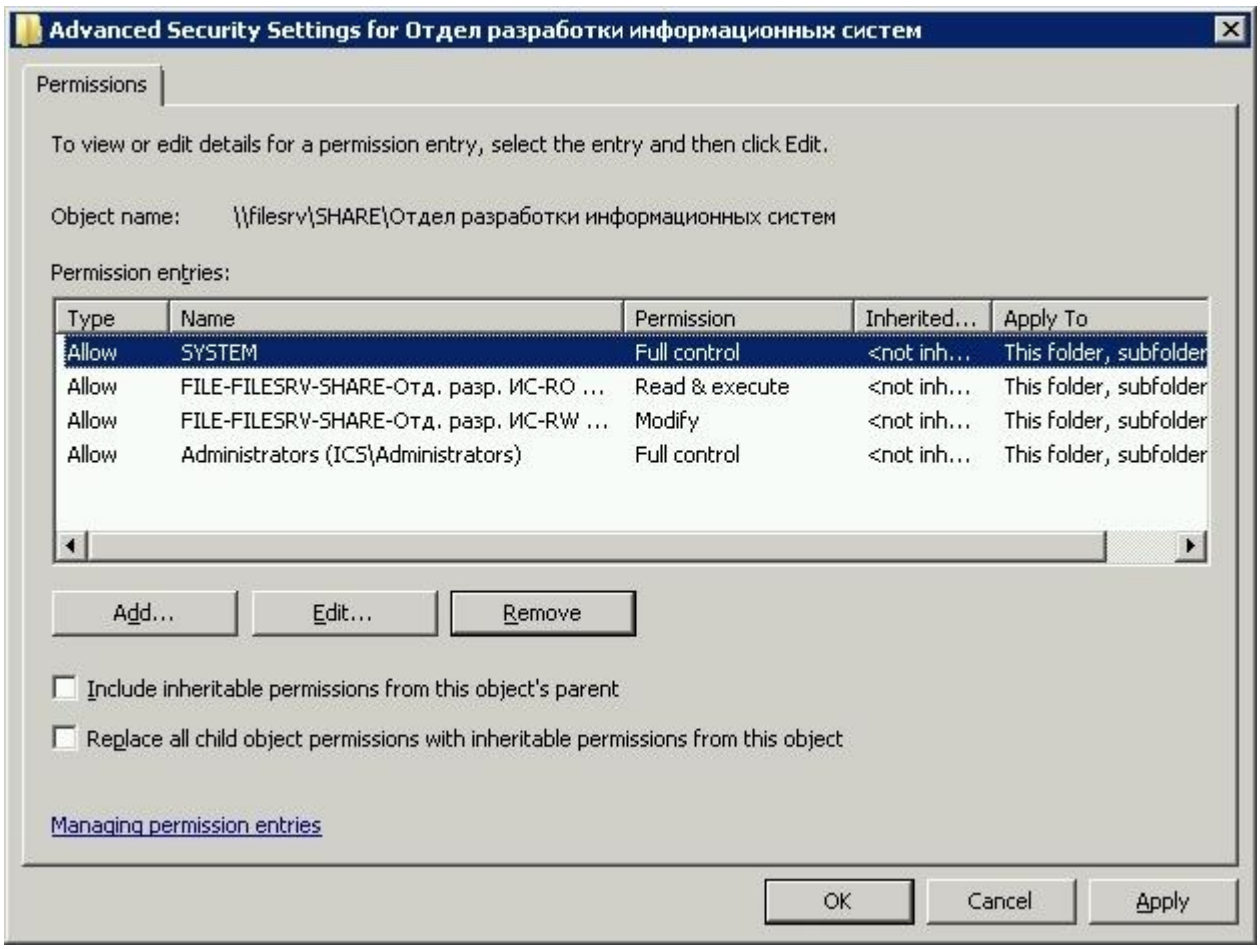
Пусть в составе организации ООО «ИнфоКриптоСервис» имеется Отдел разработки информационных систем в составе: начальника отдела Иванова Сергея Леонидовича (SL.Ivanov@domain.ics), специалиста Маркина Льва Борисовича (LB.Markin@domain.ics), и для них нужно организовать файловый информационный ресурс для хранения данных подразделения. Обоим работникам требуется доступ на чтение и запись к данному ресурсу.

Решение.

В каталоге «D:\SHARE\» сервера «FILESRV» создадим папку «D:\SHARE\Отдел разработки информационных систем\», которая будет корневым каталогом для файлового информационного ресурса. Также создадим группы доступа пользователей (глобальные группы безопасности домена «ICS») для данного ресурса:

- «FILE-FILESRV-SHARE-Отд. разр. ИС-RO»
- «FILE-FILESRV-SHARE-Отд. разр. ИС-RW»

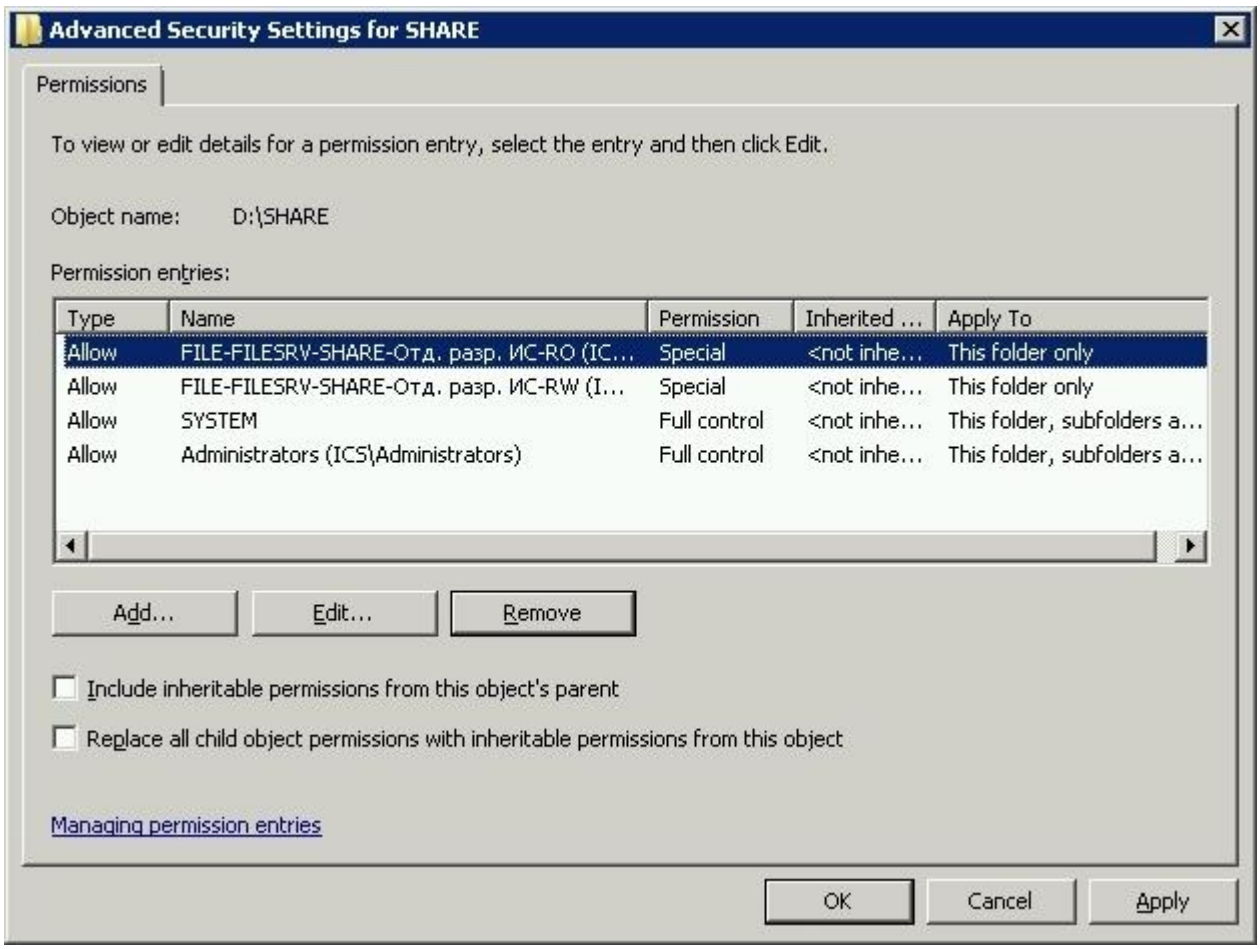
Настроим права доступа для каталога «D:\SHARE\Отдел разработки информационных систем\»:



Дамп NTFS разрешений, полученных командой cacls:

```
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-RO:(OI)(CI)R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-RW:(OI)(CI)C
NT AUTHORITY\SYSTEM:(OI)(CI)F
BUILTIN\Administrators:(OI)(CI)F
```

Каталог D:\SHARE\ является точкой входа и промежуточным каталогом для данного ресурса. Добавим в него права на проход (Traverse) для групп: «FILE-FILESRV-SHARE-Отд. разр. ИС-RO» и «FILE-FILESRV-SHARE-Отд. разр. ИС-RW»



Дамп NTFS разрешений, полученных командой cacls:

```
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-RO:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-RW:R
NT AUTHORITY\SYSTEM:(OI)(CI)F
BUILTIN\Administrators:(OI)(CI)F
```

Поскольку пользователям требуется доступ на чтение и запись, добавим их учетные запаси в группу «FILE-FILESRV-SHARE-Отд. разр. ИС-RW»

Предоставление доступа пользователю к файловому информационному ресурсу

Постановка задачи.

Предположим, в отдел разработки приняли еще одного работника – специалиста Егорова Михаила Владимировича (MB.Egorov@domain.ics), и ему, как и остальным работникам отдела, требуется доступ на чтение и запись к файловому информационному ресурсу отдела.

Решение.

Учетную запись работника необходимо добавить в группу «FILE-FILESRV-SHARE-Отд. разр. ИС-RW»

Создание вложенного информационного ресурса. Расширение доступа

Постановка задачи.

Предположим, Отдел разработки информационных систем решил улучшить качество взаимодействия с Отделом маркетинга и предоставить руководителю

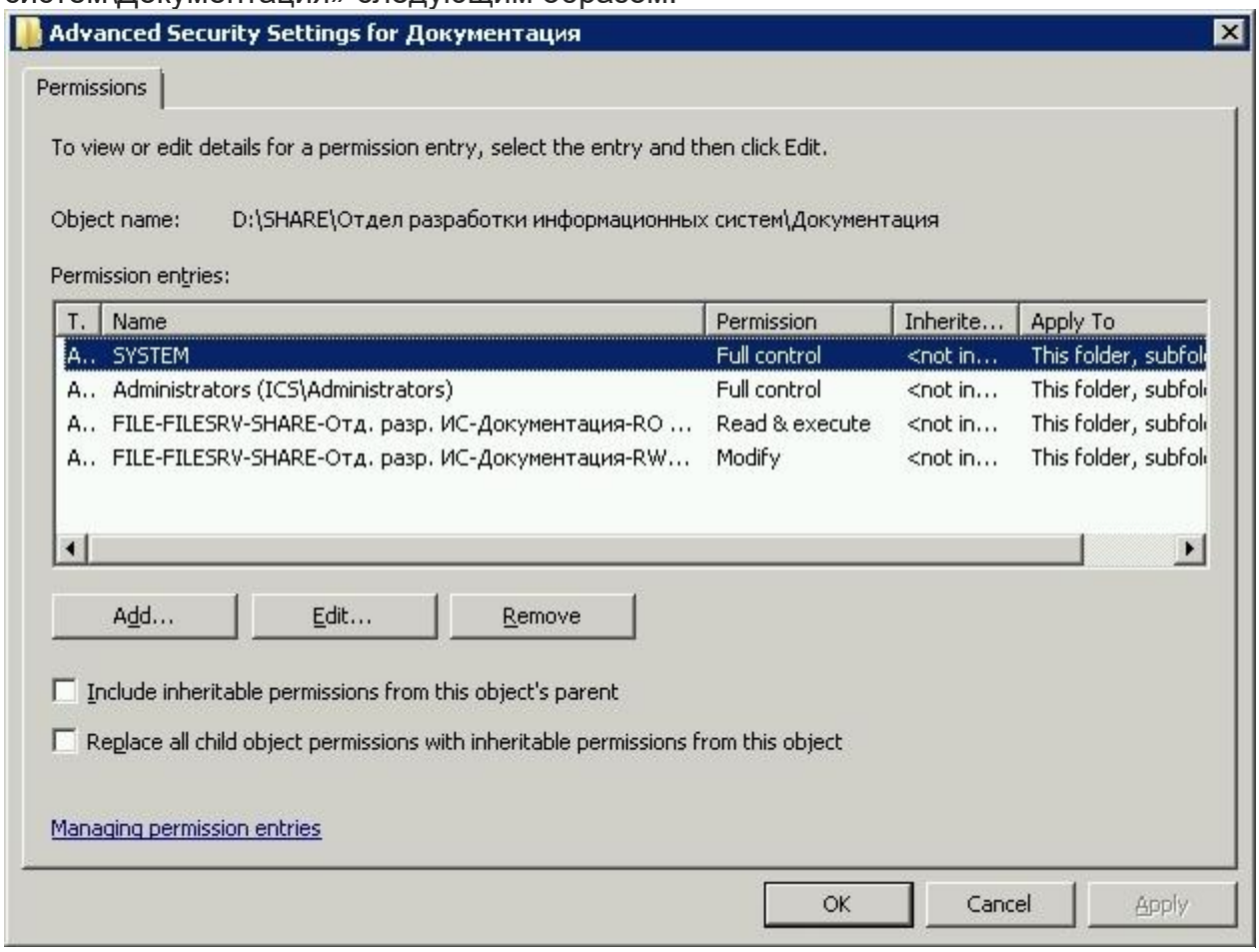
последнего — Кругликовой Наталье Евгеньевне (NE.Kruglikova@domain.ics) — доступ на чтение к актуальной документации на продукты, хранящейся в папке «Документация» файлового информационного ресурса Отдела разработки информационных систем.

Решение.
Для решения данной задачи необходимо сделать вложенный ресурс «\\FILESRV\share\Отдел разработки информационных систем\Документация», доступ к которому на чтение и запись должен быть (остаться) у всех пользователей, имевших доступ к «\\FILESRV\share\Отдел разработки информационных систем\ и добавиться доступ на чтение для пользователя Кругликовой Натальи Евгеньевне (NE.Kruglikova@domain.ics)

В каталоге «D:\SHARE\Отдел разработки информационных систем\» создадим папку «D:\SHARE\Отдел разработки информационных систем\Документация», которая будет корневым каталогом для нового ресурса. Также создадим две группы доступа пользователей:

- «FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RO»
- «FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RW»

Настроим права доступа на папку «D:\SHARE\Отдел разработки информационных систем\Документация» следующим образом:



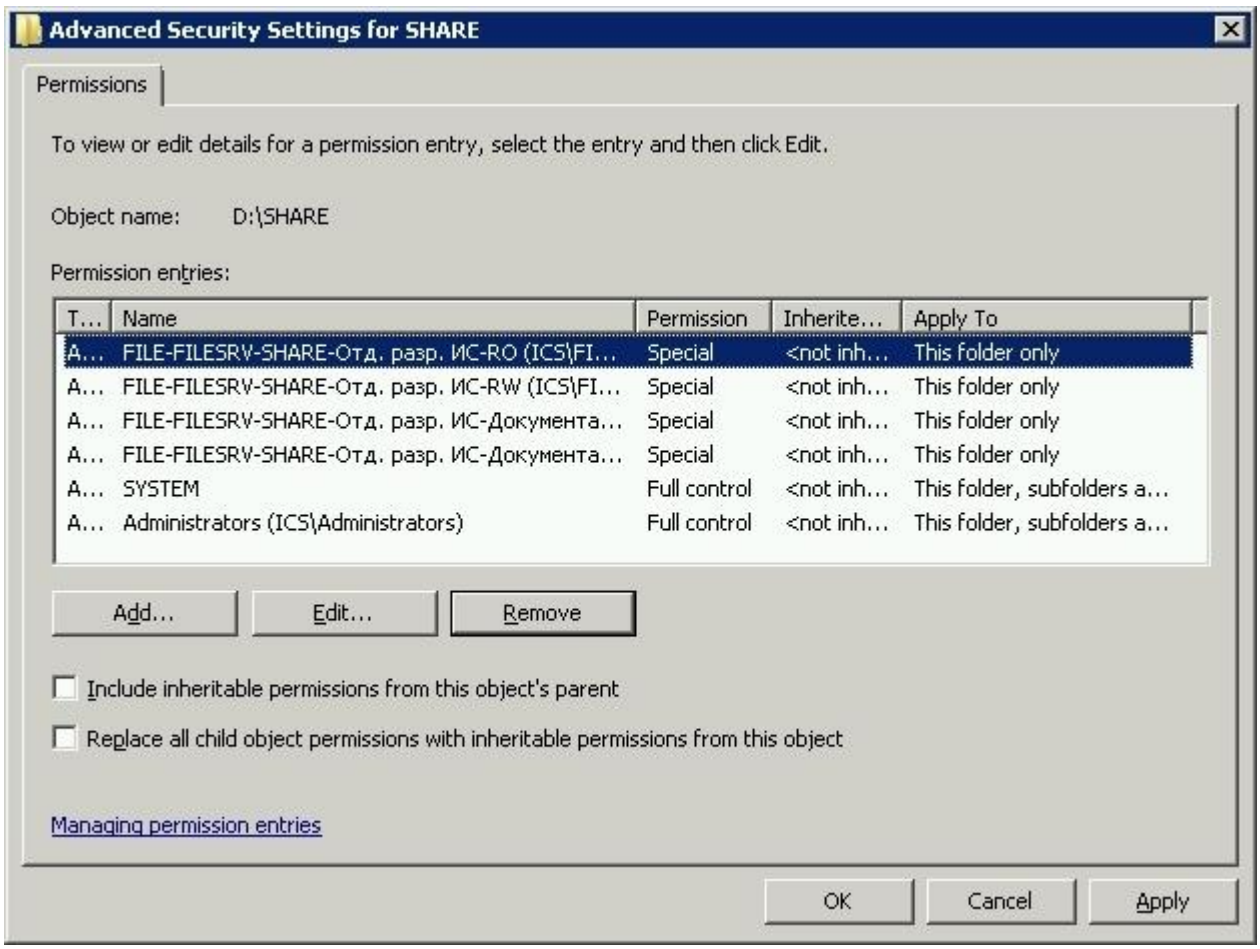
Дамп NTFS разрешений, полученных командой cacls:

```
NT AUTHORITY\SYSTEM:(OI)(CI)F
BUILTIN\Administrators:(OI)(CI)F
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RO:(OI)(CI)R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RW:(OI)(CI)C
```

Поскольку всем пользователям, имеющим доступ в «\\FILESRV\share\Отдел разработки информационных систем\», необходим аналогичный доступ в \\FILESRV\share\Отдел разработки информационных систем\Документация», то добавим группу «FILE-FILESRV-SHARE-Отд. разр. ИС-RO» в «FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RO» и «FILE-FILESRV-SHARE-Отд. разр. ИС-RW» в «FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RW» соответственно. Добавим учетную запись Кругликовой Натальи Евгеньевны (NE.Kruglikova@domain.ics) в группу «FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RW»

Теперь, если Кругликова Наталья Евгеньевна (NE.Kruglikova@domain.ics) обратится по ссылке «\\FILESRV\share\Отдел разработки информационных систем\Документация», то она сможет попасть в интересующую ее папку, но обращаться по полному пути не всегда удобно, поэтому настроим сквозной проход к данной паке от точки входа «\\FILESRV\share\» («D:\SHARE\»). Для этого настроим права доступа на промежуточные каталоги «D:\SHARE\» и «D:\SHARE\Отдел разработки информационных систем\».

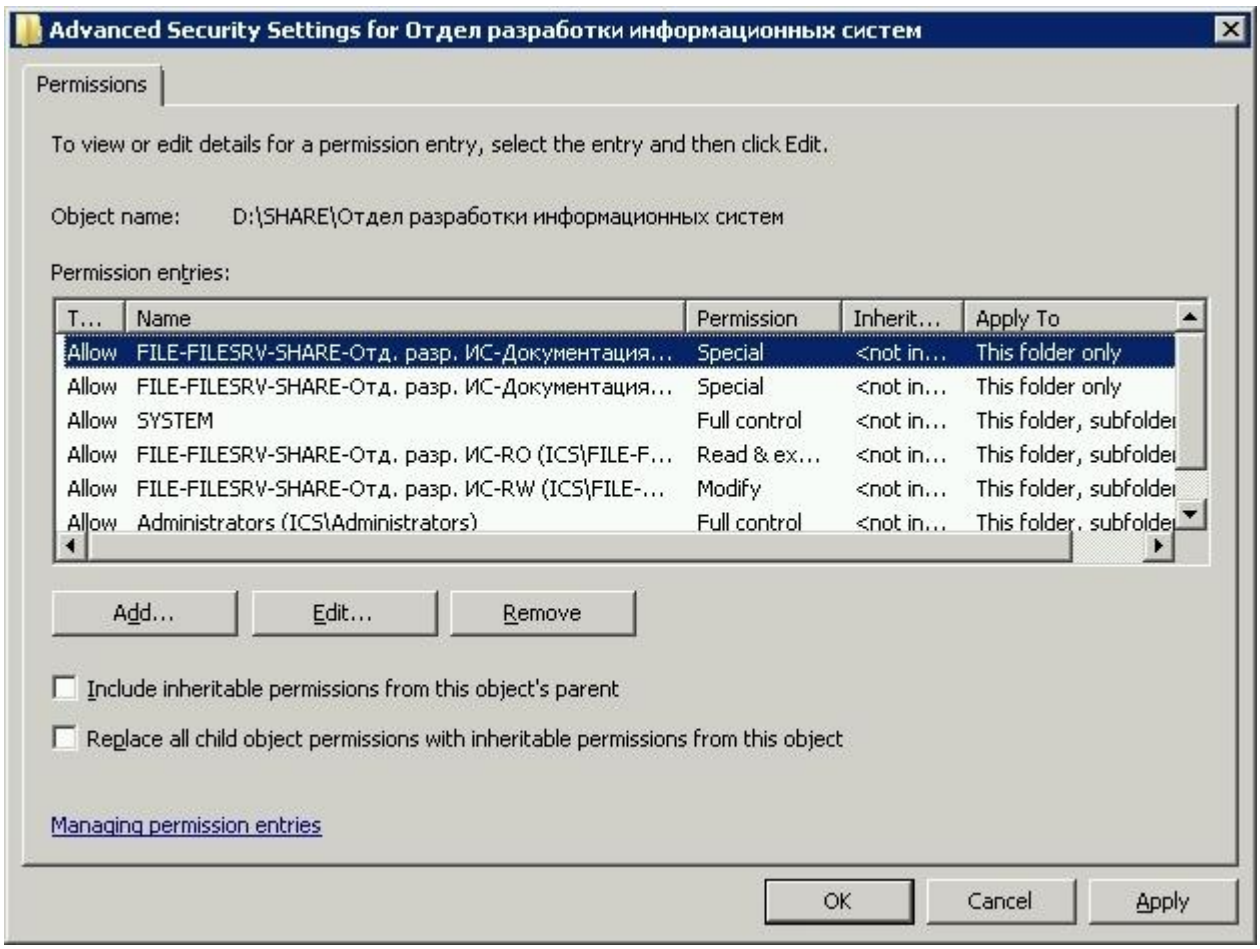
Проведем настройку «D:\SHARE\»:



Дамп NTFS разрешений, полученных командой cacls:

```
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-RO:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-RW:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RO:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RW:R
NT AUTHORITY\SYSTEM:(OI)(CI)F
BUILTIN\Administrators:(OI)(CI)F
```

и «D:\SHARE\Отдел разработки информационных систем»:



Дамп NTFS разрешений, полученных командой cacls:

```
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RO:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RW:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-RO:(OI)(CI)R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-RW:(OI)(CI)C
NT AUTHORITY\SYSTEM:(OI)(CI)F
BUILTIN\Administrators:(OI)(CI)F
```

Создание вложенного информационного ресурса. Сужение доступа

Постановка задачи

В целях организации резервного копирования наработок Отдела разработки информационных систем начальнику отдела Иванову Сергею Леонидовичу (SL.Ivanov@domain.ics), в рамках файлового информационного ресурса отдела, понадобилась сетевая папка «Архив», доступ к которой был бы только у него.

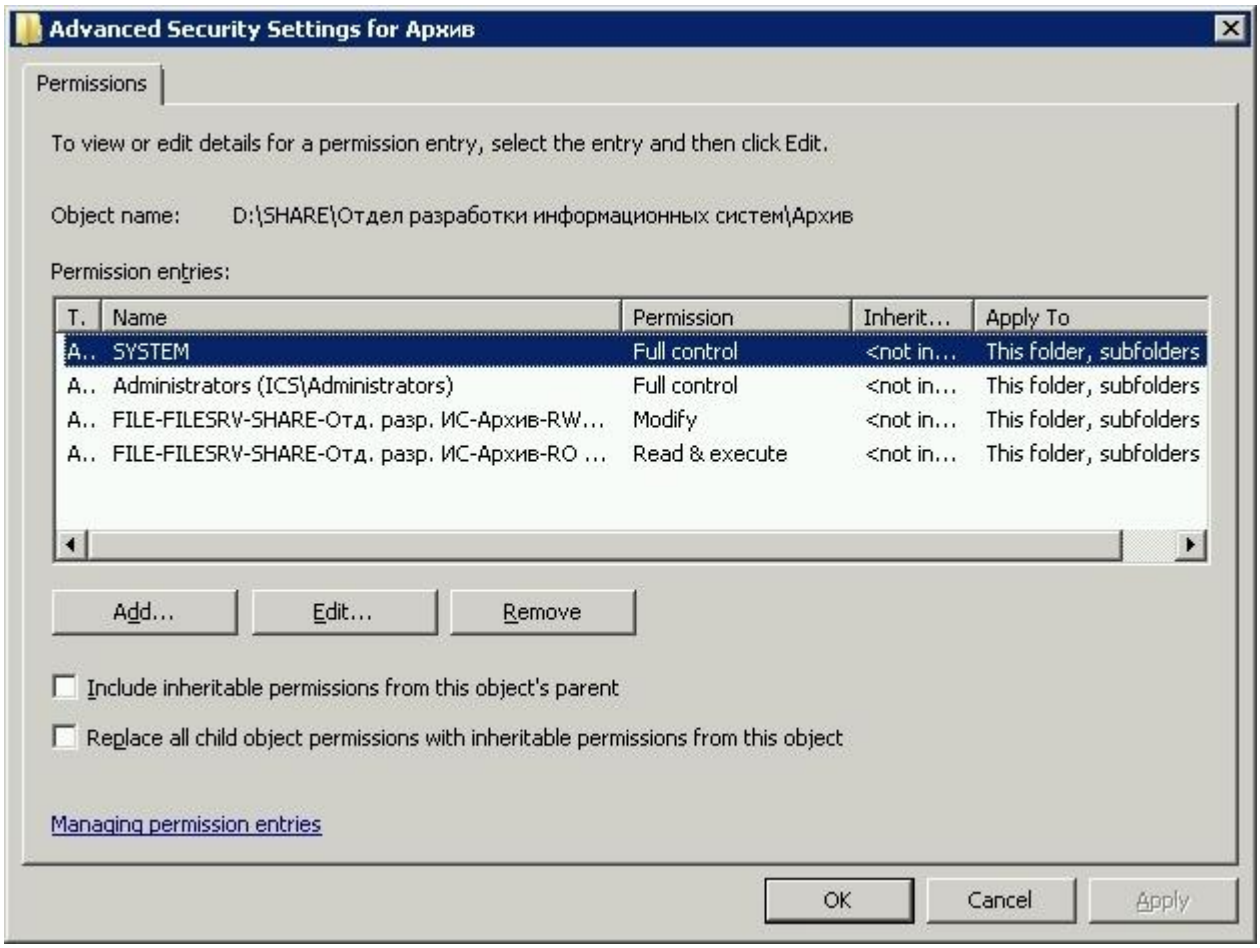
Решение.

Для решения данной задачи в файловом информационном ресурсе отдела требуется сделать вложенный ресурс «Архив» («\\FILESRV\share\Отдел разработки информационных систем\Архив»), доступ к которому предоставить только начальнику отдела.

В каталоге «D:\SHARE\Отдел разработки информационных систем\» создадим папку «D:\SHARE\Отдел разработки информационных систем\Архив», которая будет корневым каталогом для нового ресурса. Также создадим две группы доступа пользователей:

- «FILE-FILESRV-SHARE-Отд. разр. ИС-Архив-RO»
- «FILE-FILESRV-SHARE-Отд. разр. ИС-Архив-RW»

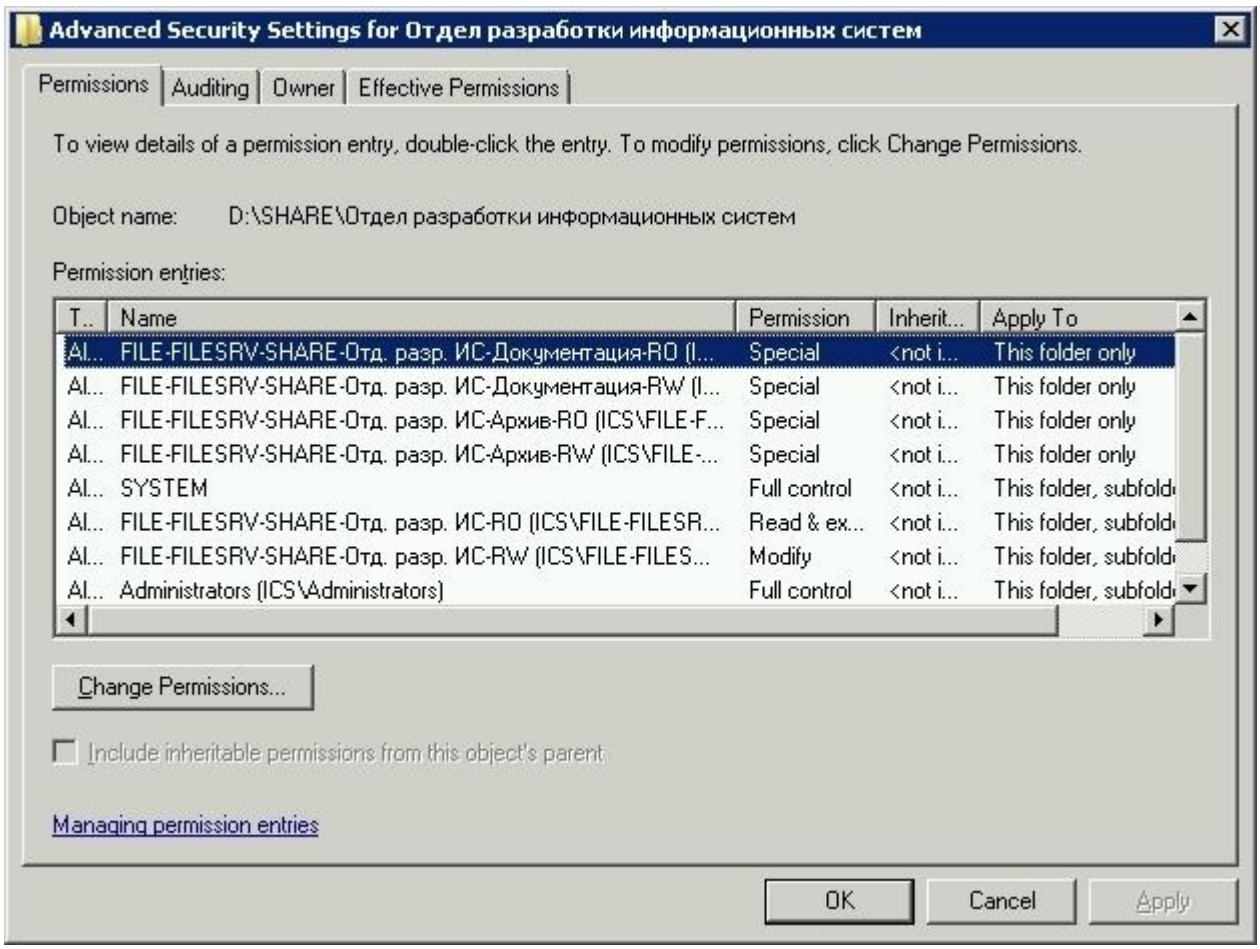
Проведем настройки прав доступа на каталоги «D:\SHARE\Отдел разработки информационных систем\Архив»:



Дамп NTFS разрешений, полученных командой cacls:

```
NT AUTHORITY\SYSTEM:(OI)(CI)F
BUILTIN\Administrators:(OI)(CI)F
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Архив-RO:(OI)(CI)R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Архив-RW:(OI)(CI)C
```

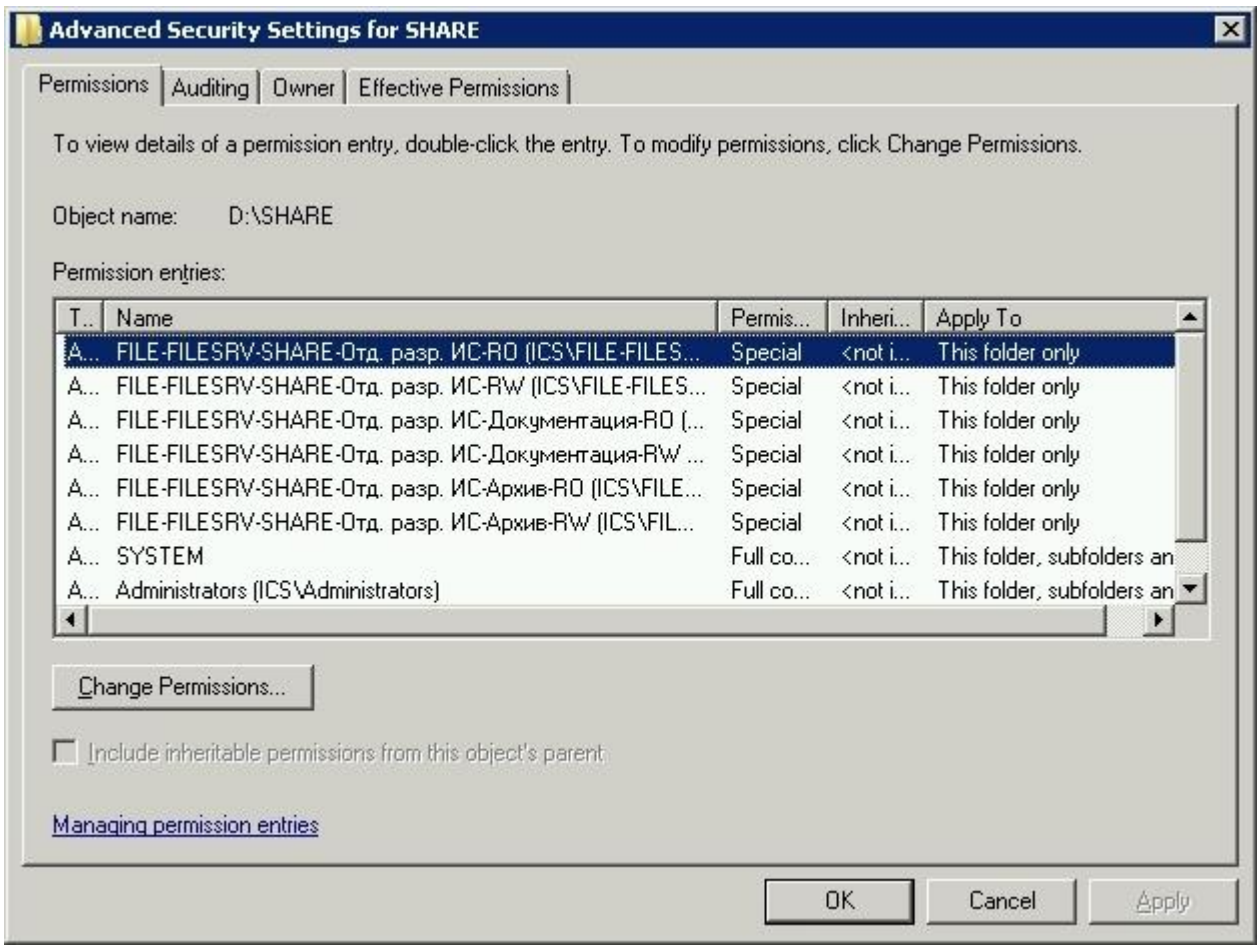
«D:\SHARE\Отдел разработки информационных систем»



Дамп NTFS разрешений, полученных командой cacls:

```
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RO:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RW:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Архив-RO:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Архив-RW:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-RO:(OI)(CI)R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-RW:(OI)(CI)C
NT AUTHORITY\SYSTEM:(OI)(CI)F
BUILTIN\Administrators:(OI)(CI)F
```

и «D:\SHARE\»:



Дамп NTFS разрешений, полученных командой cacls:

```
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-RO:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-RW:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RO:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Документация-RW:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Архив-RO:R
ICS\FILE-FILESRV-SHARE-Отд. разр. ИС-Архив-RW:R
NT AUTHORITY\SYSTEM:(OI)(CI)F
BUILTIN\Administrators:(OI)(CI)F
```

Учетную запись пользователя Иванова Сергея Леонидовича (SL.Ivanov@domain.ics) добавим в группу FILE-FILESRV-Отд. раз.ИС-Архив-RW.