Министерство образования и науки Российской Федерации

Санкт-Петербургский Политехнический Университет Петра Великого

**Институт кибербезопасности и защиты информации.**

**ЛАБОРАТОРНАЯ РАБОТА 12**

**Система контроля доступа.**

по дисциплине «Основы информационной безопасности»

Выполнил

студент гр. 4851003/10002 Лобов Е.А

Преподаватель Зубков Е.А.

Санкт-Петербург

2022

**Цель работы**

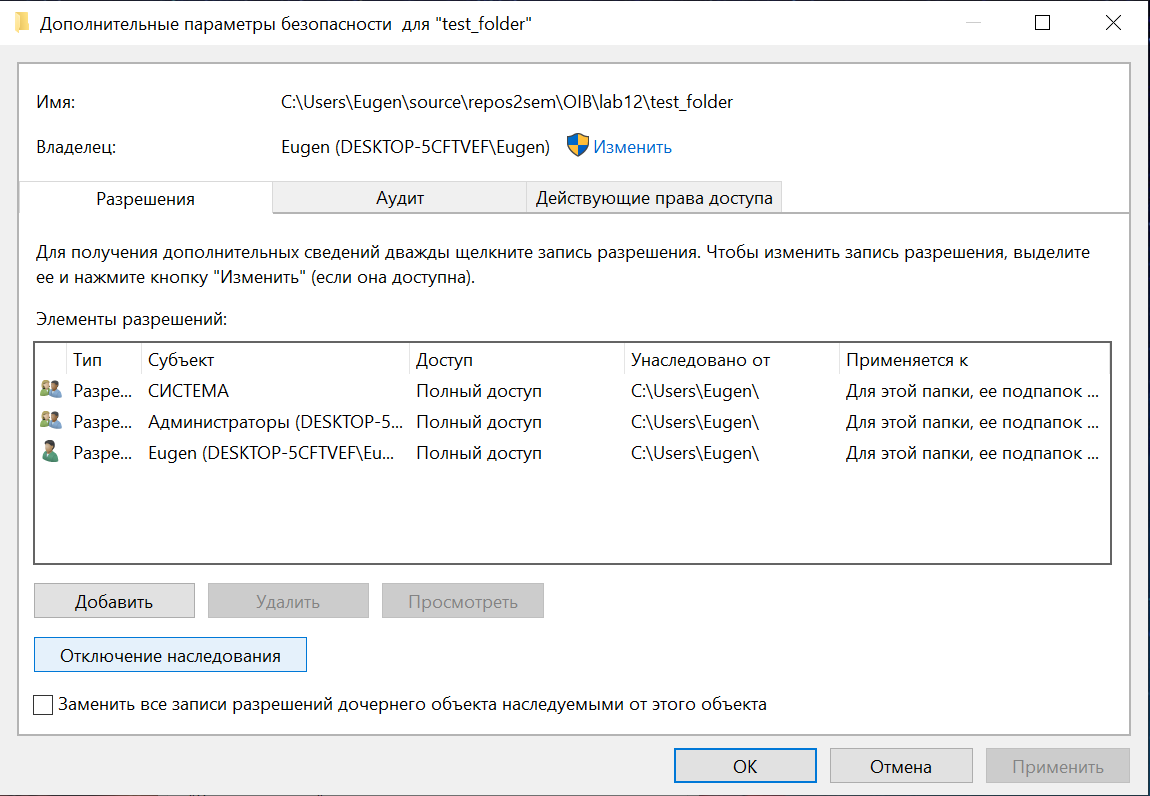
Цель работы - освоение средств контроля и управления доступом пользователей к ресурсам операционной системы, приобретение навыков распределения прав на примере файловой системы NTFS в среде Windows.

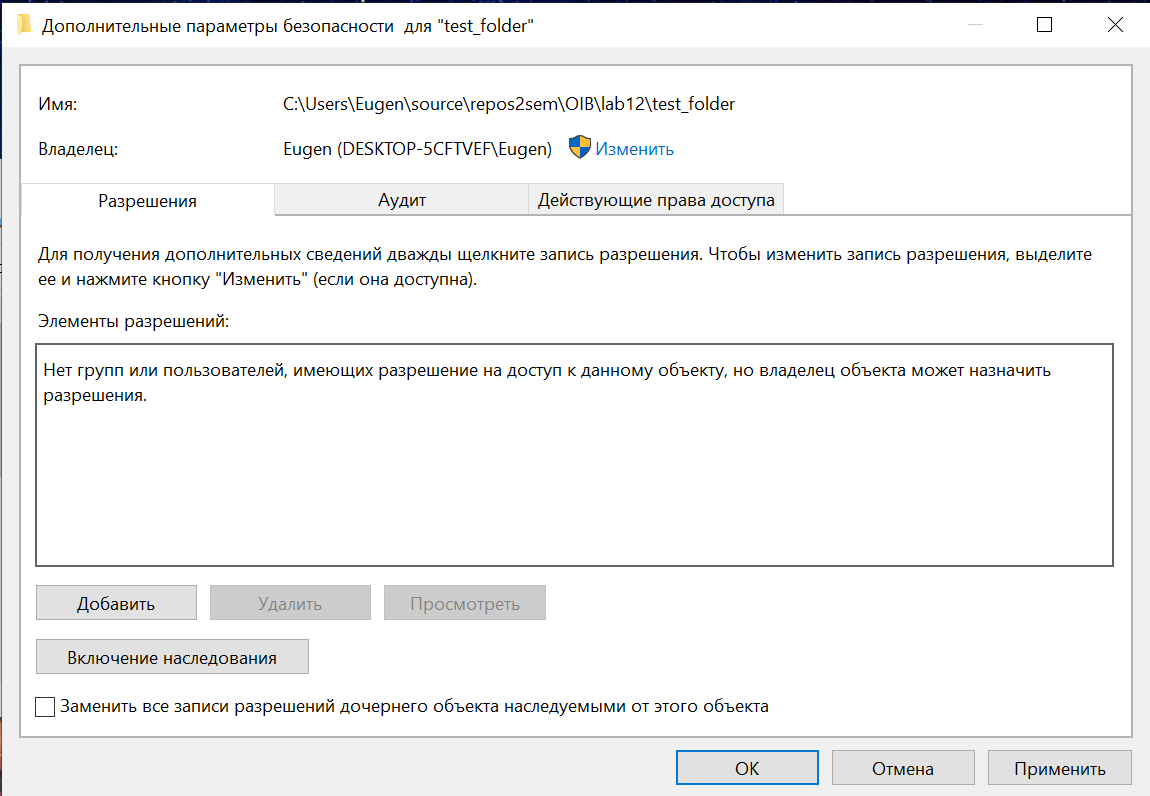
# 1.ход работы

## 1.1ACL и ACE.

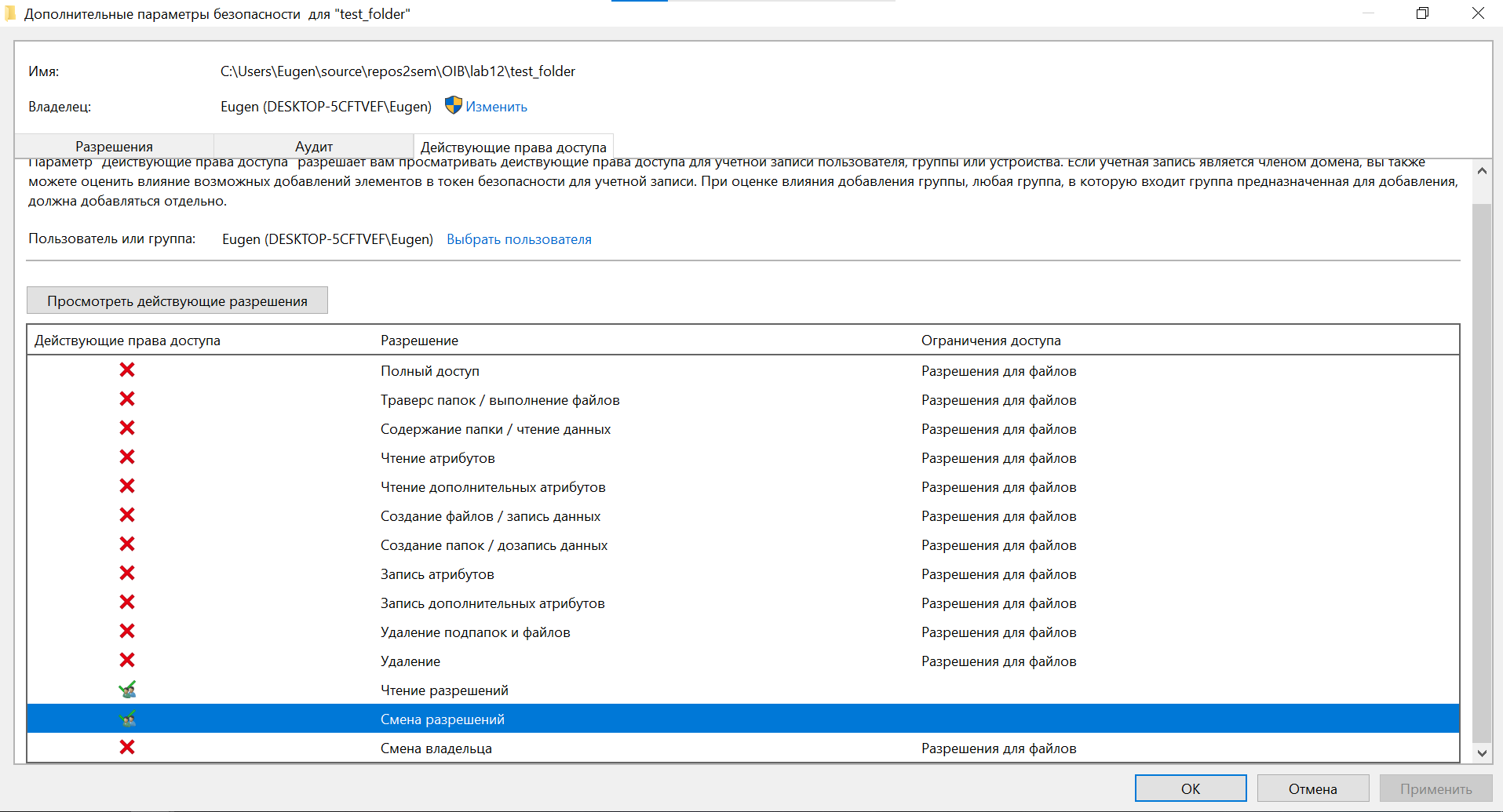
ACL(access control list) - список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей). Как правило ACL представляют собой набор записей, называемых Записями управления доступом(ACE).Каждый раз при обращении к объекту операционная система в соответствии ACL, связанным с этим объектом, проверяет, обладает ли пользователь достаточными правами доступа.

## 1.2 Произведенные модификации в структуре ACL.

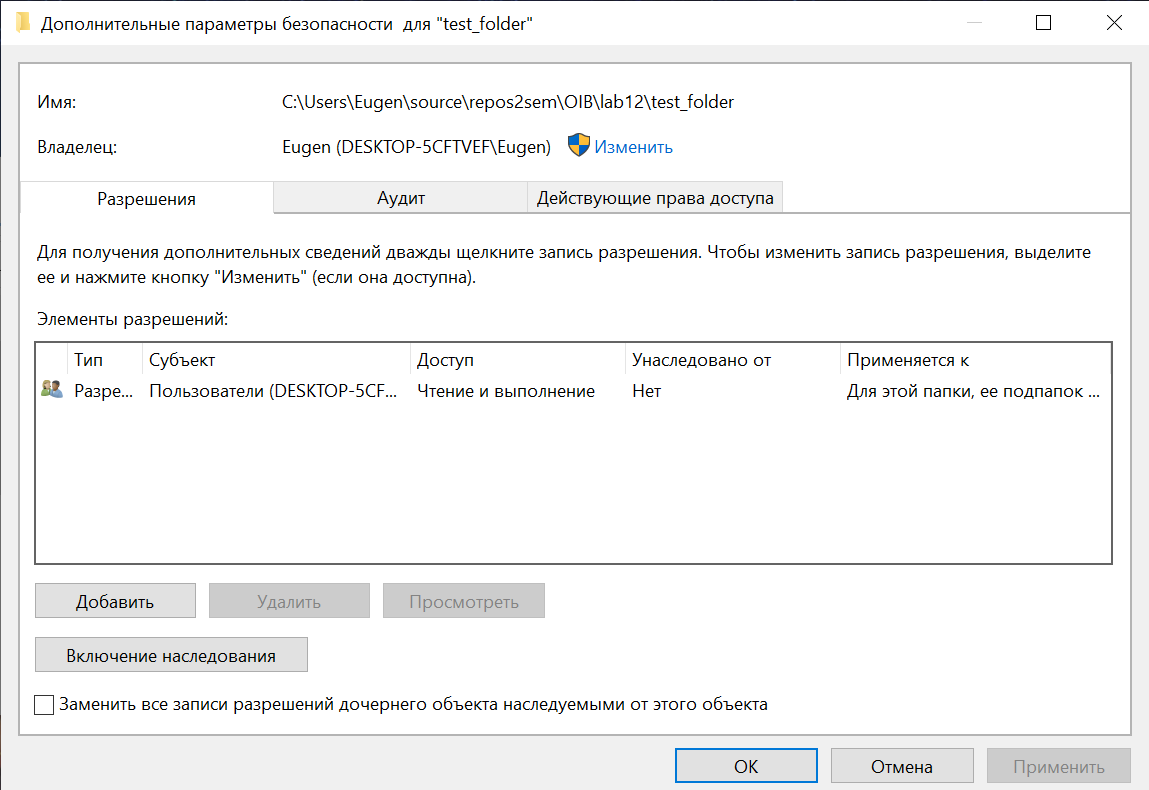


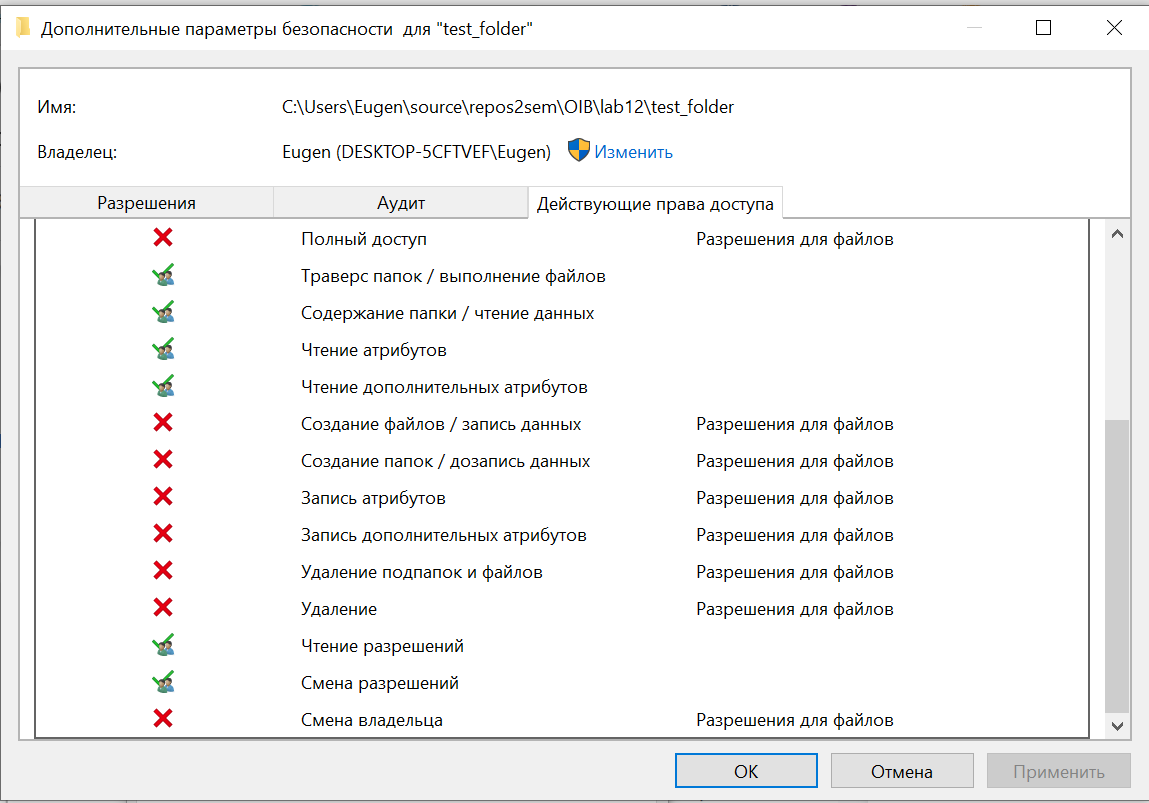
Создам папку test\_folder. Отключу наследование. Владельцем каталога по-прежнему остается текущий пользователь.

У пользователя нет действующих разрешений на данный момент.

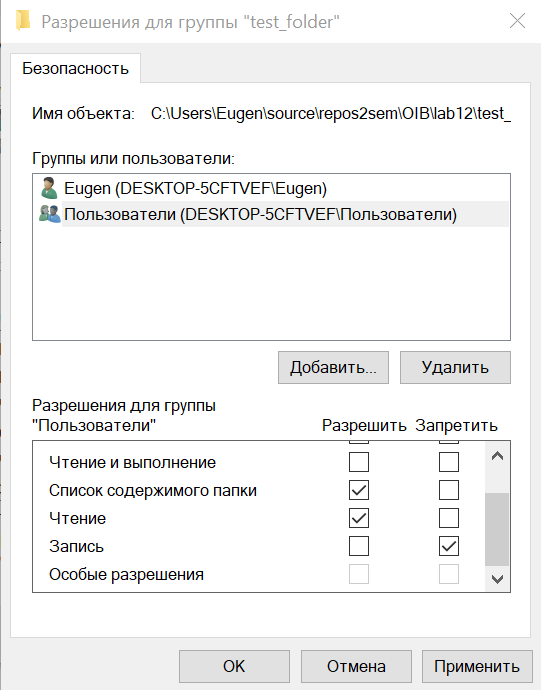
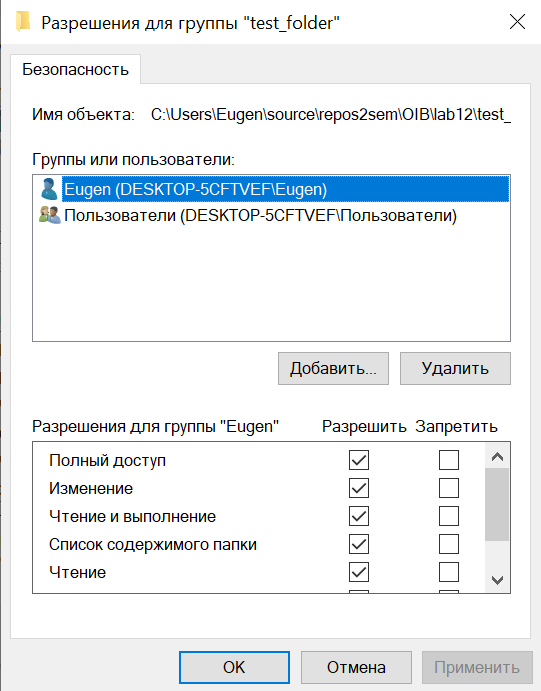


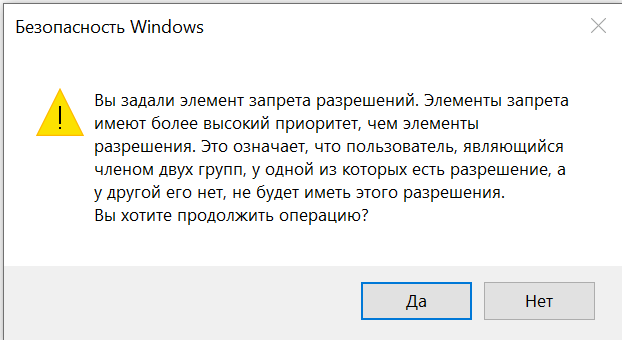
Все пользователи по-умолчанию находятся в группе пользователи. Разрешу этой группе чтение и запись в данном каталоге.



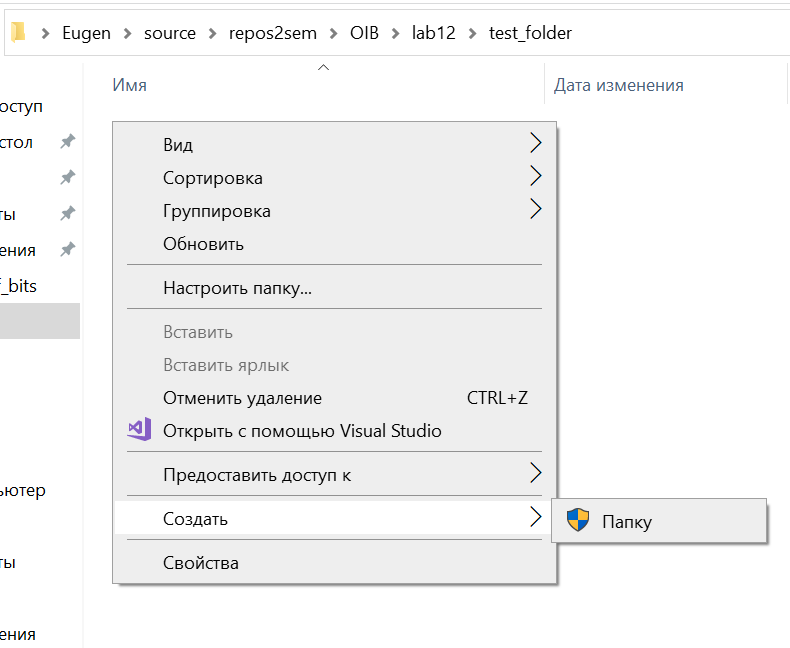


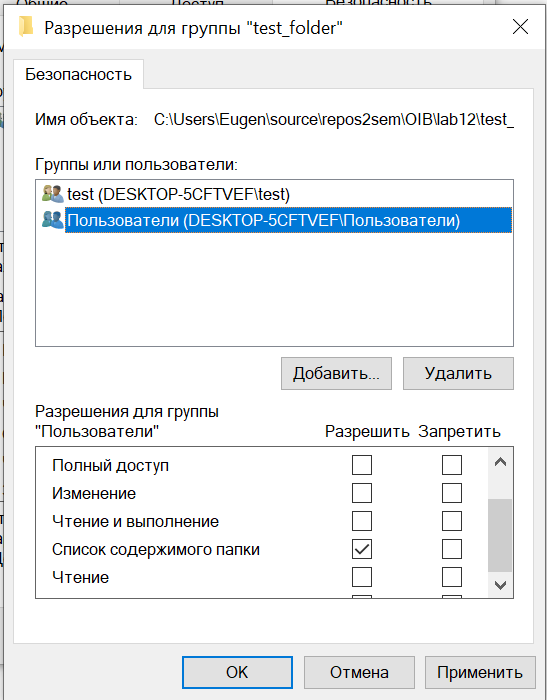
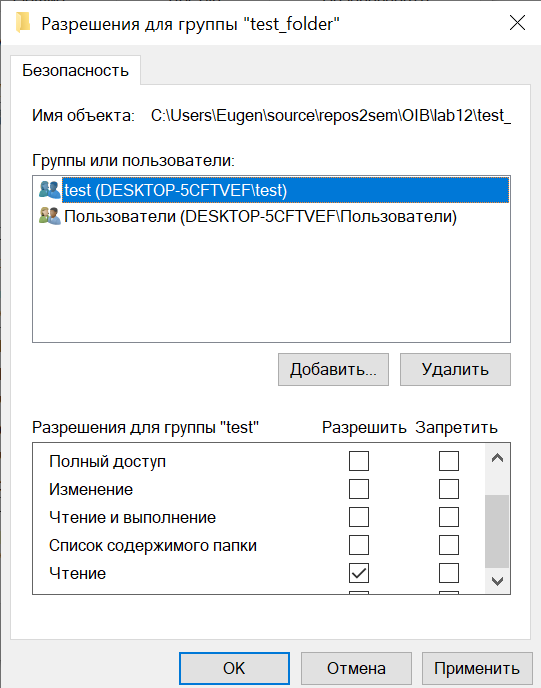
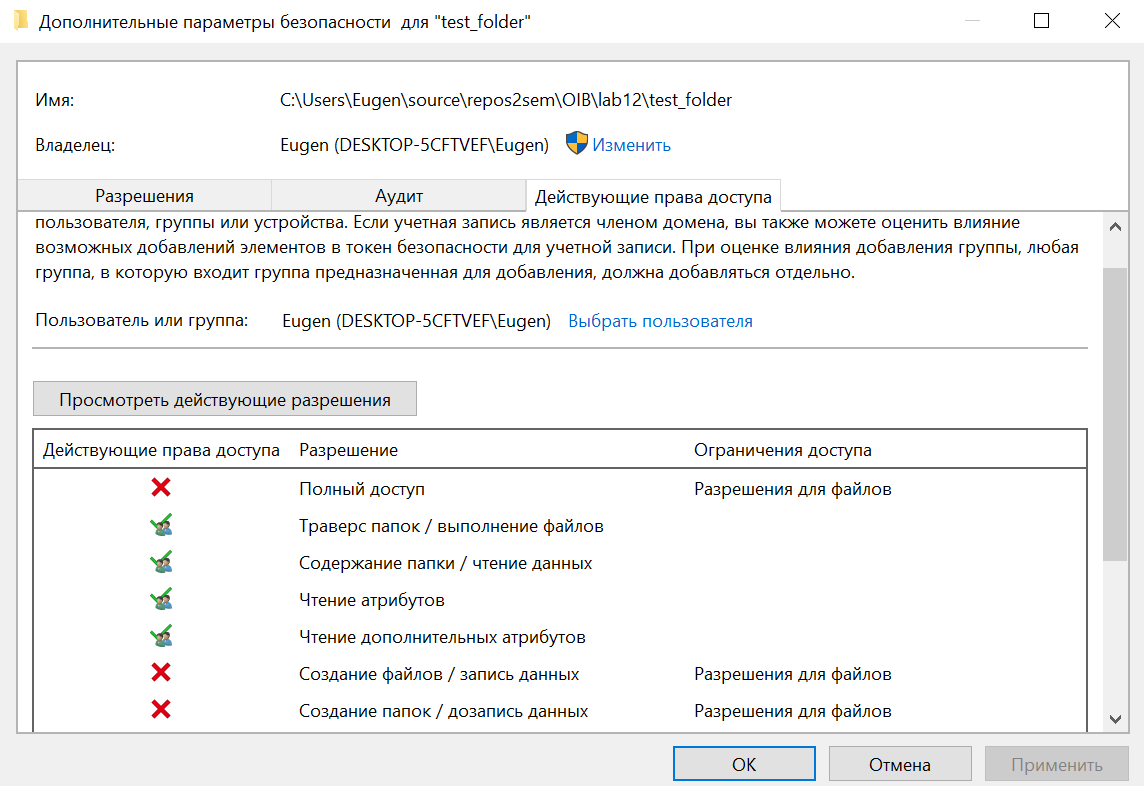
Теперь пользователь Eugen имеет права, доступные всем членам группы Пользователи.

Запрещающие права имеют приоритет над разрешающими. 



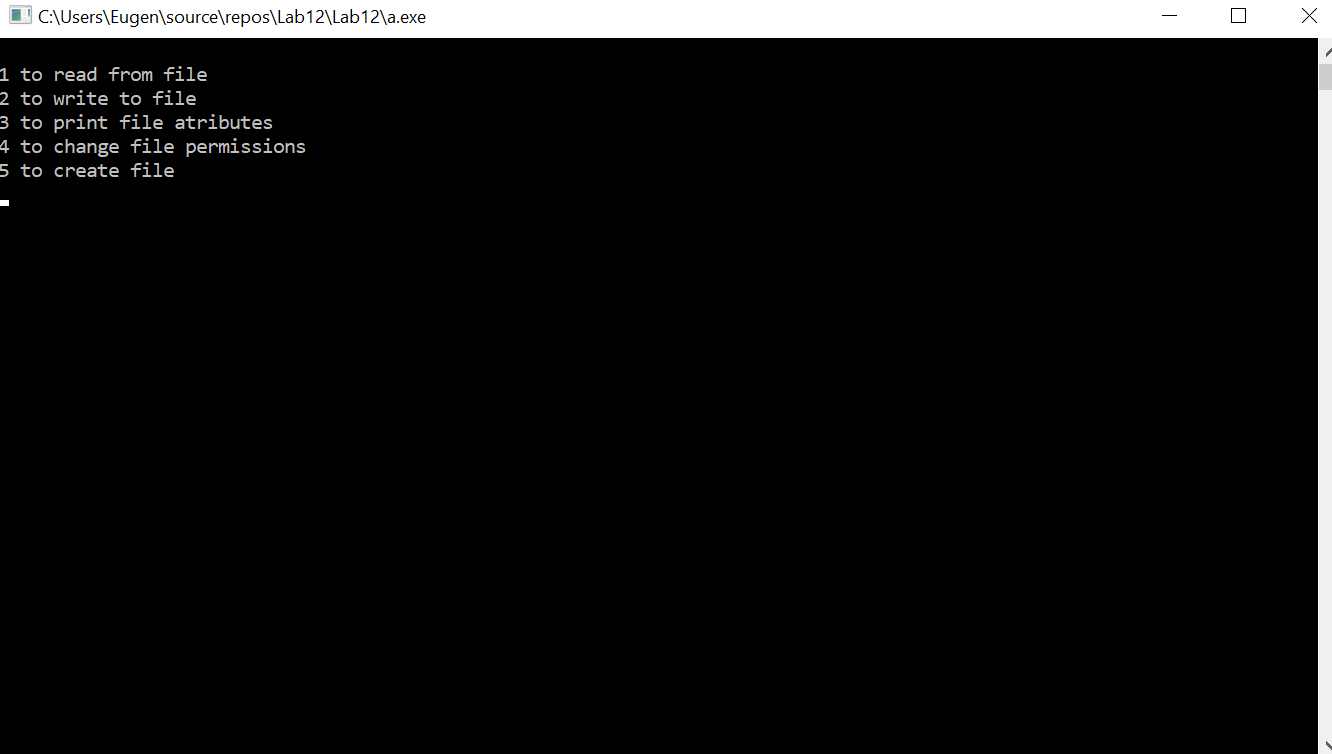
Поэтому в данном случае у пользователя Eugen не будет возможности на создание папки в каталоге.



Права суммируются : создам две ACE для двух разных групп, в которые входит пользователь.

Можно наблюдать, что права двух групп, в которые входит пользователь складываются.

Была разработана программа для работы с текстовым файлом и изменением его атрибутов. Ниже представлен скриншот работы разработанной программы.



# 2.Ответы на контрольные вопросы

1.Что такое множество действующих разрешений?

Это совокупность всех разрешений для пользователя, которые можно посмотреть через Безопастность->Действующие права доступа.

2.Почему проверка прав доступа к файлу осуществляется только при открытии файла, а не при обращении к нему?

Процесс в течении работы может осуществлять доступ ко многим объектам, а кол-во активных процессов и проверяемых ACE в каждый момент времени довольно большое, поэтому монитор безопасности проверяет возможность доступа к объекту только при его открытии.

3.Можно ли запретить администратору системы доступ к какому-либо файлу?Может ли он обойти это ограничение?

Конфигурация пользователя -> Административные шаблоны -> Компоненты Windows -> Проводник -> Удалить вкладку "Безопасность". Однако администратор может обойти данное ограничение например сменив владельца папки на себя.

4.Как изменить владельца объекта в среде Windows?

Кликните правой кнопкой мыши по файлу или папке, доступ к которому нужно получить (стать **владельцем**), в контекстном меню выберите пункт «Свойства». На вкладке «Безопасность» нажмите кнопку «Дополнительно». Напротив пункта «**Владелец**» нажмите «**Изменить**».

5.Имеет ли владелец какие-либо права к файлу, если существует ACE, запрещающая полный доступ к этому файлу на имя владельца?

Владелец по-прежнему сможет менять атрибуты безопасности файла, поэтому вернуть доступ к файлу не составит труда.

# 3.вывод

В ходе данной лабораторной работы были освоены базовые навыки работы с атрибутами безопасности NTFS, а также разработаны утилиты, позволяющие работать с атрибутами безопасности файла. Знание особенностей работы с атрибутами безопасности полезно при администрировании локальных сетей или защите файлов, просмотр которых нежелателен. Опытный пользователь, имеющий права администратора может обойти любые установленные подобным образом ограничения. Однако для контроля доступа к файлам для рядовых пользователей данные методы достаточно эффективны.