

Кекеев Алексей Баатович СКБ 181.

Порядок выполнения работы

Лабораторная работа состоит из нескольких заданий.

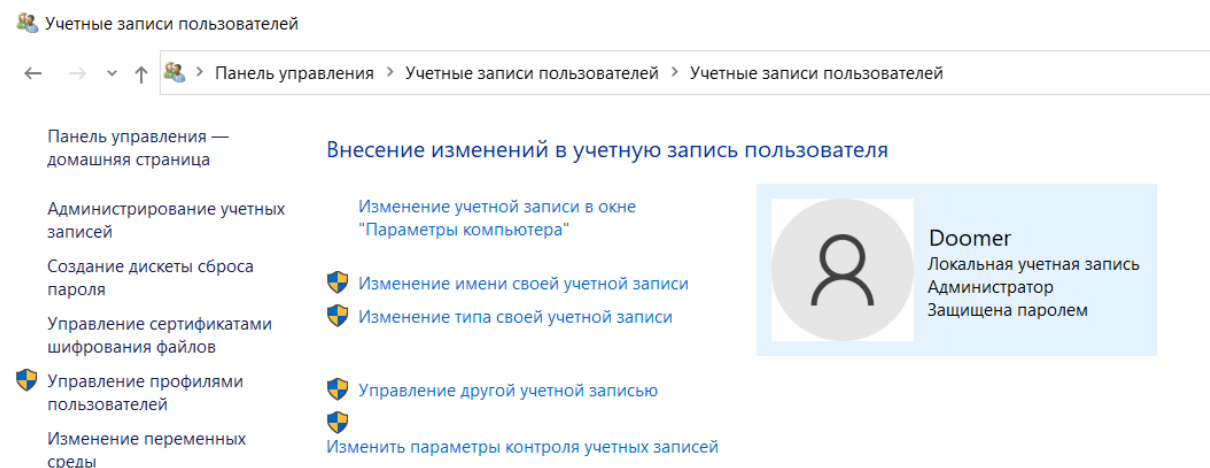
Ход работы:

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

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

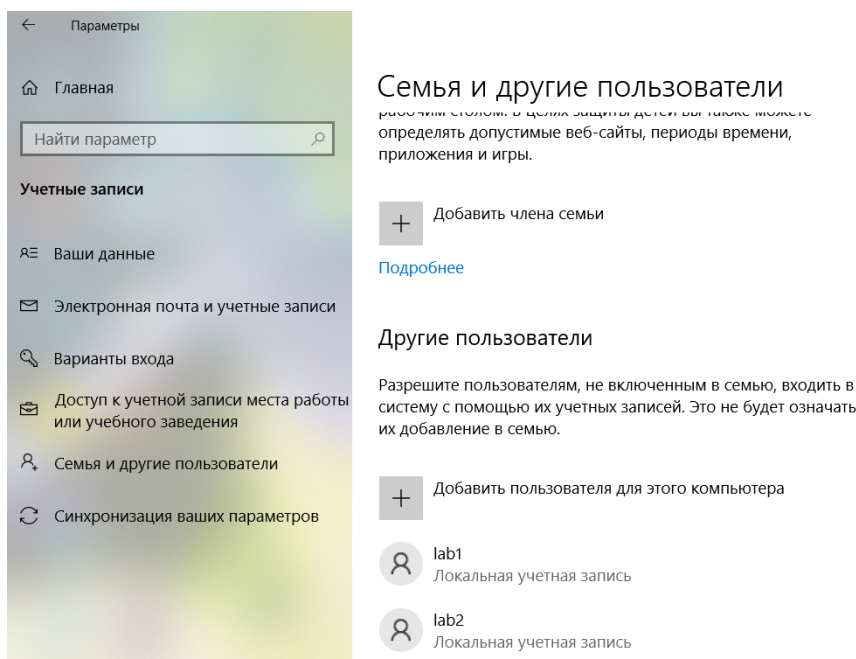
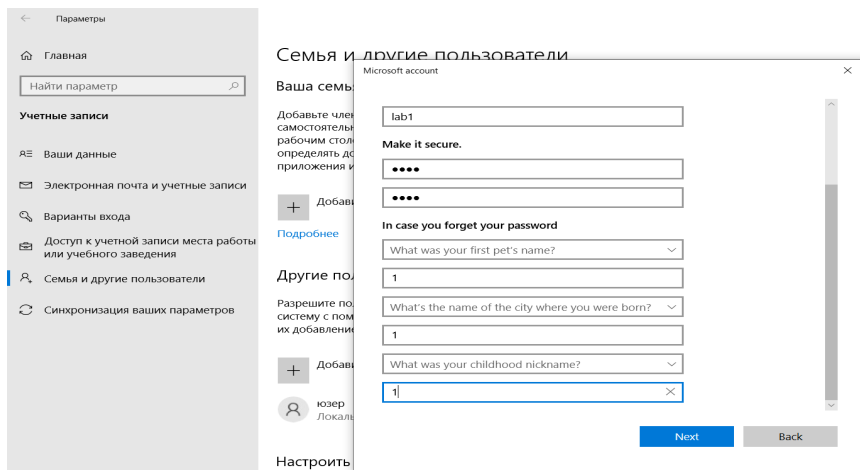
1) Зайти в систему от имени администратора, входящего в группу администраторов системы.

Где и как: зайти через панель управления...



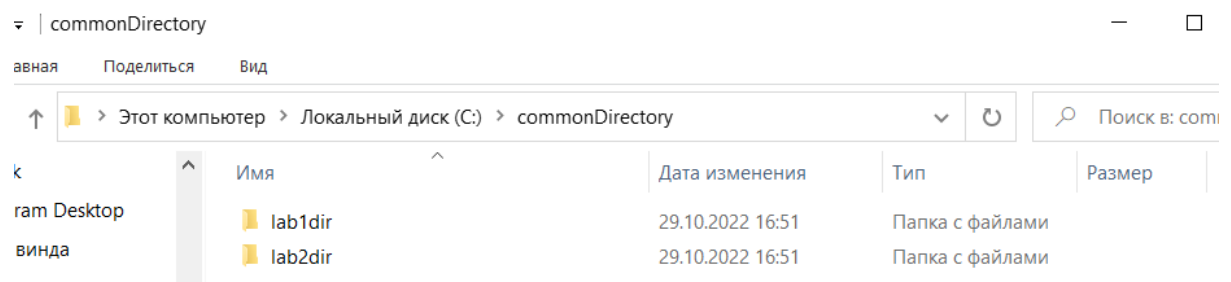
2) Создать в учетных записях двух обычных пользователей: lab1, lab2.

Где и как: Win + X. Выбираем параметры. Учетные записи. Семья и другие пользователи. Нажимаем плюс в "Другие пользователи". В зависимости от версии Windows выбираем варианты без использования электронной почты. (у меня нет данных этого человека, добавить пользователя без учетной записи Microsoft)



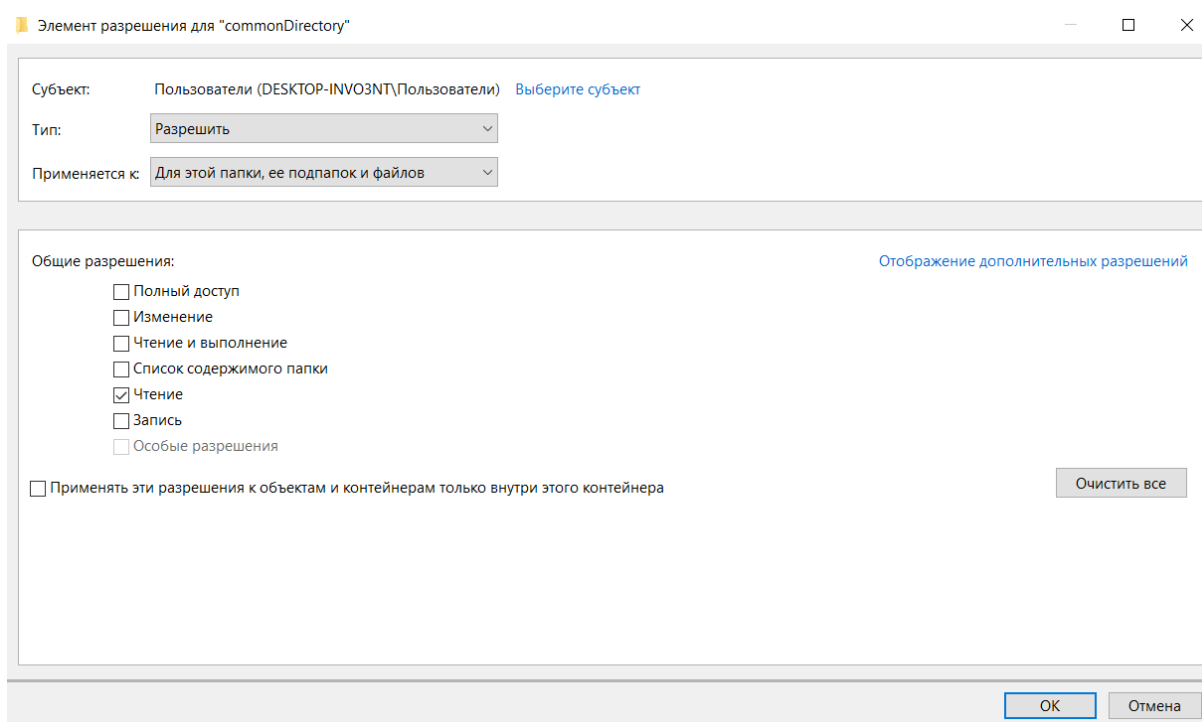
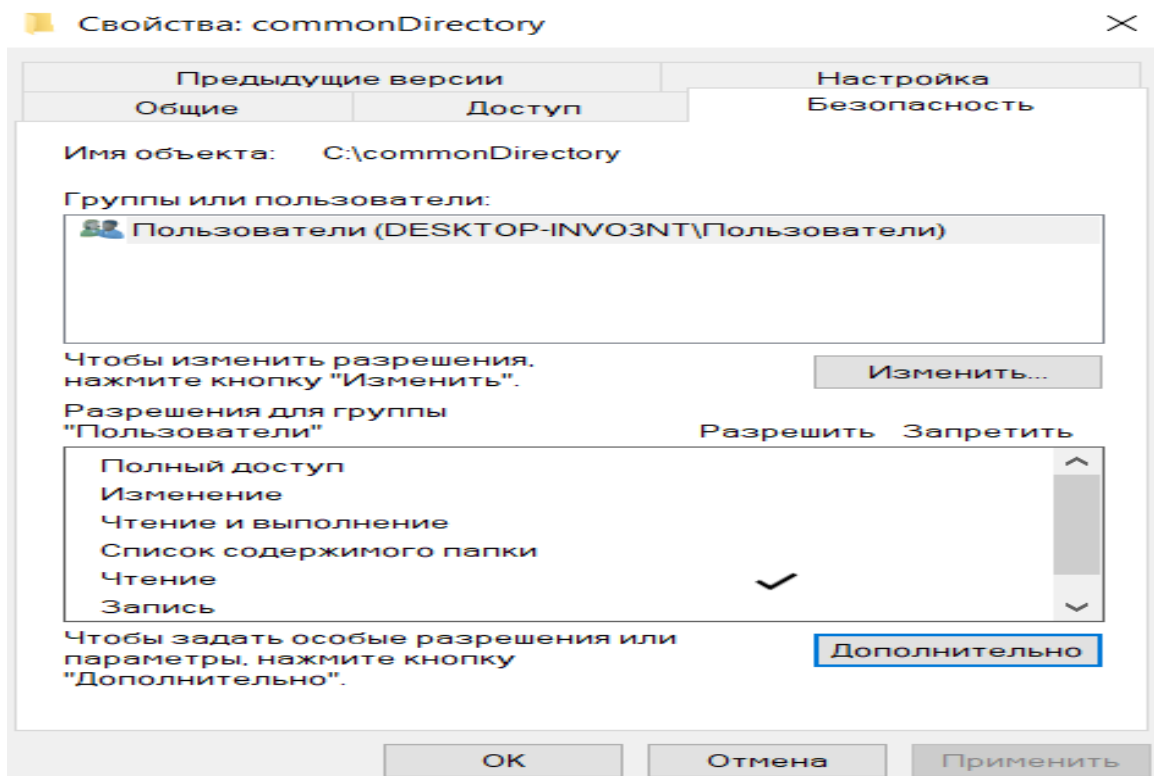
3) Создать директорию common Directory, в которой для пользователей lab1, lab2 создать свою собственную поддиректорию lab1dir, lab2dir.

Где и как: зайти в диск...



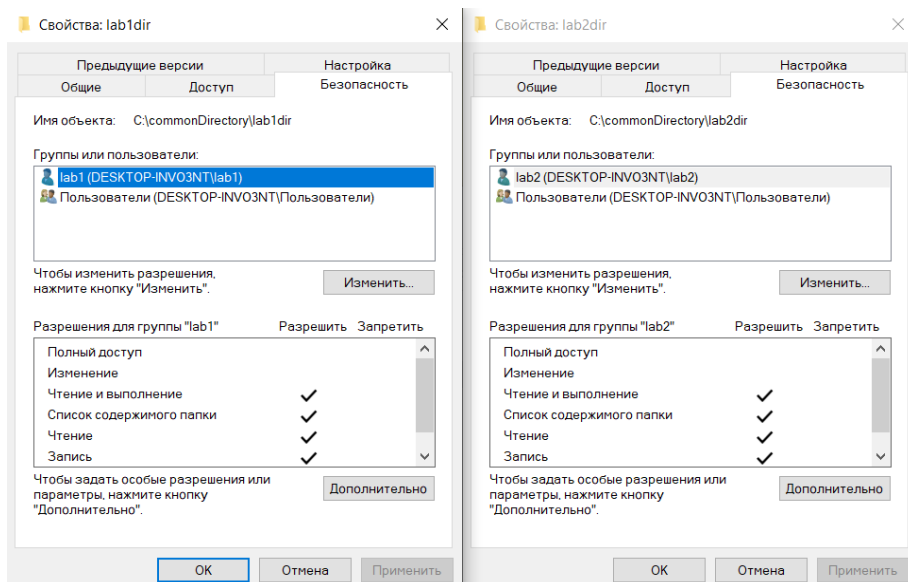
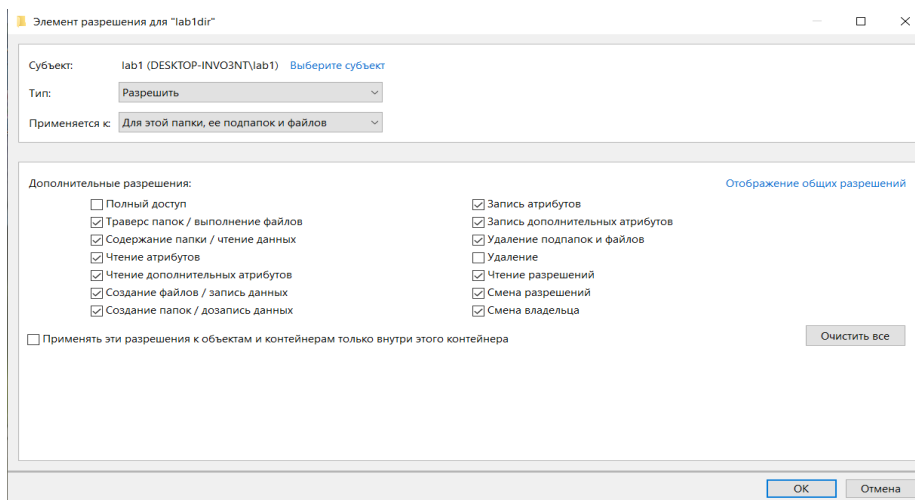
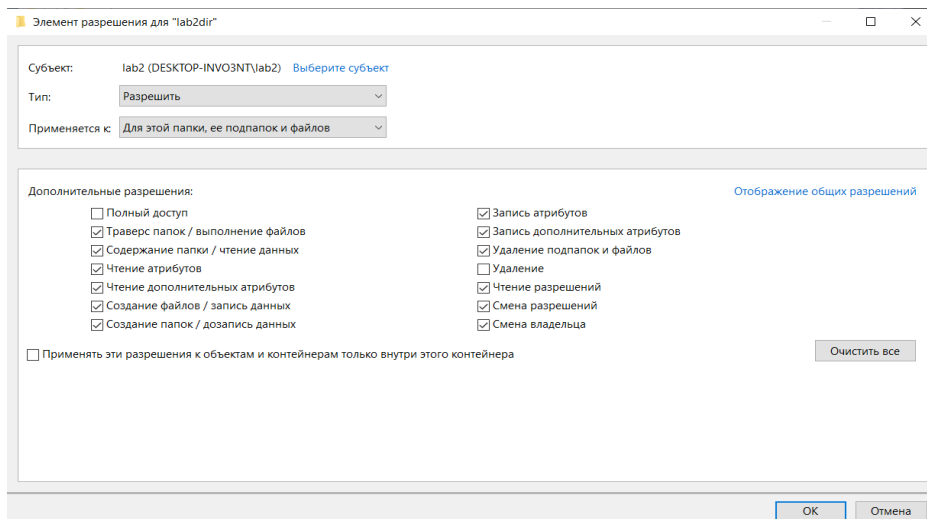
4) Установить права на директорию commonDirectory, все ее подпапки и файлы — все пользователи в ОС могут читать ее, но изменять содержимое не могут.

Где и как: в папке нажимаю ПКМ. Свойства.Безопасность.Дополнительно. Отключить наследование(если менять разрешения не получается). Настроить разрешение на чтение у Пользователей. Готово.



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.

Где и как: делаем те же шаги, что и в прошлом шаге. Только после дополнительно нажимаем добавить. И нажимаем на галочки там, где нужно. Нужно не забыть нажать кнопку применить, чтобы не очистилось.



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

Где и как:заходим под lab1 и lab2. Заходим в командную строку. Прodelываем следующее:

Командная строка

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

C:\>dir commonDirectory\lab1dir
Том в устройстве C не имеет метки.
Серийный номер тома: 0E60-58B6

Содержимое папки C:\commonDirectory\lab1dir

29.10.2022  16:51    <DIR>        .
29.10.2022  16:51    <DIR>        ..
                0 файлов             0 байт
                2 папок   191 814 389 760 байт свободно

C:\>type commonDirectory\lab1dir\3.txt
Не удается найти указанный файл.

C:\>type C:\commonDirectory\lab1dir\3.txt
Не удается найти указанный файл.

C:\>type C:\commonDirectory\lab1dir\3.txt
check
C:\>del C:\commonDirectory\lab1dir\3.txt
C:\commonDirectory\lab1dir\3.txt
Отказано в доступе.

C:\>echo e>C:\commonDirectory\lab1dir\24.txt
Отказано в доступе.
```

Командная строка

```
C:\Users\lab1>whoami
desktop-invo3nt\lab1

C:\Users\lab1>cd C:\commonDirectory\lab1dir

C:\commonDirectory\lab1dir>echo a>4.txt

C:\commonDirectory\lab1dir>type 4.txt
a

C:\commonDirectory\lab1dir>del 4.txt

C:\commonDirectory\lab1dir>../..
".." не является внутренней или внешней
командой, исполняемой программой или пакетным файлом.

C:\commonDirectory\lab1dir>cd ../../

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

C:\>dir commonDirectory\lab2dir
Том в устройстве C не имеет метки.
Серийный номер тома: 0E60-58B6

Содержимое папки C:\commonDirectory\lab2dir

07.11.2022  22:08    <DIR>        .
07.11.2022  22:08    <DIR>        ..
07.11.2022  22:08             7 5.txt
                1 файлов             7 байт
                2 папок   189 837 484 032 байт свободно

C:\>type C:\commonDirectory\lab2dir\5.txt
kcehc

C:\>del C:\commonDirectory\lab2dir\5.txt
C:\commonDirectory\lab2dir\5.txt
Отказано в доступе.

C:\>echo c>C:\commonDirectory\lab2dir\5.txt
Отказано в доступе.

C:\>
```

```
Командная строка
C:\Users\lab2>whoami
desktop-invo3nt\lab2

C:\Users\lab2>cd C:\commonDirectory\lab2dir

C:\commonDirectory\lab2dir>echo a>1.txt

C:\commonDirectory\lab2dir>type 1.txt
a

C:\commonDirectory\lab2dir>del 1.txt

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

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

C:\>dir commonDirectory\lab1dir
Том в устройстве C не имеет метки.
Серийный номер тома: 0E60-58B6

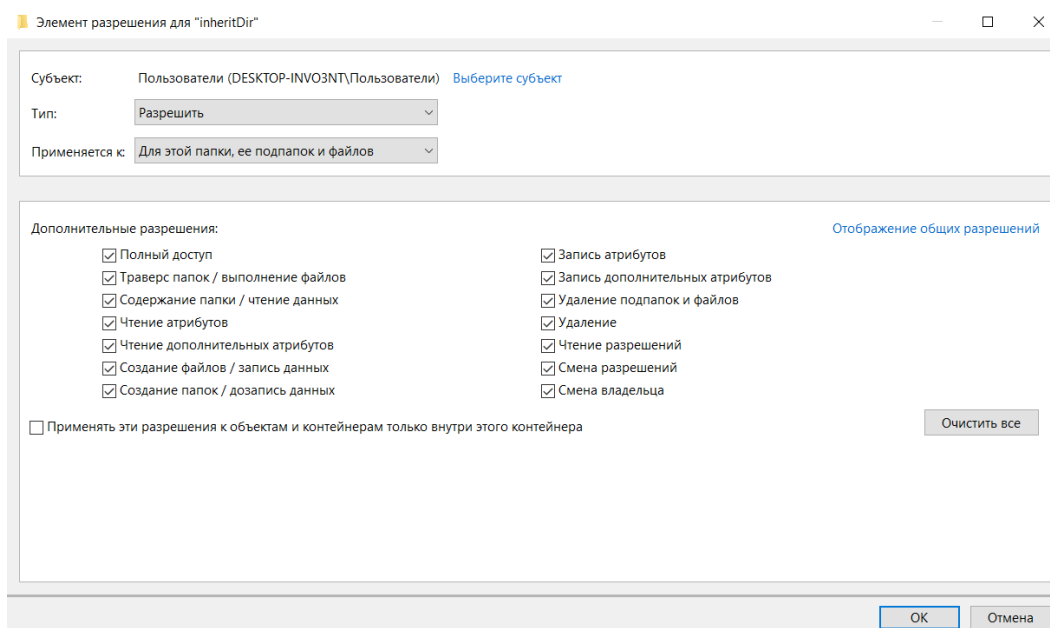
Содержимое папки C:\commonDirectory\lab1dir

29.10.2022  16:51    <DIR>        .
29.10.2022  16:51    <DIR>        ..
                0 файлов              0 байт
                2 папок   191 814 389 760 байт свободно
```

2. Управление наследованием прав доступа файлов и каталогов.

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

Где и как: делаем как в одном из прошлых шагов.



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.

Где и как: делаем аналогично: только вместо разрешения ставим запрет.

Дополнительные параметры безопасности для "inheritDir"

Имя: C:\inheritDir

Владелец: Doomer (DESKTOP-INV03NT\Doomer) [Изменить](#)

Разрешения Аудит Действующие права доступа

Для получения дополнительных сведений дважды щелкните запись разрешения. Чтобы изменить запись разрешения, выделите ее и нажмите кнопку "Изменить" (если она доступна).

Элементы разрешений:

Тип	Субъект	Доступ	Унаследовано от	Применяется к
Запре...	lab2 (DESKTOP-INV03NT\lab2)	Особые	Нет	Для этой папки, ее подпапок и ...
Разре...	Пользователи (DESKTOP-INV03...)	Полный доступ	Нет	Для этой папки, ее подпапок и ...

[Добавить](#) [Удалить](#) [Изменить](#)

[Включение наследования](#)

☐ Заменить все записи разрешений дочернего объекта наследуемыми от этого объекта

[OK](#) [Отмена](#) [Применить](#)

Элемент разрешения для "inheritDir"

Субъект: lab2 (DESKTOP-INV03NT\lab2) [Выберите субъект](#)

Тип: [Запретить](#)

Применяется к: [Только для файлов](#)

Дополнительные разрешения:

☐ Полный доступ
☐ Траверс папок / выполнение файлов
☐ Содержание папки / чтение данных
☐ Чтение атрибутов
☐ Чтение дополнительных атрибутов
☒ Создание файлов / запись данных
☒ Создание папок / дозапись данных

☐ Запись атрибутов
☐ Запись дополнительных атрибутов
☐ Удаление подпапок и файлов
☐ Удаление
☐ Чтение разрешений
☐ Смена разрешений
☐ Смена владельца

[Отображение общих разрешений](#)

☒ Применять эти разрешения к объектам и контейнерам только внутри этого контейнера

[Очистить все](#)

[OK](#) [Отмена](#)

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.

Командная строка

```
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\lab1>cd C:\inheritDir

C:\inheritDir>whoami
desktop-invo3nt\lab1

C:\inheritDir>echo a>text1.txt

C:\inheritDir>mkdir folder

C:\inheritDir>cd folder

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

C:\inheritDir\folder>
```

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

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

Где и как: проделываем команды в командной строке(4 и 5 один скрин).

Пояснение за пару команд: echo не сработала с первого раза, так как в 2.2 я не поставил запрет “только для файлов”. Из-за чего мне было отказано в доступе. Исправил.

Командная строка

```
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\lab2>cd C:\inheritDir

C:\inheritDir>whoami
desktop-invo3nt\lab2

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

C:\inheritDir>mkdir lab2subdir
Отказано в доступе.

C:\inheritDir>cd folder

C:\inheritDir\folder>echo c>text2.txt
Отказано в доступе.

C:\inheritDir\folder>whoami
desktop-invo3nt\lab2

C:\inheritDir\folder>echo cuew>text2.txt
Отказано в доступе.

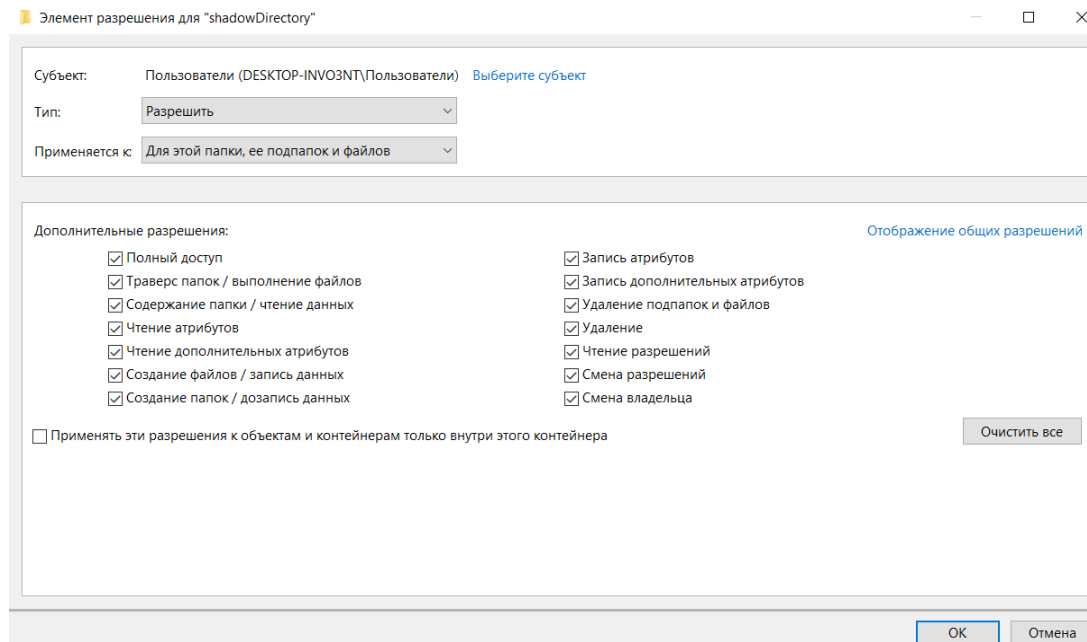
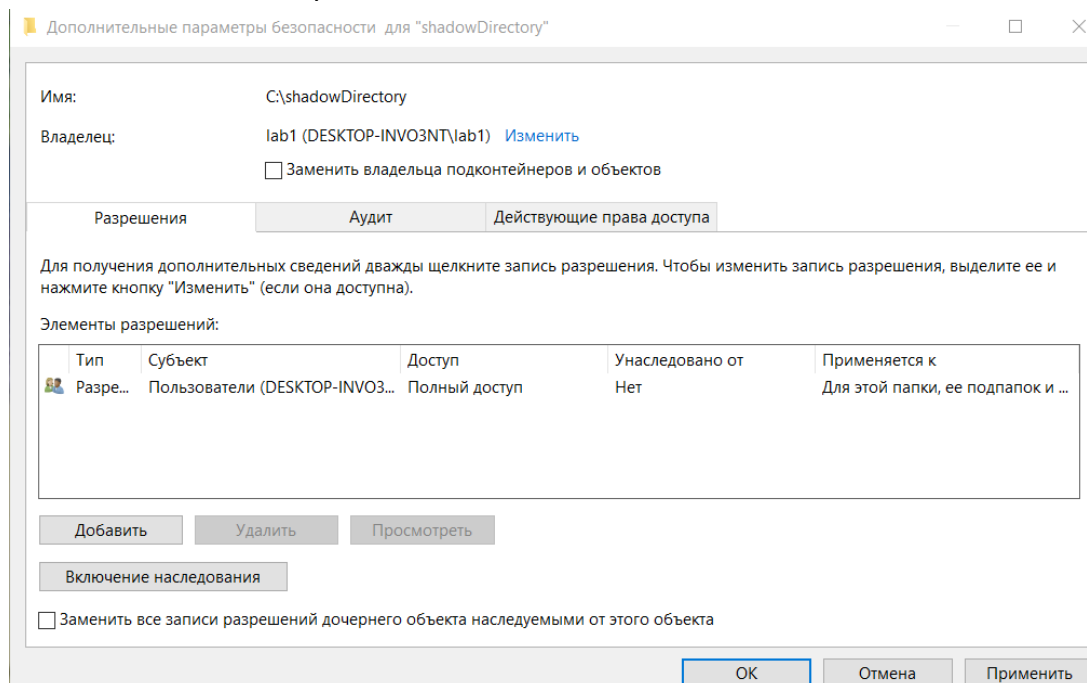
C:\inheritDir\folder>echo cuew>text2.txt

C:\inheritDir\folder>type text2.txt
cuew
```

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.

Где и как: полный контроль для пользователей. Владельца меняем на lab1.



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

Где и как: ничего сложного нет (только права владельца надо капсом писать).

Элемент разрешения для "shadowDirectory"

Субъект: ПРАВА ВЛАДЕЛЬЦА [Выберите субъект](#)

Тип: Разрешить

Применяется к: Для этой папки, ее подпапок и файлов

Дополнительные разрешения:

<input checked="" type="checkbox"/> Полный доступ	<input checked="" type="checkbox"/> Запись атрибутов
<input checked="" type="checkbox"/> Траверс папок / выполнение файлов	<input checked="" type="checkbox"/> Запись дополнительных атрибутов
<input checked="" type="checkbox"/> Содержание папки / чтение данных	<input checked="" type="checkbox"/> Удаление подпапок и файлов
<input checked="" type="checkbox"/> Чтение атрибутов	<input checked="" type="checkbox"/> Удаление
<input checked="" type="checkbox"/> Чтение дополнительных атрибутов	<input checked="" type="checkbox"/> Чтение разрешений
<input checked="" type="checkbox"/> Создание файлов / запись данных	<input checked="" type="checkbox"/> Смена разрешений
<input checked="" type="checkbox"/> Создание папок / дозапись данных	<input checked="" type="checkbox"/> Смена владельца

☐ Применять эти разрешения к объектам и контейнерам только внутри этого контейнера

[Отображение общих разрешений](#)

[Очистить все](#)

[OK](#) [Отмена](#)

Элемент разрешения для "shadowDirectory"

Субъект: Пользователи (DESKTOP-INV03NT\Пользователи) [Выберите субъект](#)

Тип: Разрешить

Применяется к: Для этой папки, ее подпапок и файлов

Дополнительные разрешения:

<input type="checkbox"/> Полный доступ	<input checked="" type="checkbox"/> Запись атрибутов
<input checked="" type="checkbox"/> Траверс папок / выполнение файлов	<input checked="" type="checkbox"/> Запись дополнительных атрибутов
<input checked="" type="checkbox"/> Содержание папки / чтение данных	<input type="checkbox"/> Удаление подпапок и файлов
<input checked="" type="checkbox"/> Чтение атрибутов	<input type="checkbox"/> Удаление
<input checked="" type="checkbox"/> Чтение дополнительных атрибутов	<input checked="" type="checkbox"/> Чтение разрешений
<input checked="" type="checkbox"/> Создание файлов / запись данных	<input checked="" type="checkbox"/> Смена разрешений
<input checked="" type="checkbox"/> Создание папок / дозапись данных	<input checked="" type="checkbox"/> Смена владельца

☐ Применять эти разрешения к объектам и контейнерам только внутри этого контейнера

[Отображение общих разрешений](#)

[Очистить все](#)

[OK](#) [Отмена](#)

Дополнительные параметры безопасности для "shadowDirectory"

Имя: C:\shadowDirectory

Владелец: lab1 (DESKTOP-INV03NT\lab1) [Изменить](#)

Разрешения **Аудит** Действующие права доступа

Для получения дополнительных сведений дважды щелкните запись разрешения. Чтобы изменить запись разрешения, выделите ее и нажмите кнопку "Изменить" (если она доступна).

Элементы разрешений:

Тип	Субъект	Доступ	Унаследовано от	Применяется к
Разре...	Пользователи (DESKTOP-INV03NT\Пользователи)	Особые	Нет	Для этой папки, ее подпапок и ...
Разре...	ПРАВА ВЛАДЕЛЬЦА	Полный доступ	Нет	Для этой папки, ее подпапок и ...

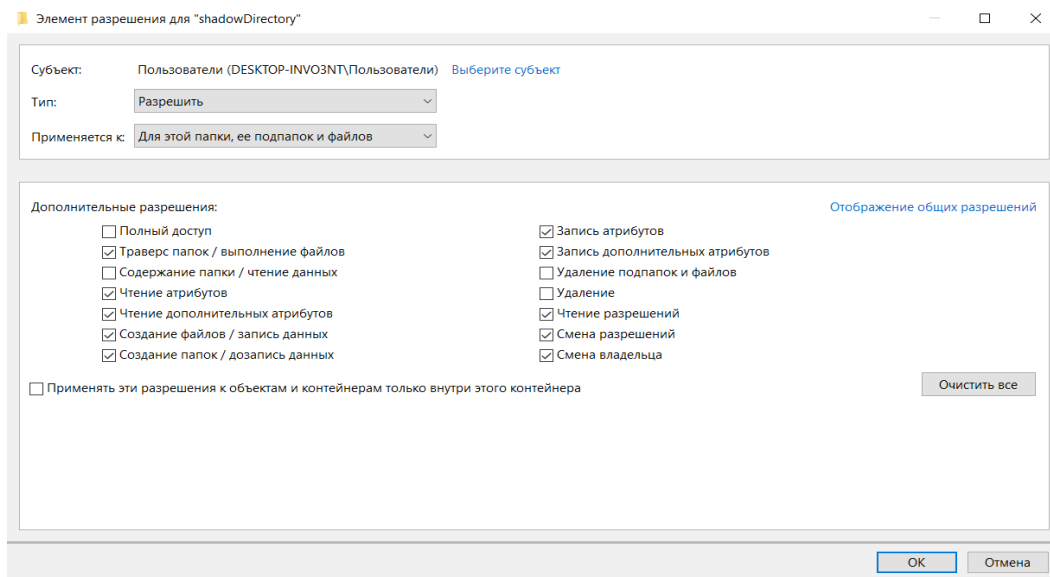
[Добавить](#) [Удалить](#) [Изменить](#)

[Включение наследования](#)

☐ Заменить все записи разрешений дочернего объекта наследуемыми от этого объекта

[OK](#) [Отмена](#) [Применить](#)

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



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

```

Командная строка
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\lab2>cd C:\shadowDirectory

C:\shadowDirectory>whoami
desktop-invo3nt\lab2

C:\shadowDirectory>echo acd>1234.txt

C:\shadowDirectory>dir
Том в устройстве C не имеет метки.
Серийный номер тома: 0E60-58B6

Содержимое папки C:\shadowDirectory

Файл не найден

C:\shadowDirectory>type 1234.txt
Отказано в доступе.

C:\shadowDirectory>del 1234.txt
Не удастся найти C:\shadowDirectory\1234.txt

C:\shadowDirectory>

```

```

Командная строка
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\lab1>whoami
desktop-invo3nt\lab1

C:\Users\lab1>cd C:\shadowDirectory

C:\shadowDirectory>echo abcdefg>123.txt

C:\shadowDirectory>dir
Том в устройстве C не имеет метки.
Серийный номер тома: 0E60-58B6

Содержимое папки C:\shadowDirectory

08.11.2022  16:17    <DIR>        .
08.11.2022  16:17    <DIR>        ..
08.11.2022  16:17                9 123.txt
08.11.2022  16:15                5 1234.txt
                2 файлов              14 байт
                2 папок   192 749 633 536 байт свободно

C:\shadowDirectory>type 123.txt
abcdefg

C:\shadowDirectory>del 123.txt

C:\shadowDirectory>type 123.txt
Не удастся найти указанный файл.

```


4. Использование привилегий.


1) Создать нового обычного пользователя lab3.


Где и как: шаг 1.2.


Семья и другие пользователи

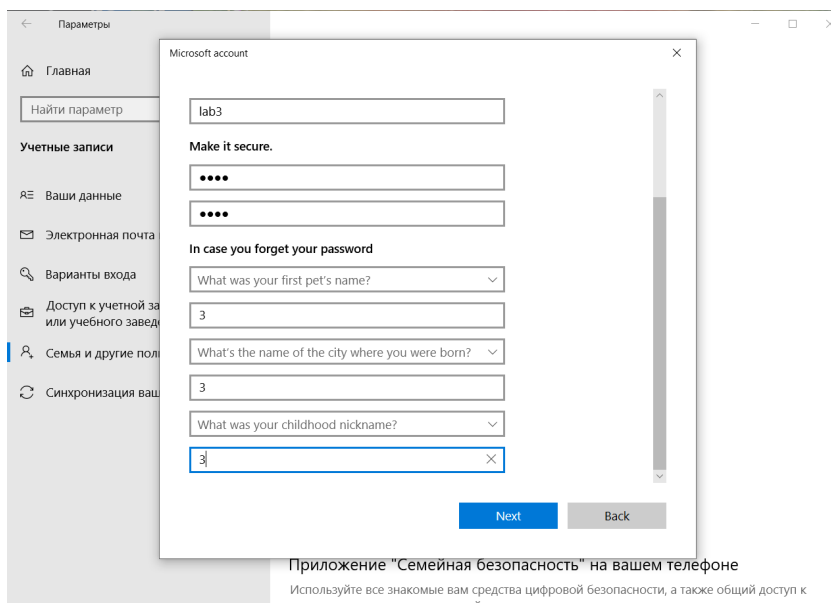
Разрешите пользователям, не включенным в семью, входить в систему с помощью их учетных записей. Это не будет означать их добавление в семью.

 Добавить пользователя для этого компьютера

 lab1
Локальная учетная запись

 lab2
Локальная учетная запись

 lab3
Локальная учетная запись



Панель задач: Главная, Найти параметр, Учетные записи, Ваши данные, Электронная почта, Варианты входа, Доступ к учетной записи или учебного заведения, Семья и другие пользователи, Синхронизация ваших устройств.

Microsoft account

lab3

Make it secure.

••••

••••

In case you forget your password

What was your first pet's name? ▾

3

What's the name of the city where you were born? ▾

3

What was your childhood nickname? ▾

3

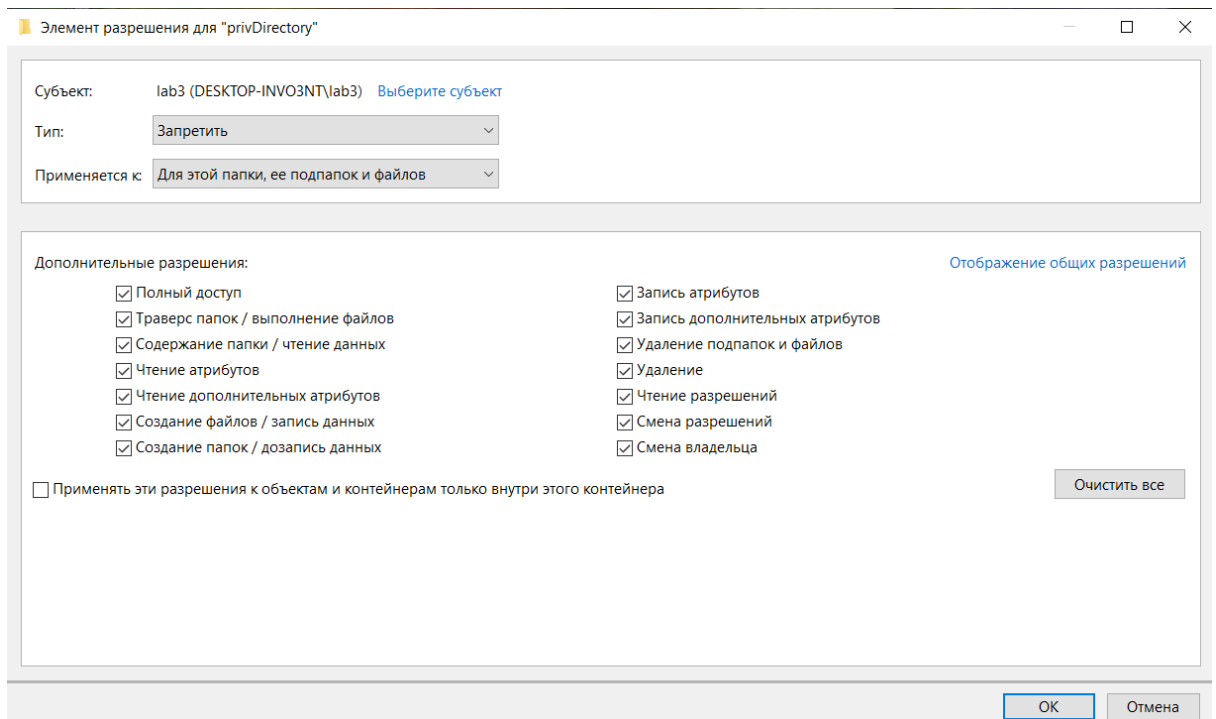
Next Back

Приложение "Семейная безопасность" на вашем телефоне

Используйте все знакомые вам средства цифровой безопасности, а также общий доступ к файлам и местонахождению всей семьи

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

Где и как: создаем через командную строку. И настраиваем запреты. Делаем как по прошлым шагам.



Командная строка

```
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\ПК>mkdir privDirectory

C:\Users\ПК>cd C:
C:\Users\ПК

C:\Users\ПК>cd C:\

C:\>mkdir privDirectory

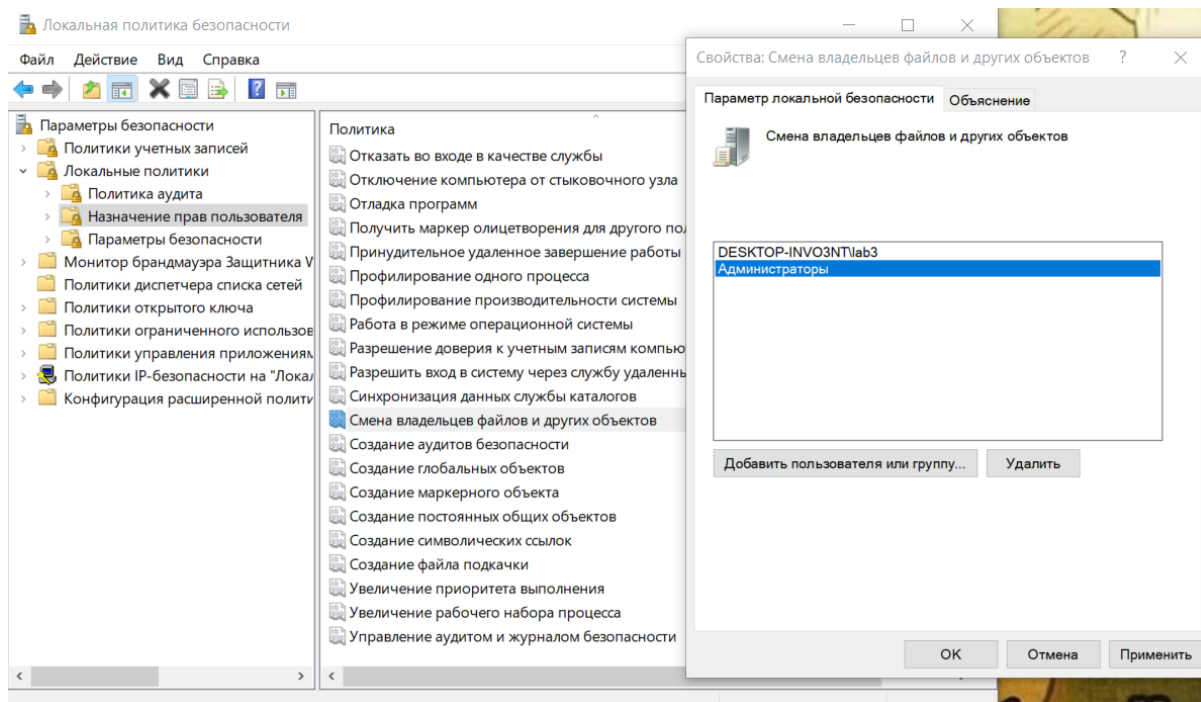
C:\>cd privDirectory

C:\privDirectory>echo sdek>lab3file.txt

C:\privDirectory>_
```

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

Где и как: в поиске пишем: средства администрирования windows. Локальная политика безопасности. Локальные политики. Назначение прав пользователя. Смена владельцев файлов и других объектов. Пишем: lab3.



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

Командная строка

```
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

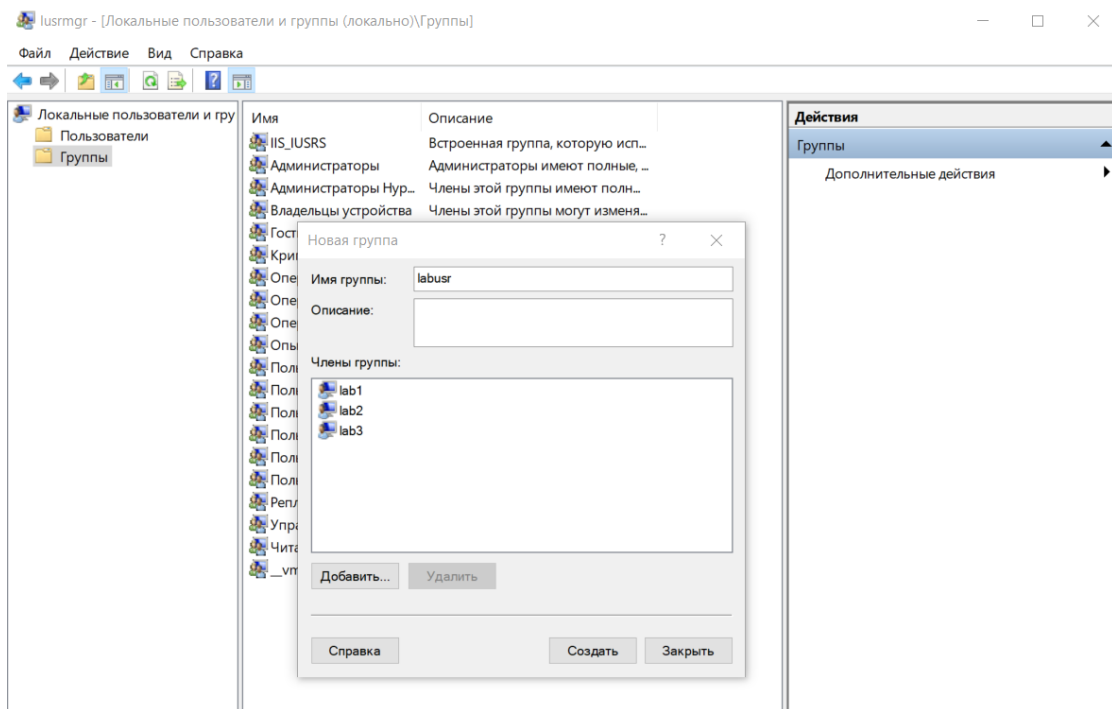
C:\Users\lab3>whoami
desktop-invo3nt\lab3

C:\Users\lab3>takeown /F "C:\privDirectory\lab3file.txt"
ОШИБКА: Отказано в доступе.

C:\Users\lab3>
```

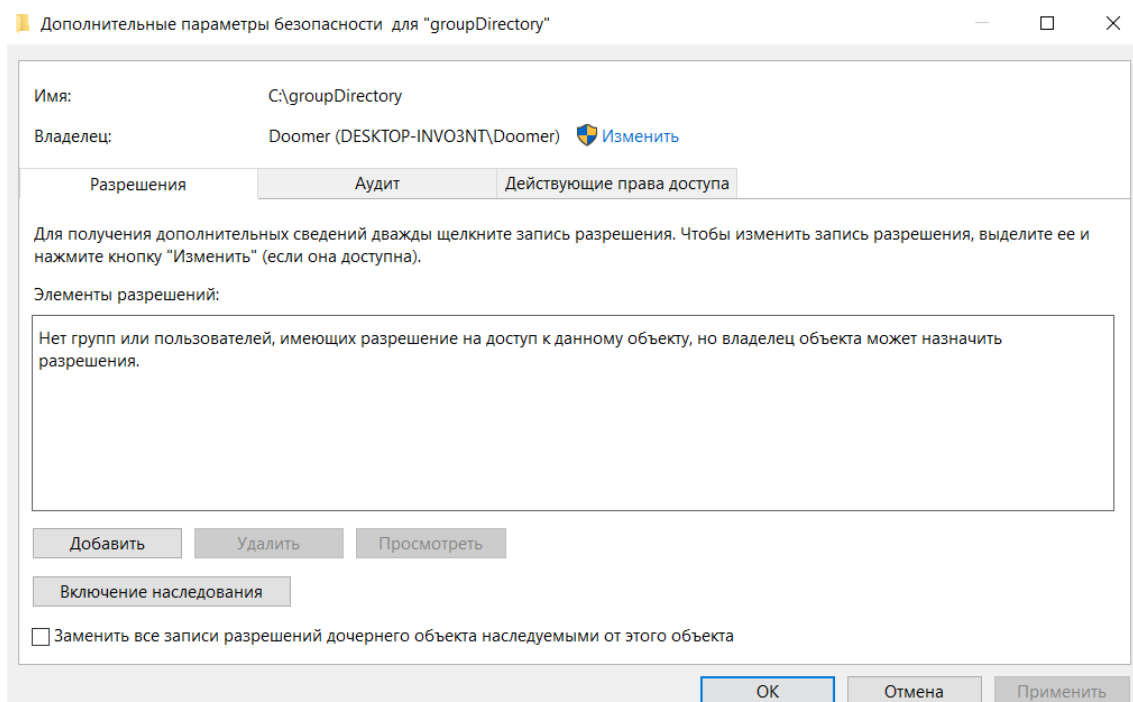
5. Изменение прав доступа к файлам и каталогам для групп пользователей.
 - 1) Создать группу пользователей labusr, добавить в нее пользователей lab1, lab2, lab3.

Где и как: нажимаем Win + R. Вводим lusrmgr.msc. Группы. В действия ждем дополнительные действия. Создать группу. Дальше называем как нам нужно.



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

Где и как: в той директории можно отменить наследие, что приведет к удалению разрешений. Объяснение: список разрешений пуст. Никакой пользователь или группа сможет получить доступ к директории. Но владелец может изменить список разрешений. (вообще при применении пустых разрешений вылезает окно, которое отвечает на вопрос, но мне лень делать скрин)



Командная строка

```
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\lab1>whoami
desktop-invo3nt\lab1

C:\Users\lab1>dir C:\groupDirectory
Том в устройстве C не имеет метки.
Серийный номер тома: 0E60-58B6

Содержимое папки C:\groupDirectory

Файл не найден

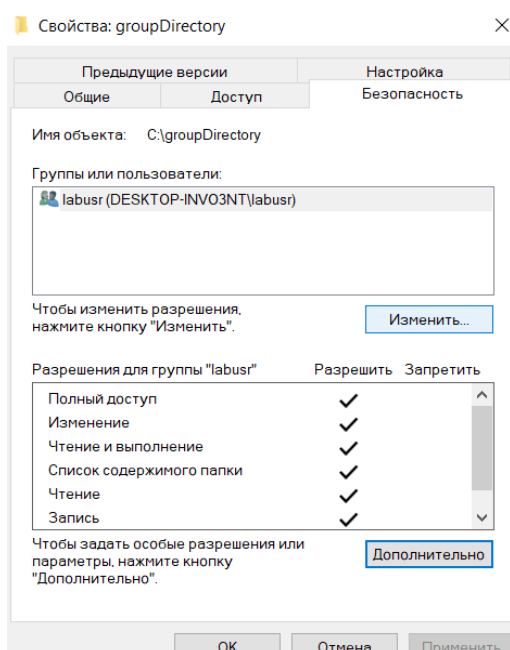
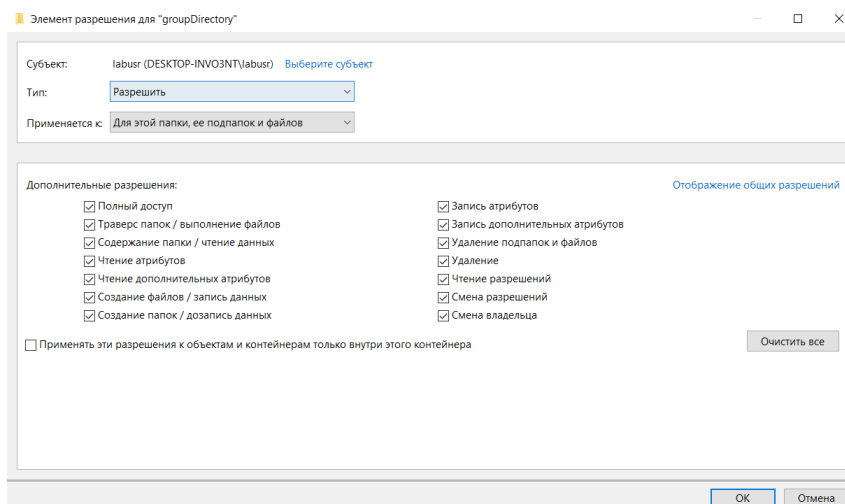
C:\Users\lab1>cd groupDirectory
Системе не удастся найти указанный путь.

C:\Users\lab1>cd C:\groupDirectory
Отказано в доступе.

C:\Users\lab1>_
```

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.

Объяснение: удалось создать файл в директории от имени пользователя lab1, потому что он является частью группы labusr, у которой есть права.



Командная строка

```
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\lab1>whoami
desktop-into3nt\lab1

C:\Users\lab1>cd C:\groupDirectory

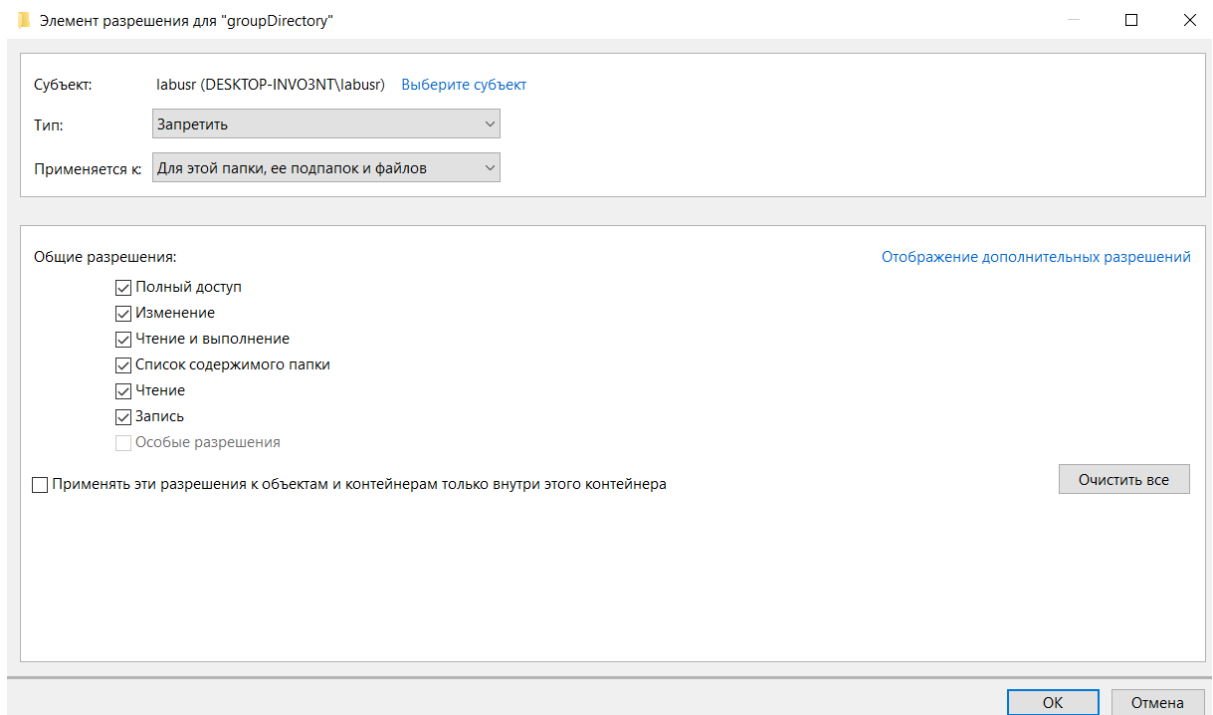
C:\groupDirectory>echo wer>textfile.txt

C:\groupDirectory>type textfile.txt
wer

C:\groupDirectory>
```

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.

Объяснение: Не удалось прочитать содержимое файла textfile.txt от имени пользователя lab1, так как запрещающие записи в списке разрешений имеют приоритет над разрешающими записями.(окошки с подсказками тоже отвечают на вопрос)



```
Командная строка
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\lab1>whoami
desktop-invo3nt\lab1

C:\Users\lab1>cd C:\groupDirectory
Отказано в доступе.

C:\Users\lab1>type C:\groupDirectory\textfile.txt
Отказано в доступе.

C:\Users\lab1>
```

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.

Объяснение: попытка чтения файла textfile.txt от пользователя lab1 оказалась неудачной. Причина все та же — запрещающие записи в списке разрешений имеют приоритет над разрешающими записями.

Элемент разрешения для "groupDirectory"

Субъект: lab1 (DESKTOP-INVO3NT\lab1) [Выберите субъект](#)

Тип: Разрешить

Применяется к: Для этой папки, ее подпапок и файлов

Дополнительные разрешения:

<input checked="" type="checkbox"/> Полный доступ	<input checked="" type="checkbox"/> Запись атрибутов
<input checked="" type="checkbox"/> Траверс папок / выполнение файлов	<input checked="" type="checkbox"/> Запись дополнительных атрибутов
<input checked="" type="checkbox"/> Содержание папки / чтение данных	<input checked="" type="checkbox"/> Удаление подпапок и файлов
<input checked="" type="checkbox"/> Чтение атрибутов	<input checked="" type="checkbox"/> Удаление
<input checked="" type="checkbox"/> Чтение дополнительных атрибутов	<input checked="" type="checkbox"/> Чтение разрешений
<input checked="" type="checkbox"/> Создание файлов / запись данных	<input checked="" type="checkbox"/> Смена разрешений
<input checked="" type="checkbox"/> Создание папок / дозапись данных	<input checked="" type="checkbox"/> Смена владельца

☐ Применять эти разрешения к объектам и контейнерам только внутри этого контейнера

[Отображение общих разрешений](#)

[Очистить все](#)

OK Отмена

Командная строка

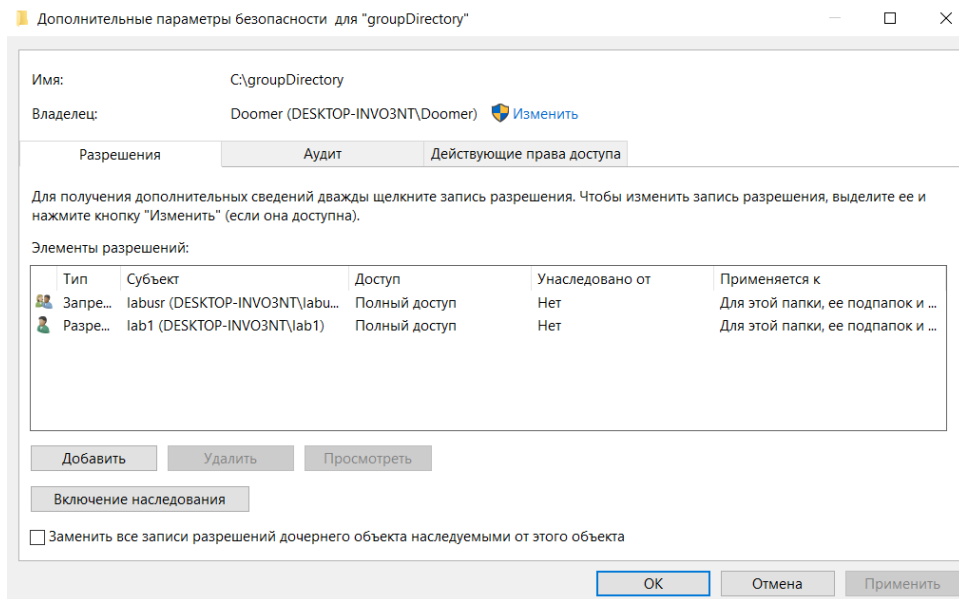
```
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\lab1>whoami
desktop-invo3nt\lab1

C:\Users\lab1>cd C:\groupDirectory
Отказано в доступе.

C:\Users\lab1>type C:\groupDirectory\textfile.txt
Отказано в доступе.

C:\Users\lab1>
```



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.

```
Командная строка
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\ПК>whoami /USER /PRIV /GROUPS

Сведения о пользователе
-----
Пользователь          SID
-----
desktop-ino3nt\doomer S-1-5-21-1932882788-122678965-1832900799-1001

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                         Псевдоним     S-1-5-32-559  Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Прошедшие проверку          Хорошо известная группа S-1-2-1       Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Данная организация         Хорошо известная группа S-1-5-11      Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Локальная учетная запись   Хорошо известная группа S-1-5-15      Обязательная группа, Включены по умолчанию, Включенная группа
ЛОКАЛЬНЫЕ                              Хорошо известная группа S-1-5-113     Обязательная группа, Включены по умолчанию, Включенная группа
NT AUTHORITY\Проверка подлинности NTLM    Хорошо известная группа S-1-2-0       Обязательная группа, Включены по умолчанию, Включенная группа
Обязательная метка\Средний обязательный уровень Метка         S-1-5-64-10   Обязательная группа, Включены по умолчанию, Включенная группа
S-1-16-8192

Сведения о привилегиях
-----
Имя привилегии          Описание          Область, край
-----
SeLockMemoryPrivilege   Блокировка страниц в памяти      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
```

```
Командная строка
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\lab3>whoami /USER /PRIV /GROUP
ОШИБКА: Неправильный параметр или аргумент - '/GROUP'.
Введите "ИМЯ\ИИ /?" для получения справки по использованию.

C:\Users\lab3>whoami /USER /PRIV /GROUPS

Сведения о пользователе
-----
Пользователь          SID
-----
desktop-invo3nt\lab3  S-1-5-21-1932882788-122678965-1832900799-1009

Сведения о группах
-----
Группа                                     Тип          SID                                     Атрибуты
-----
Все                                         Хорошо известная группа S-1-1-0      Обязательная группа, Включены по умолчанию, Включенная группа
DESKTOP-INVO3NT\lab3usr                    Псевдоним     S-1-5-21-1932882788-122678965-1832900799-1010 Обязательная группа, Включены по умолчанию, Включенная группа
BUILTIN\Пользователи                      Псевдоним     S-1-5-32-545  Обязательная группа, Включены по умолчанию, Включенная группа
BUILTIN\Пользователи журналов производительности Псевдоним     S-1-5-32-559  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   Обязательная группа, Включены по умолчанию, Включенная группа

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:

```
Administrator: Командная строка
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\WINDOWS\system32\whoami /USER /PRIV /GROUPS

Сведения о пользователе
-----

Пользователь          SID
-----
desktop-into3nt\doomer S-1-5-21-1932882788-122678965-1832900799-1001

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
BUILTIN\Пользователи журналов производительности Псевдоним     S-1-5-32-559  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
```

```
Сведения о привилегиях
-----

Имя привилегии                                     Описание                                     Область, край
-----
SeLockMemoryPrivilege                             Блокировка страниц в памяти                 Отключен
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 включен
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
```

lab3:

```
Administrator: Командная строка

Группа                                     Тип          SID          Атрибуты
-----
Все                                       Хорошо известная группа S-1-1-0      Обязательная группа, Включены по умолчанию, Включенная группа
DESKTOP-IM03NT\LocalBusr                Псевдоним     S-1-5-21-1932882788-122678965-1832900799-1010 Обязательная группа, Включены по умолчанию, Включенная группа
BUILTIN\Пользователи                    Псевдоним     S-1-5-32-545  Обязательная группа, Включены по умолчанию, Включенная группа
BUILTIN\Пользователи журналов производительности Псевдоним     S-1-5-32-559  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

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
```

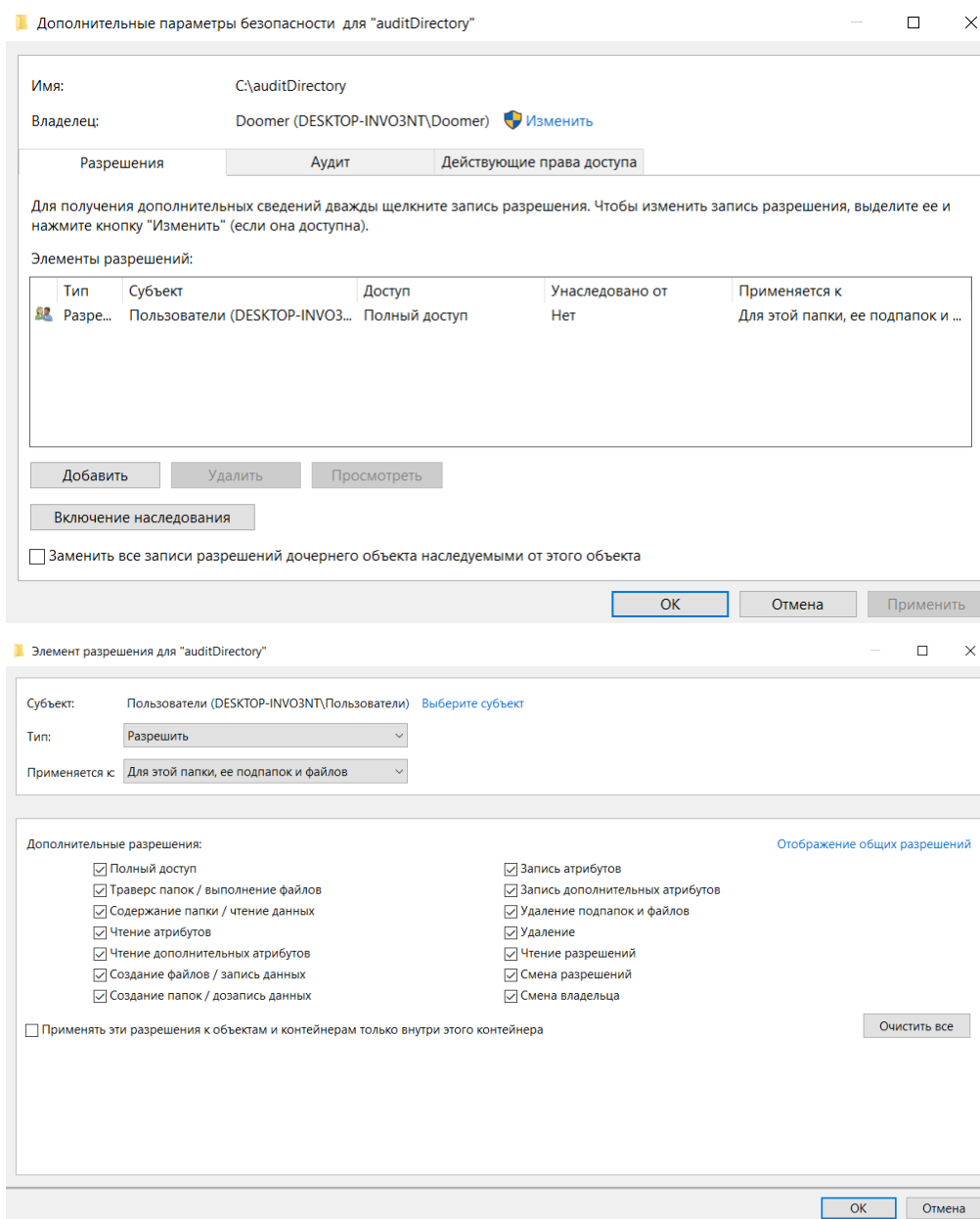
3) Описать различия в полученных списках групп и привилегий. Обратить внимание на атрибуты группы Администраторы.

Ответ:

- для обоих пользователей меняется группа: **Обязательная метка\ Средний обязательный уровень** на **Обязательная метка\ Высокий обязательный уровень**.
- для пользователя doomer меняются атрибуты групп: **BUILTIN\Администраторы** и **NT AUTHORITY\Локальная учетная запись и член группы Администраторы** с **Группа, используемая только для запрета** на **Обязательная группа, Включены по умолчанию, Включенная группа**.
- для пользователя doomer добавляются enabled привилегии: **SeImpersonatePrivilege** и **SeCreateGlobalPrivilege**.
- у lab3 отобразилось больше привилегий.

7. Работа с аудитом доступа к файлу.

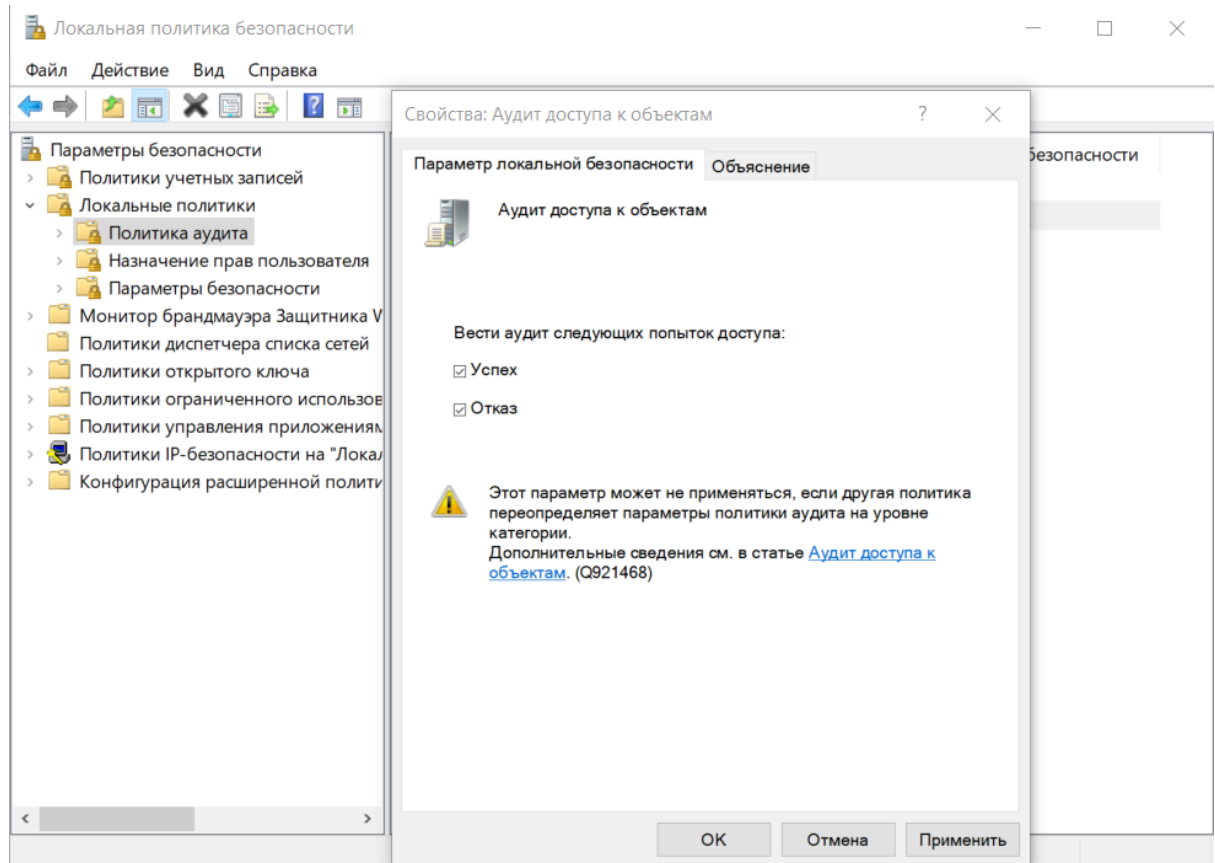
1) Создать директорию auditDirectory и разрешить к ней, ее подпапкам и файлам полный доступ всех пользователей.



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

Где и как: в локальной политике безопасности нажимаем в локальные политики на политику аудита. Ищем аудит доступа к объектам.

Далее идем в auditDirectory и заходим в параметры безопасности. Жмем во вкладку аудит. Запускаем и добавляем субъект.



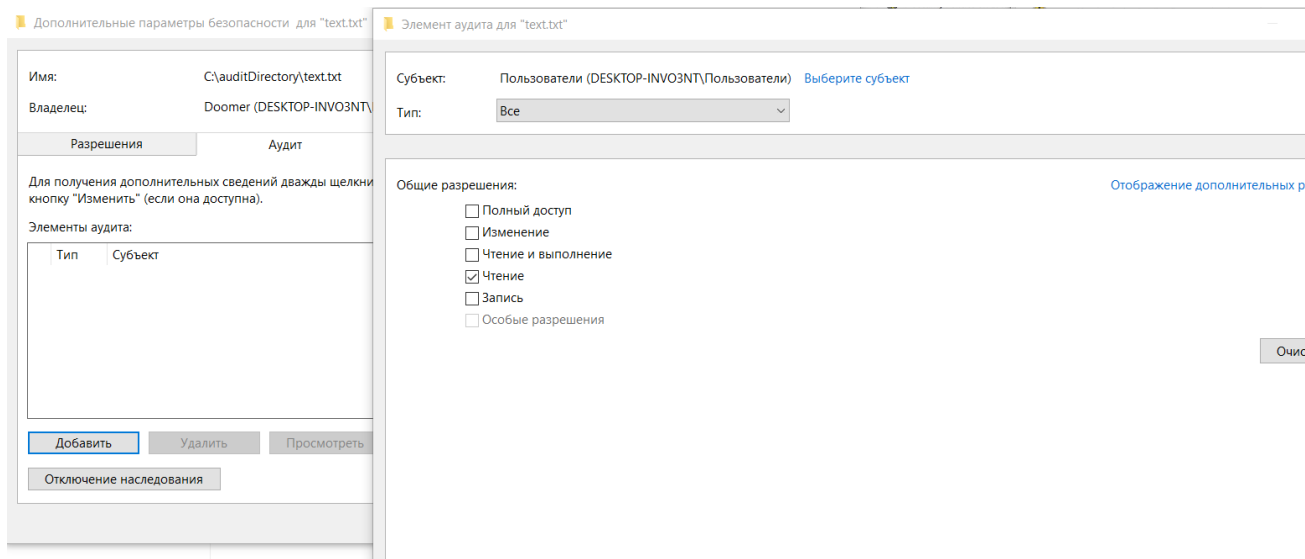
Командная строка

```
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\ПК>cd C:\auditDirectory

C:\auditDirectory>echo qwerty>text.txt

C:\auditDirectory>
```



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

```
Командная строка
Microsoft Windows [Version 10.0.19044.2130]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\lab1>whoami
desktop-invo3nt\lab1

C:\Users\lab1>cd C:\auditDirectory
Системе не удается найти указанный путь.

C:\Users\lab1>cd C:/auditDirectory

C:\auditDirectory>type text.txt
qwerty

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.

Управление компьютером

Файл Действие Вид Справка

Управление компьютером (исл...)

- Служебные программы
 - Планировщик заданий
 - Просмотр событий
 - Настраиваемые пр...
 - Журналы Windows
 - Приложение
 - Безопасность
 - Установка
 - Система
 - Перенаправлен...
 - Журналы приложе...
 - Подписки
- Общие папки
- Локальные пользоате...
- Производительность
- Диспетчер устройств
- Запоминающие устройс...
- Управление дисками
- Службы и приложения

Ключевые сл...	Дата и время	Источник	Код события	Категория зад...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит успеха	13.11.2022 15:53:52	Microsoft Win...	5156	Filtering Platfo...
Аудит успеха	13.11.2022 15:53:52	Microsoft Win...	5158	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...
Аудит отказа	13.11.2022 15:53:52	Microsoft Win...	5152	Filtering Platfo...

Событие 5152, Microsoft Windows security auditing.

Общие

Подробности

Платформа фильтрации Windows заблокировала пакет.

Сведения о приложении:

Имя журнала: Безопасность

Источник: Microsoft Windows security ; Дата: 13.11.2022 15:53:52

Код: 5152 Категория задачи: Filtering Platform Packet Drop

Уровень: Сведения Ключевые слова: Аудит отказа

Пользов.: Н/Д Компьютер: DESKTOP-INFO3NT

Код операции: Сведения

Подробности: [Справка в Интернете для](#)

Активация Windows
Чтобы активировать Windows, п...

Ключевые сл...	Дата и время	Источник	Код события	Категория задачи
Аудит отказа	13.11.2022 15:33:57	Microsoft Windows...	4656	Kernel Object
Аудит отказа	13.11.2022 15:33:57	Microsoft Windows...	4656	Kernel Object
Аудит успеха	13.11.2022 15:33:56	Microsoft Windows...	5158	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:56	Microsoft Windows...	5158	Filtering Platform Connection
Аудит отказа	13.11.2022 15:33:56	Microsoft Windows...	4656	Kernel Object
Аудит отказа	13.11.2022 15:33:56	Microsoft Windows...	4656	Kernel Object
Аудит успеха	13.11.2022 15:33:55	Microsoft Windows...	5158	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:55	Microsoft Windows...	5158	Filtering Platform Connection
Аудит отказа	13.11.2022 15:33:55	Microsoft Windows...	4656	Kernel Object
Аудит отказа	13.11.2022 15:33:55	Microsoft Windows...	4656	Kernel Object
Аудит отказа	13.11.2022 15:33:54	Microsoft Windows...	5152	Filtering Platform Packet Drop
Аудит отказа	13.11.2022 15:33:54	Microsoft Windows...	5152	Filtering Platform Packet Drop
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	5158	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	5158	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	5156	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	5158	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	5158	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	4658	File System
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	4663	File System

Событие 4663, Microsoft Windows security auditing.

Общие

Подробности

☒ Понятное представление

☐ Режим XML

ObjectType

File

ObjectName

C:\auditDirectory\text.txt

HandleId

0x134

AccessList

%*4416

AccessMask

0x1

ProcessId

0x427c

ProcessName

C:\Windows\System32\cmd.exe

ResourceAttributes

S:AI

Активация Windows
Чтобы активировать Windo

Ключевые сл...	Дата и время	Источник	Код события	Категория задачи
Аудит отказа	13.11.2022 15:33:54	Microsoft Windows...	5152	Filtering Platform Packet Drop
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	5158	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	5158	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	5156	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	5158	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	5158	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	4658	File System
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	4663	File System
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	4656	File System
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	4658	File System
Аудит успеха	13.11.2022 15:33:54	Microsoft Windows...	4690	Handle Manipulation
Аудит отказа	13.11.2022 15:33:54	Microsoft Windows...	4656	Kernel Object
Аудит отказа	13.11.2022 15:33:54	Microsoft Windows...	4656	Kernel Object
Аудит успеха	13.11.2022 15:33:53	Microsoft Windows...	5156	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:53	Microsoft Windows...	5158	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:53	Microsoft Windows...	5156	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:53	Microsoft Windows...	5158	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:53	Microsoft Windows...	5158	Filtering Platform Connection
Аудит успеха	13.11.2022 15:33:52	Microsoft Windows...	5156	Filtering Platform Connection

Событие 4656, Microsoft Windows security auditing.

Общие

Подробности

☒ Понятное представление

☐ Режим XML

ObjectType

File

ObjectName

C:\auditDirectory\text.txt

HandleId

0x134

TransactionId

{00000000-0000-0000-0000-000000000000}

AccessList

%*1538 %*1541 %*4416 %*4419 %*4423

AccessReason

%*1538: %*1804 %*1541: %*1801 D:(A;ID;FA;;;BU) %*4416: %*1801 D:(A;ID;FA;;;BU) %*4419: %*1801 D:(A;ID;FA;;;BU) %*4423: %*1801 D:(A;ID;FA;;;BU)

AccessMask

0x120089

PrivilegeList

-

Активация Windows
Чтобы активировать Windows,
"Параметры".

(лс ий пре vs ен кен ите > 3 ТВ 1	Ключевые сл...	Дата и время	Источник	Код события	Категория задачи
	Аудит отказа	13.11.2022 15:32:00	Microsoft Windows...	5152	Filtering Platform Packet Drop
	Аудит успеха	13.11.2022 15:32:00	Microsoft Windows...	5156	Filtering Platform Connection
	Аудит успеха	13.11.2022 15:32:00	Microsoft Windows...	5158	Filtering Platform Connection
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	5156	Filtering Platform Connection
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	5158	Filtering Platform Connection
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	5158	Filtering Platform Connection
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	5158	Filtering Platform Connection
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	5156	Filtering Platform Connection
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	5156	Filtering Platform Connection
	Аудит отказа	13.11.2022 15:31:59	Microsoft Windows...	4656	Kernel Object
	Аудит отказа	13.11.2022 15:31:59	Microsoft Windows...	4656	Kernel Object
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	4658	File System
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	4663	File System
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	4656	File System
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	4658	File System
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	4690	Handle Manipulation
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	4658	File System
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	4663	File System
	Аудит успеха	13.11.2022 15:31:59	Microsoft Windows...	4656	File System

Событие 4656, Microsoft Windows security auditing.

Общие Подробности

Запрошен дескриптор объекта.

Имя журнала: Безопасность

Источник: Microsoft Windows security : Дата: 13.11.2022 15:31:59

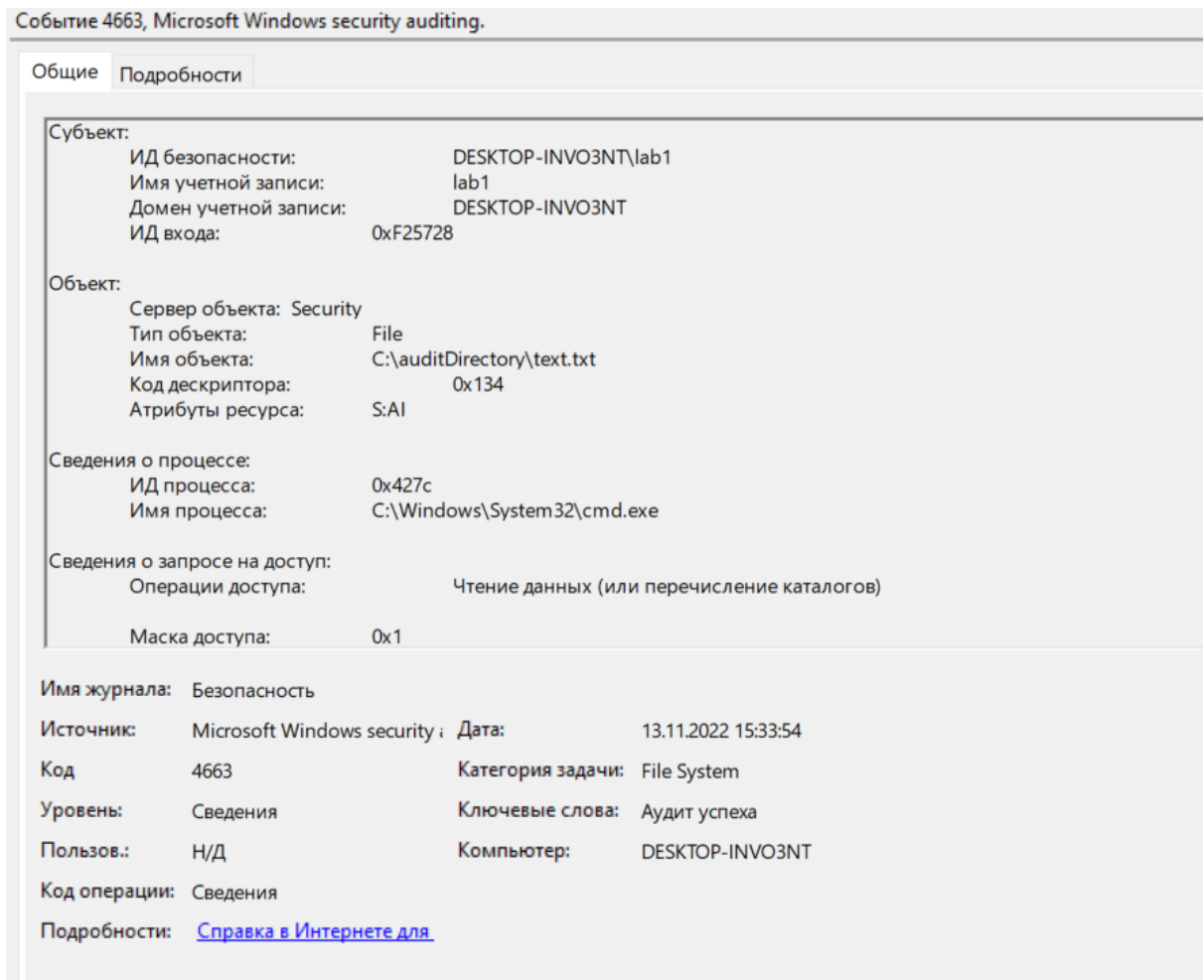
Код: 4656 Категория задачи: File System

Уровень: Сведения Ключевые слова: Аудит успеха

Пользов.: Н/Д Компьютер: DESKTOP-INV03NT

Код операции: Сведения

Подробности: [Справка в Интернете для](#)



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

Дискреционное управление доступом является основой управления доступом в ОС Windows.

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

Общие разрешения:

- Полный доступ
- Изменение
- Чтение и выполнение
- Чтение
- Запись

Дополнительные разрешения:

- Траверс папок / выполнение файлов
- Содержание папки / чтение данных
- Чтение атрибутов
- Чтение дополнительных атрибутов
- Создание файлов / запись данных
- Создание папок / дозапись данных
- Запись атрибутов
- Запись дополнительных атрибутов

- Удаление
- Чтение разрешений
- Смена разрешений
- Смена владельца

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

Необходимо с помощью ПКМ зайти в свойства файла, раздел "Безопасность". При помощи кнопки "Изменить..." можно назначить общие разрешения, а при помощи кнопки "Дополнительно" — дополнительные разрешения. Для этого выбираем пользователя или группу, а затем выбираем нужные разрешения для нее.

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

Заходим в "Локальную политику безопасности" (secpol.msc) , потом "Локальные политики" . Затем на "Назначение прав пользователя". Там выбираем нужную привилегию и добавляем туда пользователя.