

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики

Лабораторная работа №2
Дисциплина «Информационная безопасность»

Выполнили:

Баев Дмитрий Владимирович
Съестов Дмитрий Вячеславович
Группа Р3417

Преподаватель:

Оголюк Александр Александрович

Санкт-Петербург

2020

Иерархия каталогов:

F:

|_ lab2

|_ a

|_ hiew32demo.exe

|_ LAB2.txt

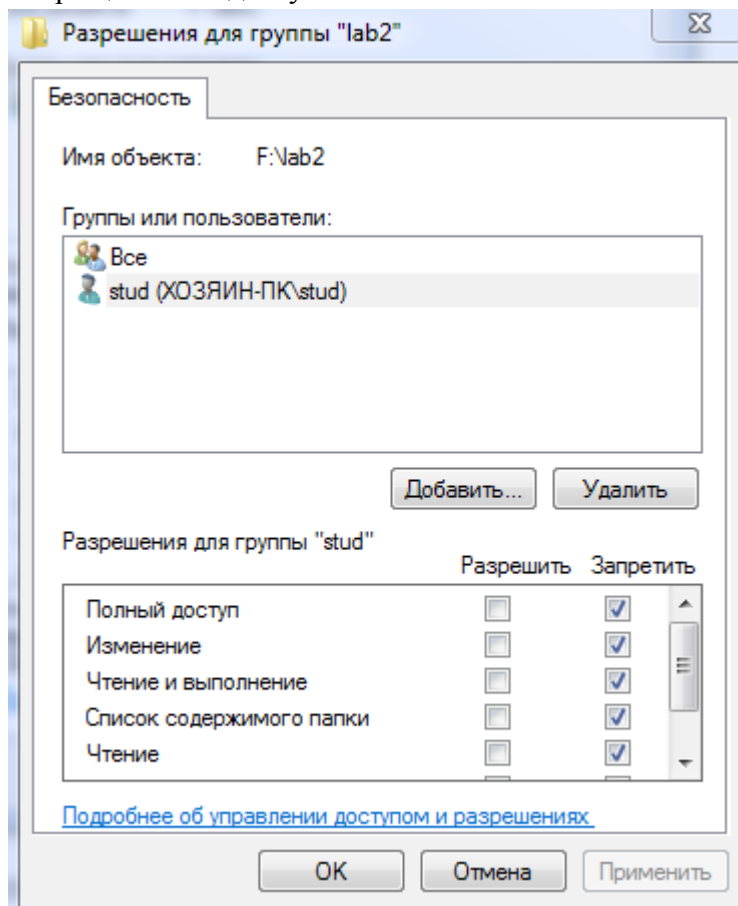
|_ hiew32demo.exe

|_ LAB2.txt

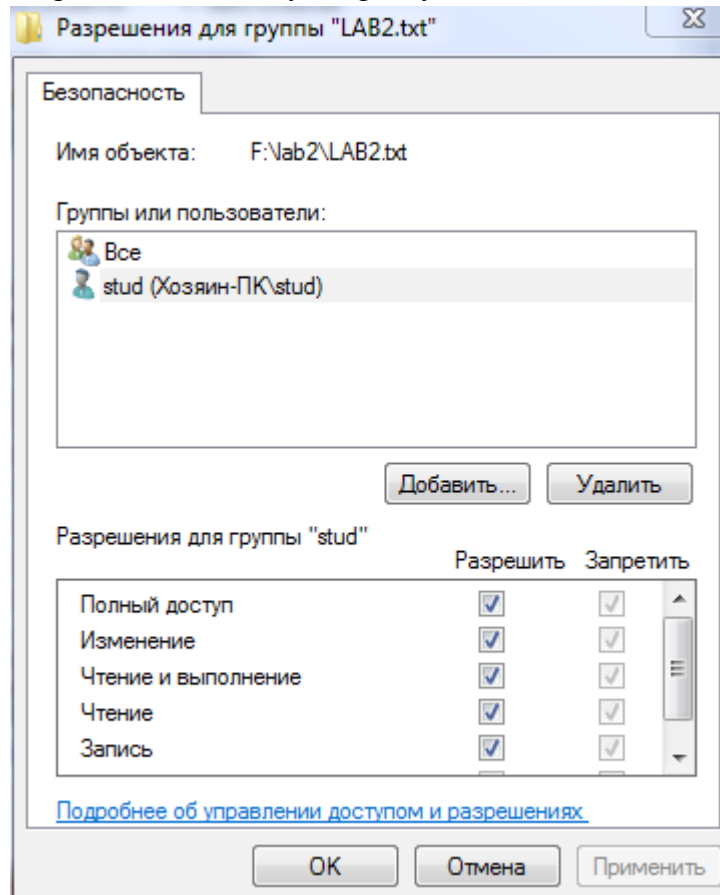
Проверить правила:

1. Разрешения, установленные на файл, играют более важную роль при определении типа доступа пользователя, чем разрешения на папку.

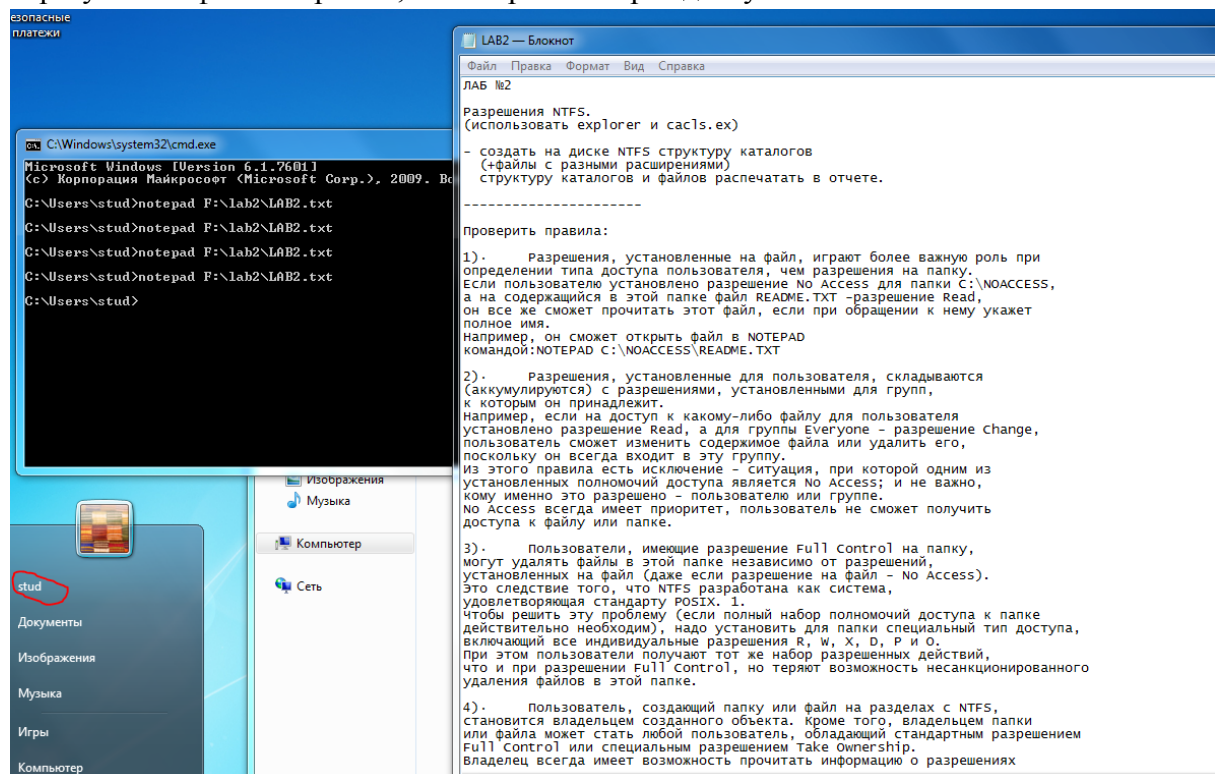
Запрещаем stud доступ к папке lab2:



Разрешаем stud доступ к файлу lab2/LAB2.txt:



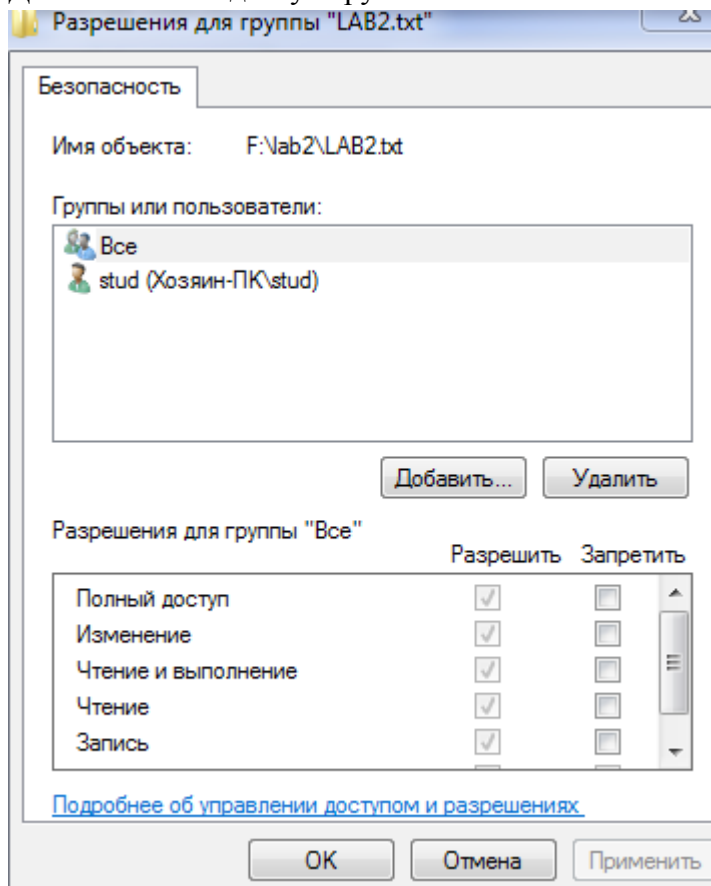
В результате файл открылся, несмотря на запрет доступа к папке:



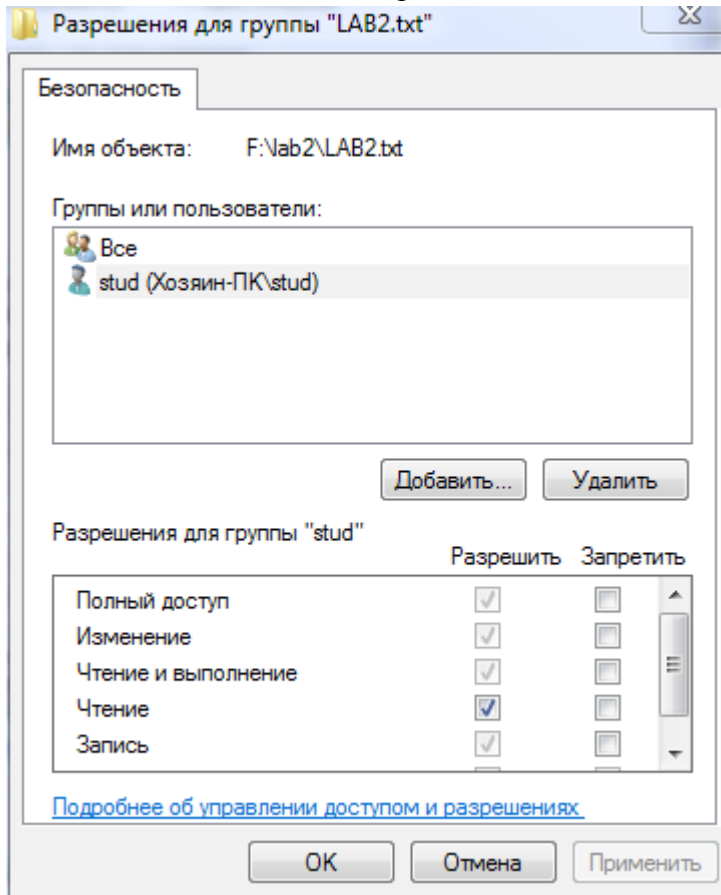
Таким образом, правило верно.

2. Разрешения, установленные для пользователя, складываются (аккумулируются) с разрешениями, установленными для групп, к которым он принадлежит. Из этого правила есть исключение - ситуация, при которой одним из установленных полномочий доступа является No Access; и не важно, кому именно это разрешено - пользователю или группе. No Access всегда имеет приоритет, пользователь не сможет получить доступа к файлу или папке.

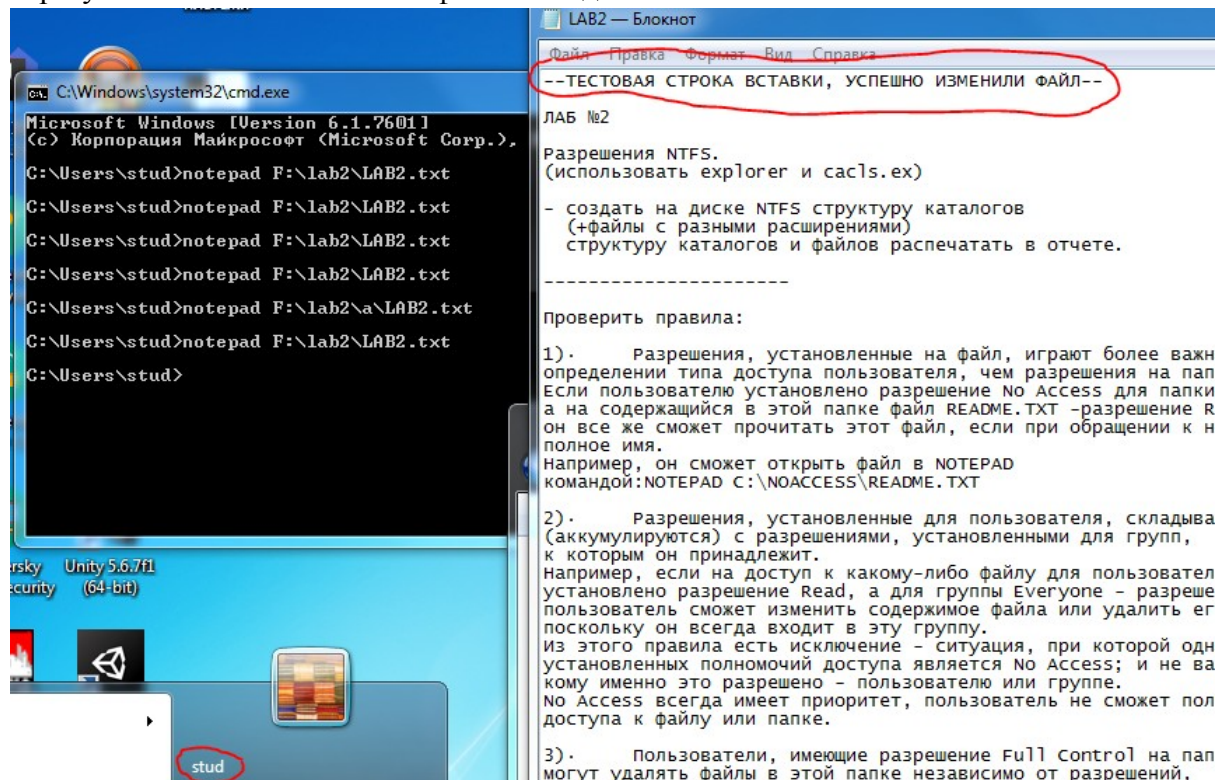
Делаем полный доступ группе “Все”:



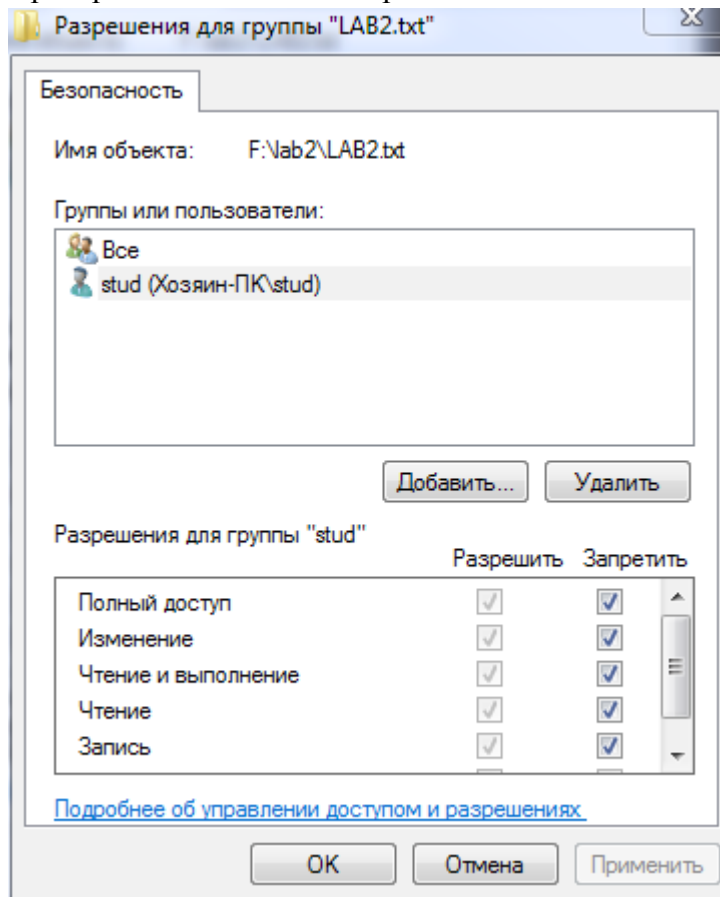
Пользователю stud выдаем права только на чтение:



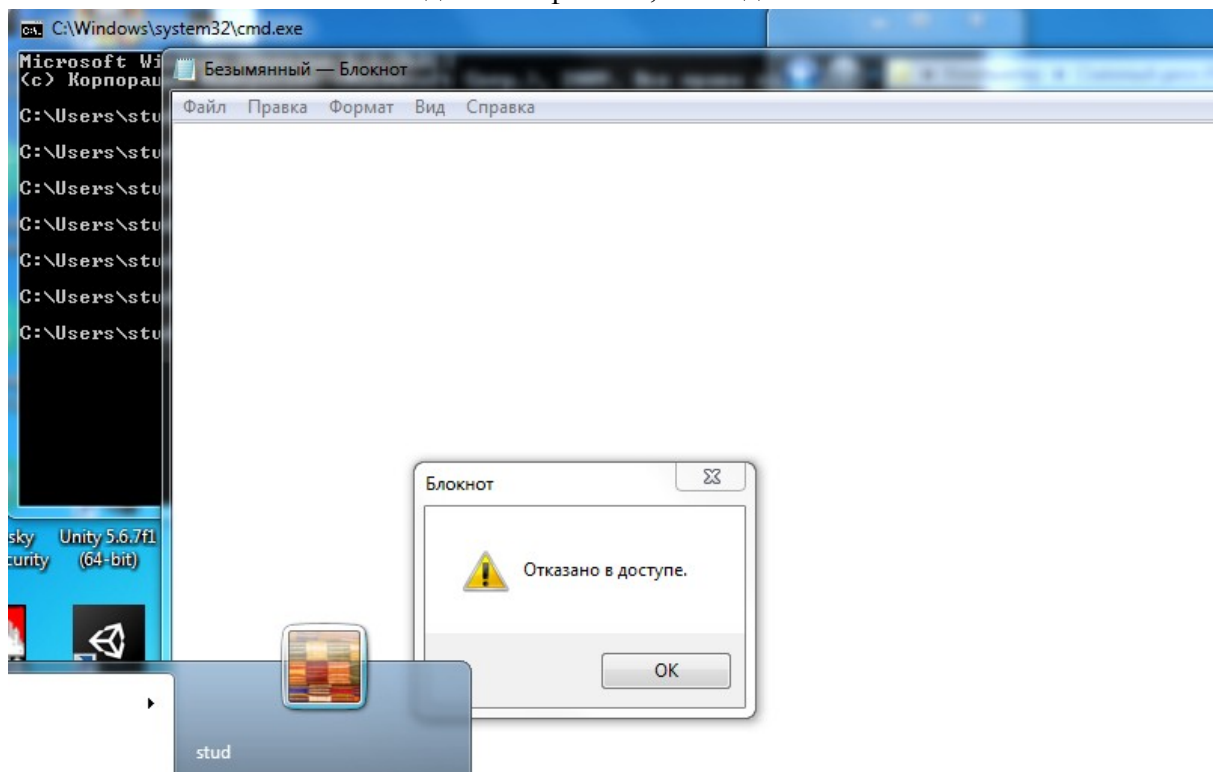
В результате смогли изменить файл из-под пользователя stud:



Проверим исключение. Запретим все пользователю stud:



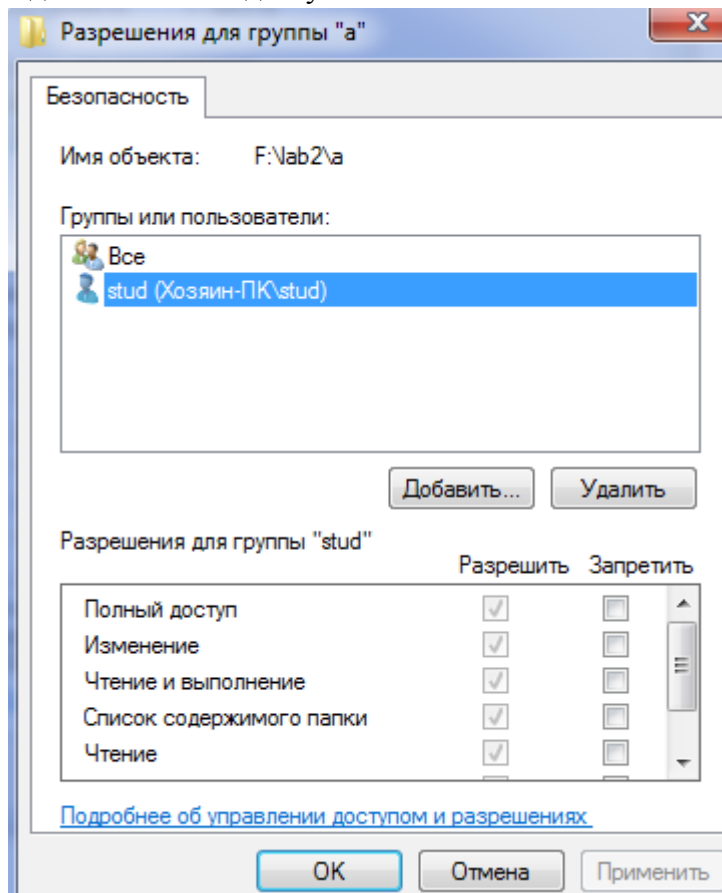
В итоге мы не можем ничего сделать с файлом, как и должно быть:



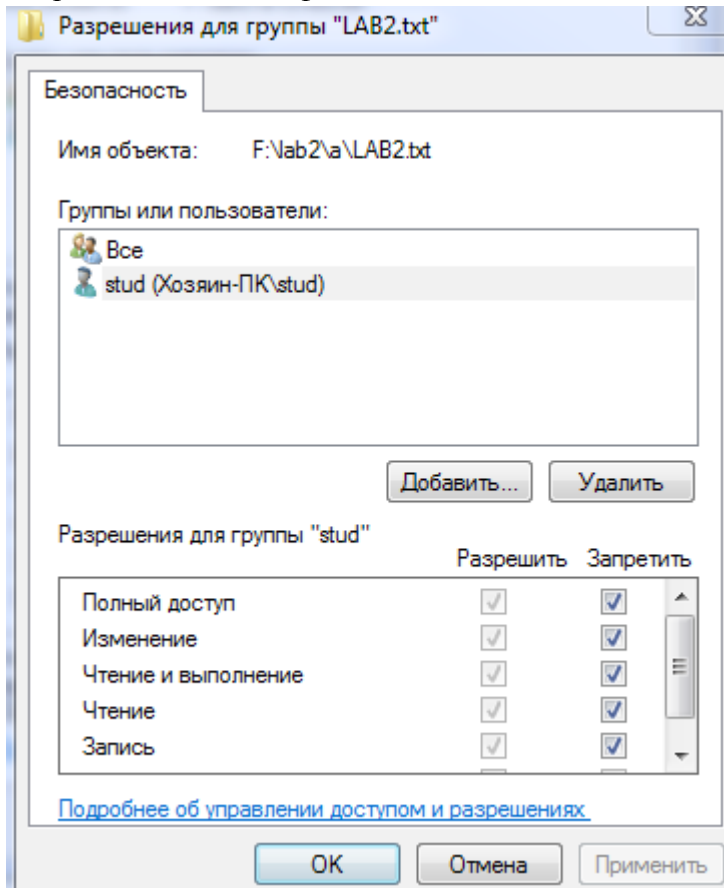
Правило верно.

3. Пользователи, имеющие разрешение Full Control на папку, могут удалять файлы в этой папке независимо от разрешений, установленных на файл (даже если разрешение на файл - No Access).

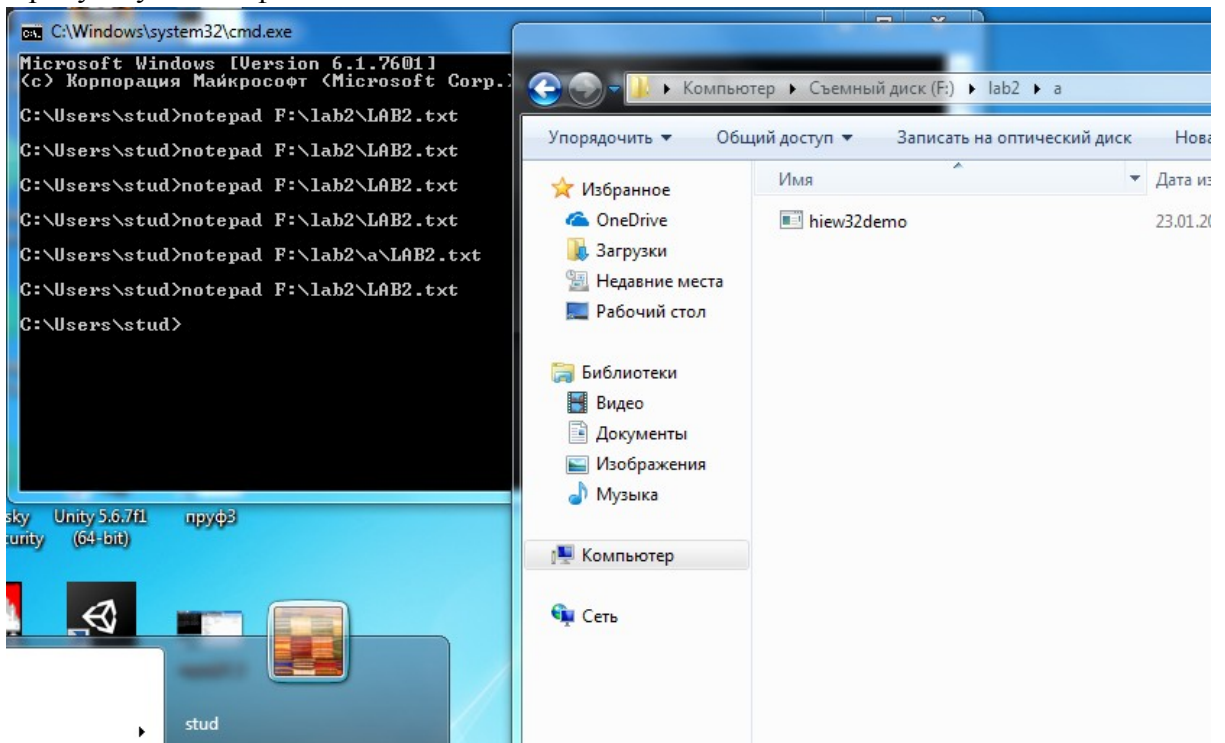
Сделаем полный доступ stud к папке lab2\а:



Запретим все stud на файл lab2\а\LAB2.txt:



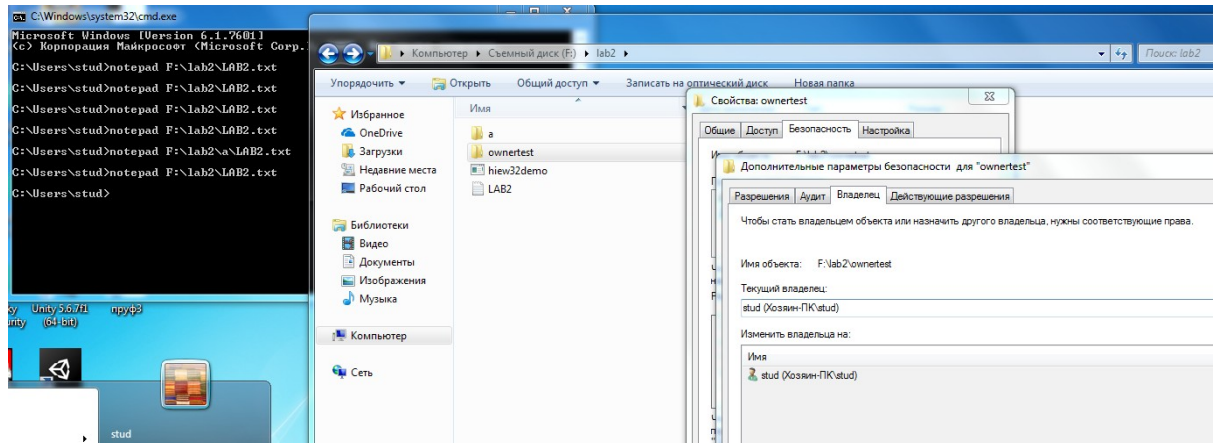
Пробуем удалить файл:



Смогли удалить файл, правило верно.

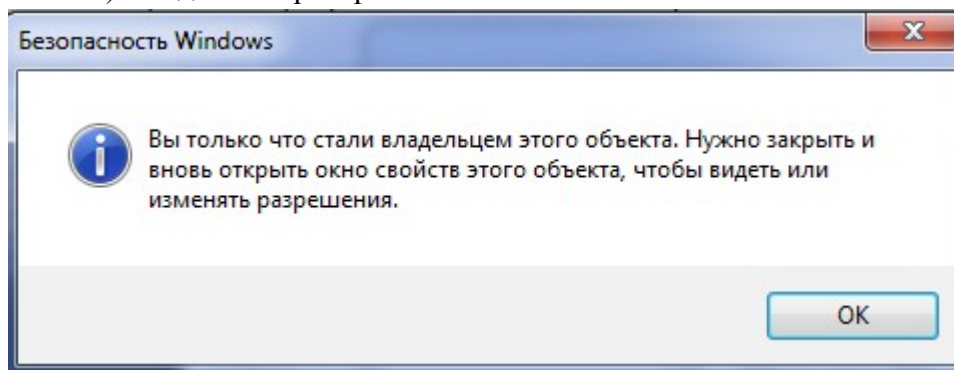
4. Пользователь, создающий папку или файл на разделах с NTFS, становится владельцем созданного объекта. Кроме того, владельцем папки или файла может стать любой пользователь, обладающий стандартным разрешением Full Control или специальным разрешением Take Ownership.

Создадим папку ownertest с пользователя stud и проверим владельца:



Владельцем действительно является пользователь stud.

Также попробуем изменить владельца с учетки администратора (имеет Full Control) на администратора.



Успешно. Правило верно.

Заменить разрешения для всех файлов *.exe (должны присутств. в иерархии созданных каталогов) со stud (Full Access) на Администратор (Full Access).
[Не добавит права для польз. Администратор , а заменить права stud на права Администратор, после операции в списке доступа stud быть не должно.]

Необходимая команда:

*cacls *.exe /S:D:PAI(A;;;FA;;;BA)*

эта команда заменяет разрешения на BA (Built-in Administrators)