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:

_____ Сухоруков В.А.

(подпись) (фамилия, и.,о.)

19-ВМ

(шифр группы)

Работа защищена «___»_____

С оценкой _____

Нижний Новгород 2022

Оглавление

Цель работы

Ознакомиться с основными задачами управления доступом к ресурсам, составом и назначением встроенных субъектов безопасности Windows. Изучить смысл и применение 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 доступом к ресурсам Windows

Теория:

Субъект безопасности - это любая сущность, которая может быть проверена службой операционной системы, например учетная запись пользователя, учетная запись компьютера или поток или процесс, который выполняется в контексте безопасности пользователя, учетная запись компьютера или группы безопасности для этих учетных записей. Субъекты безопасности являются основой для управления доступом к защищаемым ресурсам на компьютерах с Windows. Каждому субъекту безопасности представлен уникальный идентификатор безопасности (SID) в операционной системе.

Субъекты безопасности выполняют действия (включая чтение, запись, изменение или полный доступ) над объектами. В число объектов входят файлы, папки, принтеры, ключи реестра и объекты доменных служб Active Directory (AD DS). Общие ресурсы используют списки управления доступом (ACL) для назначения разрешений. Это позволяет диспетчерам ресурсов реализовывать управление доступом следующими способами:

- ❖ отказ в доступе неавторизованным пользователям и группам;
- ❖ установка четко определенных ограничений на доступ, предоставляемый авторизованным пользователям и группам.

Состав субъектов безопасности можно получить в свойствах объекта безопасности, на вкладке «Безопасность». Выбрать пункт «Изменить», «Добавить».

Практическое выполнение:

- Приведем в таблице состав субъектов безопасности для узла-члена домена, размещенных на компьютере.

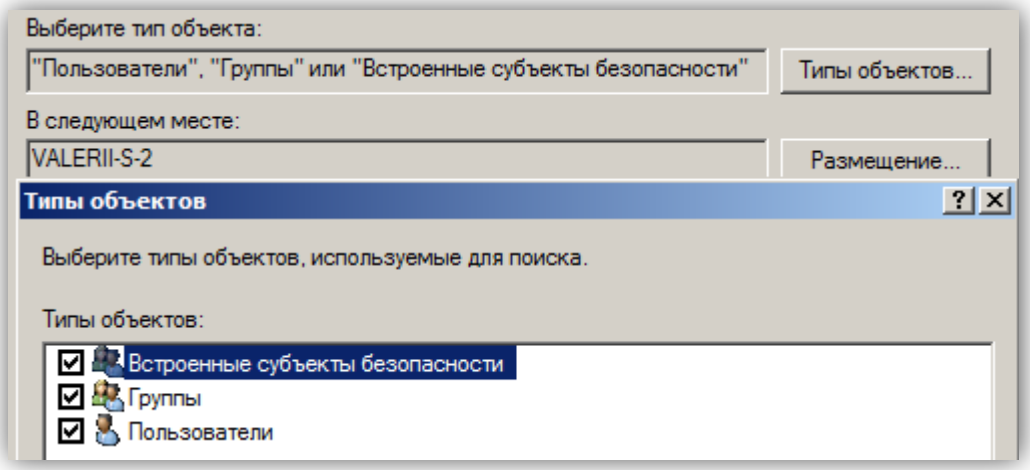


Рис 1.

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
Валерий	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

Таблица 1.

- На контроллере домена отсутствуют локальные субъекты безопасности.

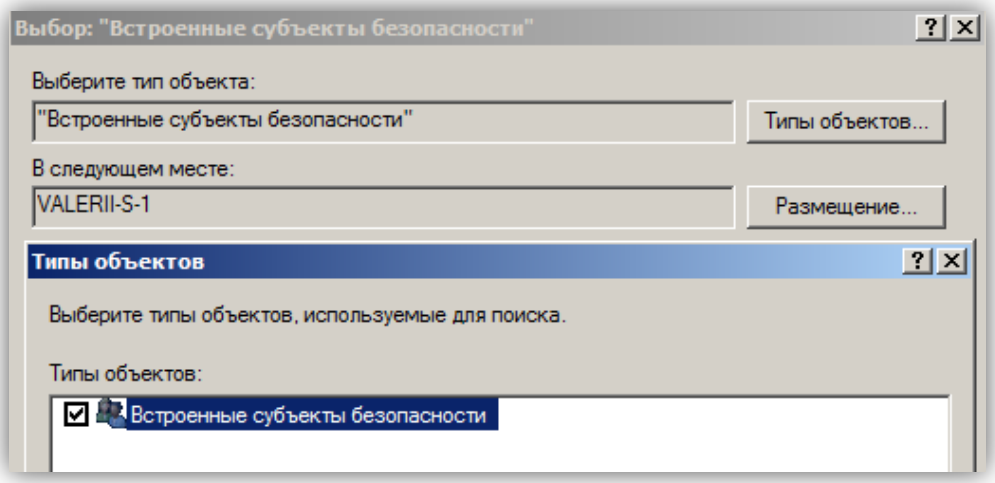


Рис 2.

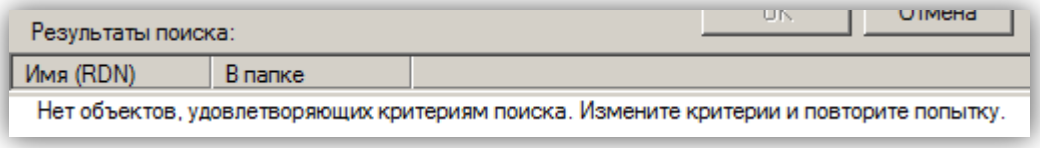


Рис 3.

- Приведем в таблице состав субъектов безопасности для узла-члена домена, размещенных в домене.

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
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
Яша	Добавленная учетная запись пользователя домена	S-1-5-21-4675…024-1009
Сотрудник службы охраны	Добавленная глобальная группа домена	S-1-5-21-4675…024-1116

Таблица 2.

Учетные записи служб и специальные группы совпадают с таблицей 1.

- 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 собранных данных:

❖ 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.

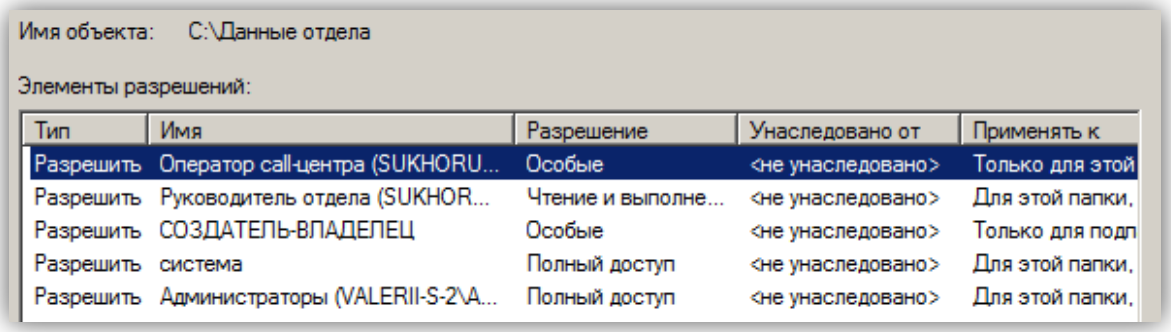
❖ Доменные субъекты безопасности могут быть использованы для ограничения/разрешения доступа к ресурсам по сети, поскольку они имеют уникальные SID'ы.

2. Доступ к каталогам и файлам

2.1. Назначение разрешений

Практическое выполнение:

В корне диска С создадим папку «Данные отдела». Разрешим доступ к ней группам «Оператор call-центра» и «Руководитель отдела».

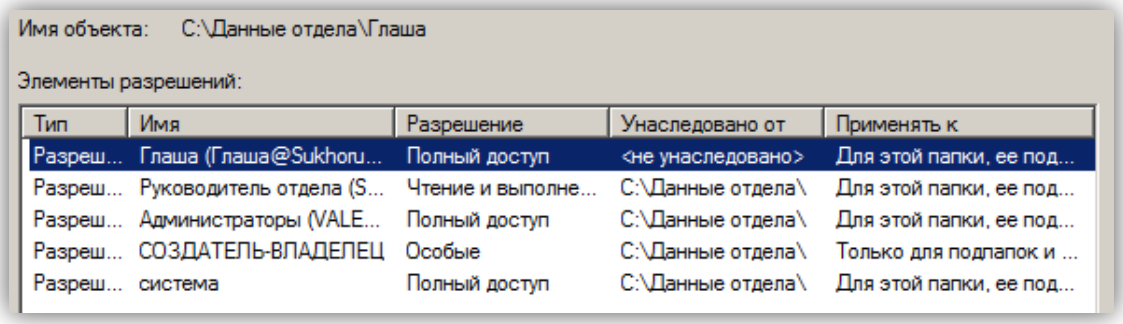

Имя объекта: C:\Данные отдела

Элементы разрешений:

Тип	Имя	Разрешение	Унаследовано от	Применять к
Разрешить	Оператор call-центра (SUKHORU...	Особые	<не унаследовано>	Только для этой
Разрешить	Руководитель отдела (SUKHOR...	Чтение и выполне...	<не унаследовано>	Для этой папки,
Разрешить	СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ	Особые	<не унаследовано>	Только для подп
Разрешить	система	Полный доступ	<не унаследовано>	Для этой папки,
Разрешить	Администраторы (VALERII-S-2\A...	Полный доступ	<не унаследовано>	Для этой папки,

Рис 4.

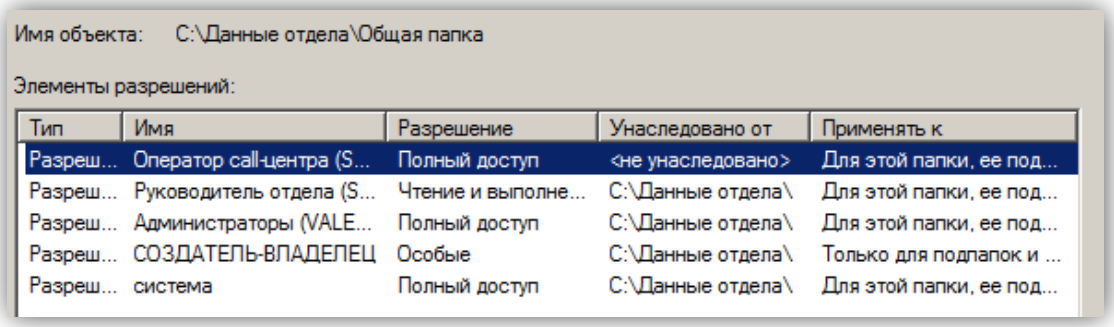
Внутри создадим каталоги для каждого члена отдела с соответствующими правами (Рис 5), и общий каталог (Рис 6).


Имя объекта: C:\Данные отдела\Глаша

Элементы разрешений:

Тип	Имя	Разрешение	Унаследовано от	Применять к
Разреш...	Глаша (Глаша@Sukhoru...	Полный доступ	<не унаследовано>	Для этой папки, ее под...
Разреш...	Руководитель отдела (S...	Чтение и выполне...	C:\Данные отдела\	Для этой папки, ее под...
Разреш...	Администраторы (VALE...	Полный доступ	C:\Данные отдела\	Для этой папки, ее под...
Разреш...	СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ	Особые	C:\Данные отдела\	Только для подпапок и ...
Разреш...	система	Полный доступ	C:\Данные отдела\	Для этой папки, ее под...

Рис 5.


Имя объекта: C:\Данные отдела\Общая папка

Элементы разрешений:

Тип	Имя	Разрешение	Унаследовано от	Применять к
Разреш...	Оператор call-центра (S...	Полный доступ	<не унаследовано>	Для этой папки, ее под...
Разреш...	Руководитель отдела (S...	Чтение и выполне...	C:\Данные отдела\	Для этой папки, ее под...
Разреш...	Администраторы (VALE...	Полный доступ	C:\Данные отдела\	Для этой папки, ее под...
Разреш...	СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ	Особые	C:\Данные отдела\	Только для подпапок и ...
Разреш...	система	Полный доступ	C:\Данные отдела\	Для этой папки, ее под...

Рис 6.

Проверим выполнение разрешений с учетной записи Саша.

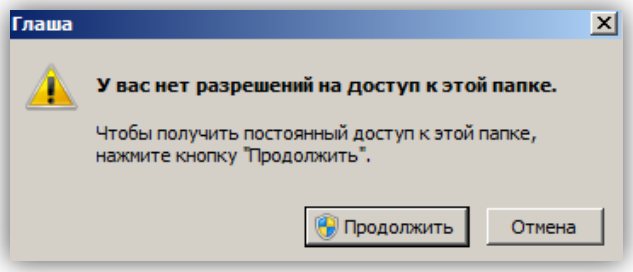


Рис 7.

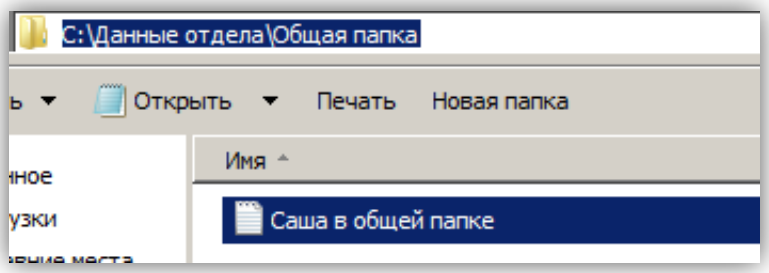


Рис 8.

2.2. Использование команды icacls

Теория:

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) - системный список управления доступом.
- Discretionary Access-Control List (DACL) - список управления избирательным доступом.

SACL управляется системой и используется для обеспечения аудита попыток доступа к объектам файловой системы, определяя условия при которых генерируется события безопасности. SACL используется еще и для реализации механизма защиты системы с использованием уровней целостности (Integrity Level, IL).

DACL - список управления доступом ACL, формирует правила, определяющие, кому разрешить доступ к объекту, а кому - запретить.

Каждый список контроля доступа (ACL) представляет собой набор элементов (записей) контроля доступа - Access Control Entries, или ACE) . Записи ACE бывают двух типов (разрешающий и запрещающий доступ), и содержит три поля:

- SID пользователя или группы, к которому применяется данное правило
- Вид доступа, на которое распространяется данное правило
- Тип ACE - разрешающий или запрещающий.

Практическое выполнение:

Команда icacls позволяет отображать или изменять списки управления доступом (Access Control Lists) к файлам и папкам файловой системы.

```
C:\Данные отдела\Глаша>icacls "C:\Данные отдела\Глаша"
C:\Данные отдела\Глаша SUKHORUKOV\Глаша:(OI)(CI)(F)
                       SUKHORUKOV\Руководитель отдела:(I)(OI)(CI)(RX)
                       BUILTIN\Администраторы:(I)(F)
                       СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ:(I)(OI)(CI)(IO)(F)
                       NT AUTHORITY\система:(I)(OI)(CI)(F)
                       BUILTIN\Администраторы:(I)(OI)(CI)(IO)(F)

Успешно обработано 1 файлов; не удалось обработать 0 файлов
```

Рис 9.

- Для учетной записи «Глаша» включено наследование для файлов(CI) и каталогов(OI) и полный доступ к данному каталогу (F).
- Для группы «Руководитель отдела» разрешения унаследованы от родительского каталога (I), разрешено наследования для файлов и каталогов нижнего уровня (CI и OI), установлен доступ на чтение и выполнение(RX).
- Создатель владелец имеет полный доступ и наследует данные разрешения для файлов и каталогов.

С помощью ключа /inheritance:d отключим наследование разрешений.

```
C:\Users\Администратор.SUKHORUKOV>icacls "C:\Данные отдела\Глаша" /inheritance:d
обработанный файл: C:\Данные отдела\Глаша
Успешно обработано 1 файлов; не удалось обработать 0 файлов

C:\Users\Администратор.SUKHORUKOV>icacls "C:\Данные отдела\Глаша"
C:\Данные отдела\Глаша SUKHORUKOV\Глаша:(OI)(CI)(F)
                       SUKHORUKOV\Руководитель отдела:(OI)(CI)(RX)
                       BUILTIN\Администраторы:(F)
                       СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ:(OI)(CI)(IO)(F)
                       NT AUTHORITY\система:(OI)(CI)(F)
                       BUILTIN\Администраторы:(OI)(CI)(IO)(F)

Успешно обработано 1 файлов; не удалось обработать 0 файлов
```

Рис 10.

3. Варианты разрешений доступа к каталогам и файлам

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

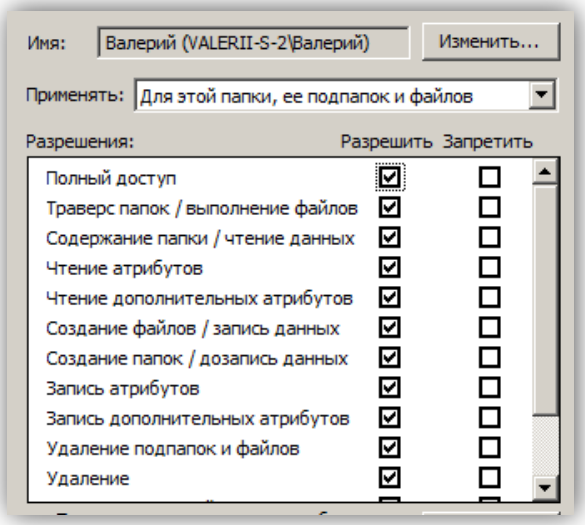


Рис 11.

Соотнесем допустимые действия для файлов и каталогов с разрешениями, которые необходимы для выполнения этих действий.

- ❖ Создание файлов и папок. Необходимо разрешить:
  - Содержание папки/Чтение данных
  - Создание файлов/Запись данных
  - Создание папок/Дозапись данных
- ❖ Удаление не пустой папки. Необходимо разрешить:
  - Содержание папки/Чтение данных
  - Удаление подпапок и файлов
  - Удаление
- ❖ Копирование файла. Необходимо разрешить:
  - Чтение атрибутов
  - Чтение дополнительных атрибутов
  - Содержание папки/Чтение данных
- ❖ Перемещение. Необходимо разрешить:
  - Удаление
- ❖ Получение информации о свойствах. Необходимо разрешить:
  - Чтение атрибутов

Рассмотрим случай, когда разрешение «Удаление» установлено для папки, но не установлено для файлов, входящих в эту папку. При попытке удалить папку возникает ошибка доступа для внутреннего файла.

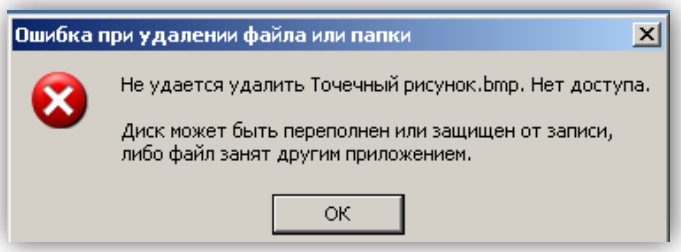


Рис 12.

Соотнесём стандартные для NTFS разрешения для каталогов с возможными действиями над каталогом:

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	+	+	-	-	-	-

Таблица 3.

Возможность смены владельца есть только у учетной записи администратора, и у текущего владельца.

Соотнесём стандартные для NTFS разрешения для файлов с возможными действиями над каталогом:

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

Таблица 4.

Вывод:

Для каталогов существует 6 стандартных разрешений, а для файлов 5. Комбинируя стандартные разрешения можно получить необходимую нам конфигурацию разрешенных и запрещенных действий для каталога или файла.

4. Наследование разрешений

Теория:

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.

Недостаток данного свойства в том, что для сложной иерархии каталогов трудно согласовывать разрешения при наследовании.

Особенности наследования при копировании и перемещении файлов:

- ❖ При копировании объекта с одного тома на другой, копируемый объект всегда получает права или разрешения того раздела (или расположенного в нём каталога), в который он копируется. Те же правила действуют при перемещении файлов между разными томами.
- ❖ При перемещении в пределах одного тома, перемещаемый объект сохраняет свою ACL.
- ❖ При копировании в пределах одного тома копируемый объект получает ACL от ближайшего вышестоящего родительского каталога.

Практическое выполнение:

4.1. Использование наследования

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

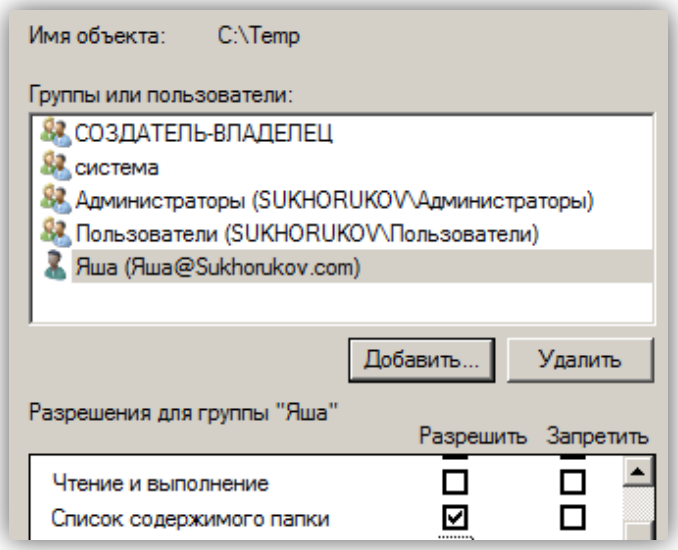


Рис 13.

Далее создадим вложенный каталог и проверим его разрешения, как видим каталог Temp2 унаследовал разрешение L от каталога Temp.

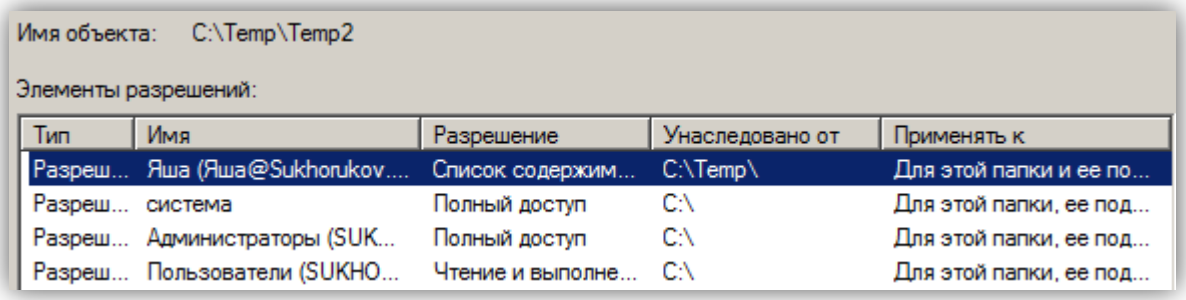


Рис 14.

Теперь попробуем указать разрешения для вложенного каталога явно. Добавим к унаследованным разрешениям дополнительное разрешение W.

В списке разрешений вложенного каталога Temp2 появилось ещё одно разрешение(W) для пользователя Яша и оно не унаследовано.

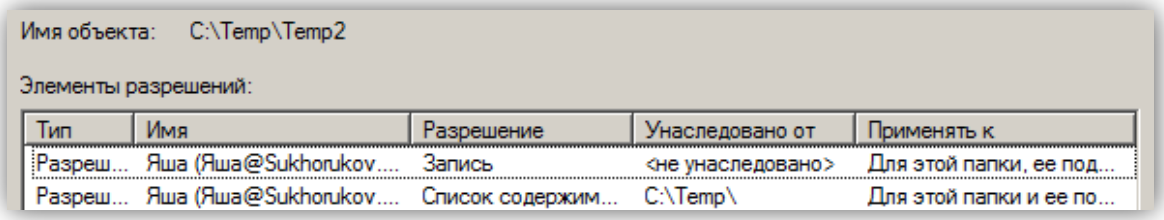


Рис 15.

Зайдем, используя учетную запись Яша и попробуем произвести запись в каталоге.

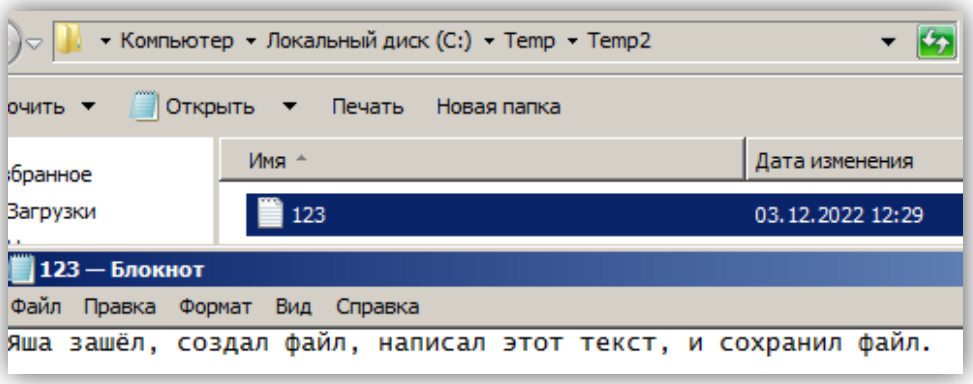


Рис 16.

Вывод:

Таким образом, можно сделать вывод, что явно указанные разрешения преобладают над унаследованными.

4.2. Целесообразное и нецелесообразное применения наследования.

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).

4.3. 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 **test**, а в каталоге **test** создадим каталог **FC**.

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

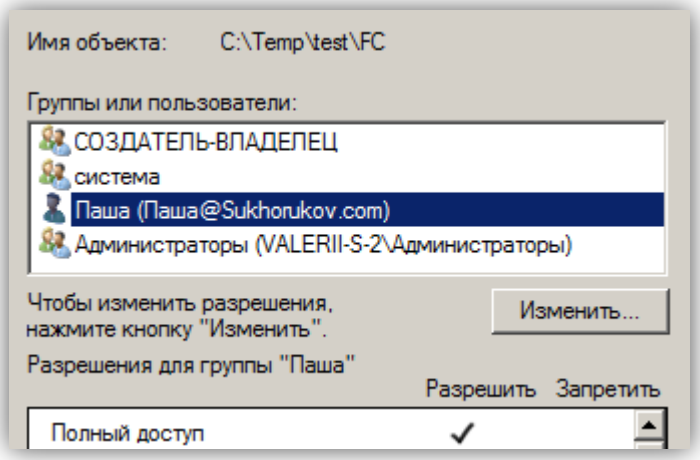


Рис 17.

Зайдем, используя учетную запись Паша. Попробуем перейти в каталог **test**, как видно на скриншоте ниже, нам отказано в доступе.

```
C:\Users\Паша>cd C:\Temp\test
Отказано в доступе.
```

Теперь попробуем перейти напрямую в каталог **FC**, как видно на скриншоте ниже нам удалось это сделать.

```
C:\Users\Паша>cd C:\Temp\test\FC

C:\Temp\test\FC>
```

Проверим разрешения доступа к каталогам используя команду **icacls.**

```
C:\Temp\test\FC>icacls C:\Temp\test
C:\Temp\test: Отказано в доступе.
Успешно обработано 0 файлов; не удалось обработать 1 файлов

C:\Temp\test\FC>icacls C:\Temp\test\FC
C:\Temp\test\FC SUKHORUKOV\Паша:(OI)(CI)(F)
                NT AUTHORITY\система:(I)(OI)(CI)(F)
                BUILTIN\Администраторы:(I)(OI)(CI)(F)
                СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ:(I)(OI)(CI)(IO)(F)
```

К каталогу **test** у нас нет доступа, а на каталог **FC** мы имеем полный доступ.

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.

5. Владение объектом

Теория:

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.

5.1. Опробовать смену владельца объекта.

Практическое выполнение:

Для некоторой каталога «Тест владельца» назначим владельца «Маша» и удалим из вкладки «Разрешения» всех, кому был доступен этот каталог. То есть, мы сделали этот каталог недоступным никому.

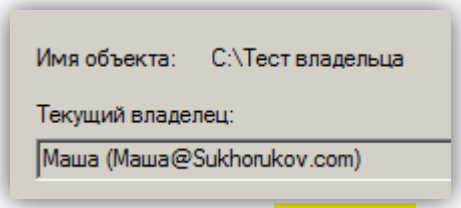


Рис 18.

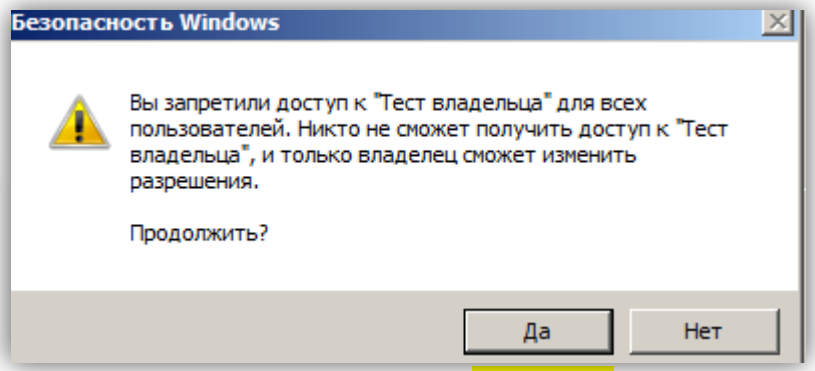


Рис 19.

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.

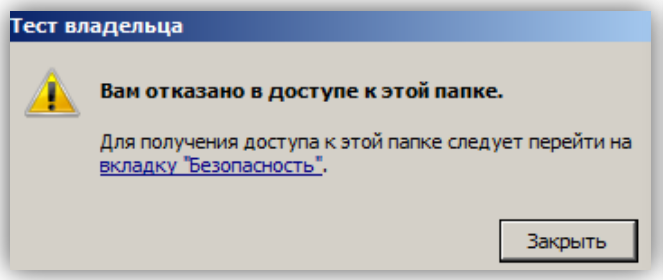


Рис 20.

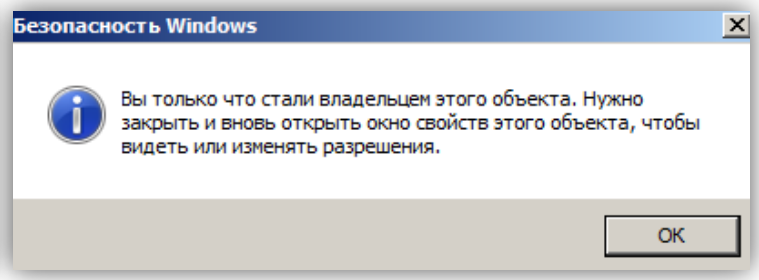


Рис 21.

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.

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

Цель:

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.

Практическое выполнение:

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.

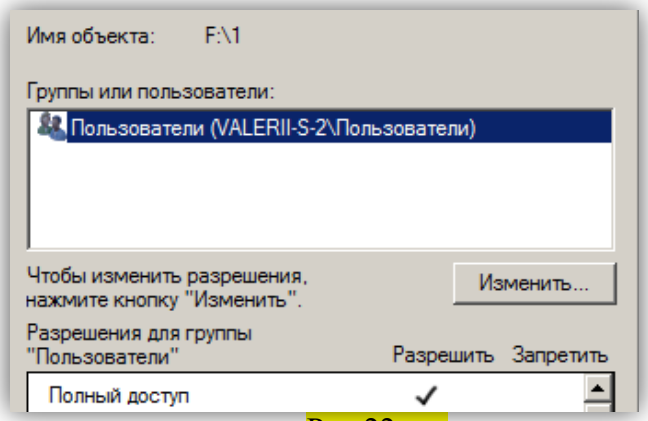


Рис 22.

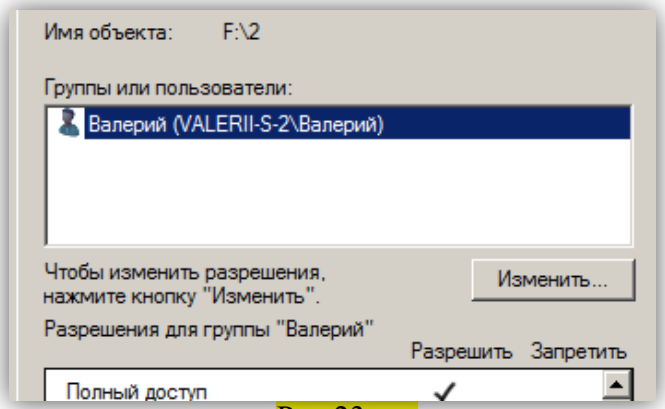


Рис 23.

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.

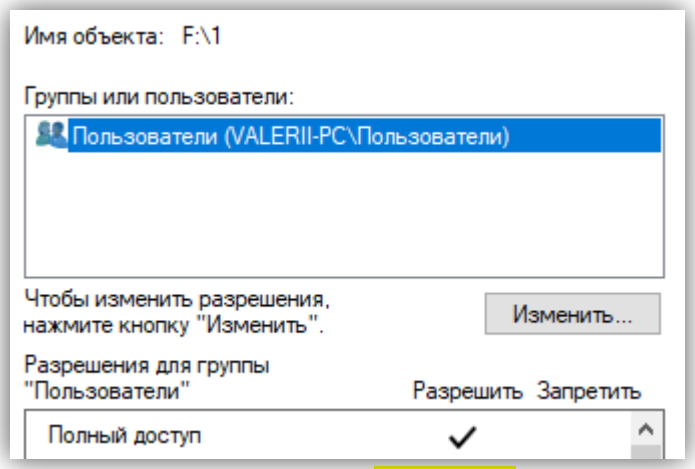


Рис 24.

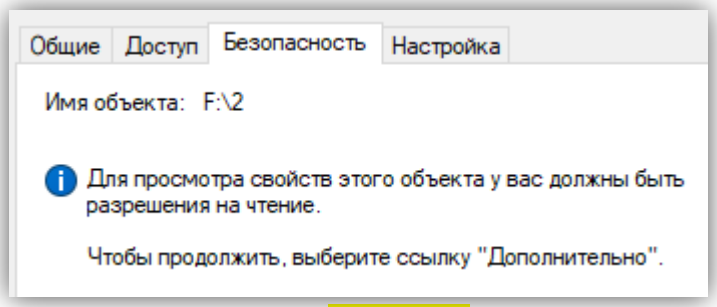


Рис 25.

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

Используя привилегию администратора, установим владельцем каталога группу «Пользователи».

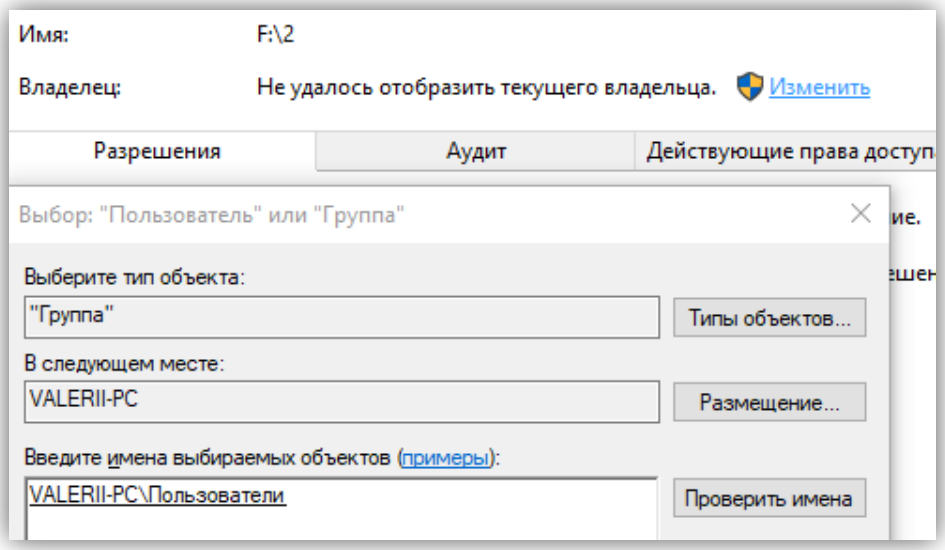


Рис 26.

Установим разрешения доступа для локальной учетной записи «Валерий».

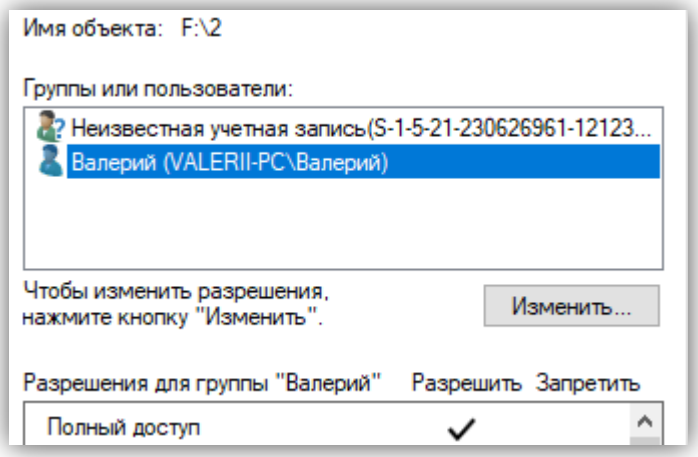


Рис 27.

Вывод:

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

6. Разрешение системных каталогов

6.1. Разрешения доступа к каталогам системного диска у разных групп, установленные по умолчанию

Выполнение:

Рассмотрим 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

Для каталогов «Windows», «Windows\system32», «Program files» действуют следующие разрешения:

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

Таблица 5.

Для каталога «Program Files» действуют следующие разрешения:

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

Таблица 6.

Для каталога «Users» действуют следующие разрешения:

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\Валерий» действуют следующие разрешения:

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	Валерий	Этой папки, её подпапок и файлов

Таблица 7.

Для Junction Point «Users\Валерий\AppData» действуют следующие разрешения:

Владелец	Разрешение	Субъекты безопасности	Применять для
Валерий	Полный доступ	Система	Этой папки, её подпапок и файлов
	Полный доступ	Администраторы	Этой папки, её подпапок и файлов
	Полный доступ	Валерий	Этой папки, её подпапок и файлов

Таблица 8.

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.

6.2. Действующие разрешения к каталогам системного диска.

В Windows есть способ просто и быстро определить, какие именно разрешения имеет конкретный пользователь на данный объект файловой системы. Для этого надо в окне расширенных свойств безопасности перейти на вкладку «Действующие разрешения», нажать «Выбрать пользователя» и найти нужного пользователя или группу.

Составим таблицу действующих разрешений для локальной группы компьютера «Valerii-S-2\Администраторы».

Разрешение	C:\	C:\Windows	C:\Program Files	C:\Users	C:\Users\ Валерий	C:\Users \Валерий \AppData
Траверс папок	+	+	+	+	+	+
Просмотр содержимого папки	+	+	+	+	+	+
Создание файлов	+	+	+	+	+	+
Создание папок	+	+	+	+	+	+
Удаление подпапок и файлов	+	-	-	+	+	+
Удаление каталога	-	-	-	+	+	+
Чтение разрешений	+	+	+	+	+	+

Смена разрешений	+	-	+	-	+	+
Смена владельца	-	-	+	-	+	+

Таблица 9.

Вывод:

Локальная группа «Администраторы», имеет возможность создания каталогов внутри служебных каталогов, но не имеет возможности их удалять. Внутри каталога пользователи у администратора полные права.

Составим таблицу действующих разрешений встроенного субъекта безопасности компьютера «Valerii-S-2\Система».

Разрешение	**C:**	**C:\Windows**	**C:\Program Files**	**C:\Users**	**C:\Users\ Валерий**	**C:\Users \Валерий \AppData**
Траверс папок	+	+	+	+	+	+
Просмотр содержимого папки	+	+	+	+	+	+
Создание файлов	+	+	+	+	+	+
Создание папок	+	+	+	+	+	+
Удаление подпапок и файлов	+	+	+	+	+	+
Удаление каталога	+	+	+	+	+	+
Чтение разрешений	+	+	+	+	+	+
Смена разрешений	+	+	+	+	+	+
Смена владельца	+	+	+	+	+	+

Таблица 10.

Вывод:

Встроенный субъект безопасности «Система» используется для управления системными каталогами: создание, удаление, редактирование внутренних каталогов. С помощью «Системы» происходит установка и удаление программ.

Составим таблицу действующих разрешений для локальной учетной записи компьютера «Valerii-S-2\Валерий».

Разрешение	**C:**	**C:\Windows**	**C:\Program Files**	**C:\Users**	**C:\Users\ Валерий**	**C:\Users \Валерий \AppData**
Траверс папок	+	+	+	+	+	+
Просмотр содержимого папки	+	+	+	+	+	+
Создание файлов	-	-	-	-	+	+
Создание папок	+	-	-	-	+	+
Удаление подпапок и файлов	-	-	-	-	+	+
Удаление каталога	-	-	-	-	+	+
Чтение разрешений	+	+	+	+	+	+
Смена разреше-	-	-	-	-	+	+

ний						
Смена владельца	-	-	-	-	+	+

Таблица 11.

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.

7. Сетевой доступ к общим файловым ресурсам

Выполнение:

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 «Оператор call-центра» были прописаны явные разрешения для файлов и каталогов на полный доступ. *Владельцем каталога устанавливается группа «Администраторы».*

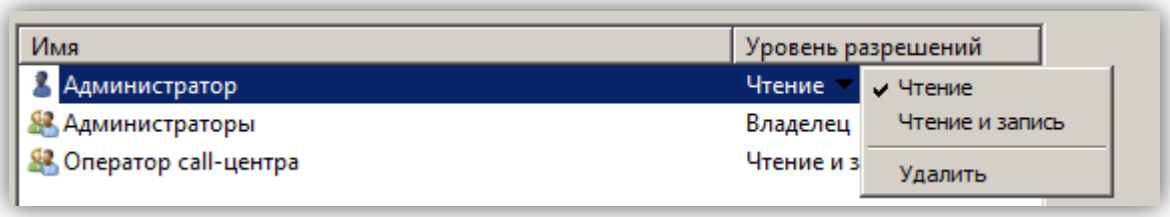


Рис 28.

На второй машине подключим папку как сетевой диск (Рис 29). Зайдем из под учетной записи, которая не входит в группу «Оператор call-центра». При попытке открытия папки выводится сообщение об ошибке доступа (Рис 30).

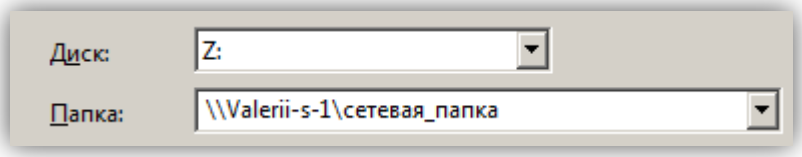


Рис 29.

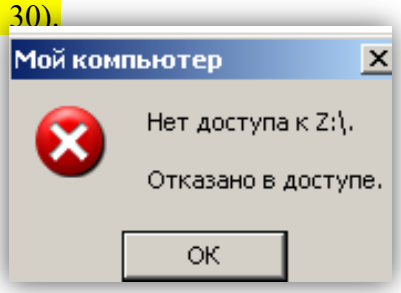


Рис 30.

Зайдем из под учетной записи Администратор. Открытие папки произошло успешно.

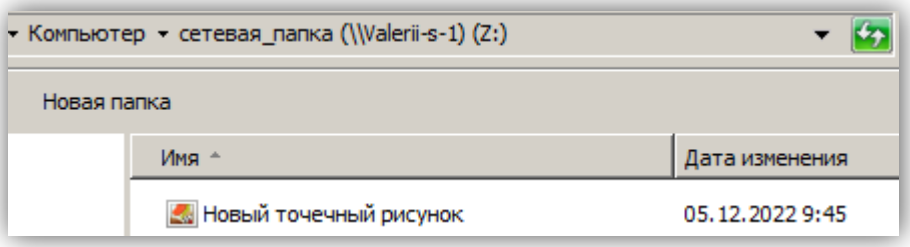


Рис 31.

Рассмотрим разрешения для сетевых ресурсов на типичные действия

Действие	FC	R	C
Чтение содержимого файла	+	+	+
Чтение владельца	+	+	+
Выполнение файла	+	+	+
Изменение файла	+	-	+
Изменение разрешений	+	-	-
Удаление файла	+	-	+
Смена владельца	-	-	-

Таблица 12.

8. Реализовать сетевую печать и проверить разрешения доступа к принтеру

8.1. Разрешения доступа

Откроем оснастку «Устройства и принтеры». Для просмотра настроек безопасности перейдём в «Свойства принтера»->»Безопасность». (Рис 32).

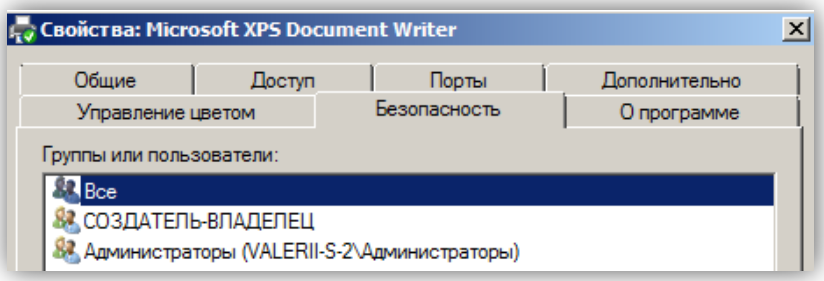


Рис 32.

Составим таблицу разрешений для субъектов безопасности.

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

Таблица 13.

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».

8.2. Сетевая печать

«Стандартный» принтер Microsoft XPS Document Writer нельзя выделить в общий доступ. Создадим новый виртуальный принтер Brother DCP-116C. Далее откроем принтер для общего доступа.

Выберем виртуальный принтер -> Свойства -> Доступ -> Общий доступ к данному принтеру. Так же отметим галочку «Внести в Active Directory» (Рис 33).

Проверим возможность печати с другого сервера, для чего установим сетевой принтер на удалённой машине (рис. 34).

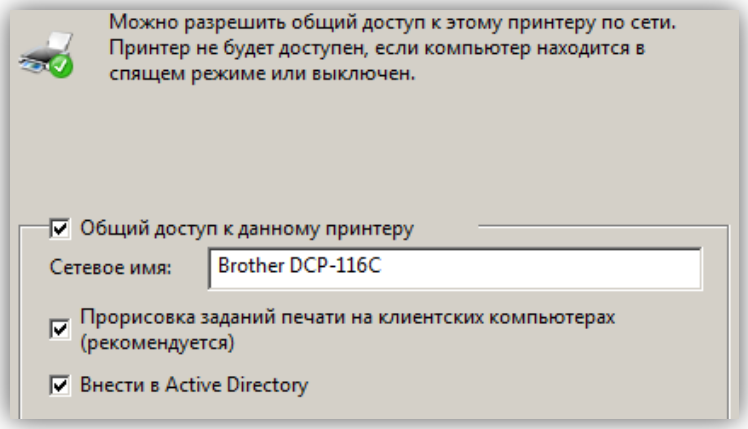


Рис 33.

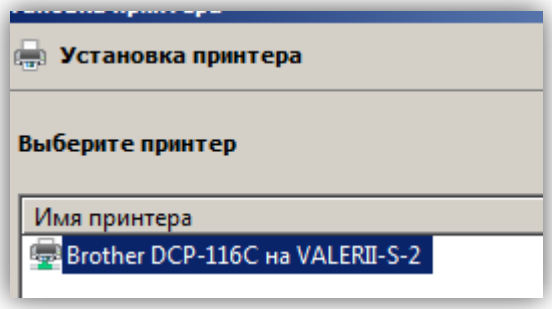


Рис 34.

Попробуем распечатать документ. В окне печати присутствует только что установленный принтер Brother DCP-116C (Рис 35). Файл появился в очереди на печать на машине Valerii-s-2 (Рис 36).

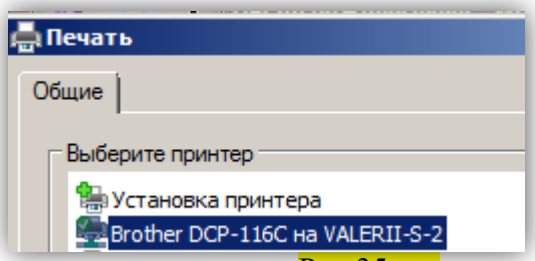


Рис 35.

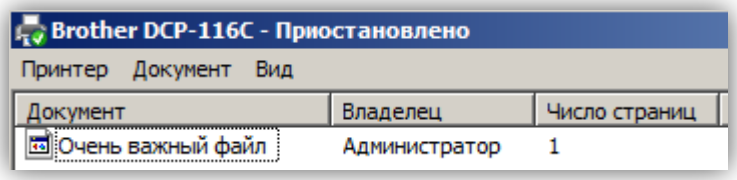


Рис 36.

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.

9. Реализовать сетевую структуру совместного использования данных

9.1. Создание структуры

Для данного пункта берутся сведения из 1 лабораторной работы. Мною была рассмотрена модель отдела call-центра, занимающегося обработкой обратной связи от клиентов и приёмом заказом.

В её состав вошли такие глобальные доменные группы, как:

- Руководитель отдела
- Оператор call-центра
- Сотрудник службы охраны

Реализуем сетевую структуру для совместного использования данных разными пользователями, использующие разные компьютеры. На компьютере члене домена авторизуемся под доменной учетной записью «Тимур_Игоревич», которая входит в глобальную доменную группу «Руководитель отдела». Создадим каталог «Данные отдела call-центра», который будет хранить данные, необходимые для работы отдела.

В созданный каталог добавим каталог «общие данные», хранящий файл базы данных клиентов организации. Для простоты, он будет иметь формат «.txt».

Клиенты организации — Блокнот

Файл Правка Формат Вид Справка

ФИО	Номер телефона	Электронная почта	Последний разговор
1. Иванов Иван Иванович	8-800-555-35-35	ivan@mail.ru	28.12.2020
2. Петров Петр Петрович	8-999-888-77-66	petr@mail.ru	28.12.2021
3. Сидоров Николай Анатольевич	8-999-888-77-66	nikolay@mail.ru	28.12.2022

Рис 37.

Создадим личный каталог для каждого оператора.

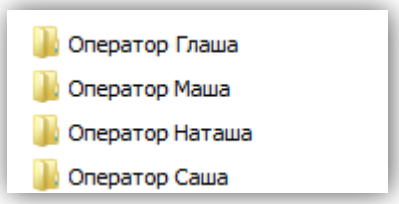


Рис 38.

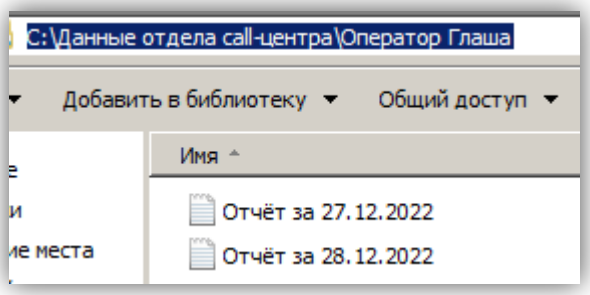


Рис 39.

Создадим каталог «Охрана», хранящий файл «Журнал охраны», в котором будет содержаться информация и входящих, и выходящих людях.

Журнал охраны — Блокнот

Файл Правка Формат Вид Справка

ФИО	Вошёл/Вышел	Дата	Время
1. Иванова Глафира Ивановная	Вошла	27.12.2022	08:12:27
2. Петрова Мария Петровна	Вошла	27.12.2022	07:38:10
3. Сидорова Наталья Николаевна	Вошла	27.12.2022	07:38:40
4. Смирнов Александр Иванов	Вошёл	27.12.2022	08:10:11

Рис 40.

9.2. Установлений разрешений NTFS

Для доступа к данным на текущем компьютере установим разрешения доступа для разных групп пользователей.

Установим разрешения доступа к каталогу «Данные отдела call-центра». Для групп, являющихся сотрудниками отдела, установим разрешение по чтению без наследования.

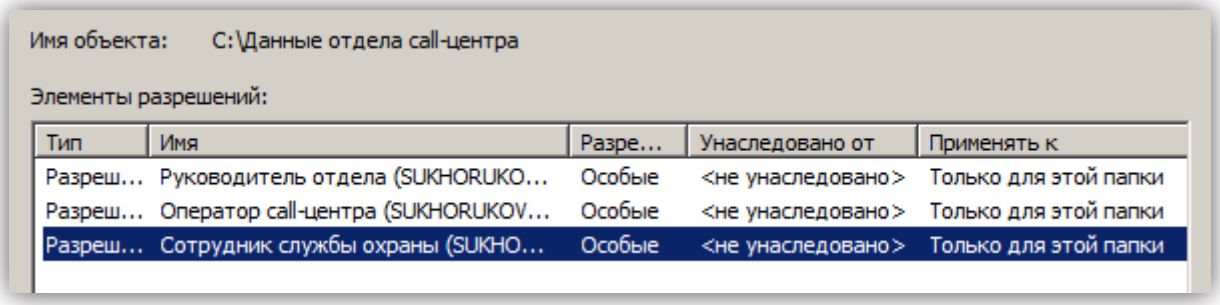


Рис 41.

На личные каталоги операторов установим полный доступ с наследованием для файлов и каталогов для соответствующего оператора, и разрешение на чтение для группы «Руководитель отдела» с наследованием для файлов и каталогов.

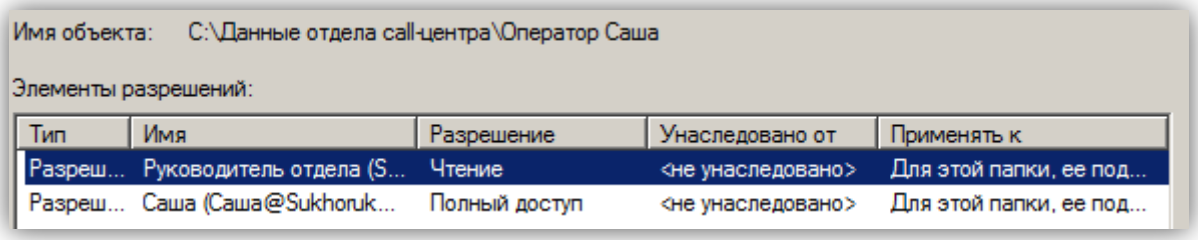


Рис 42.

Для каталога «Общий каталог», хранящего файл «Клиенты организации» установим разрешение на чтение и запись для группы «Операторы call-центра», и на чтение для группы «Руководитель отдела».

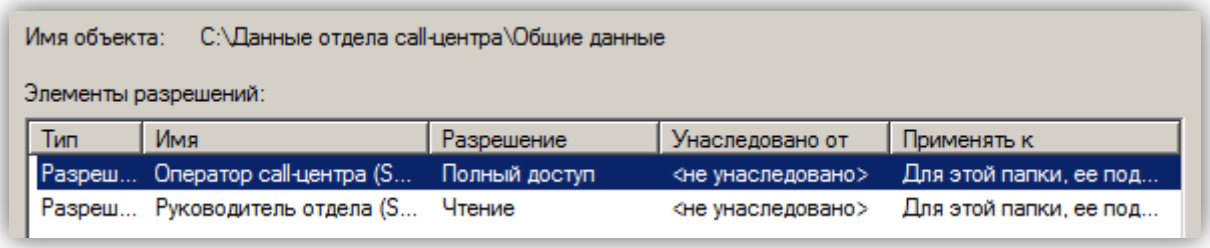


Рис 43.

Для каталога «Охрана» с файлом «Журнал охраны» установим разрешение на изменение для группы «Сотрудник службы охраны», и на чтение для группы «Руководитель отдела».

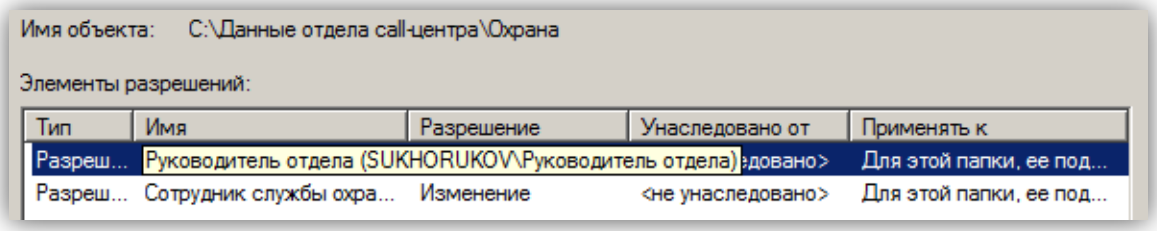


Рис 44.

9.3. Выделение каталога в общий доступ, и установление сетевых разрешений

Для доступа к данным на других компьютерах домена, необходимо выделить каталог в общий доступ. Для добавления каталога в общий доступ необходимо разрешение. Установим разрешения полного доступа для корневого каталога и всех внутренних каталогов для группы «Администраторы домена» на текущем компьютере.

В свойствах каталога перейдем на вкладку «Доступ» и выберем группы, которым хотим предоставить доступ.

Установим разрешения доступа к каталогу «Данные отдела call-центра». Для групп, являющихся сотрудниками отдела и для группы «Администраторы домена», установим разрешение по чтению.

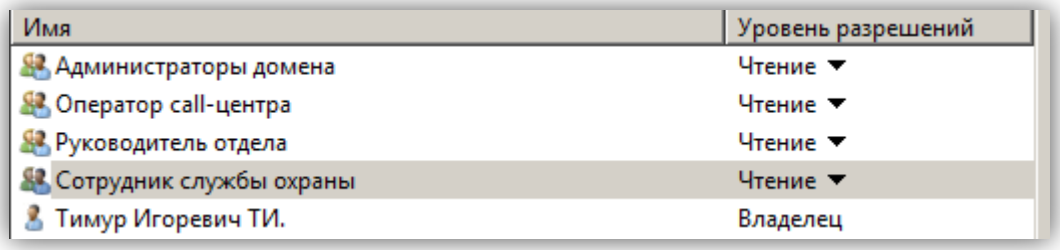


Рис 45.

На личные каталоги операторов установим полный доступ для соответствующего оператора и разрешение на чтение для группы «Руководитель отдела».

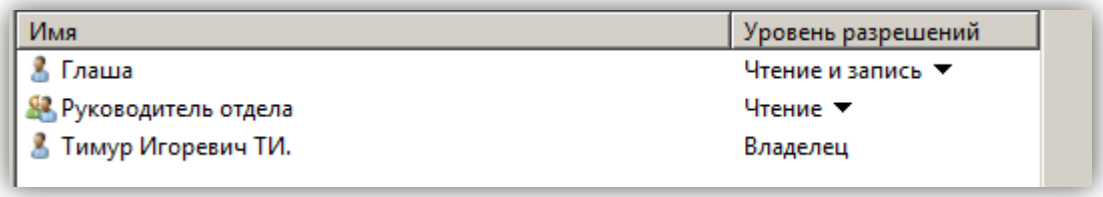


Рис 46.

Для каталога «Общий каталог», хранящего файл «Клиенты организации» установим разрешение на чтение и запись для группы «Операторы call-центра», и на чтение для группы «Руководитель отдела».

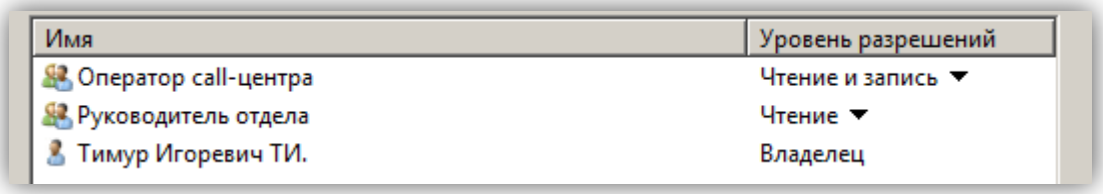


Рис 47.

Для каталога «Охрана» с файлом «Журнал охраны» установим разрешение на изменение для группы «Сотрудник службы охраны», и на чтение для группы «Руководитель отдела».

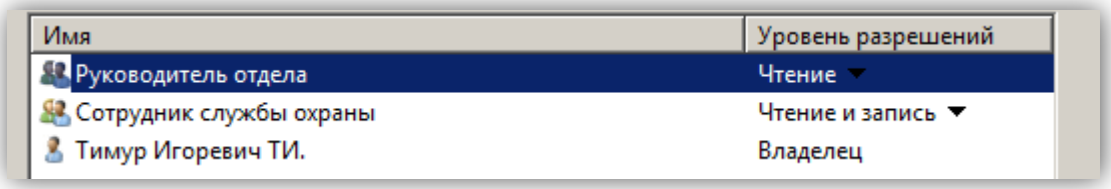


Рис 48.

9.4. Подключение каталога, как сетевого диска

Авторизуемся другом компьютере-члене домена под учетной записью «Саша», входящей в состав группы «Операторы call-центра». Подключим каталог, как сетевой диск и посмотрим состав доступных каталогов.

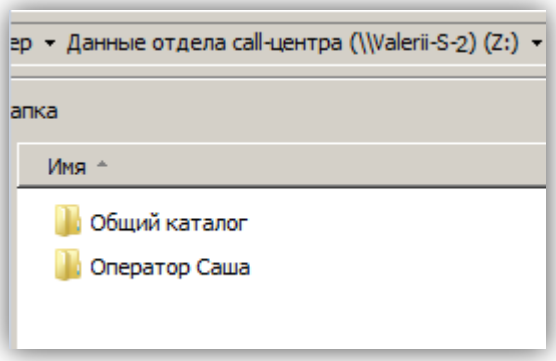


Рис 49.

Текущей учетной записи доступны два каталога- личный каталог оператора и общий каталог со списком клиентов организации.

Авторизуемся под учетной записью «Тимур_Игоревич», входящей в группу «Руководители отдела», и повторим подключение сетевого диска.

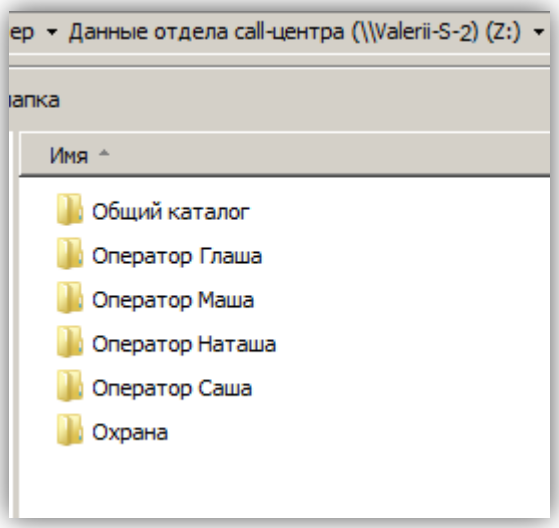


Рис 50.

Данной учетной записи доступны все каталоги, что соответствует разрешениям доступа.

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.