Дисциплина «Защита в операционных систем»

Лабораторная работа № 3

Тема: Управление правами доступа в операционных системах семейства Windows.

Цель: Изучить способы управления правами доступа к файлам и папкам в ОС семейства Windows.

Время выполнения лабораторной работы (аудиторные часы) – 4 часа.

Порядок выполнения лабораторной работы: работа выполняется самостоятельно под руководством преподавателя.

Оборудование и программное обеспечение: работа выполняется на ПЭВМ типа IBM PC с использованием стандартных функций ОС.

1. Теоретические сведения

Для каждого объекта, который хранится в томе NTFS, поддерживается контрольный список доступа (ACL). Этот список определяет перечень пользователей, которым разрешен доступ к данному объекту. Каждая запись в таком списке именуется ACE (access control entry). Для того, чтобы разрешить или отказать в доступе к объекту (файлу или папке), необходимо модифицировать ACE. Делать это могут владельцы объекта, члены группы "Администраторы" и обычные пользователи, которым разрешили это сделать либо первые, либо вторые.

В Windows при включенной опции "Использовать простой общий доступ ко всем файлам" возможности по изменению прав доступа весьма ограничены. Заблокировав эту опцию (в меню "Проводника": "Сервис" > "Свойства папки" > "Вид"), получите доступ к набору прав NTFS.

В Windows управление доступом к ресурсам реализовано с помощью набора ***предопределенных базовых прав доступа*** (их шесть): полный доступ, чтение, запись и так далее. Но есть еще и одиннадцать ***специальных прав доступа***, с помощью которых разрешения настраиваются более тонко. Получить доступ к ним можно, нажав "Дополнительно" на вкладке "Безопасность", после

чего нужно два раза щелкнуть на имени пользователя. Использование предопределенных прав упрощает процесс администрирования. Фактически, если вы устанавливаете флаг "Чтение и выполнение", операционная система (ОС) сама устанавливает пять отдельных прав доступа: выполнение файлов; чтение данных, атрибутов, дополнительных атрибутов, разрешений. Считается, что шести предопределенных прав в обычных случаях вполне достаточно.

Права доступа предоставляются установкой флажка в столбце "Разрешить". Флажки "Запретить" устанавливаются, когда требуется явно запретить применение указанного права доступа пользователю. Они имеют высший приоритет, по сравнению с разрешениями, и применяются, в основном, для внесения ясности при наложении прав нескольких пользователей. Если требуется полностью блокировать доступ к объекту, выберите для ненавистного пользователя "Запретить" в строке "Полный доступ".

Кроме прав доступа, устанавливаемых индивидуально, объекты могут наследовать их от родительских папок. По умолчанию, разрешения передаются от папки всем подпапкам. Для просмотра опций наследования следует на вкладке "Безопасность" выбрать "Дополнительно". Если в Windows 2000 единственным признаком наследования являлось затемнение пиктограммы ключей, то в XP и более поздних версиях ОС появился даже специальный столбец "Унаследовано от". Дважды щелкнув по соответствующей записи пользователя, можно будет указать метод наследования разрешений: для этой папки ее подпапок и файлов, только для этой папки и так далее.

Для отмены наследования в дополнительных параметрах безопасности следует убрать флажок "Наследовать от родительского объекта..." в Windows XP или «Добавить разрешения, наследуемые от родительского объекта» в Windows 7. Следует иметь в виду, что при удалении наследуемых папкой прав она сама становится новым родительским объектом. По умолчанию, любые права доступа, присваиваемые этой папке, будут передаваться вниз по иерархии к вложенным подпапкам.

Нередко случается, что перемещенные или скопированные объекты получают совершенно новые права доступа. Может быть даже такое, что двойной щелчок по файлу может привести к сообщению "Доступ запрещен", даже если пользователю предоставлены все возможные права к текущей папке. Чтобы понять причины возникновения подобных проблем, необходимо разобраться с тем, что происходит, когда мы перемещаем или копируем объекты с одного места на другое. Естественно, в нашем случае речь идет только о дисках с файловой системой NTFS.

Каждый файл или папка в разделе NTFS имеют владельца, который может предоставлять или отказывать в правах доступа другим пользователям или группам. Владельцы могут заблокировать любого пользователя, включая членов группы "Администраторы". Владелец может предоставлять свои права другому пользователю, если тот является членом группы "Администраторы". Если же другой пользователь имеет ограниченную учетную запись, то вначале нужно изменить ACE объекта и разрешить пользователю полный доступ к файлу или папке, чтобы затем передать ему право владения. Кроме того, любой администратор может получить право собственности на любой объект, хотя и не может передать это право другим пользователям. Меняется владелец здесь: закладка "Безопасность"→"Дополнительно"→"Владелец".

2. Задание

Для выполнения данной лабораторной работы потребуется включить расширенные настройки общего доступа к папкам. Для этого необходимо выбрать нажать ПКМ→ «Параметры папок», перейти на вкладку «Вид» и снять галочку с пункта «Использовать мастер общего доступа (рекомендуется)» (рис. 5.1).

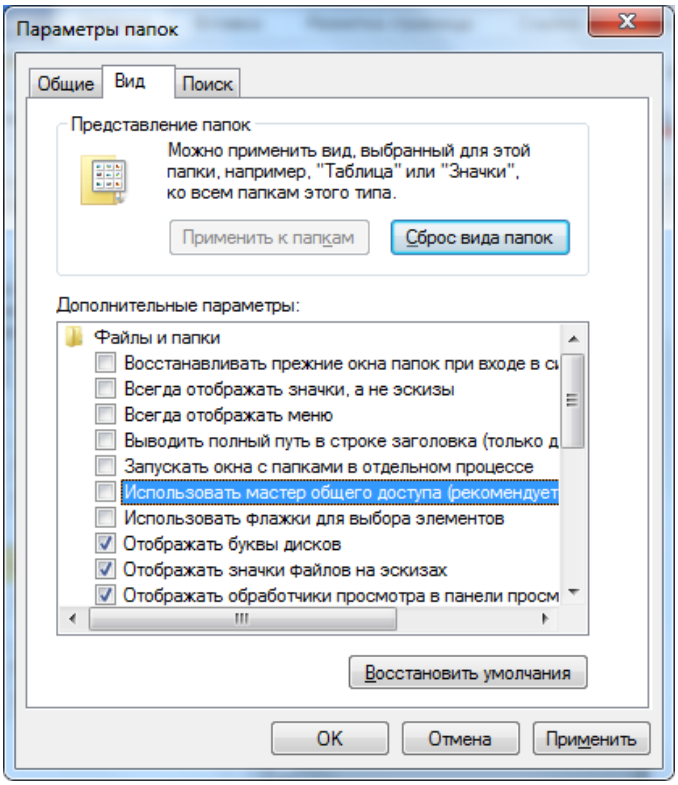

Рис. 5.1 Окно включения расширенных настроек общего доступа к папкам

1. Создайте на диске C:\ папку с именем test и удалите все установленные для неё по умолчанию разрешения (см. рис. 5.2). Для этого:

— нажмите правой кнопкой на папку и выберите пункт контекстного меню «Свойства»;

— перейдите на вкладку «Безопасность»;

— нажмите кнопку «Дополнительно»;

— в появившемся диалоговом окне снимите галочку с пункта «Добавить разрешения, наследуемые от родительского объекта»;

— в следующем окне нажмите кнопку «Удалить».

Вернувшись к окну «Дополнительные параметры безопасности для test» нажмите кнопку «Применить». Сделайте скриншот полученного результата.

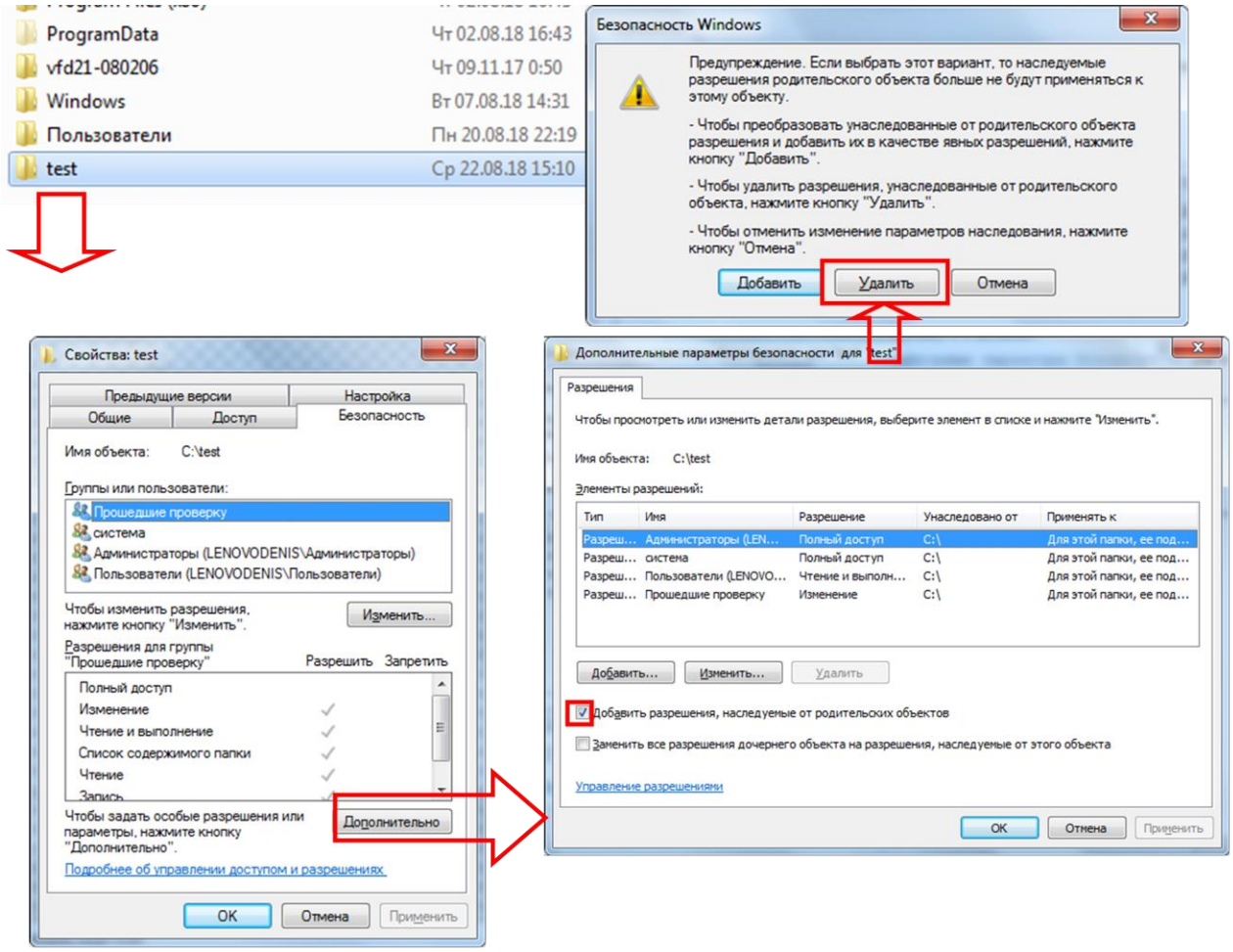

Рис. 5.2 Удаление разрешений для созданной папки test

Попытайтесь выполнить какое-либо действие с папкой test (например открыть, скопировать или удалить). Объясните полученные результаты.

2. Разрешите текущему пользователю просмотр содержимого папки. Для этого:

— откройте окно дополнительные параметры безопасности;

— нажмите кнопку «Добавить»;

— в появившемся окне введите имя текущего пользователя и нажмите «OK» (рис. 5.3);

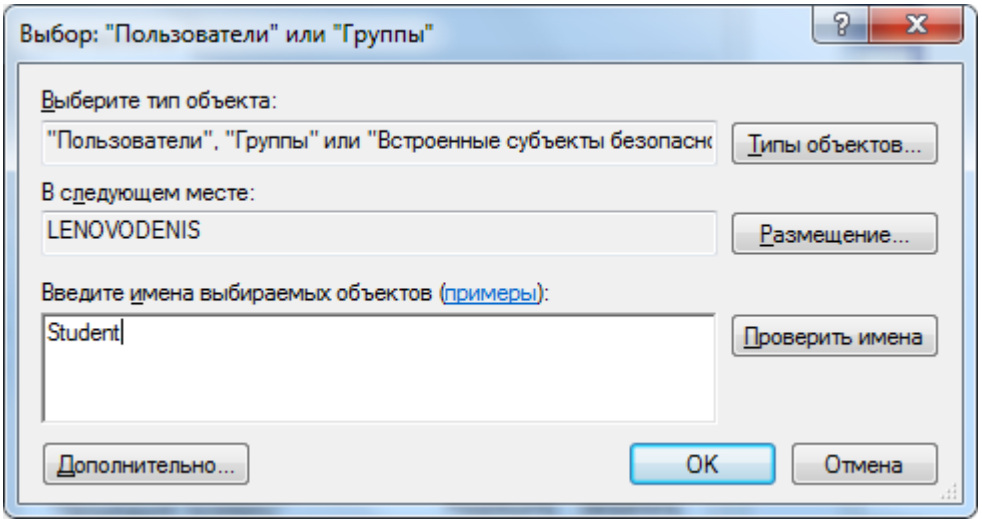

Рис. 5.3 Добавление пользователя к правам доступа

— в следующем окне поставьте галочку в столбце «Разрешить» напротив «Содержание папки / Чтение данных» и нажмите «OK» (см. рис. 5.4);

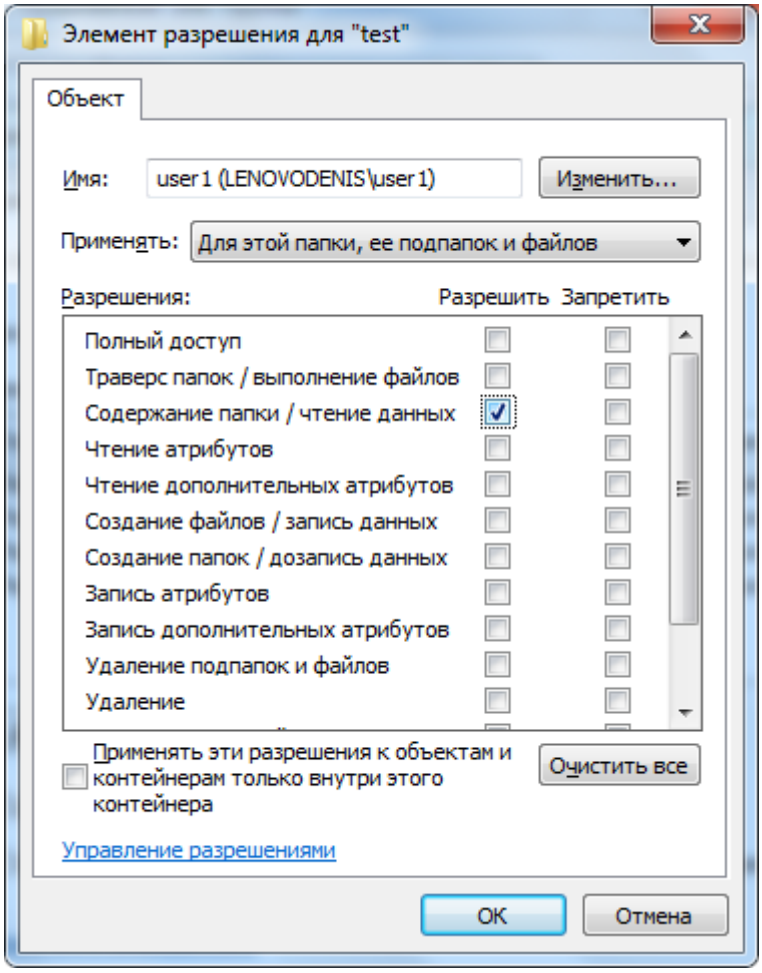

Рис. 5.4 Добавление права «Содержание папки / Чтение данных»

— нажмите «Применить» и зайдите в папку test.

3. Попытайтесь создать в папке test еще одну папку или файл. После сообщения об отказе в доступе выдайте соответствующие права текущему пользователю (см. рис. 5.5). Для этого:

— в окне дополнительных параметров безопасности выделите строку, отвечающую за разрешения текущего пользователя, созданную на предыдущем этапе и нажмите кнопку «Изменить».

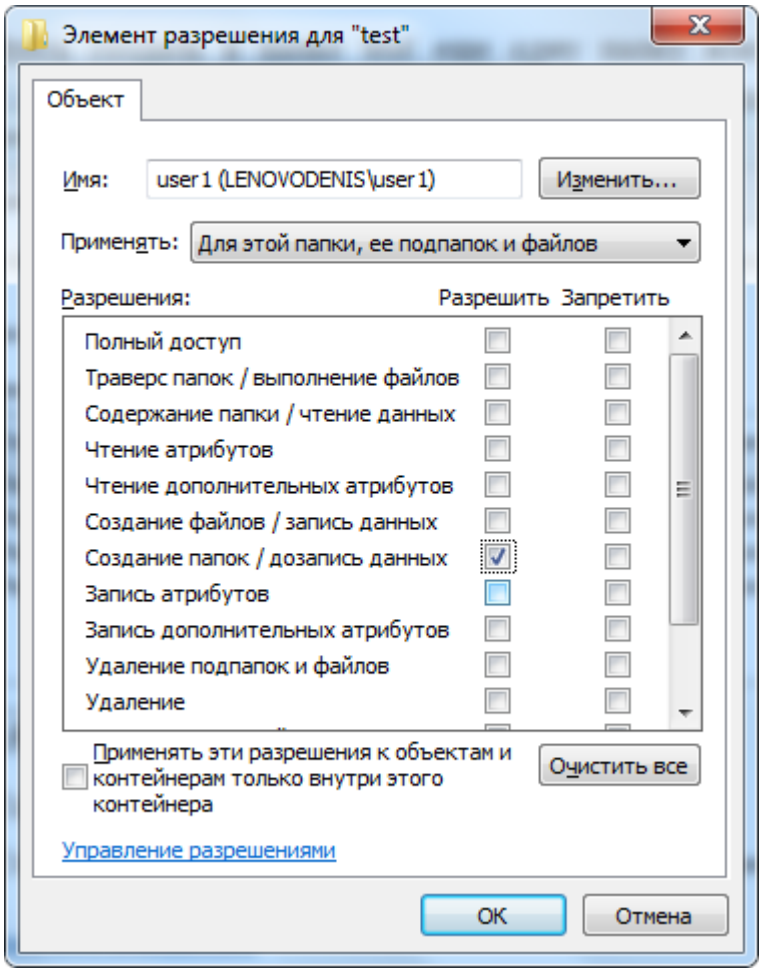

Рис. 5.5 Предоставление права «Создание папок / Дозапись данных»

— в появившемся окне поставьте галочку в столбце «Разрешить» напротив «Создание папок / Дозапись данных» и нажмите «ОК»;

— нажмите «Применить» и еще раз попытайтесь создать папку в папке test.

4. Проверьте наличие разрешений у созданной папки, сделайте скриншот результата и объясните откуда взялись данные разрешения.

5. Попытайтесь создать любой файл в папке test. После сообщения об отказе в доступе выдайте текущему пользователю права создание файлов по аналогии с предыдущим заданием.

6. Создайте в папке test пустой текстовый файл и попытайтесь записать в него какой-либо текст. После сообщения об отказе в доступе выдайте текущему пользователю следующие разрешения:

— Чтение атрибутов,

— Чтение дополнительных атрибутов,

— Запись атрибутов,

— Запись дополнительных атрибутов.

Снова попытайтесь записать в файл какой-либо текст. Сделайте скриншот текущего набора разрешений для папки test.

Обратите внимание что в окне свойств папки test на вкладке «Безопасность» появилась галочка в столбце «Разрешить» напротив пункта «Запись» (рис. 5.6).

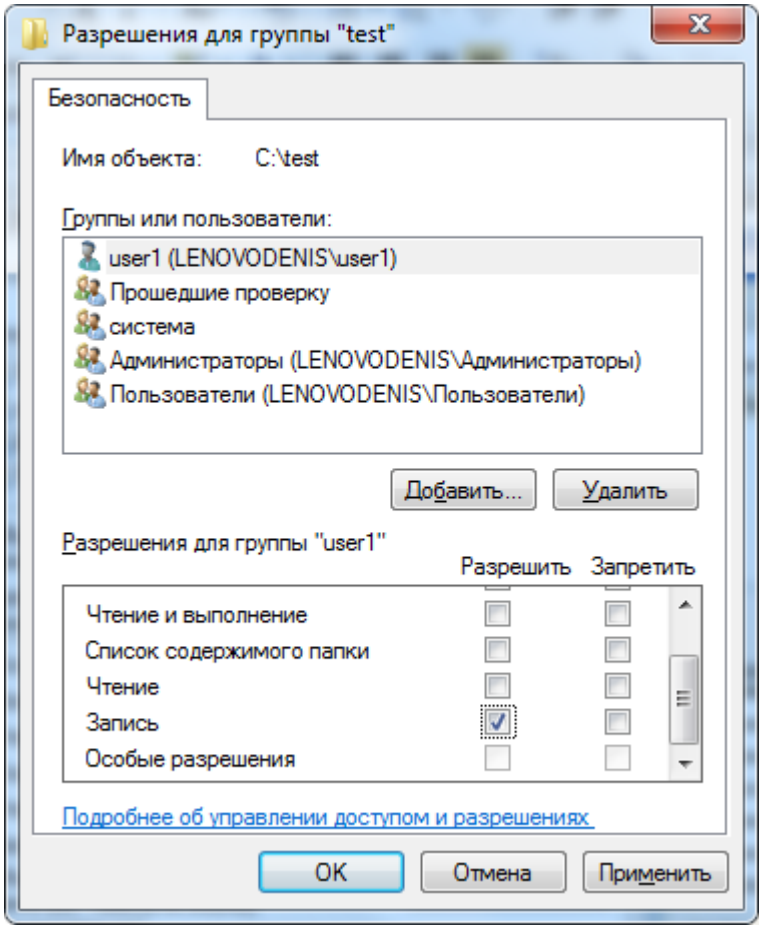

Рис. 5.6 Применение разрешающего права на запись для пользователя

Это произошло из-за того, что в окне дополнительных параметров безопасности пользователю были выданы специальные права доступа входящие в предопределённое базовое правило «Запись».

7. Удалите все выданные ранее разрешения и, последовательно ставя галочку напротив каждого из 6 предопределённых базовых правил в окне свойств папки, определите, какие специальные права (в окне дополнительных параметров безопасности) входят в него.

8. Разрешите текущему пользователю полный доступ к папке test и создайте в ней папку test2. Проверьте разрешения текущего пользователя в свойствах папки test2. Так как они были унаследованы от объекта более высокого уровня, то пользователь должен иметь к ней полный доступ.

В свойствах папки test2 поставьте галочку в графе «Запретить» напротив пункта «Запись» и попытайтесь создать в этой папке файл. Объясните полученный результат.

9. Откройте окно дополнительных параметров безопасности начальной папки test, выделите единственное заданное для неё правило и нажмите кнопку «Изменить».

В появившемся окне выберите из выпадающего меню пункт «Только для этой папки» и нажмите «ОК», а затем «Применить» (рис. 5.7).

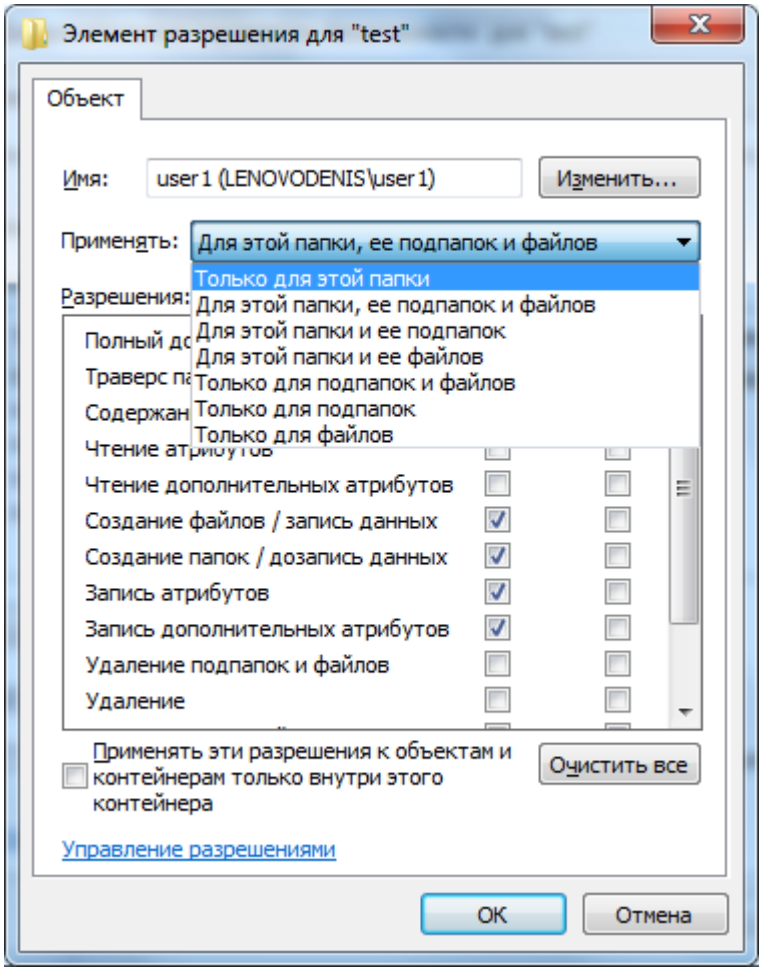

Рис. 5.7 Определение правил доступа для конкретного объекта

Попытаётесь зайти в папку test2, проверьте права доступа к ней и объясните полученный результат.

2.1 Задание для самостоятельного выполнения

1. Создайте структуру папок, изображенную на рис. 5.8:

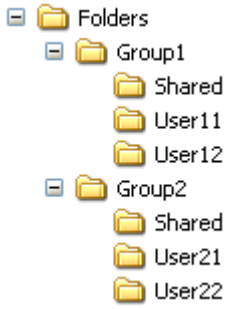

Рис. 5.8 Иерархическая структура папок

2. Создайте пользователей user11, user12, user21, user22; а также две группы: group1 и group2. Поместите пользователей user11 и user12 в группу group1, а пользователей user21 и user22 в группу group2 соответственно.

3. Задайте права доступа к папкам в соответствии со следующими требованиями:

— содержимое папки Folders может просматривать кто угодно
— никто не может создавать, удалять или изменять файлы и папки, находящиеся непосредственно в папке Folders
— просматривать содержимое папки Group1 могут только члены группы group1
— просматривать содержимое папки Group2 могут только члены группы group2
— только пользователь user11 может создавать новые папки внутри Group1 и назначать им владельцев
— только пользователь user21 может создавать новые папки внутри Group2 и назначать им владельцев
— все пользователи, входящие в группу group1, могут записывать файлы в папку Group1\Shared, но не могут их оттуда удалять
— все пользователи, входящие в группу group2, могут записывать файлы в папку Group2\Shared, но не могут их оттуда удалять
— удалить файл из папки Shared может только тот, кто его туда записал

— каждый пользователь имеет к своей папке полный доступ
— никто из пользователей не может просматривать содержимое личных папок других пользователей

3. Контрольные вопросы

1. Как получить доступ к набору прав NTFS?
2. Кто может изменять права доступа к файлу?
3. Какие существуют предопределённые права доступа?
4. Какие существуют специальные права доступа?
5. В чем заключаются приоритеты прав доступа к файлу.
6. Кто и что сможет делать с файлом или папкой, если для него не заданы никакие разрешения?
7. Что такое наследование прав доступа?

4. Требования к отчёту

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4. На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, группа, проверил: преподаватель ФИО (образец титульного листа представлен в приложении 1).

Отчёт по лабораторной работе должен содержать:

— титульный лист,
— цель работы,
— краткие теоретические сведения, ответы на контрольные вопросы;
— описание хода выполнения работы и скриншоты результатов,
— выводы.

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Факультет Информатика и вычислительная техника

Кафедра Кибербезопасность информационных систем

Лабораторная работа № ____
на тему «_____»

Выполнил обучающийся гр._____

_____
(Фамилия, Имя, Отчество)

Проверил:

_____
(должность, Фамилия, Имя, Отчество)

Ростов-на-Дону
20___