

Отчет

Лабораторная работа по Windows

Выполнила: Рымкулова Диана СКБ181

Предварительно создать в системе пользователя администратора, входящего в группу администраторов системы.

1. Изменение прав доступа к файлам и каталогам для пользователей.

1) Зайти в систему от имени администратора, входящего в группу администраторов системы.

Ваши данные



DIANA

Локальная учетная запись
Администратор

2) Создать в учетных записях двух обычных пользователей: lab1, lab2.

Семья и другие пользователи

Ваша семья

Войдите, используя учетную запись, чтобы просмотреть здесь сведения о членах семьи. У каждого члена семьи есть свой профиль, в котором вы можете указать приложения и игры.

Войти с учетной записью Майкрософт

Другие пользователи

Разрешите пользователям использовать этот компьютер с помощью их учетных записей.

Добавить пользователя

Настроить терминал

Ограниченный доступ
Настройте это устройство, чтобы ограничить доступ к интернету, приложениям и играм.

Создать пользователя для этого компьютера

Если вы хотите использовать пароль - выберите что-то, что вам запомнится легко, а другим будет сложно угадать.

Кто будет использовать данный компьютер?

lab1

Обеспечьте безопасность.

В случае, если вы забыли свой пароль

Кличка первого домашнего животного?

1

В каком городе вы родились?

1

В каком городе встретились ваши родители?

1

Далее

Назад

Семья и другие пользователи

Ваша семья

Войдите, используя учетную запись, чтобы просмотреть здесь сведения о членах семьи. У каждого члена семьи есть свой профиль, в котором вы можете указать приложения и игры.

Войти с учетной записью Майкрософт

Другие пользователи

Разрешите пользователям использовать этот компьютер с помощью их учетных записей.

Добавить пользователя

lab1

Локальная учетная запись

Настроить терминал

Ограниченный доступ
Настройте это устройство, чтобы ограничить доступ к интернету, приложениям и играм.

Создать пользователя для этого компьютера

Если вы хотите использовать пароль - выберите что-то, что вам запомнится легко, а другим будет сложно угадать.

Кто будет использовать данный компьютер?

lab2

Обеспечьте безопасность.

В случае, если вы забыли свой пароль

Кличка первого домашнего животного?

1

В каком городе вы родились?

1

Далее

Назад

Другие пользователи

Разрешите пользователям, не включенным в семью, входить в систему с помощью их учетных записей. Это не будет означать их добавление в семью.



Добавить пользователя для этого компьютера



lab1

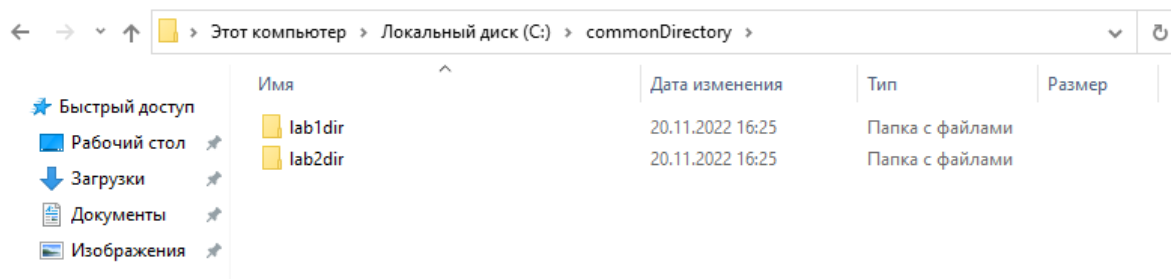
Локальная учетная запись



lab2

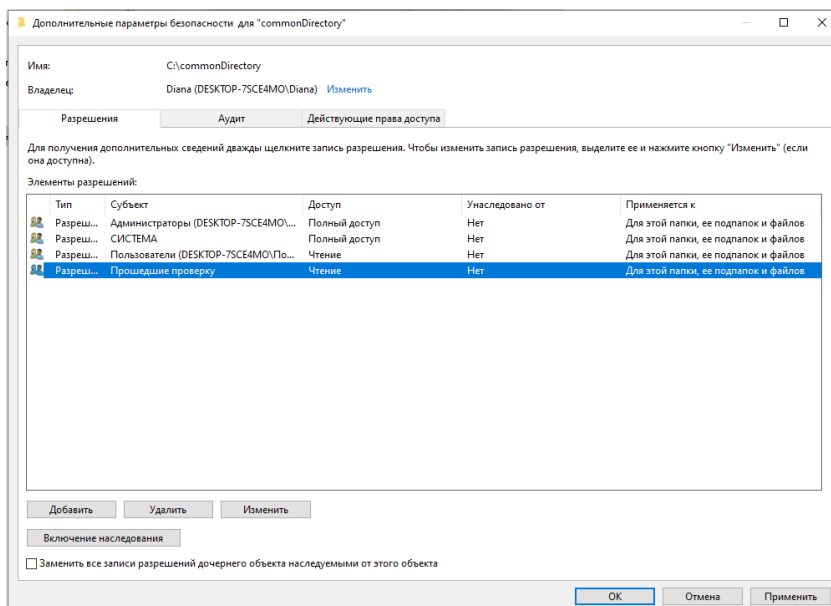
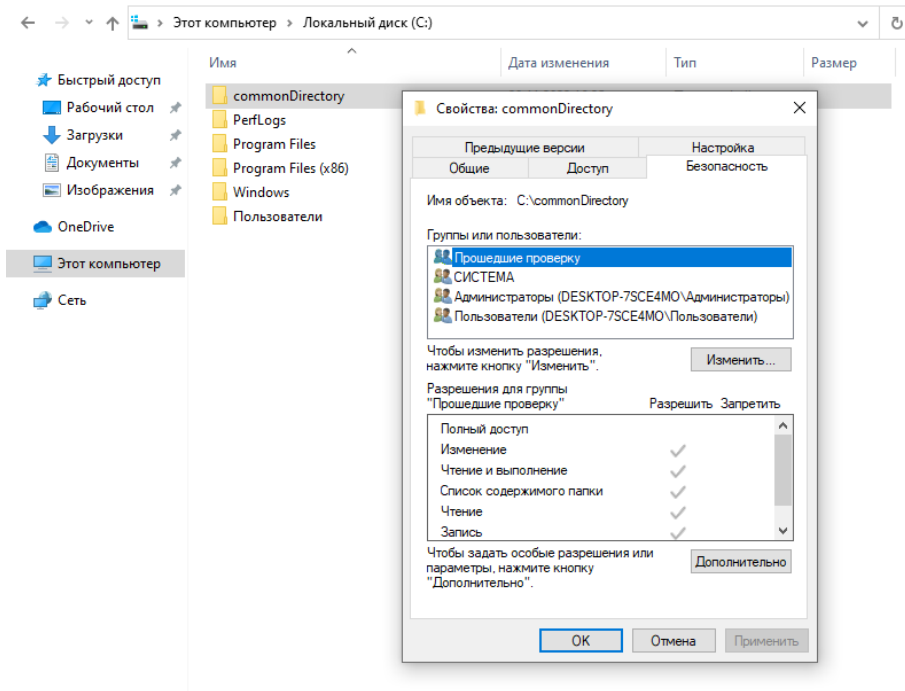
Локальная учетная запись

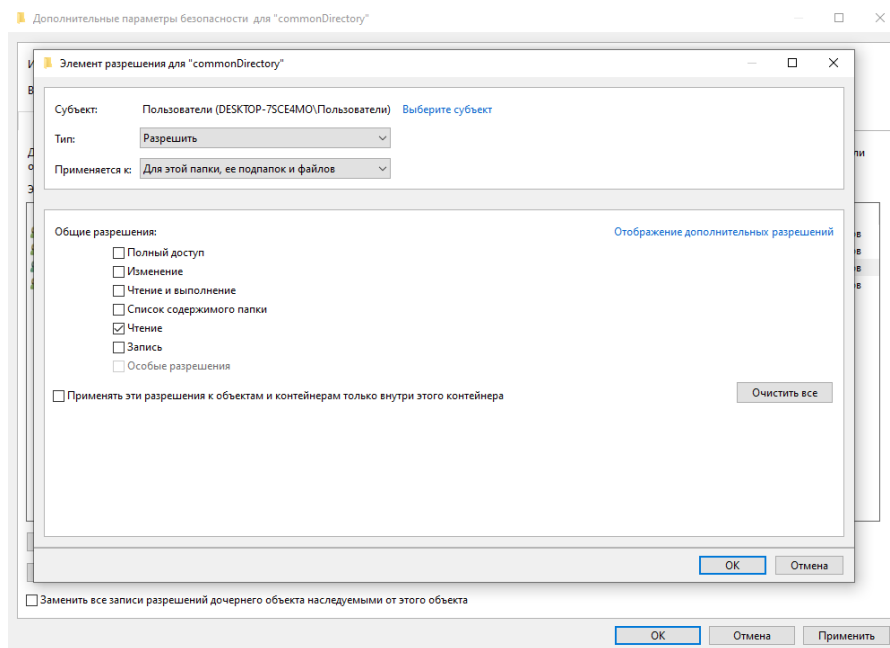
3) Создать директорию *commonDirectory*, в которой для пользователей *lab1*, *lab2* создать свою собственную поддиректорию *lab1dir*, *lab2dir*.



4) Установить права на директорию *commonDirectory*, все ее подпапки и файлы — все пользователи в ОС могут читать ее, но изменять содержимое не могут.

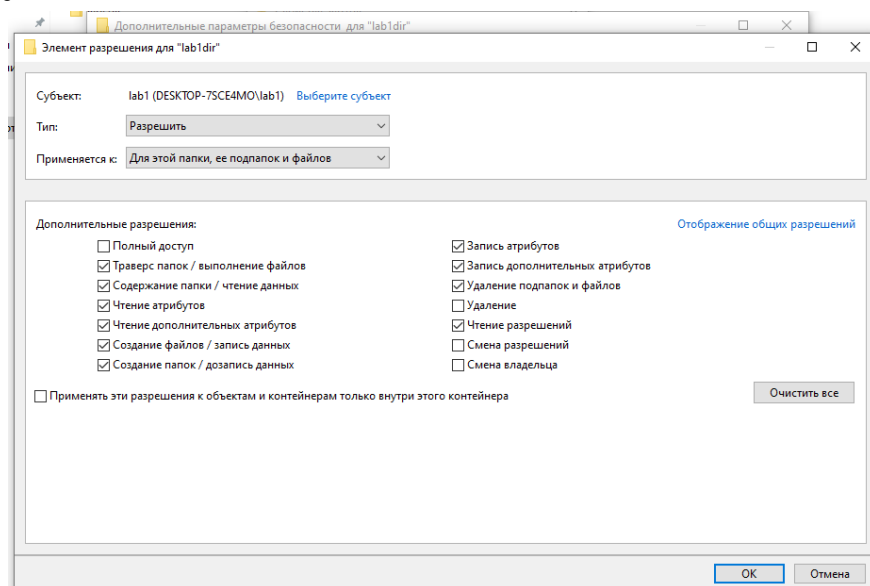
Для установки прав необходимо открыть свойства директории, перейти во вкладку “безопасность”, затем нажать “дополнительно”, чтобы задать разрешения. Для того, чтобы появилась возможность редактировать доступы, необходимо отключить наследование.

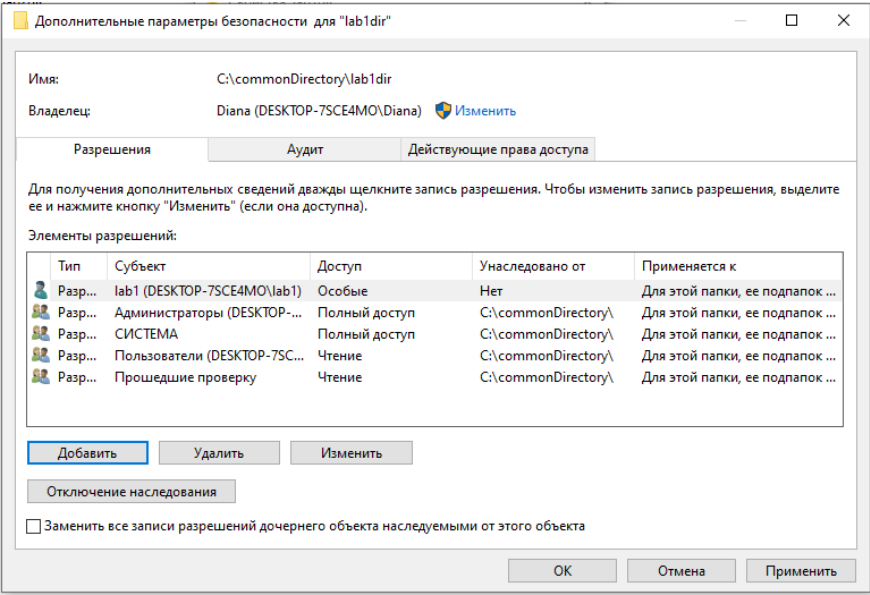




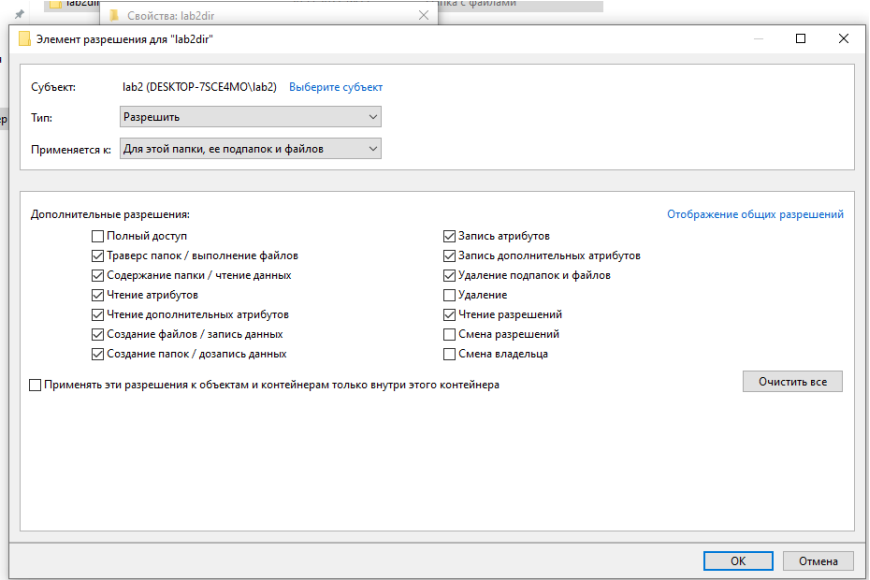
5) Установить права на поддиректории следующим образом: в собственной поддиректории пользователь имеет полный доступ к поддиректориям и файлам, а в чужих поддиректориях пользователи могут только читать. Но удалять свою собственную поддиректорию пользователь не может.

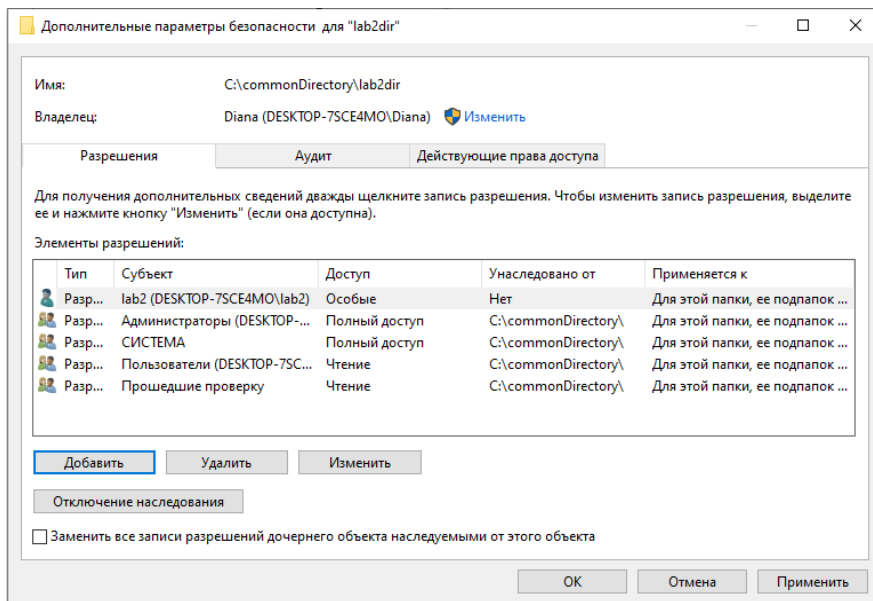
Также, как и в предыдущем пункте открываем настройку доступов и добавляем новый субъект lab1 и для него отдельно настраиваем необходимые разрешения, за исключением удаления, смены разрешений и владельца (два последних, так как выдача таких прав нивелирует отсутствие удаления и можно самостоятельно выдать себе на это доступ)





Аналогично проделываем для lab2





б) Продемонстрировать, что установленные права строго соблюдаются для пользователей lab1, lab2. Обязательно показать попытку удаления собственной директории (lab1 – lab1dir, lab2 – lab2dir).

Проверяем для пользователя lab1 его права для своей директории

```
C:\commonDirectory\lab1dir>whoami
desktop-7sce4mo\lab1

C:\commonDirectory\lab1dir>echo hello > file.txt

C:\commonDirectory\lab1dir>mkdir hello

C:\commonDirectory\lab1dir>rmdir hello

C:\commonDirectory\lab1dir>del file.txt

C:\commonDirectory\lab1dir>
```

В удалении директории отказано

```
C:\>rmdir commonDirectory\lab1dir
Отказано в доступе.

C:\>
```

Аналогично проделываем для lab2

```

C:\commonDirectory\lab2dir>whoami
desktop-7sce4mo\lab2

C:\commonDirectory\lab2dir>echo hello > file.txt

C:\commonDirectory\lab2dir>mkdir hello

C:\commonDirectory\lab2dir>rmdir hello
"rmdir" не является внутренней или внешней
командой, исполняемой программой или пакетным файлом.

C:\commonDirectory\lab2dir>rmdir hello

C:\commonDirectory\lab2dir>del file.txt

C:\commonDirectory\lab2dir>cd ../../..

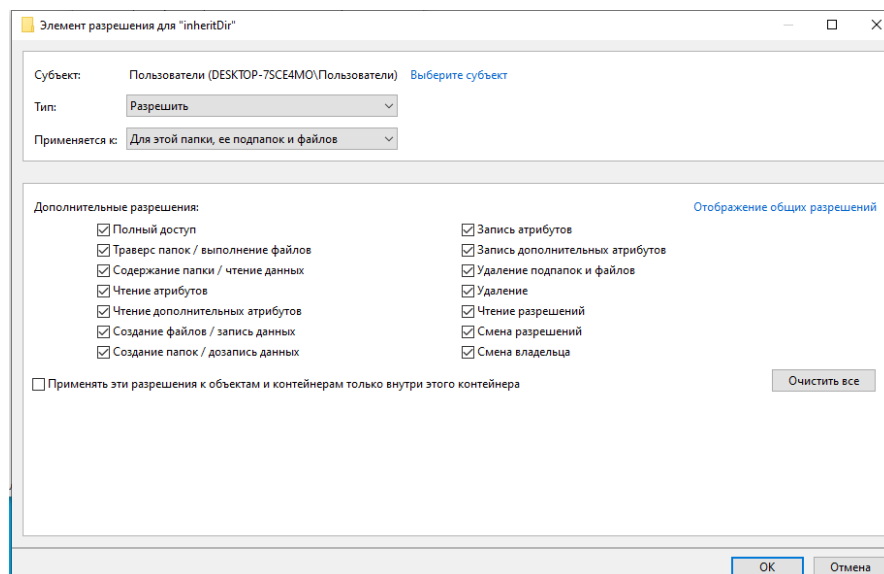
C:\>rmdir commonDirectory\lab2dir
Отказано в доступе.

C:\>

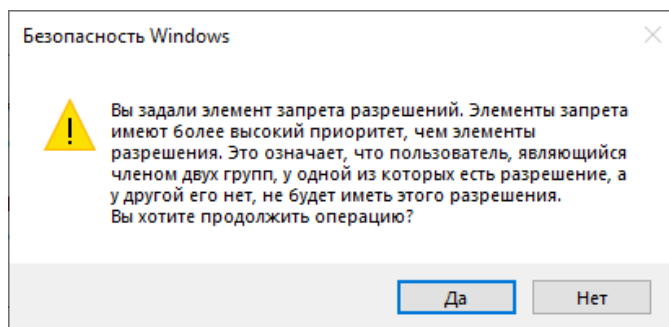
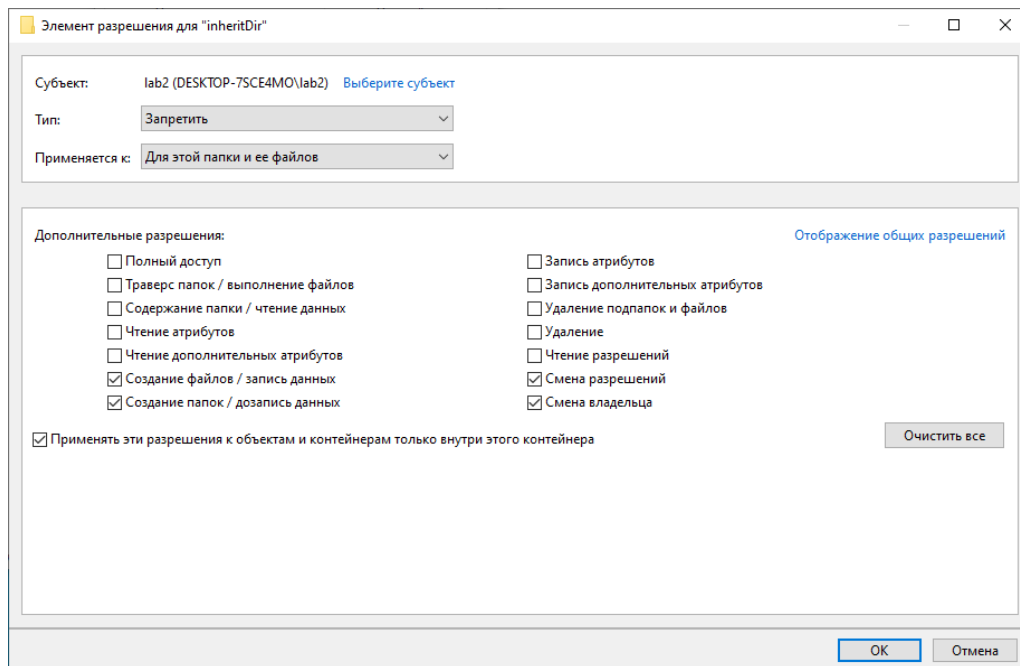
```

2. Управление наследованием прав доступа файлов и каталогов.

1) Создать директорию *inheritDir*. Разрешить к ней, ее подпапкам и файлам полный доступ для всех пользователей.



2) Назначить права доступа к ней следующим образом: в этой директории пользователь *lab2* не может редактировать файлы, а в любой поддиректории – может. При этом пользователь *lab2* имеет полный доступ ко всем директориям.



Исходя из этого доступы у lab2 останутся, которые были до этого: полный доступ ко всем директориям, но заданные запреты будут приоритетнее, чем разрешения, что соответствует заданию.

3) От имени пользователя lab1 создать в директории inheritDir файл text1.txt с произвольным содержимым, директорию folder, в директории folder создать файл text2.txt с произвольным содержимым.

```
C:\>cd inheritDir

C:\inheritDir>whoami
desktop-7sce4mo\lab1

C:\inheritDir>echo hello > text1.txt

C:\inheritDir>mkdir folder

C:\inheritDir>cd folder

C:\inheritDir\folder>echo hello > text2.txt

C:\inheritDir\folder>_
```

4) От имени пользователя lab2 в директории inheritDir совершить попытку редактирования файла text1.txt, попытку создания поддиректории lab2subdir.

```
C:\inheritDir>echo hello > text1.txt
Отказано в доступе.

C:\inheritDir>mkdir lab2subdir
Отказано в доступе.

C:\inheritDir>_
```

5) От имени пользователя lab2 совершить попытку редактировать файл text2.txt.

```
C:\inheritDir>cd folder

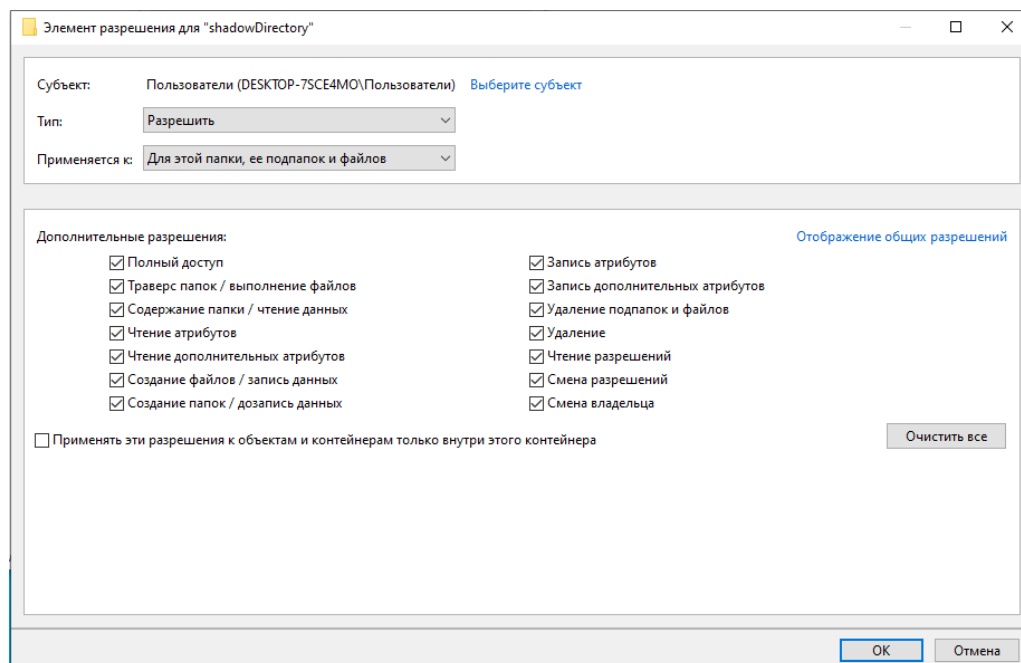
C:\inheritDir\folder>whoami
desktop-7sce4mo\lab2

C:\inheritDir\folder>echo hello > text2.txt

C:\inheritDir\folder>
```

3. Создание общедоступной темной папки.

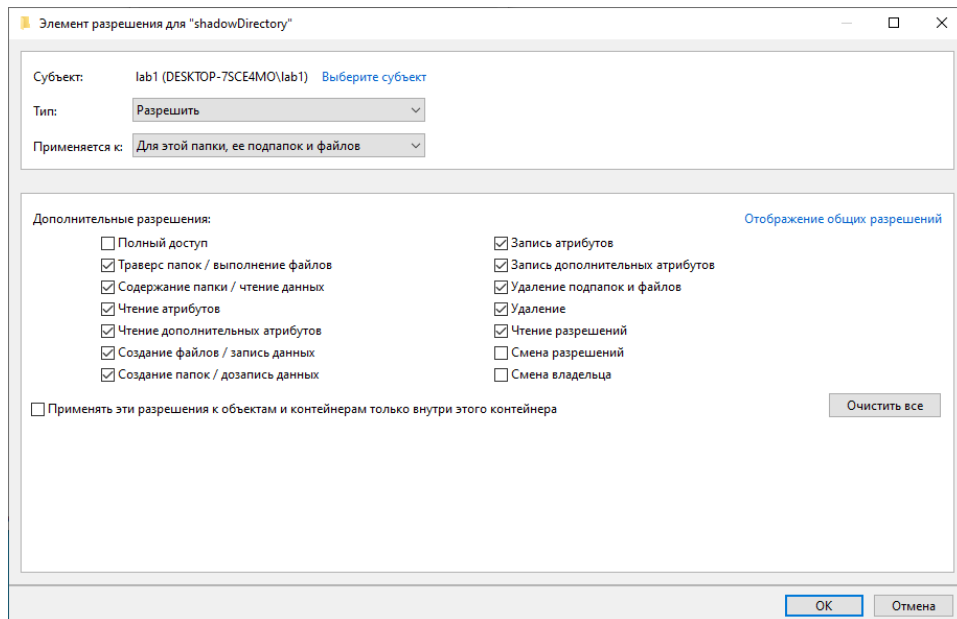
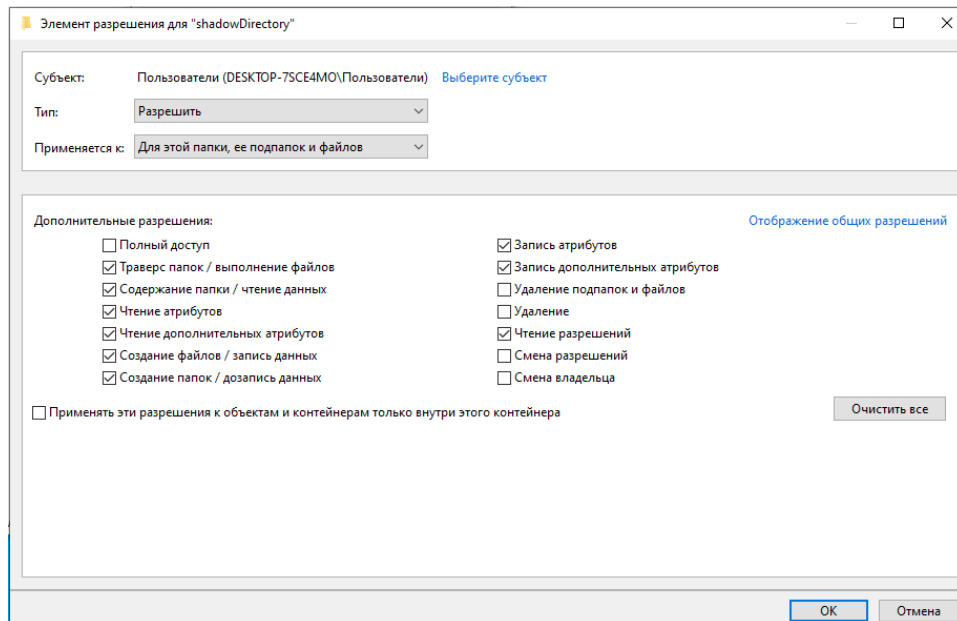
1) Создать директорию shadowDirectory и разрешить к ней, ее поддиректориям и файлам полный доступ всех пользователей. Назначить пользователя lab1 владельцем данной директории.



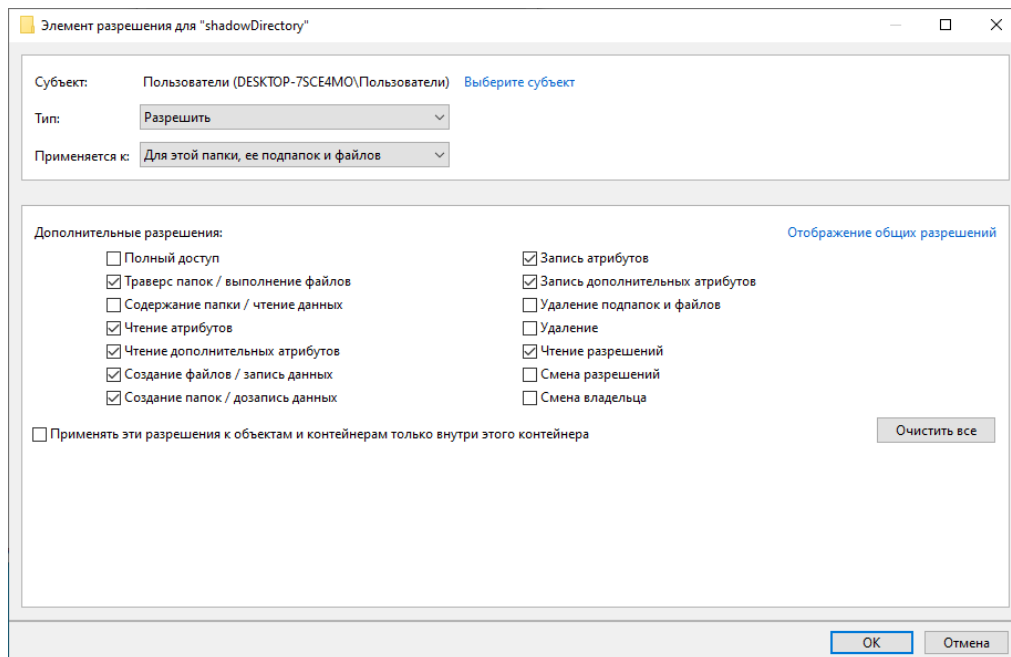
Имя: C:\shadowDirectory

Владелец: lab1 (DESKTOP-7SCE4MO\lab1) [Изменить](#)

2) Установить права на директорию так, чтобы в нее мог писать, изменять файлы любой пользователь, а удалять – только владелец (lab1).



3) Отобрать у всех пользователей, кроме владельца (lab1), право чтения содержимого директории.



4) Продемонстрировать средствами командной строки, что установленные права строго соблюдаются для пользователей lab1, lab2.

```
C:\shadowDirectory>whoami
desktop-7sce4mo\lab2

C:\shadowDirectory>echo hello > file.txt

C:\shadowDirectory>type file.txt
Отказано в доступе.

C:\shadowDirectory>dir
Том в устройстве C не имеет метки.
Серийный номер тома: 0E9E-AE33

Содержимое папки C:\shadowDirectory
Файл не найден

C:\shadowDirectory>mkdir hello

C:\shadowDirectory>rmdir hello
Отказано в доступе.

C:\shadowDirectory>_
```

Пользователь может создавать файлы и директории, но не может их удалять и просматривать содержимое файлов и директорий

```

C:\>cd shadowDirectory

C:\shadowDirectory>whoami
desktop-7sce4mo\lab1

C:\shadowDirectory>echo hello > file1.txt

C:\shadowDirectory>type file1.txt
hello

C:\shadowDirectory>dir
Том в устройстве C не имеет метки.
Серийный номер тома: 0E9E-AE33

Содержимое папки C:\shadowDirectory

20.11.2022  19:05    <DIR>          .
20.11.2022  19:05    <DIR>          ..
20.11.2022  18:52             8 file.txt
20.11.2022  19:05             8 file1.txt
20.11.2022  18:57    <DIR>          hello
                2 файлов             16 байт
                3 папок   40 809 824 256 байт свободно

C:\shadowDirectory>mkdir hello1

C:\shadowDirectory>rmdir hello1

C:\shadowDirectory>

```


Тут может увидеть, что у владельца lab1 есть возможность редактирования файлов/директорий, а также их просмотр и удаление

4. Использование привилегий.

1) Создать нового обычного пользователя lab3.

Другие пользователи

Разрешите пользователям, не включенным в семью, входить в систему с помощью их учетных записей. Это не будет означать их добавление в семью.

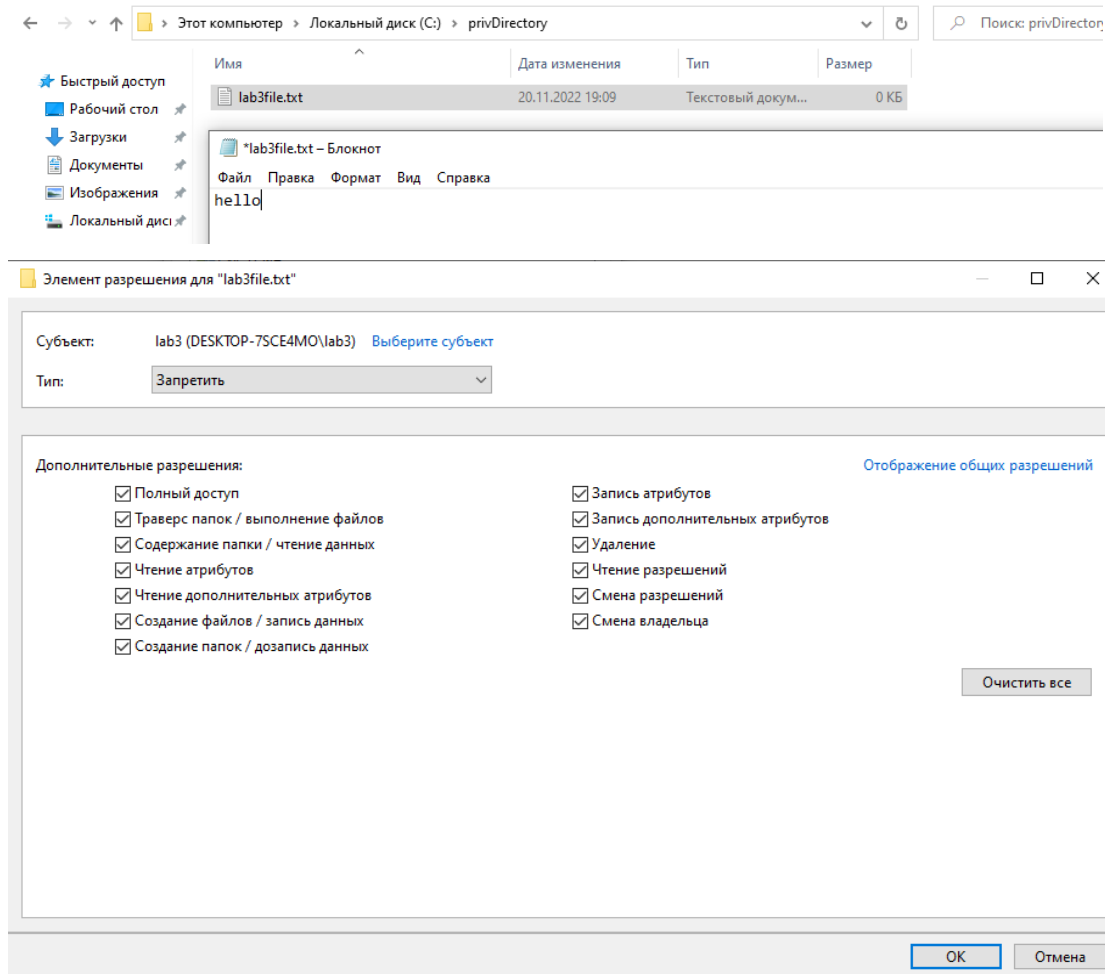
 Добавить пользователя для этого компьютера

 lab1
Локальная учетная запись

 lab2
Локальная учетная запись

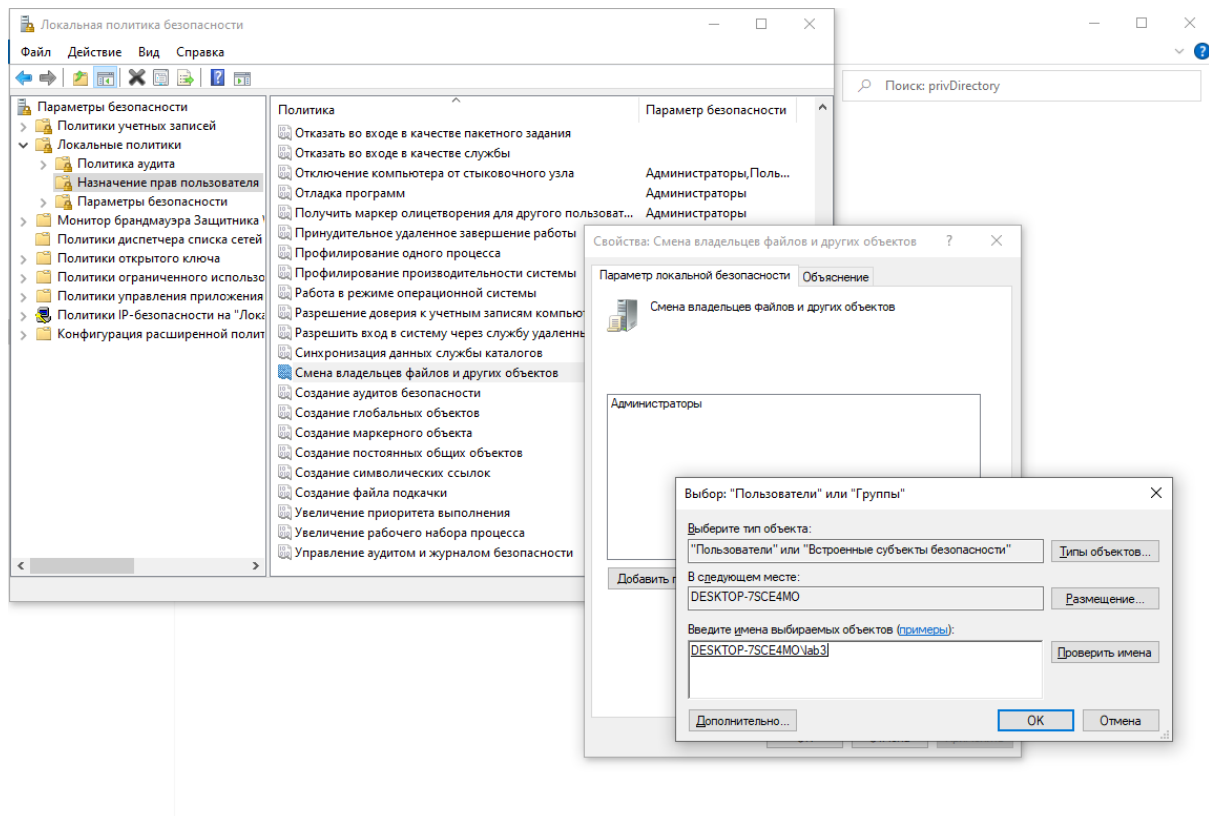
 lab3
Локальная учетная запись

2) Создать директорию *privDirectory*, создать в ней файл *lab3file.txt* с произвольным содержимым и запретить к нему полный доступ для пользователя *lab3*.



3) Добавить пользователю привилегию «*SeTakeOwnershipPrivilege*» (смена владельцев файлов и других объектов).

Необходимо открыть локальную политику безопасности -> локальные политики -> назначение прав пользователя -> смена владельцев файлов и других объектов



4) Войти в систему от имени пользователя lab3, воспользоваться предоставленной привилегией и прочитать файл lab3file.txt.
(Подсказка: воспользоваться командой командной строки takeown)

```
C:\privDirectory>type lab3file.txt
Отказано в доступе.

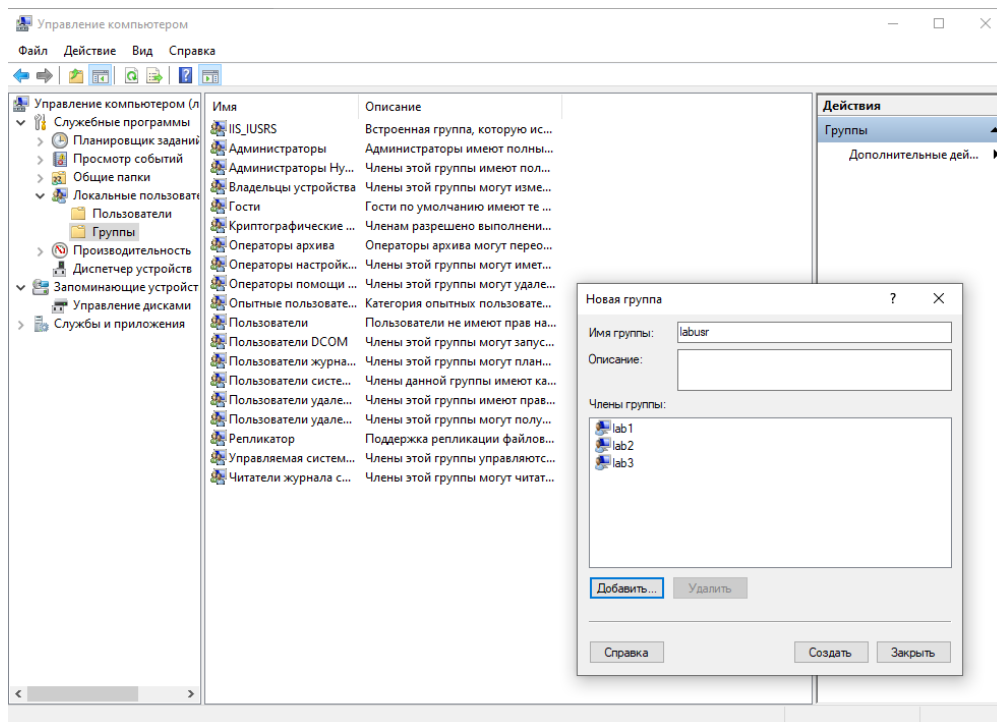
C:\privDirectory>takeown /f "lab3file.txt"
ОШИБКА: Отказано в доступе.

C:\privDirectory>
```

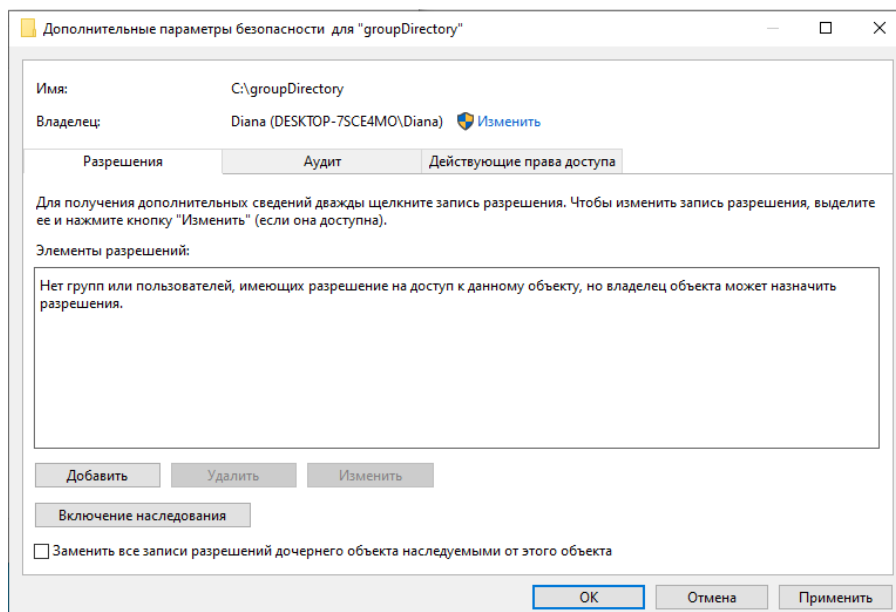
5. Изменение прав доступа к файлам и каталогам для групп пользователей.

1) Создать группу пользователей дфи1, добавить в нее пользователей lab1, lab2, lab3.

Необходимо открыть управление компьютером -> локальные пользователи -> группы



2) Создать директорию *groupDirectory*, во вкладке *безопасность* созданной директории оставить пустым список элементов разрешений. Совершить попытку прочитать содержимое директории от имени пользователя *lab1*. Объяснить результат.




```

C:\>whoami
desktop-7sce4mo\lab1

C:\>dir groupDirectory
Том в устройстве C не имеет метки.
Серийный номер тома: 0E9E-AE33

Содержимое папки C:\groupDirectory

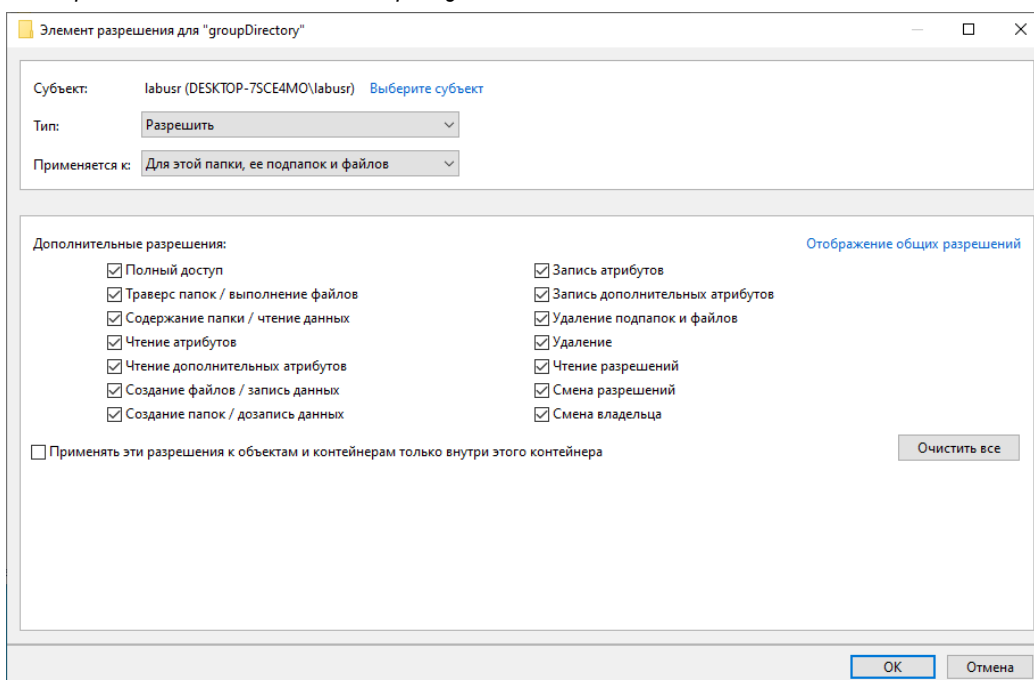
Файл не найден

C:\>

```

Пользователь lab1 не смог прочитать содержимое директории, так как не заданы никакие разрешения, следовательно ни один из пользователей, кроме владельца в таком случае не имеет доступ.

3) Разрешить членам группы labusr полный доступ к директории groupDirectory, ее подпапкам и файлам. От имени пользователя lab1 войти в директорию и создать в ней файл textfile.txt с произвольным содержимым. Объяснить результат.



```

C:\>whoami
desktop-7sce4mo\lab1

C:\>cd groupDirectory

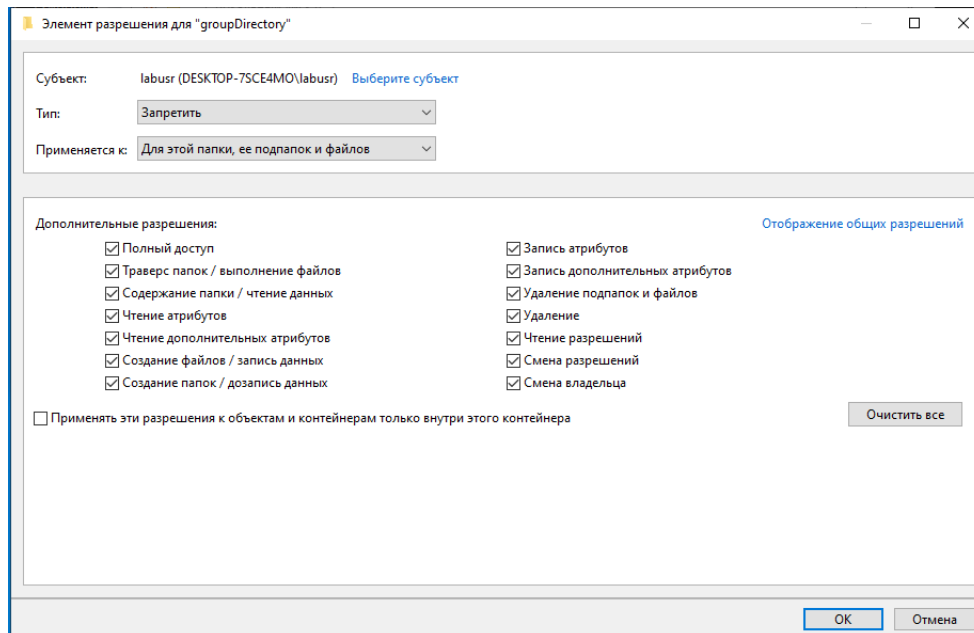
C:\groupDirectory>echo hello > textfile.txt

C:\groupDirectory>

```

lab1 находится в группе labusr, соответственно, если у группы есть соответствующий доступ, то и у всех пользователей группы.

4) Добавить в список элементов разрешений запись, запрещающую членам группы labusr полный доступ к директории groupDirectory, ее подпапкам и файлам. Совершить попытку прочитать содержимое файла textfile.txt от имени пользователя lab1. Объяснить результат.



```
C:\>whoami
desktop-7sce4mo\lab1

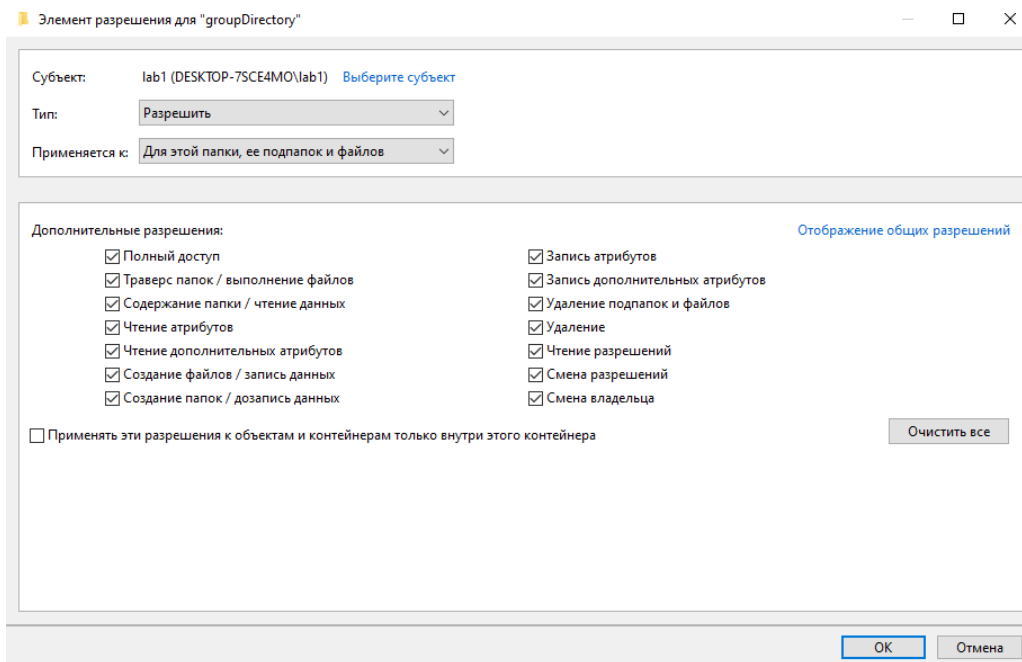
C:\>cd groupDirectory
Отказано в доступе.

C:\>type groupDirectory\textfile.txt
Отказано в доступе.

C:\>
```

Как и обнаруживалось ранее запрет на доступ приоритетнее, чем разрешение, поэтому в доступе отказано

5) Добавить в список элементов разрешений запись, разрешающую пользователю lab1 полный доступ к директории groupDirectory, ее подпапкам и файлам. Совершить попытку прочитать содержимое файла textfile.txt от имени пользователя lab1. Объяснить результат.



```
C:\>whoami
desktop-7sce4mo\lab1

C:\>cd groupDirectory
Отказано в доступе.

C:\>type groupDirectory\textfile.txt
Отказано в доступе.

C:\>
```

Результат аналогичен по той же причине приоритетности запретов

6. Работа с маркером доступа.

1) Запустить командную строку в обычном режиме. Посмотреть с помощью команды `whoami` командной строки идентификаторы пользователей `lab3`, `admin` доступные им привилегии, а также группы, в которые входят данные пользователи.

admin:

```
C:\Users\whoami>desktop-7sce4mo\diana
C:\Users\whoami /all

Сведения о пользователе
-----

Пользователь          SID
-----
desktop-7sce4mo\diana S-1-5-21-3479258768-1280350526-2449581956-1000

Сведения о группах
-----

Группа                                     Тип          SID          Атрибуты
-----
Все                                       Хорошо известная группа S-1-1-0      Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Локальная учетная запись и член группы "Администраторы" Хорошо известная группа S-1-5-114    Группа, используемая только для запрета
BUILTIN\Администраторы                  Псевдоним     S-1-5-32-544  Группа, используемая только для запрета
BUILTIN\Пользователи                    Псевдоним     S-1-5-32-545  Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\ИНТЕРАКТИВНЫЕ                Хорошо известная группа S-1-5-4       Обязательная группа, Включены по умолчанию, Включенная группа
КОНСОЛЬНЫЙ ВХОД                         Хорошо известная группа S-1-2-1       Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Прошедшие проверку           Хорошо известная группа S-1-5-11      Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Данная организация          Хорошо известная группа S-1-5-15      Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Локальная учетная запись    Хорошо известная группа S-1-5-113     Обязательная группа, Включены по умолчанию, Включенная группа
ЛОКАЛЬНЫЕ                               Хорошо известная группа S-1-2-0       Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Проверка подлинности NTLM     Хорошо известная группа S-1-5-64-10   Обязательная группа, Включены по умолчанию, Включенная группа
Обязательная метка\Средний обязательный уровень Метка         S-1-16-8192

Сведения о привилегиях
-----

Имя привилегии      Описание      Область, край
-----
SeShutdownPrivilege Завершение работы системы      Отключен
SeChangeNotifyPrivilege Обход перекрестной проверки     Включен
SeUndockPrivilege    Отключение компьютера от стыковочного узла Отключен
SeIncreaseWorkingSetPrivilege Увеличение рабочего набора процесса Отключен
SeTimeZonePrivilege  Изменение часового пояса        Отключен
```

lab3:

```
C:\Users\lab3>whoami /ALL

Сведения о пользователе
-----

Пользователь          SID
-----
desktop-7sce4mo\lab3 S-1-5-21-3479258768-1280350526-2449581956-1003

Сведения о группах
-----

Группа                                     Тип          SID          Атрибуты
-----
Все                                       Хорошо известная группа S-1-1-0      Обязательная группа, Включены по умолчанию, Включенная группа
BUILTIN\Пользователи                    Псевдоним     S-1-5-32-545  Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\ИНТЕРАКТИВНЫЕ                Хорошо известная группа S-1-5-4       Обязательная группа, Включены по умолчанию, Включенная группа
КОНСОЛЬНЫЙ ВХОД                         Хорошо известная группа S-1-2-1       Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Прошедшие проверку           Хорошо известная группа S-1-5-11      Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Данная организация          Хорошо известная группа S-1-5-15      Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Локальная учетная запись    Хорошо известная группа S-1-5-113     Обязательная группа, Включены по умолчанию, Включенная группа
ЛОКАЛЬНЫЕ                               Хорошо известная группа S-1-2-0       Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Проверка подлинности NTLM     Хорошо известная группа S-1-5-64-10   Обязательная группа, Включены по умолчанию, Включенная группа
Обязательная метка\Средний обязательный уровень Метка         S-1-16-8192

Сведения о привилегиях
-----

Имя привилегии      Описание      Область, край
-----
SeShutdownPrivilege Завершение работы системы      Отключен
SeChangeNotifyPrivilege Обход перекрестной проверки     Включен
SeUndockPrivilege    Отключение компьютера от стыковочного узла Отключен
SeIncreaseWorkingSetPrivilege Увеличение рабочего набора процесса Отключен
SeTimeZonePrivilege  Изменение часового пояса        Отключен
```

2) Запустить командную строку в режиме работы от имени администратора. Посмотреть с помощью команды `whoami` командной строки идентификаторы пользователей `lab3`, `admin` доступные им привилегии, а также группы, в которые входят данные пользователи.

admin:

```
C:\Windows\system32\whoami /ALL

Сведения о пользователе
-----

Пользователь          SID
-----
desktop-7sce4mo\diana S-1-5-21-3479258768-1280350526-2449581956-1000

Сведения о группах
-----

Группа                                     Тип          SID          Атрибуты
-----
Все                                       Хорошо известная группа S-1-1-0      Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Локальная учетная запись и член группы "Администраторы" Хорошо известная группа S-1-5-114     Обязательная группа, Включены по умолчанию, Включенная группа
BUILTIN\Администраторы                  Псевдоним     S-1-5-32-544  Обязательная группа, Включены по умолчанию, Включенная группа, Владелец группы
BUILTIN\Пользователи                    Псевдоним     S-1-5-32-545  Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\ИНТЕРАКТИВНЫЕ                Хорошо известная группа S-1-5-4       Обязательная группа, Включены по умолчанию, Включенная группа
КОНСОЛЬНЫЙ ВХОД                         Хорошо известная группа S-1-2-1       Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Прошедшие проверку          Хорошо известная группа S-1-5-11      Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Данная организация        Хорошо известная группа S-1-5-15      Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Локальная учетная запись   Хорошо известная группа S-1-5-113     Обязательная группа, Включены по умолчанию, Включенная группа
ЛОКАЛЬНЫЕ                               Хорошо известная группа S-1-2-0       Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Проверка подлинности NTLM   Хорошо известная группа S-1-5-64-10   Обязательная группа, Включены по умолчанию, Включенная группа
Обязательная метка\Высокий обязательный уровень Метка         S-1-16-12288  Обязательная группа, Включены по умолчанию, Включенная группа

Сведения о привилегиях
-----

Имя привилегии          Описание          Область, край
-----
SeIncreaseQuotaPrivilege Настройка квот памяти для процесса Отключен
SeSecurityPrivilege      Управление аудитом и журналом безопасности Отключен
SeTakeOwnershipPrivilege Смена владельцев файлов и других объектов Отключен
SeLoadDriverPrivilege   Загрузка и выгрузка драйверов устройств Отключен
SeSystemProfilePrivilege Профилирование производительности системы Отключен
SeSystemTimePrivilege   Изменение системного времени Отключен
SeProfileSingleProcessPrivilege Профилирование одного процесса Отключен
SeIncreaseBasePriorityPrivilege Увеличение приоритета выполнения Отключен
SeCreatePagefilePrivilege Создание файла подкачки Отключен
SeBackupPrivilege       Архивация файлов и каталогов Отключен
SeRestorePrivilege      Восстановление файлов и каталогов Отключен
SeShutdownPrivilege     Завершение работы системы Отключен
SeDebugPrivilege        Отладка программ Отключен
SeSystemEnvironmentPrivilege Изменение параметров среды изготовителя Отключен
SeChangeNotifyPrivilege Обход перекрестной проверки включен
SeRemoteShutdownPrivilege Принудительное удаленное завершение работы Отключен
SeUndockPrivilege       Отключение компьютера от стыковочного узла Отключен
SeManageVolumePrivilege Выполнение задач по обслуживанию томов Отключен
SeImpersonatePrivilege  Имитация клиента после проверки подлинности Оключен
SeCreateGlobalPrivilege Создание глобальных объектов включен
SeIncreaseWorkingSetPrivilege Увеличение рабочего набора процесса Отключен
SeTimeZonePrivilege     Изменение часового пояса Отключен
SeCreateSymbolicLinkPrivilege Создание символических ссылок Отключен
SeDelegateSessionUserImpersonatePrivilege Получить маркер олицетворения для другого пользователя в том же сеансе Отключен

C:\Windows\system32>
```

lab3:

```
C:\Windows\system32\whoami /ALL

Сведения о пользователе
-----

Пользователь          SID
-----
desktop-7sce4mo\lab3 S-1-5-21-3479258768-1280350526-2449581956-1003

Сведения о группах
-----

Группа                                     Тип          SID          Атрибуты
-----
Все                                       Хорошо известная группа S-1-1-0      Обязательная группа, Включены по умолчанию, Включенная группа
DESKTOP-7SCE4MO\labusr                  Псевдоним     S-1-5-21-3479258768-1280350526-2449581956-1004 Обязательная группа, Включены по умолчанию, Включенная группа
BUILTIN\Пользователи                    Псевдоним     S-1-5-32-545  Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\ИНТЕРАКТИВНЫЕ                Хорошо известная группа S-1-5-4       Обязательная группа, Включены по умолчанию, Включенная группа
КОНСОЛЬНЫЙ ВХОД                         Хорошо известная группа S-1-2-1       Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Прошедшие проверку          Хорошо известная группа S-1-5-11      Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Данная организация        Хорошо известная группа S-1-5-15      Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Локальная учетная запись   Хорошо известная группа S-1-5-113     Обязательная группа, Включены по умолчанию, Включенная группа
ЛОКАЛЬНЫЕ                               Хорошо известная группа S-1-2-0       Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Проверка подлинности NTLM   Хорошо известная группа S-1-5-64-10   Обязательная группа, Включены по умолчанию, Включенная группа
Обязательная метка\Высокий обязательный уровень Метка         S-1-16-12288  Обязательная группа, Включены по умолчанию, Включенная группа

Сведения о привилегиях
-----

Имя привилегии          Описание          Область, край
-----
SeTakeOwnershipPrivilege Смена владельцев файлов и других объектов Отключен
SeShutdownPrivilege     Завершение работы системы Отключен
SeChangeNotifyPrivilege Обход перекрестной проверки включен
SeUndockPrivilege       Отключение компьютера от стыковочного узла Отключен
SeIncreaseWorkingSetPrivilege Увеличение рабочего набора процесса Отключен
SeTimeZonePrivilege     Изменение часового пояса Отключен
```

3) Описать различия в полученных списках групп и привилегий.

Обратить внимание на атрибуты группы Администраторы.

admin:

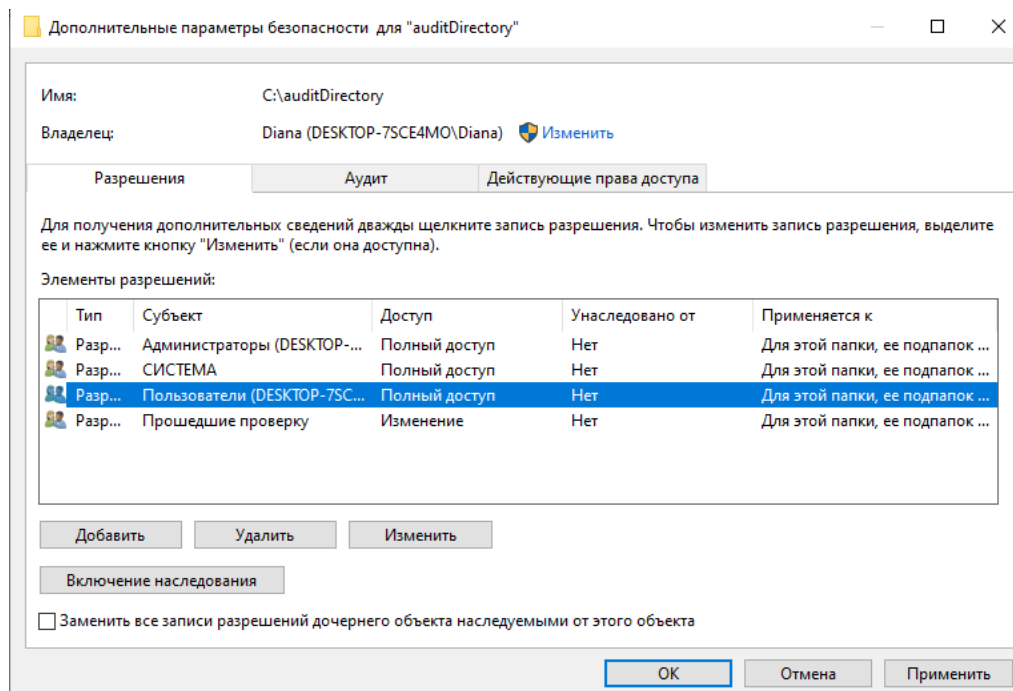
- Изменился SID для Обязательной метки и уровень меняется со среднего на высокий
- Изменяются Атрибуты групп BUILTIN\Администраторы и NT AUTHORITY\Локальная учетная запись и член группы Администраторы
- Добавляется 19 привилегий

lab3:

- Добавляется группа DESKTOP-7SCE4MO\labusr
- Изменился SID для Обязательной метки и уровень меняется со среднего на высокий
- Добавились привилегии SeTakeOwnershipPrivilege и SeShutdownPrivilege

7. Работа с аудитом доступа к файлу.

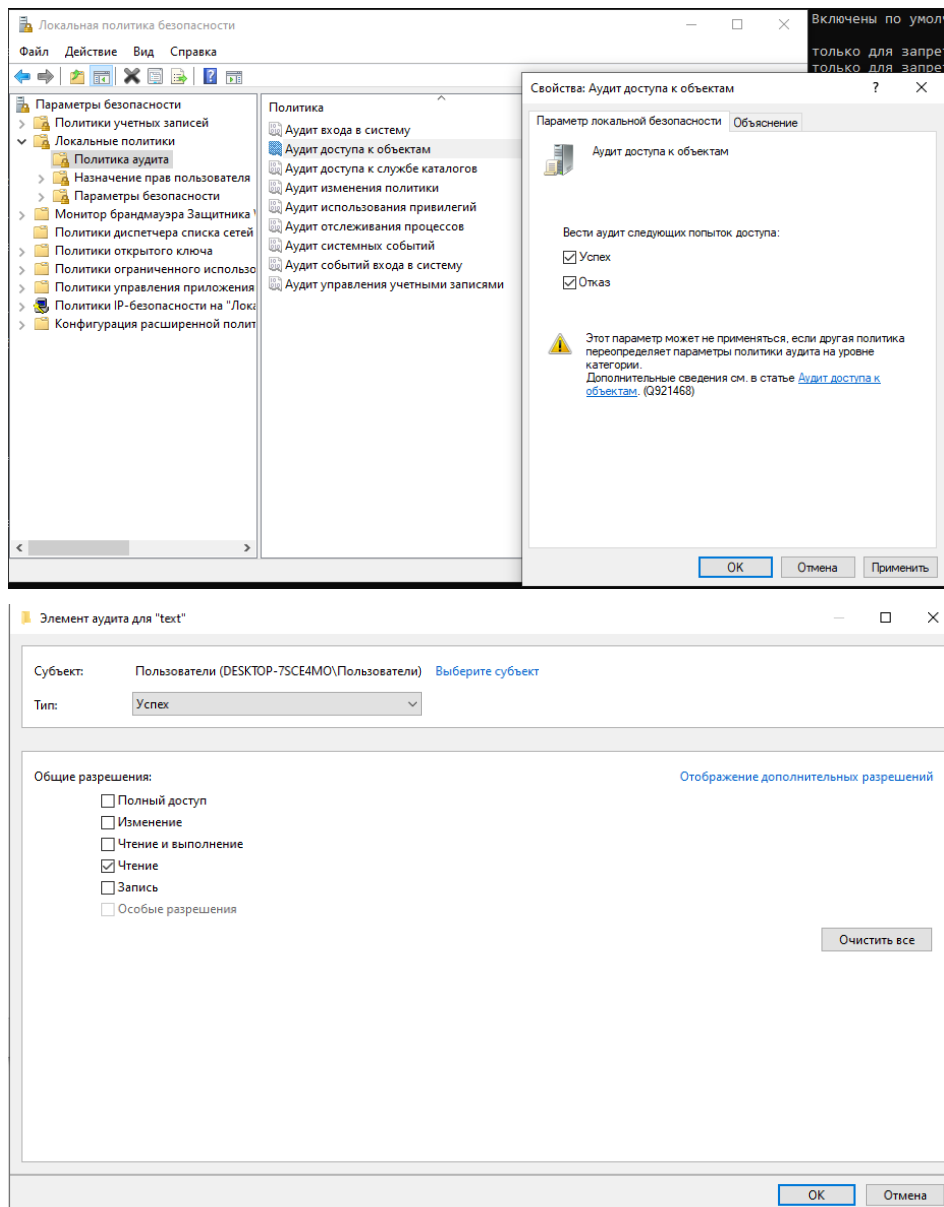
1) Создать директорию *auditDirectory* и разрешить к ней, ее подпапкам и файлам полный доступ всех пользователей.



2) Создать файл *text.txt* с произвольным содержимым в директории *auditDirectory* и включить для него аудит на чтение для всех пользователей.

```
C:\>cd auditDirectory
C:\auditDirectory>echo hello > text.txt
C:\auditDirectory>
```

Необходимо открыть локальную политику безопасности -> локальные политики -> политика аудита -> аудит доступа к объектам



3) Прочитать содержимое файла `text.txt` пользователем `lab1`. Удалить содержимое этого файла, сохранить пустой текстовый файл `text.txt`

```
C:\>cd auditDirectory

C:\auditDirectory>whoami
desktop-7sce4mo\lab1

C:\auditDirectory>type text.txt
hello

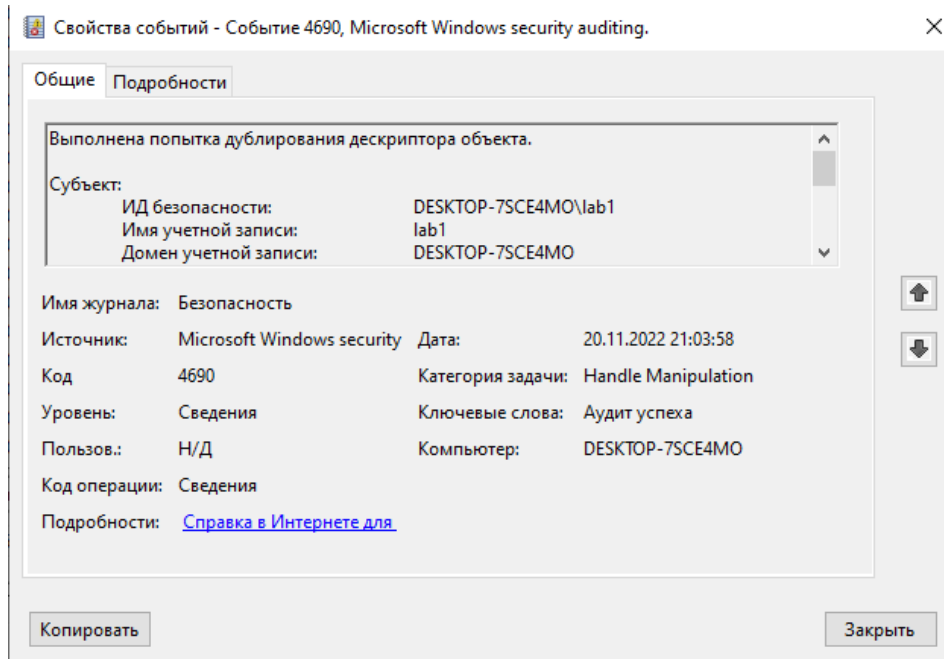
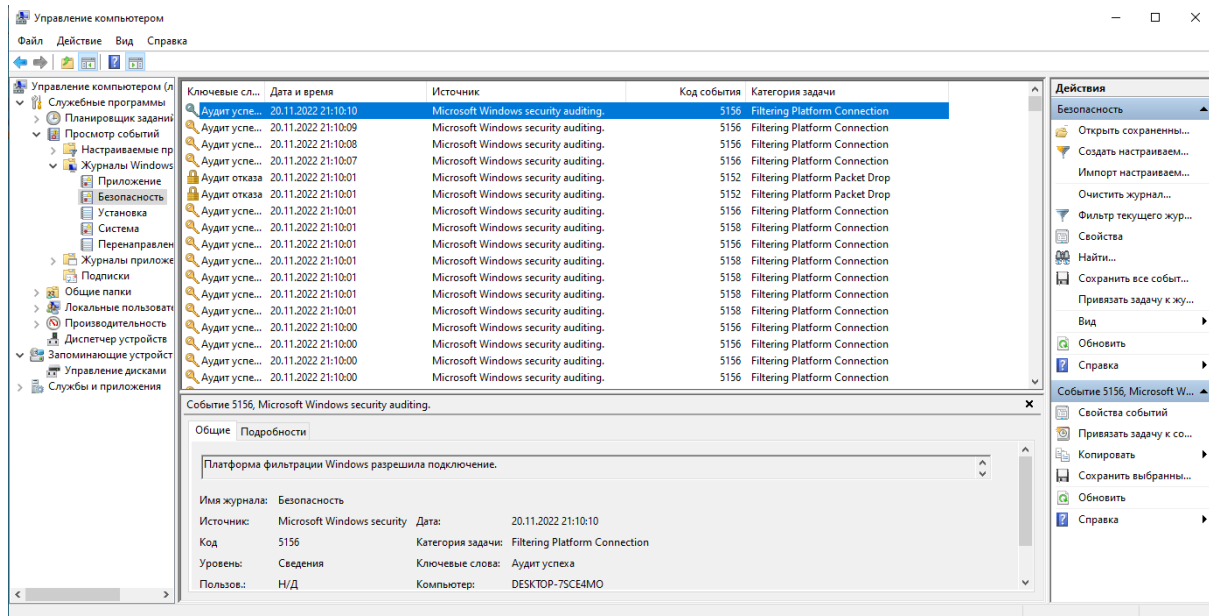
C:\auditDirectory>del text.txt

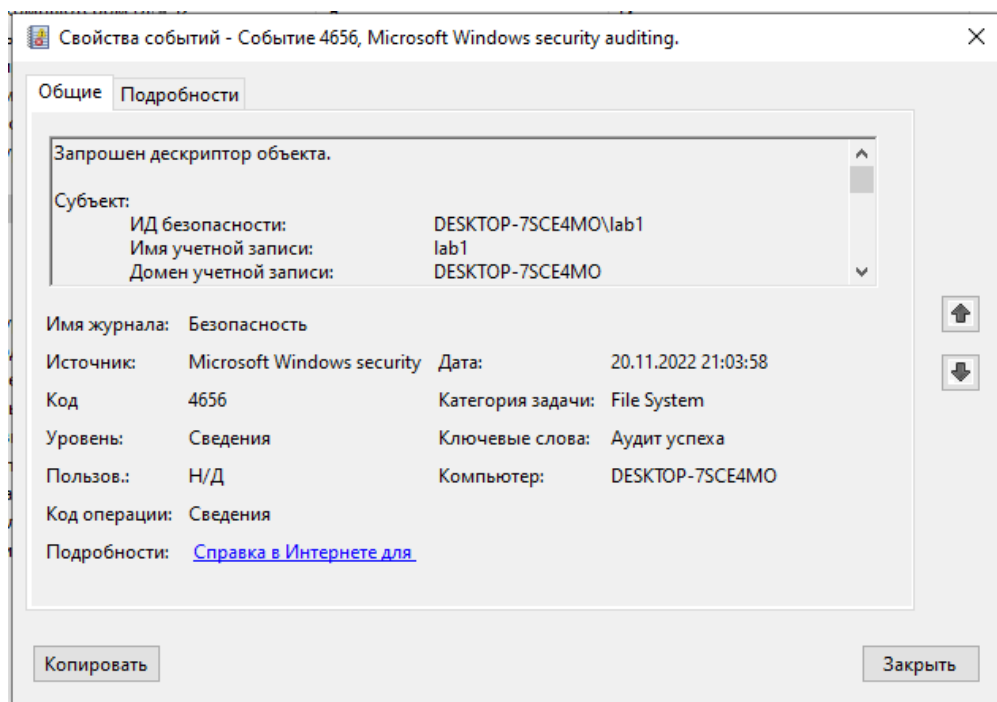
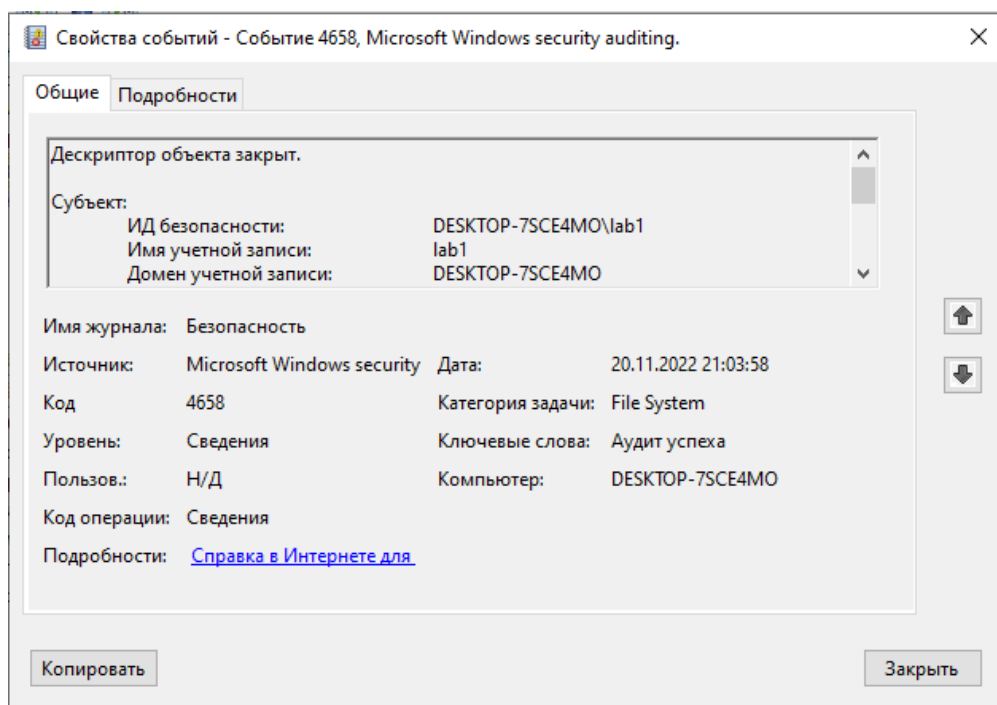
C:\auditDirectory>copy NUL text.txt
Скопировано файлов:      1.

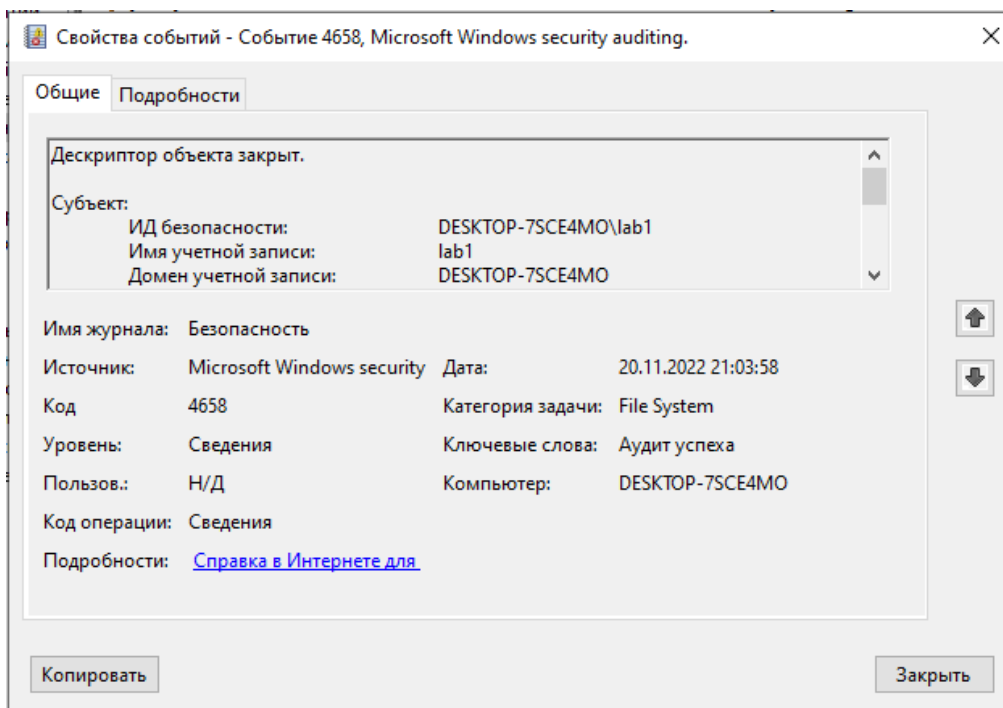
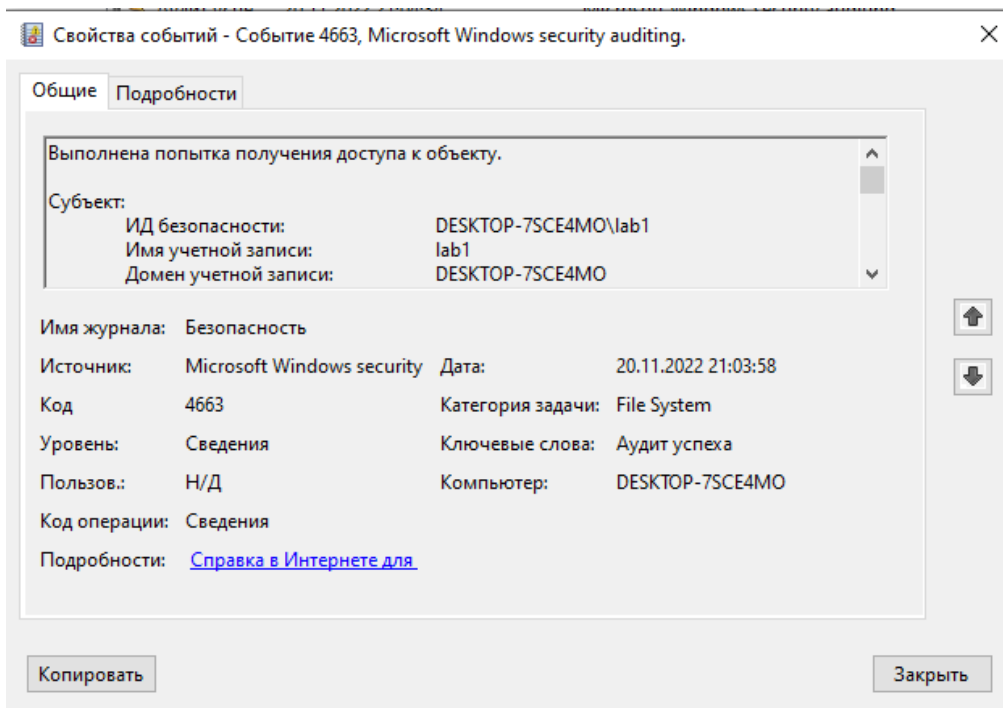
C:\auditDirectory>
```

4) Просмотреть результат аудита и убедиться в наличии в журнале записей с попыткой чтения и записи данных для файла text.txt и пользователя lab1.

Необходимо открыть управление компьютером -> просмотр событий -> журналы Windows -> безопасность







Контрольные вопросы

1. Что лежит в основе управления доступом в ОС Windows?

Одним из важнейших компонентов системы безопасности ОС Windows является система контроля и управления дискреционным доступом. Дискреционная модель разграничения доступа предполагает назначение каждому объекту списка контроля доступа, элементы которого определяют права доступа к объекту конкретного субъекта. Правом редактирования

дискреционного списка контроля доступа обычно обладают владелец объекта и администратор безопасности.

2. Какие разрешения можно предоставить любому объекту в ОС Windows?

Для любого объекта можно предоставить разрешения на:

- группы, пользователи и другие объекты с идентификаторами безопасности в домене;
- группы и пользователи в этом домене и любые доверенные домены;
- локальные группы и пользователи на компьютере, где находится объект.

Права доступа к объекту зависят от типа объекта. Например, разрешения, которые можно прикрепить к файлу, отличаются от разрешений, которые можно прикрепить к разделу реестра. Однако некоторые разрешения являются общими для большинства типов объектов:

- чтение;
- изменение;
- смена владельца;
- удаление

3. Каким образом можно назначать права доступа к файлу в ОС Windows?

Для установки прав необходимо открыть свойства файла, перейти во вкладку “безопасность”, затем нажать “дополнительно”, чтобы задать разрешения. Для того, чтобы появилась возможность редактировать доступы, необходимо отключить наследование.

4. Каким образом можно назначать привилегии пользователей в ОС Windows?

Для назначения привилегий необходимо открыть локальную политику безопасности, затем локальные политики, назначение прав пользователя и выбрать необходимую политику для пользователя.