

## Лабораторная работа 5. Файловые службы и общие сетевые файловые ресурсы в ОС Windows (SMB). Разрешения NTFS.

### Задание.

Использовать виртуальные машины из предыдущих лабораторных работ. Развернуть на Windows Server 2019 общий сетевой файловый ресурс. Настроить NTFS разрешения для доступа к ресурсу, реализовав модель управления доступом на основе ролей (RBAC по принципу AGDLP). Настроить подключение сетевого диска у доменных пользователей с помощью групповой политики. Протестировать механизм перечисления на основе доступа (Access-Based Enumeration) и механизм теневого копирования (VSS).

### Этапы выполнения.

1) В Oracle VM VirtualBox для VM Windows Server 2019 добавить новый виртуальный жесткий диск (рис. 1). Параметры диска оставить в значениях по умолчанию.

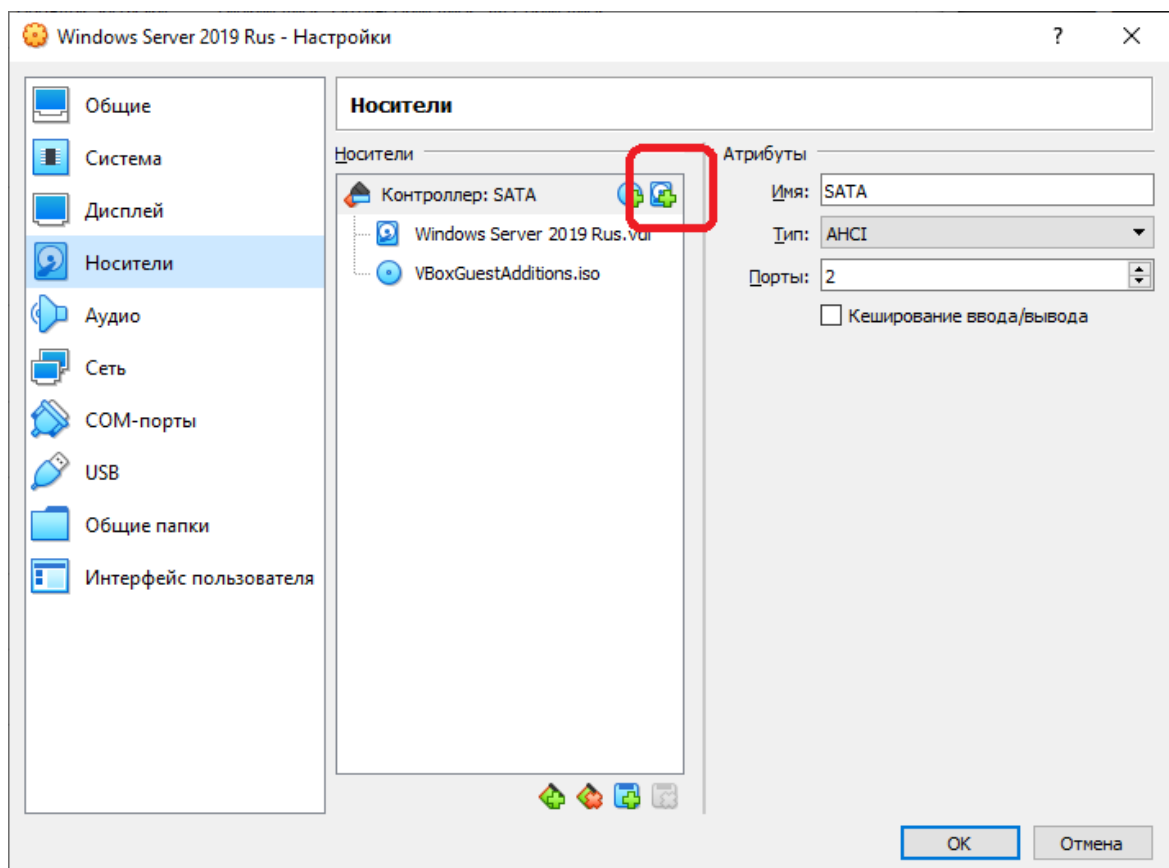


Рис.1. Добавление жесткого диска.

2) Запустить Windows Server 2019. Провести разметку нового диска. Для этого перейти в Диспетчер серверов — Файловые службы и службы хранилища — Тома — Диски.

Выбрать в списке диск, у которого в поле «Раздел» указано «Нет данных», и создать на этом диске новый том (рис.2).

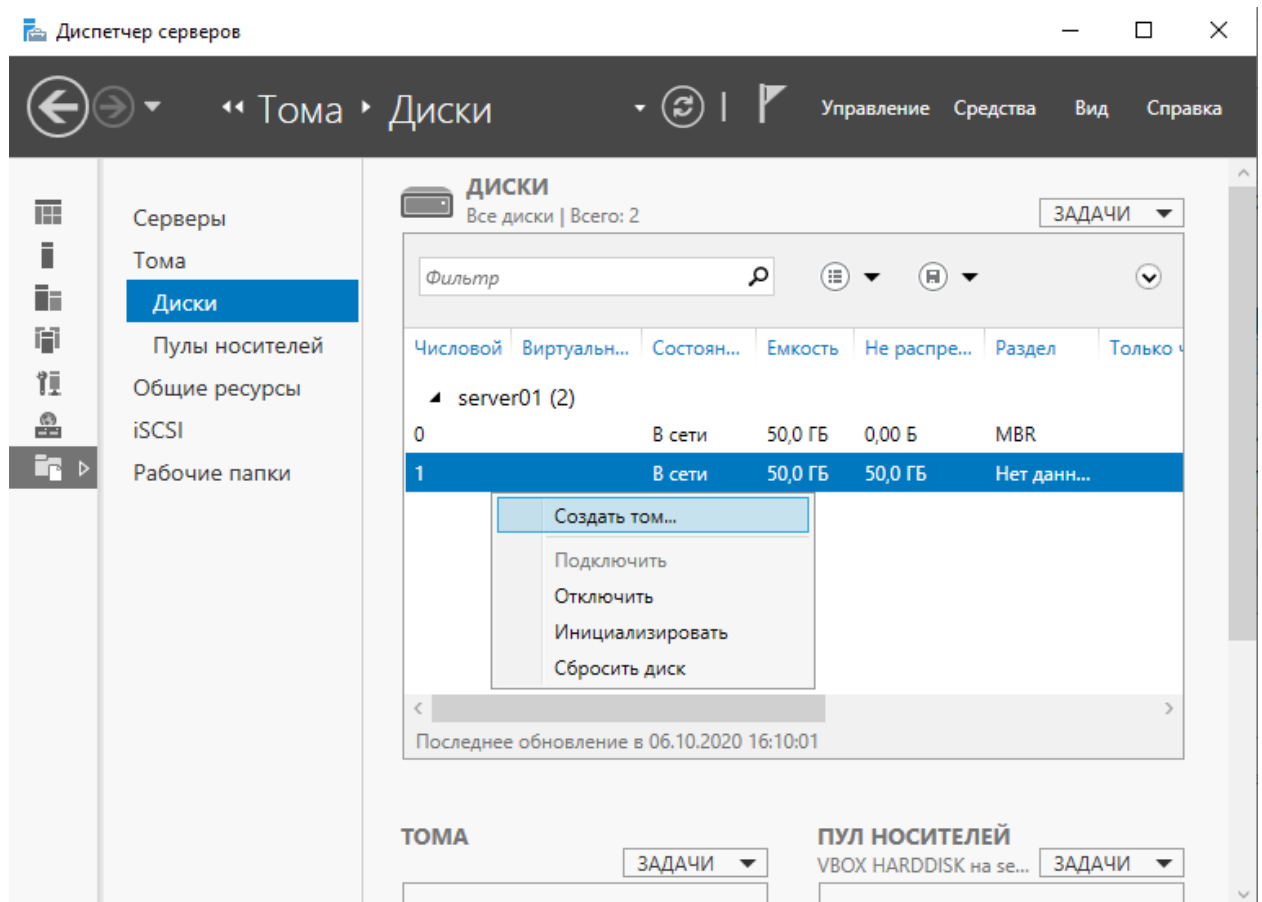


Рис.2. Создание тома на диске.

Следовать указаниям мастера создания томов, все параметры оставить в значениях по умолчанию, создать GPT запись, назначить букву диска, выбрать файловую систему NTFS (рис3.)

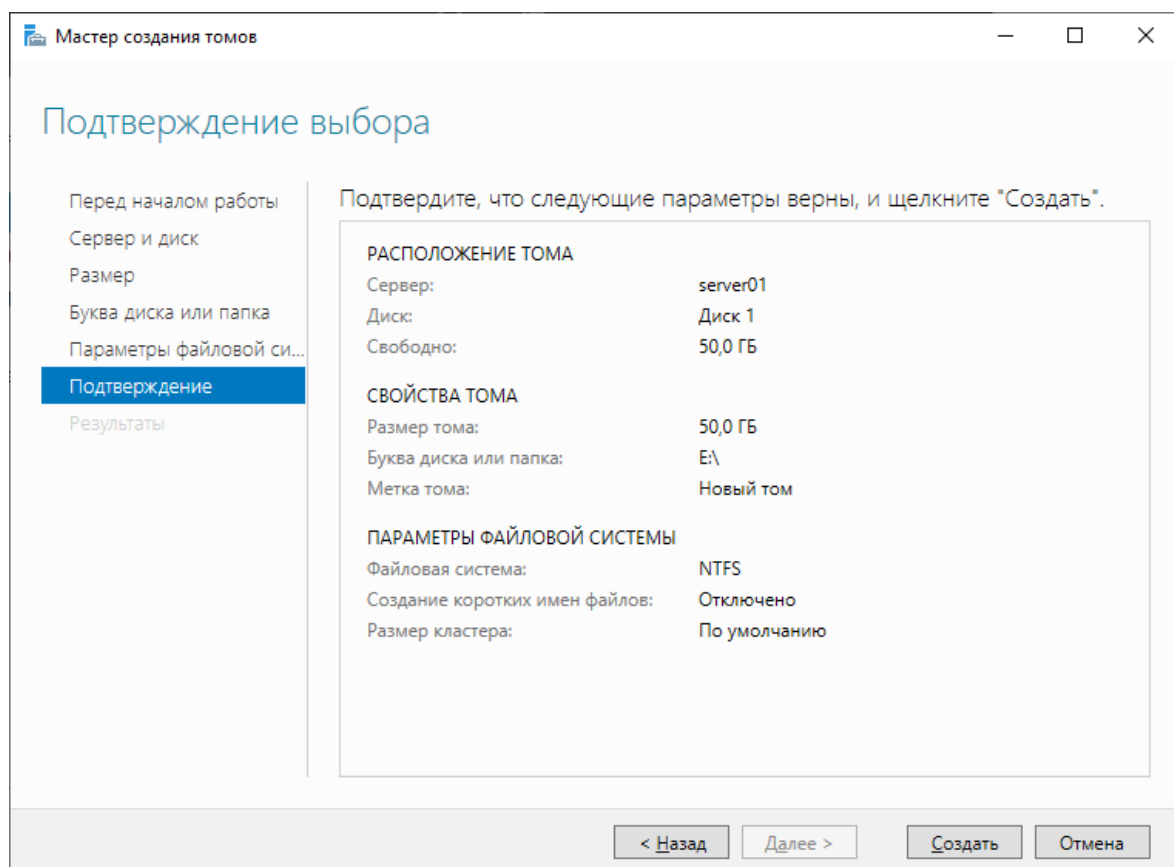


Рис.3. Параметры создания тома.

3) После завершения мастера в той же оснастке задать букву созданному тому (рис. 4).

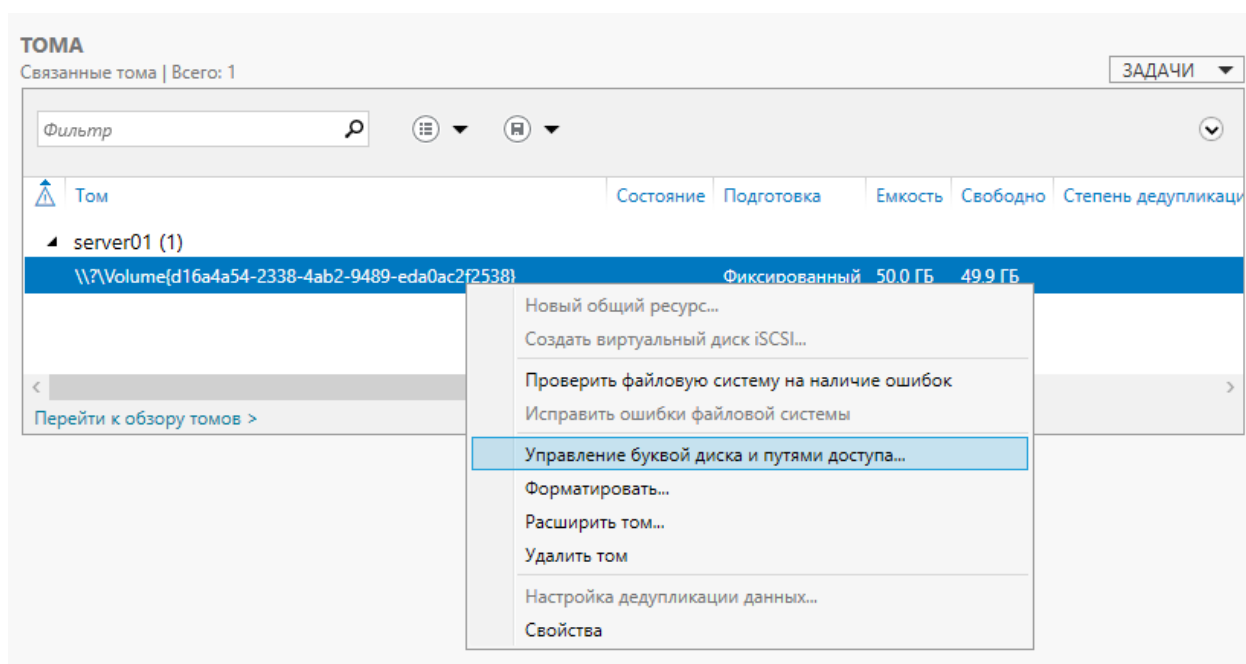


Рис.4. Задание буквы тома.

После этого в проводнике появится новый раздел с назначенной буквой.

Снимок окна Диспетчер серверов — Файловые службы и службы хранилища — Тома — Диски, с информацией о созданном томе — в отчет.

4) В проводнике Windows настроить теневые копии для нового раздела (рис.5). При необходимости проверить параметры создания теневых копий (кнопка «Параметры...»), после чего включить теневое копирование (рис.6).

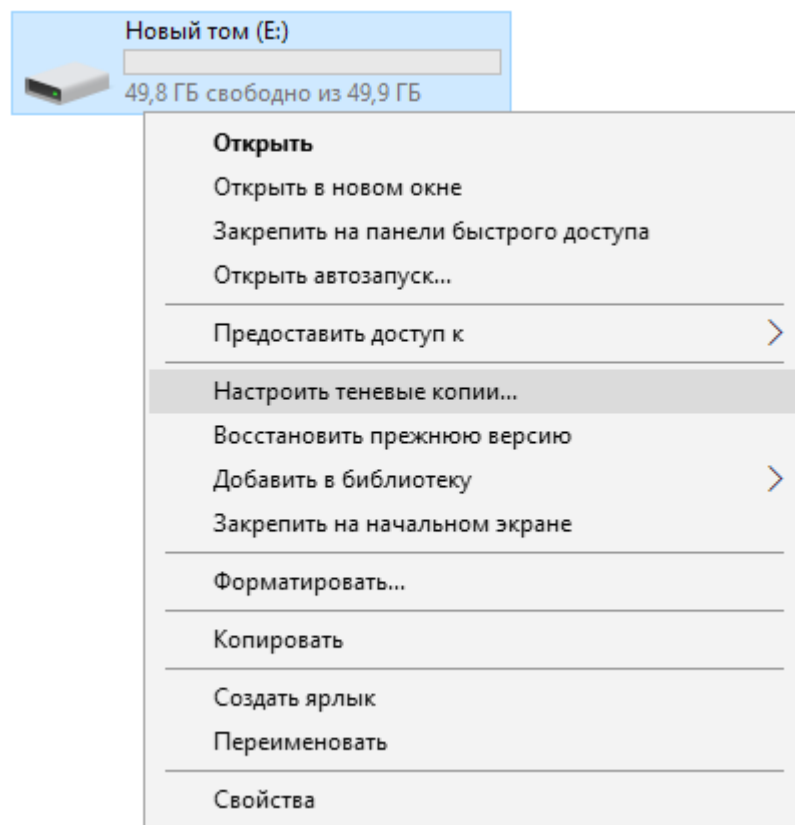


Рис.5. Настройка теневого копирования.

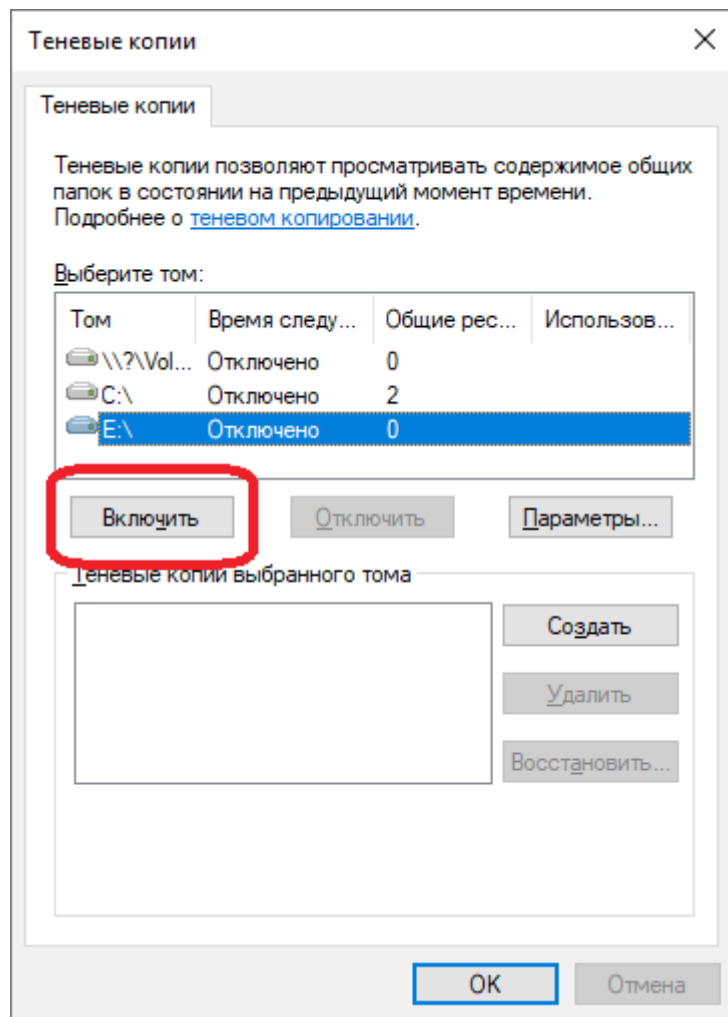


Рис. 6. Включение теневого копирования.

- 5) На контроллере домена в оснастке «Active Directory – пользователи и компьютеры» создать несколько доменных пользователей. Распределить пользователей по подразделениям — переместить во вложенные OU Пользователи в каждом из созданных ранее структурных подразделений организации (например, Организация/Управление 1/Пользователи). В каждом таком подразделении должно быть не менее двух пользователей.
- 6) Создать подразделение (OU) «Группы» в OU организации (например, Организация/Группы).
- 3) В OU «Группы» для каждого структурного подразделения организации создать глобальную группу безопасности, добавить в нее пользователей соответствующего структурного подразделения (пример для одной из групп — на рисунках 7, 8, 9, 10, 11, 12).

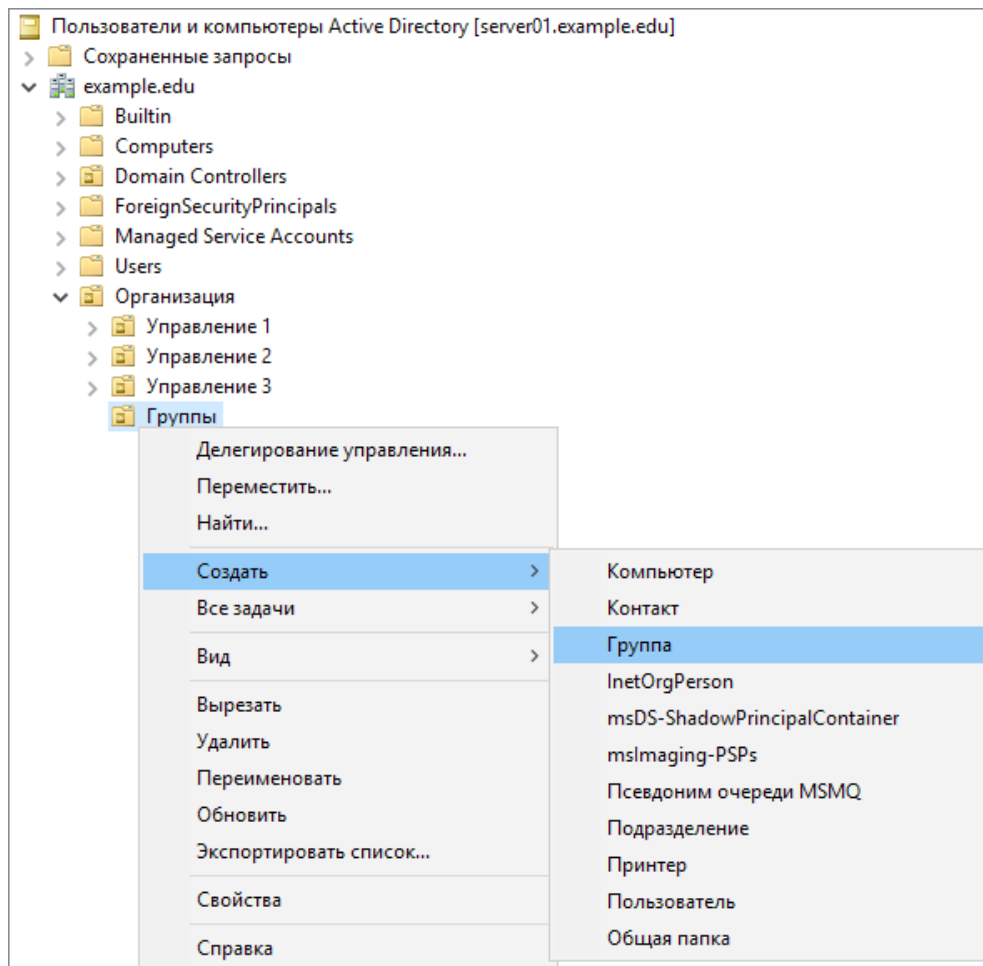


Рис.7. Создание группы.

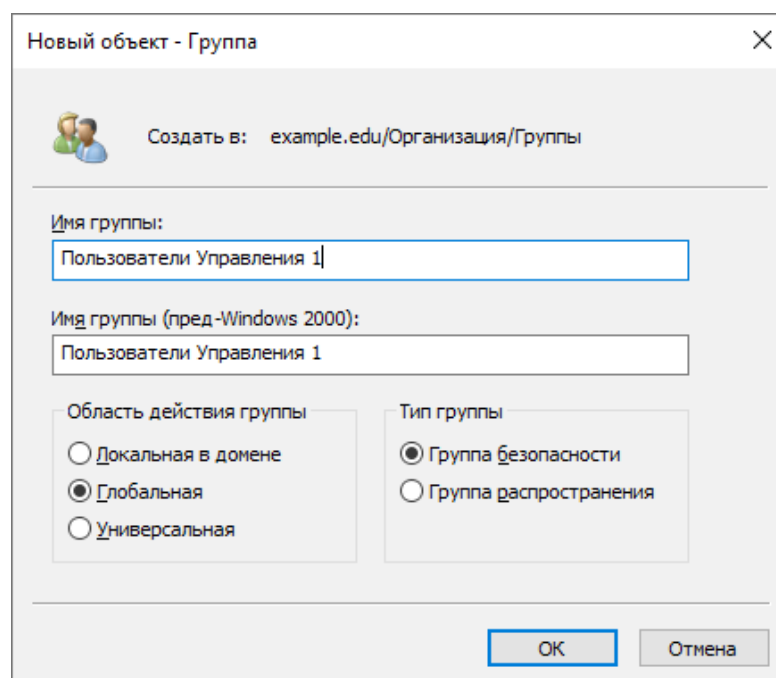


Рис.8. Параметры группы.

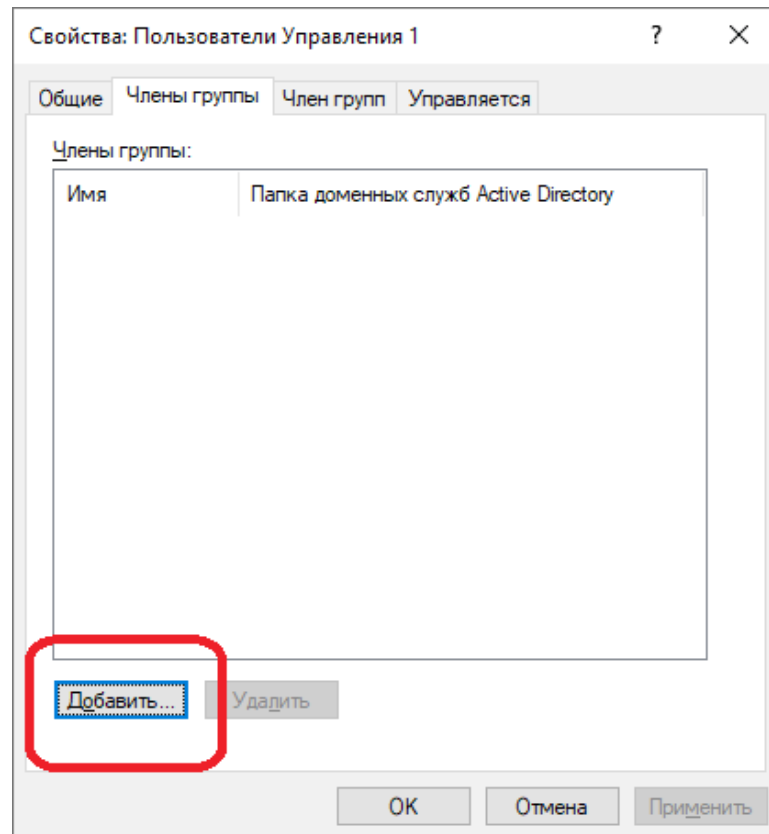


Рис.9. Члены группы.

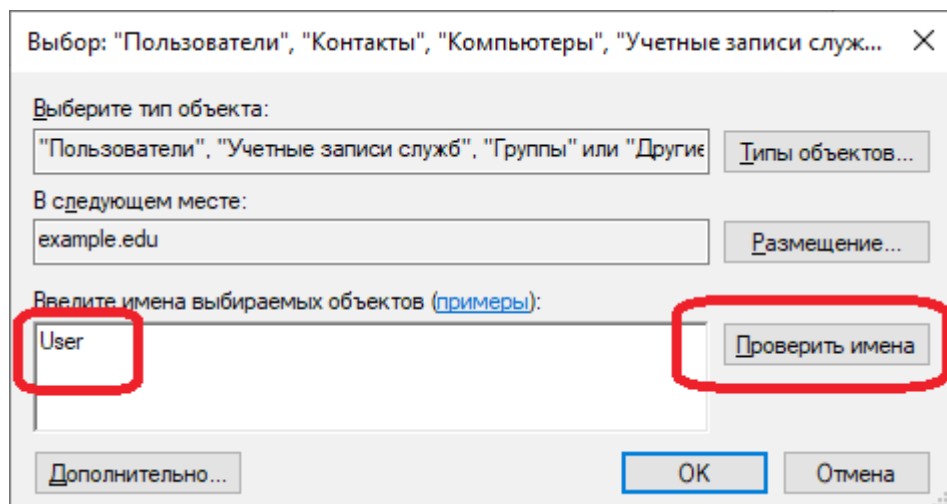


Рис.10. Добавление пользователей в группу.

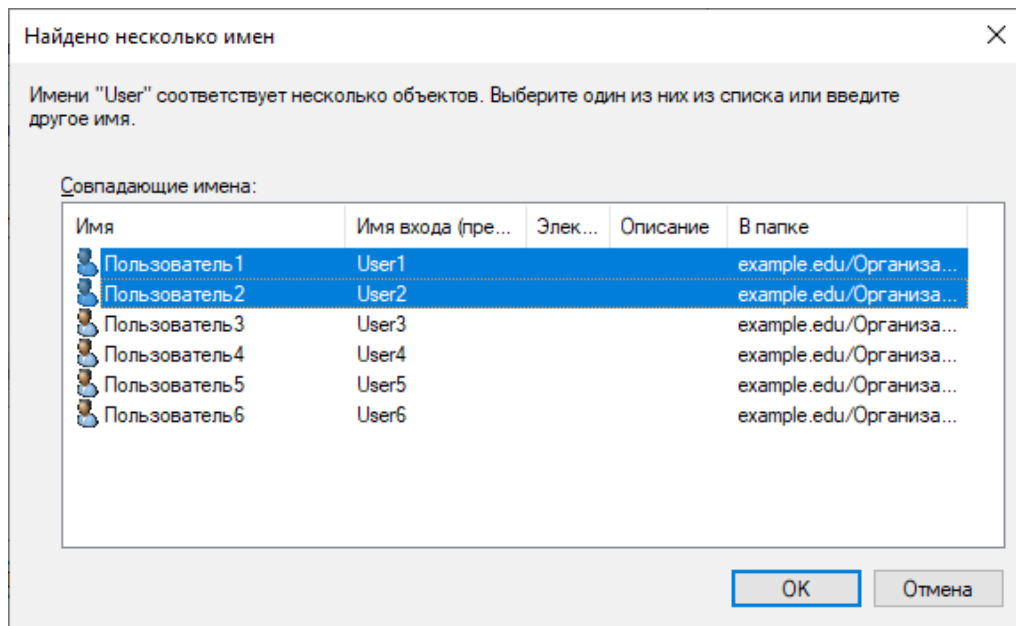


Рис.11. Выбор пользователей для включения в группу.

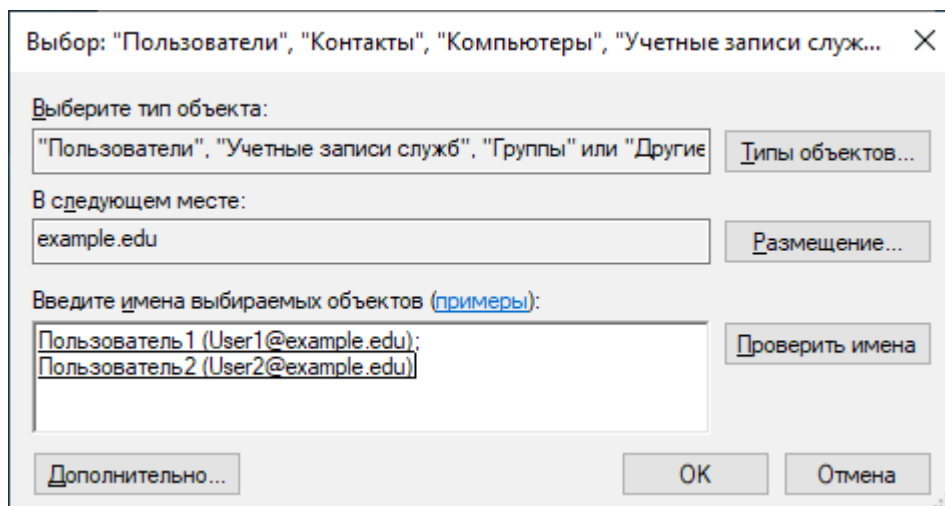


Рис.12. Добавление пользователей в группу.

7) Подготовить каталог для общего сетевого доступа. Создать на подготовленном ранее разделе диска папку Share (например, E:\Share).

Настроить разрешения NTFS на папку. Для этого перейти в свойства папки — вкладка Безопасность — Дополнительно (рис.13).



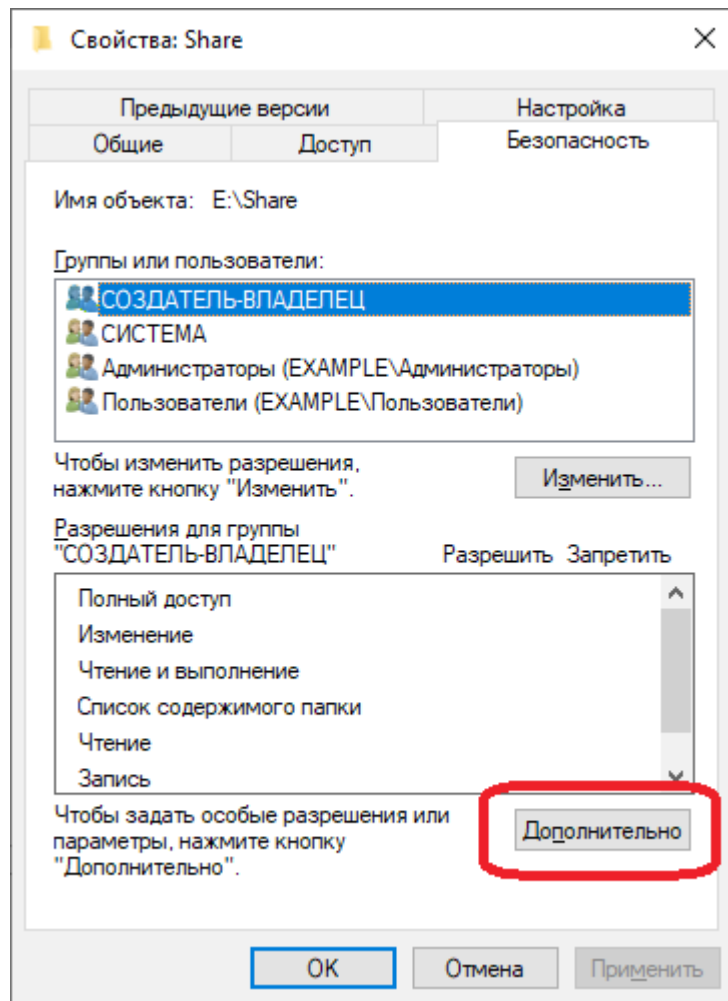


Рис.13. Вкладка Безопасность.

Отключить наследование разрешений (рис.14) и удалить все унаследованные разрешения для этой папки (рис.15).

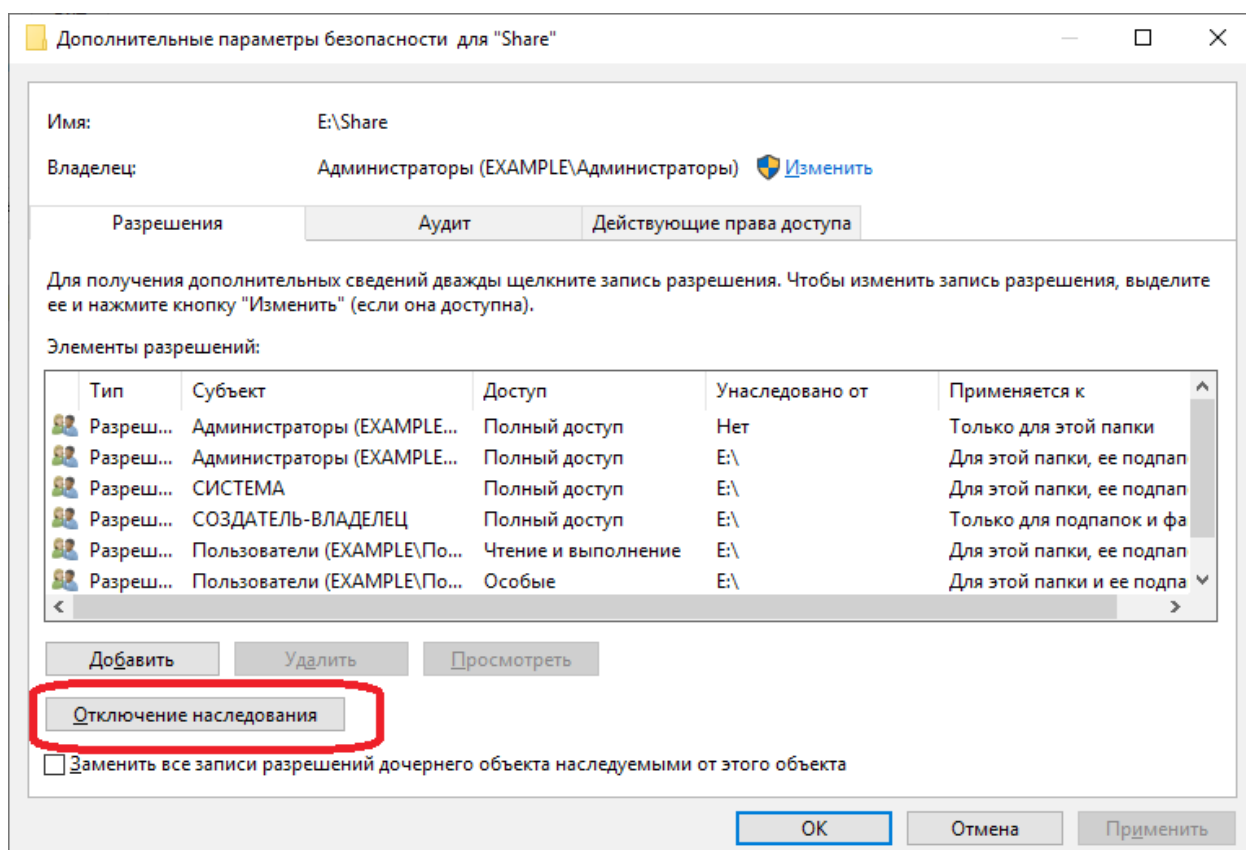


Рис.14. Отключение наследования.

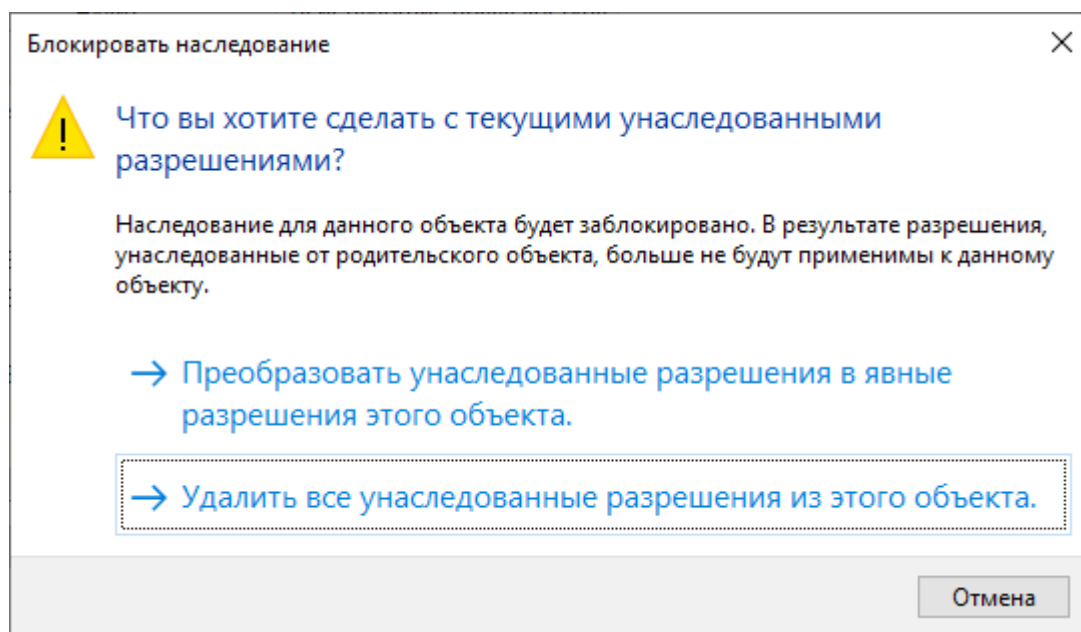


Рис.15. Удаление унаследованных разрешений.

Изменить оставшееся разрешение (или добавить новое разрешение) для группы «Администраторы» — разрешить «Полный доступ» «Для этой папки, ее подпапок и файлов» (рис.16).

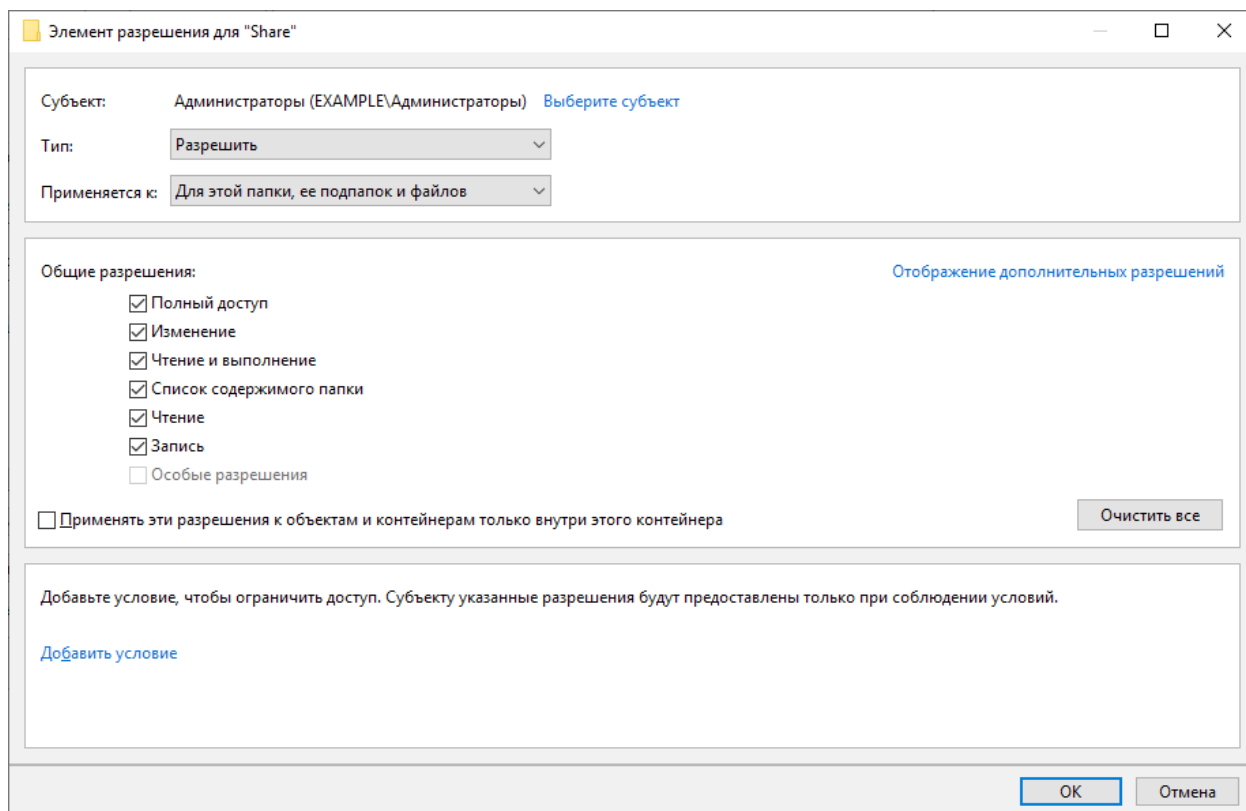


Рис 16. Разрешение для группы «Администраторы».

Добавить разрешение для группы «Пользователи домена» с областью применения «Только для этой папки» - включить отображение дополнительных разрешений и разрешить только «Траверс папок / выполнение файлов» и «Содержание папки / чтение данных» (рис. 17.)

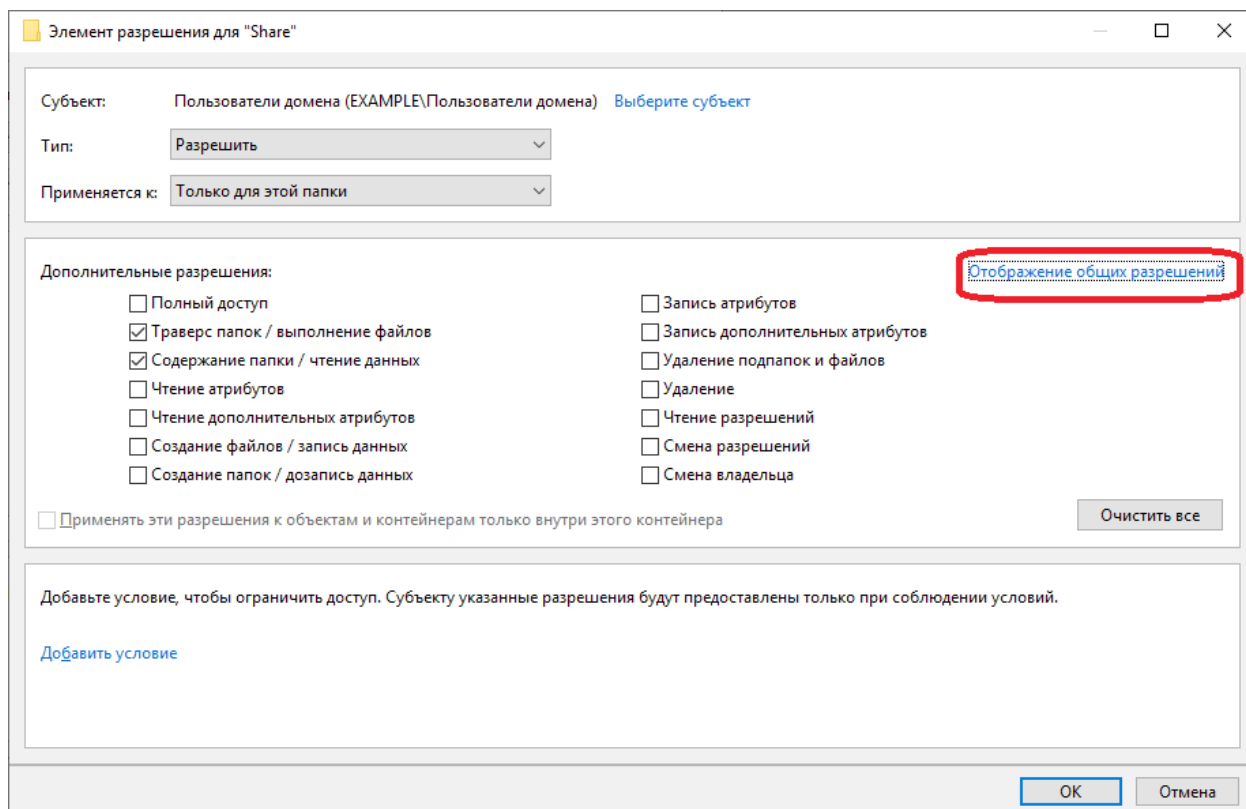


Рис.17. Дополнительные разрешения.

Добавить разрешение для группы «СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ» с областью применения «Для этой папки, ее подпапок и файлов» - разрешить «Изменение».

Снимок окна дополнительных параметров безопасности с настроенными разрешениями на папку Share – в отчет.

8) Подготовить структуру каталогов для общего доступа. В папке Share создать несколько вложенных папок — по одной папке для каждого структурного подразделения организации и еще одну общую папку для обмена файлами между подразделениями. Пример структуры каталогов — на рис.18.

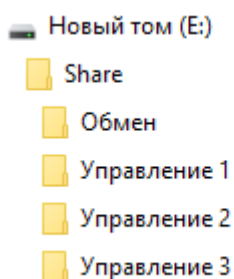


Рис.18. Пример структуры каталогов.

9) В оснастке «Active Directory – пользователи и компьютеры» в OU «Группы» создать ресурсные группы — группы безопасности с областью действия «Локальные в домене». Для каждого структурного подразделения создать по 3

группы — для предоставления прав только на чтение, на изменение и для полного доступа. Примерный список групп — на рис. 19.













Имя	Тип
 Пользователи Управления 1	Группа безопасности - Глобальная
 Пользователи Управления 2	Группа безопасности - Глобальная
 Пользователи Управления 3	Группа безопасности - Глобальная
 Управление 1 Изменение	Группа безопасности - Локальная в домене
 Управление 1 Полный доступ	Группа безопасности - Локальная в домене
 Управление 1 Чтение	Группа безопасности - Локальная в домене
 Управление 2 Изменение	Группа безопасности - Локальная в домене
 Управление 2 Полный доступ	Группа безопасности - Локальная в домене
 Управление 2 Чтение	Группа безопасности - Локальная в домене
 Управление 3 Изменение	Группа безопасности - Локальная в домене
 Управление 3 Полный доступ	Группа безопасности - Локальная в домене
 Управление 3 Чтение	Группа безопасности - Локальная в домене

Рис.19. Примерный список групп безопасности.

Список всех созданных групп безопасности (содержание ОУ «Группы») — в отчет.

10) В группы, предназначенные для предоставления прав на изменение добавить глобальные группы пользователей соответствующих структурных подразделений (например, в группу «Управление 1 Изменение» включить группу «Пользователи Управления 1», рис. 20).

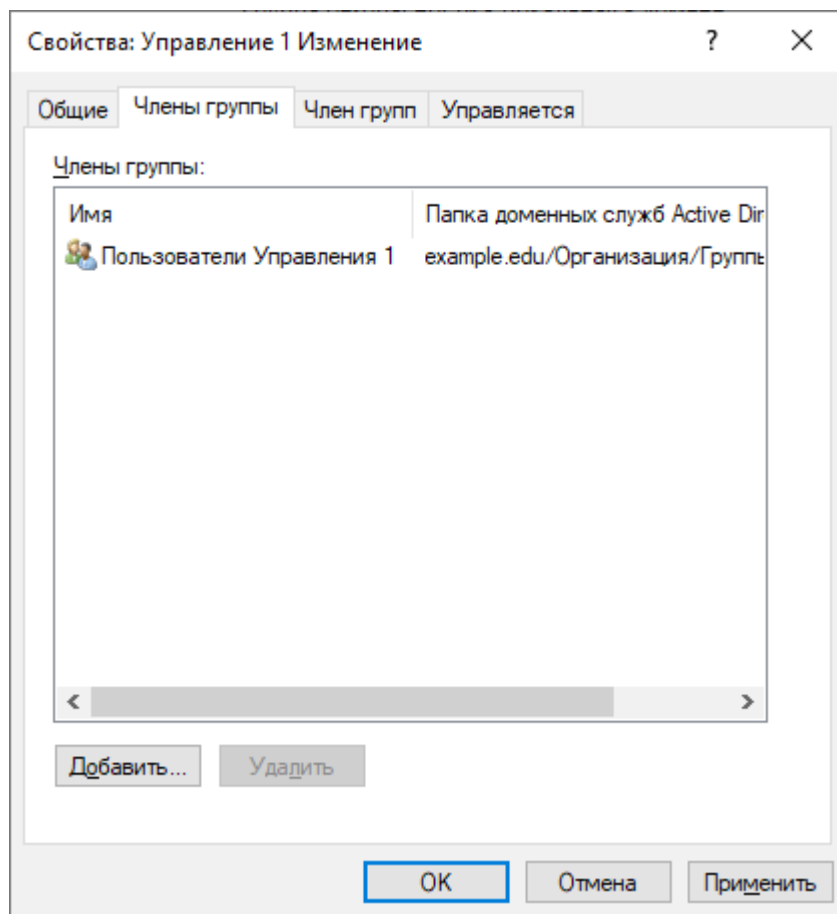


Рис. 20. Включение глобальных групп в локальные группы безопасности.

11) Выставить NTFS разрешения на папки, предназначенные для общего доступа. На каждую папку выставить разрешения для трех групп безопасности соответствующего структурного подразделения. Т.е., например, на папку «E:\Share\Управление 1» добавить разрешения:

- для группы «Управление 1 Чтение» - разрешить «Чтение и выполнение»;
- для группы «Управление 1 Изменение» - разрешить «Изменение»;
- для группы «Управление 1 Полный доступ» - разрешить «Полный доступ».

Аналогично — для других папок. Пример выставленных разрешений — на рис.21.

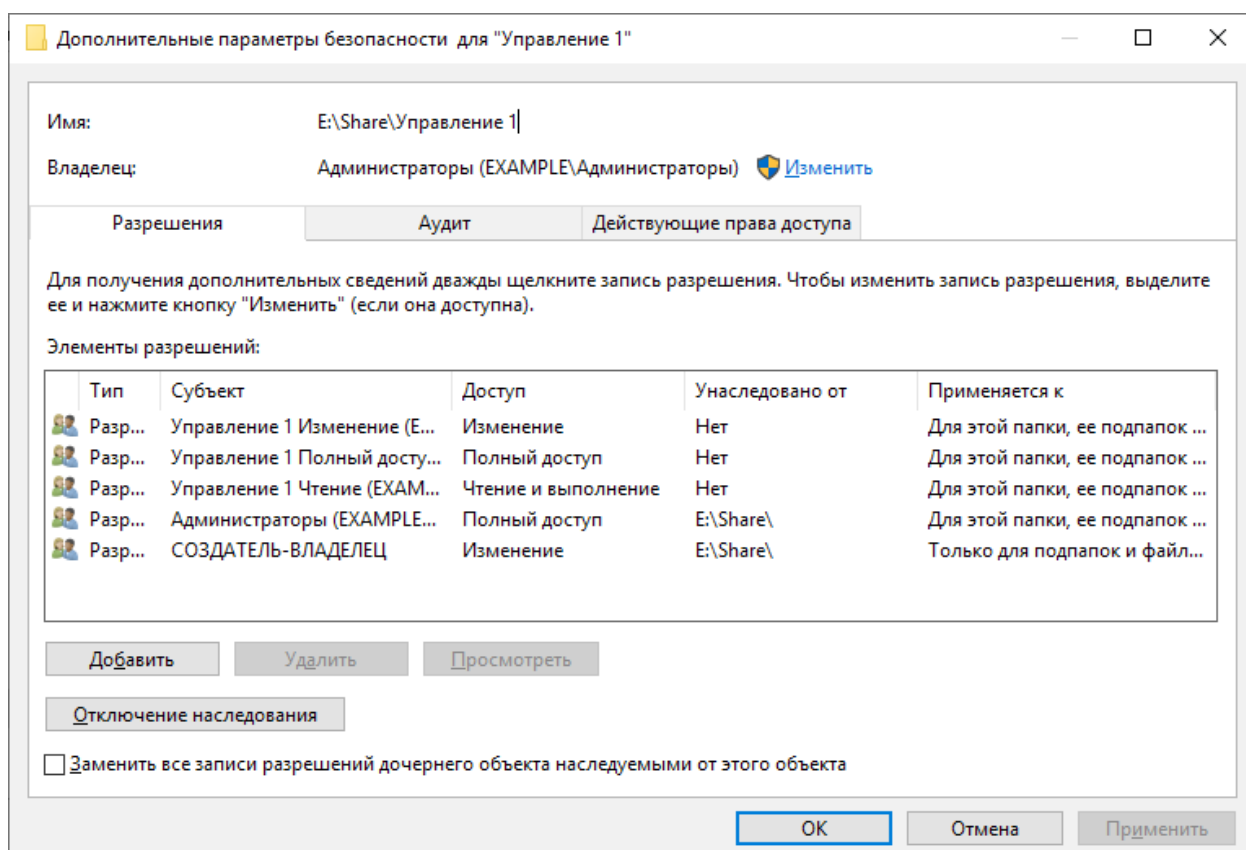


Рис.21. Пример выставленных разрешений.

Для папки, предназначенной для обмена файлами между подразделениями для группы «Пользователи домена» разрешить «Изменение».

Снимок окна дополнительных параметров безопасности с настроенными разрешениями для групп безопасности на одну из папок (кроме папки обмена) — в отчет.

12) Открыть общий доступ к папке Share через меню расширенной настройки (рис.22). В разрешениях общего ресурса (кнопка «Разрешения») предоставить полный доступ для группы «Все» (рис.23).

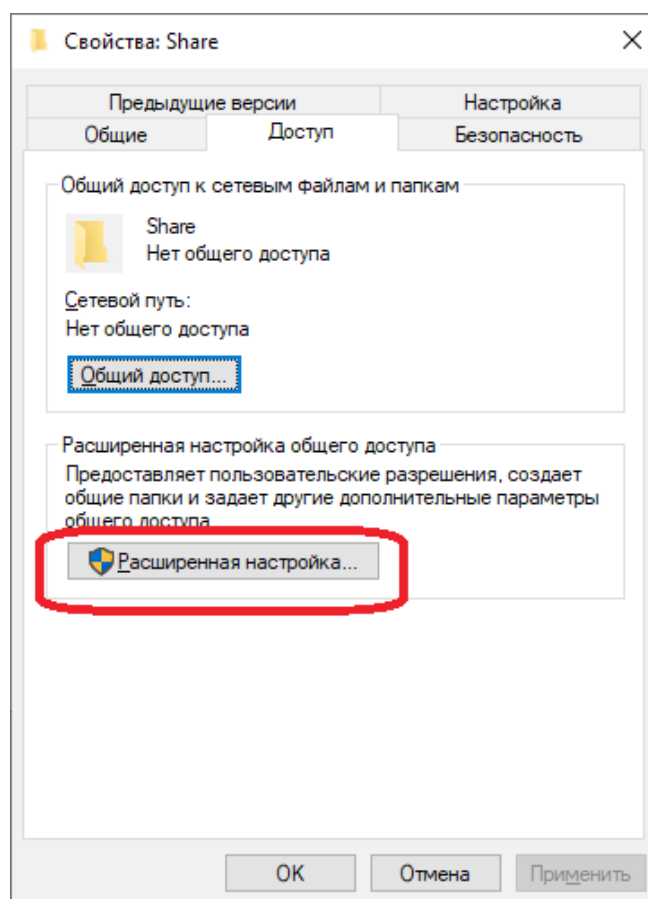


Рис.22. Настройка общего доступа.

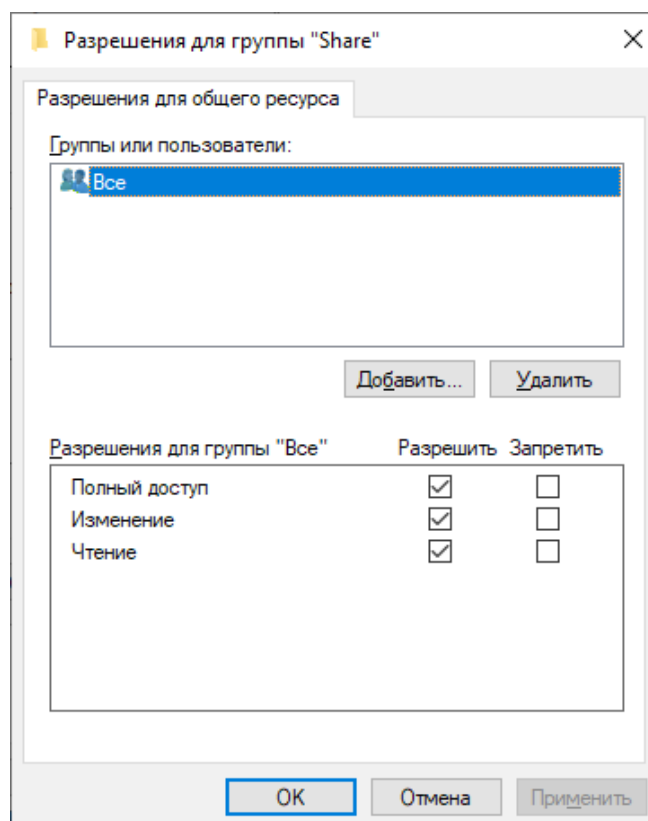


Рис.23. Разрешения для общего ресурса.



13) Запустить Windows 10, выполнить вход под доменной учетной записью. В проводнике подключиться к созданной сетевой папке, которая будет доступна по пути:

\\<имя сервера>\Share

Например:

\\server01\Share

рекомендуется использовать полное доменное имя сервера (FQDN):

\\server01.example.edu\Share

Пример успешного подключения — на рис. 24.

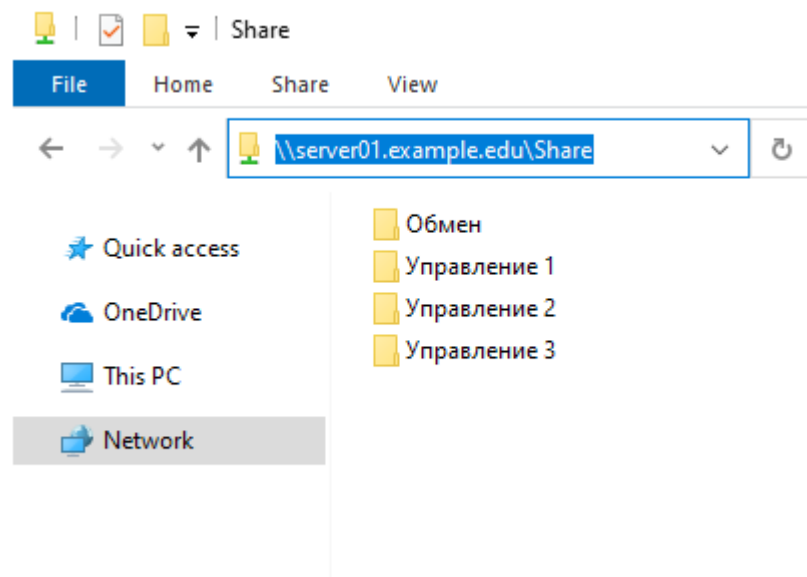


Рис.24. Подключение к сетевой папке.

14) Сетевую папку можно подключить в качестве сетевого диска. В проводнике Windows 10 запустить функцию «Map network drive...» (рис.25).

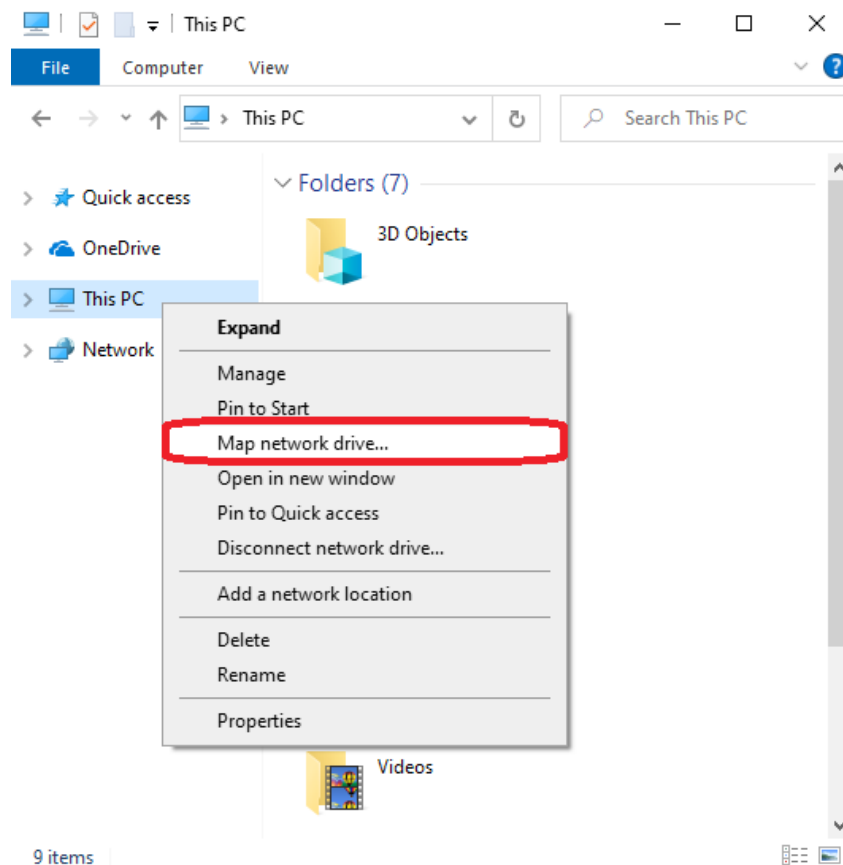


Рис. 25. Подключение сетевого диска.

Указать букву диска и полный путь к сетевой папке (рис.26).

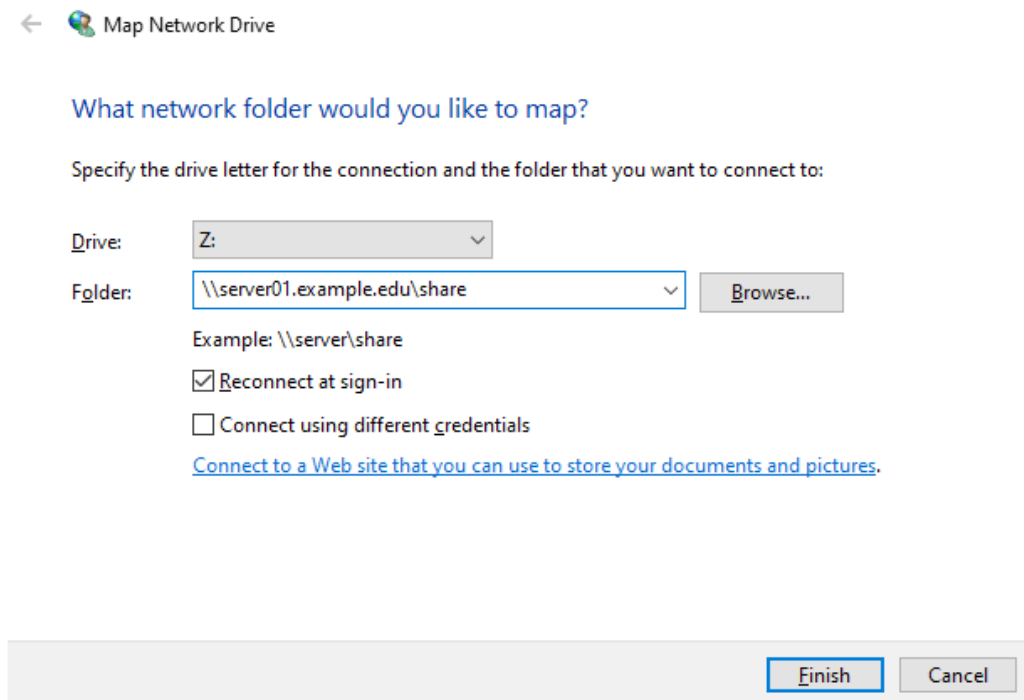


Рис.26. Настройка сетевого диска.

После применения настроек диск будет доступен в проводнике (рис. 27).

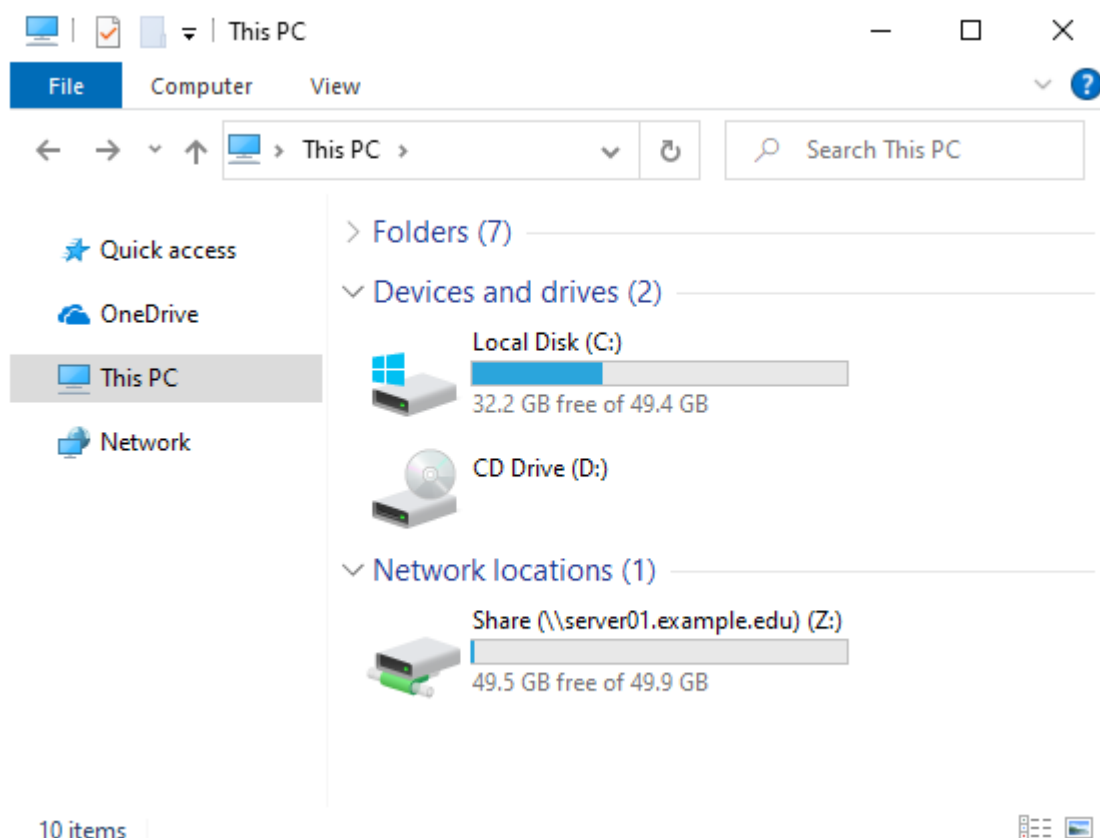


Рис.27. Подключенный сетевой диск.

В доменной среде с большим количеством пользователей выполнять данную процедуру вручную для каждого пользователя трудоемко. Необходимо применить групповую политику. Предварительно следует удалить созданный вручную сетевой диск — в проводнике вызвать контекстное меню диска и выбрать «Disconnect».

15) На Windows Server 2019 создать групповую политику для автоматического подключения сетевого диска у доменных пользователей. Для этого создать GPO с названием, например, «Network drive» и связать его с OU организации (например, example.edu\Организация).

В редакторе групповой политики перейти в раздел Конфигурация пользователя — Настройка — Конфигурация Windows — Сопоставления дисков. Создать «Сопоставленный диск». В настройках диска указать полный путь к сетевой папке, название, букву диска (рис. 28). На вкладке «Общие параметры» включить параметры «Выполнять в контексте безопасности вошедшего пользователя» и «Удалить этот элемент, когда он более не применяется» (при отключении политики сетевой диск удалится). (рис.29).

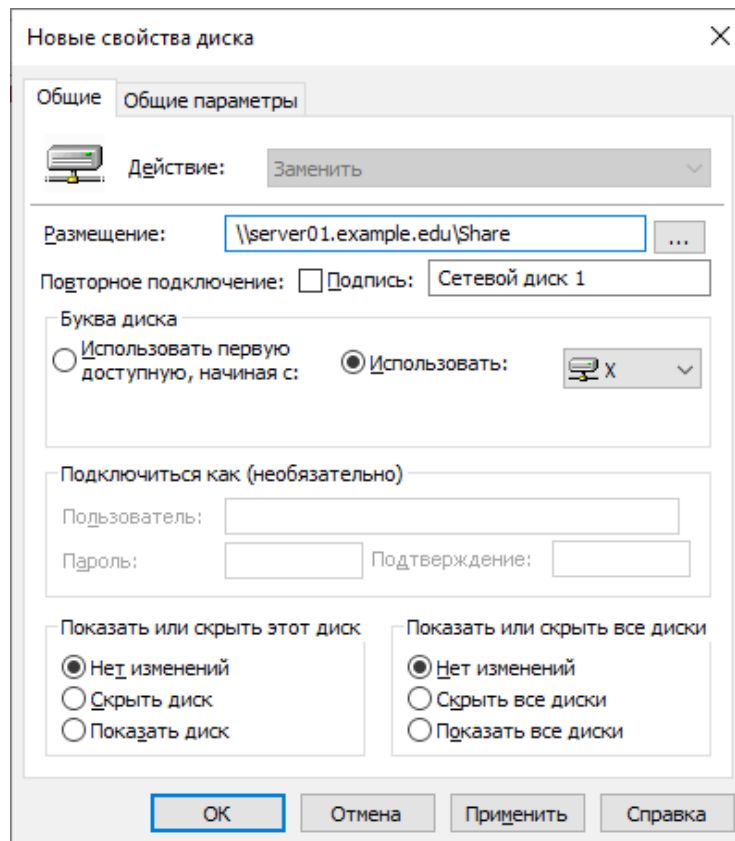


Рис. 28. Настройка сопоставления диска

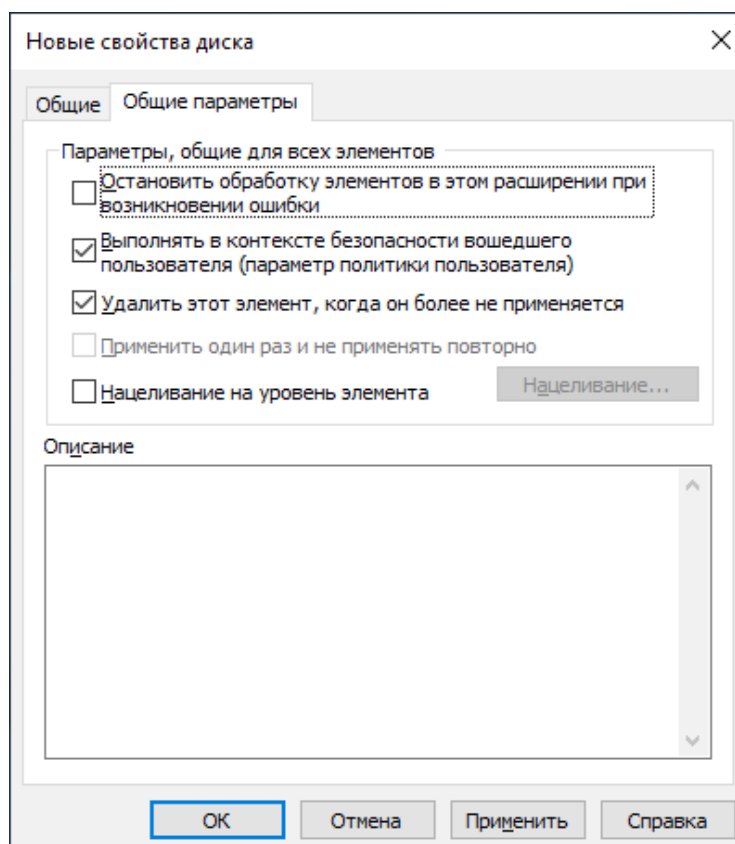


Рис.29. Общие параметры политики.

16) Выполнить вход на Windows 10 под доменной учетной записью и проверить, что в проводнике появился сетевой диск. При необходимости выполнить принудительную синхронизацию групповых политик.

Проверить доступность папок в соответствии с настроенными разрешениями NTFS. У пользователя должен быть доступ к папке своего структурного подразделения и к папке обмена, но при попытках перехода в папки других подразделений должно появляться сообщение об ошибке доступа.

Снимок окна проводника с подключенным сетевым диском на Windows 10 – в отчет.

17) На Windows Server 2019 перейти в Диспетчер серверов — Файловые службы и службы хранилища — Общие ресурсы, открыть свойства ресурса «Share». В разделе параметры включить перечисление на основе доступа (рис .30).

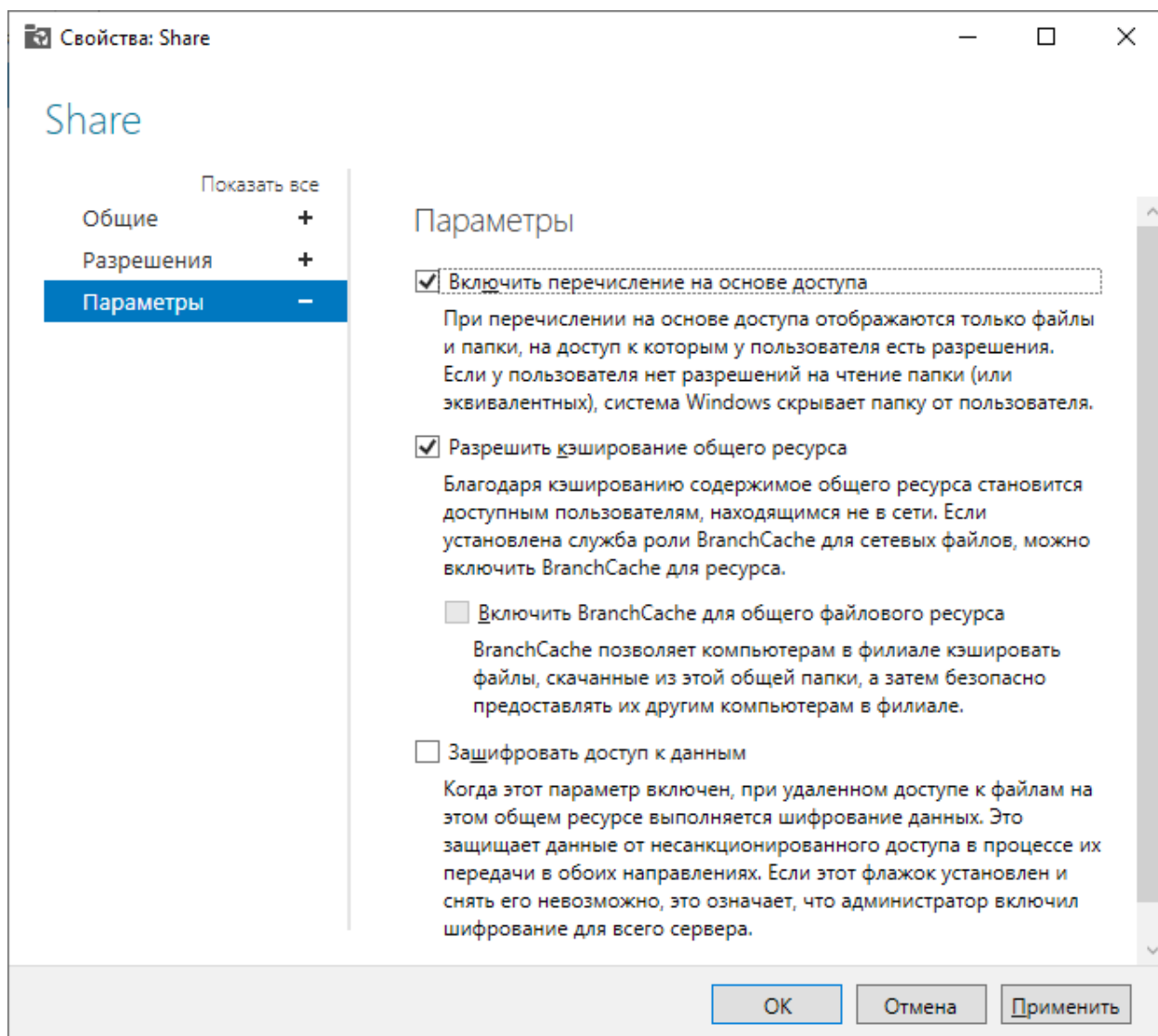


Рис.30. Параметры общего ресурса.

18) На Windows 10 открыть сетевой диск. В проводнике будут отображаться только те папки, к которым у текущего пользователя есть доступ. Для применения перечисления на основе доступа в ряде случаев необходимо выполнить выход и повторный вход пользователя в ОС.

19) Проверить механизм восстановления теневой копии файлов.

- в сетевой папке создать два текстовых файла, вписать в них любой текст;
- на Windows Server 2019 перейти к настройкам теневых копий (рис.5, 6) и вручную создать теневую копию;
- в сетевой папке внести текстовые изменения в один из файлов, а второй файл удалить;
- открыть свойства измененного файла и на вкладке «Предыдущие версии» («Previous versions») восстановить изначальную версию файла;
- открыть свойства папки, в которой был создан и удален второй файл; на вкладке «Предыдущие версии» («Previous versions») открыть теневую копию папки и просмотреть копию удаленного файла, который при необходимости можно восстановить.

Снимок окна настроек теневого копирования с перечнем копий для созданного тома (диска) (рис.6)— в отчет.

**Отчет:**

- снимок окна Диспетчер серверов — Файловые службы и службы хранилища — Тома — Диски, с информацией о созданном томе на втором виртуальном диске;
- снимок окна дополнительных параметров безопасности с настроенными разрешениями на папку Share;
- список всех созданных групп безопасности (содержание ОУ «Группы»);
- снимок окна дополнительных параметров безопасности с настроенными разрешениями на одну из папок, вложенных в Share (кроме папки обмена);
- снимок окна проводника с подключенным сетевым диском на Windows 10;
- снимок окна настроек теневого копирования с перечнем копий для созданного тома (диска) (рис.6).