

Лабораторная работа №12

Тема: «Возможности файловой системы NTFS 5.0 по безопасности и надежности хранения данных на дисковых накопителях»

Теоретическая часть

Назначение разрешений для папок или файлов

Примечание: Работа проводится не с Виртуальной Машиной! Перед тем, как приступить к работе, создайте дополнительного пользователя. Устанавливая пользователям определенные разрешения для файлов и каталогов (папок), администраторы системы могут защищать конфиденциальную информацию от несанкционированного доступа (НСД). Каждый пользователь имеет определенный набор разрешений на доступ к конкретному объекту файловой системы. Администратор может назначить себя владельцем любого объекта файловой системы (обратная передача владения невозможна).

Разрешения пользователя на доступ к объектам файловой системы работают по принципу «аддитивности». Это значит, что действующие разрешения в отношении конкретного файла или каталога образуются из всех прямых и косвенных разрешений, назначенных пользователю для данного объекта с помощью логической функции «ИЛИ». Для назначения пользователю или группе разрешения на доступ к некоторому файлу нужно выполнить следующие действия:

1) Щелкнуть по файлу правой кнопкой мыши, выбрать в контекстном меню команду «Свойства» и в открывшемся окне перейти на вкладку «Безопасность» (рис. 1);

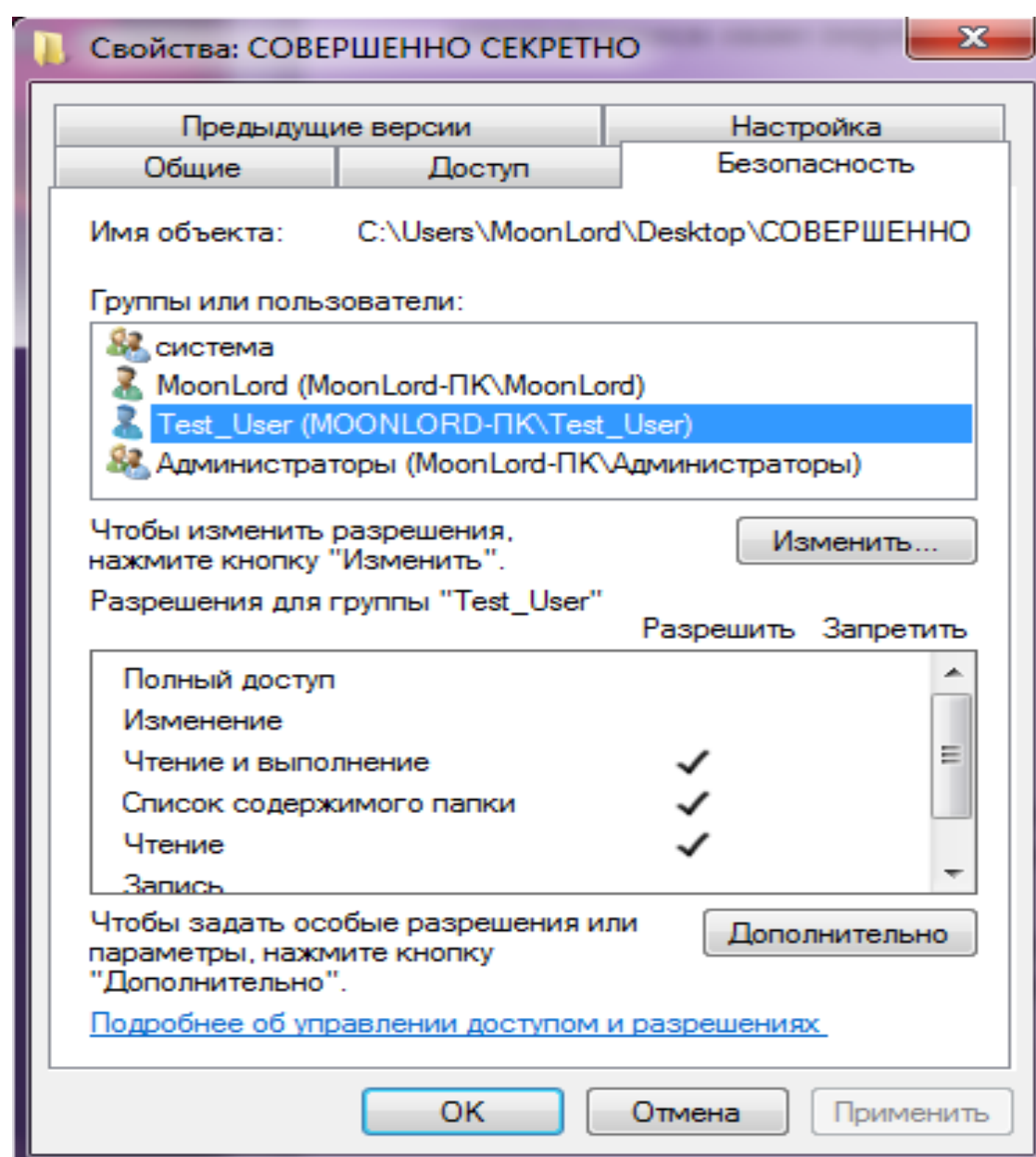


Рис. 1

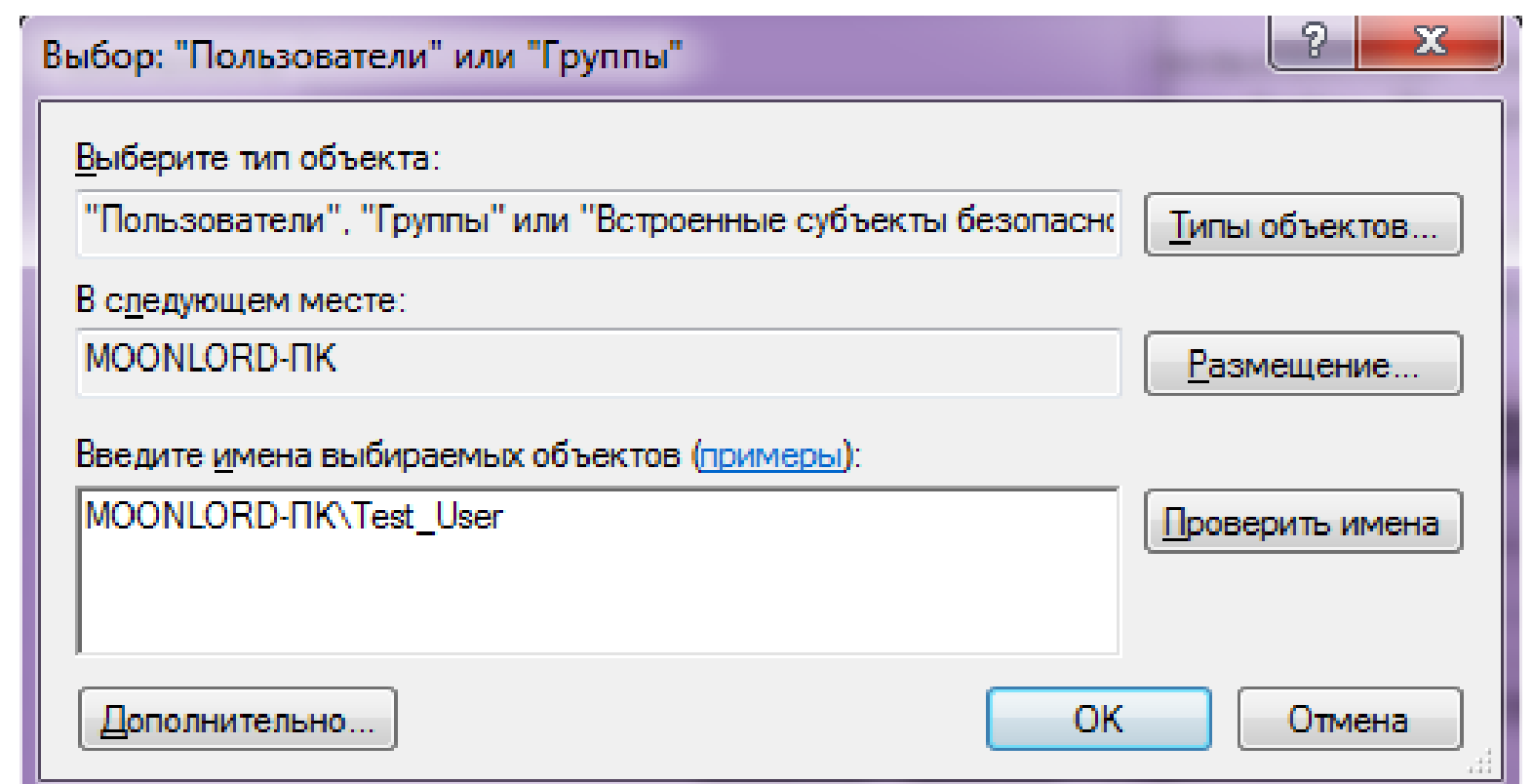


Рис. 2

2) В верхней части окна «Группы и пользователи» отображен список пользователей и групп, которым уже предоставлены разрешения для данного файла. Для добавления или удаления пользователя нужно нажать кнопку «Добавить» или «Удалить»;

3) В новом окне (рис. 2) ввести имя нужного объекта (в нашем случае пользователя – Test_User), проверить это имя, нажав кнопку «Проверить имена», нажать кнопку «Добавить», а затем «ОК», чтобы вернуться на вкладку «Безопасность»;

4) Теперь можно назначить или запретить стандартные разрешения для файлов. Если нужно назначить разрешения более детально, по видам возможных действий, то следует нажать кнопку «Дополнительно», после чего в новом окне (рис. 3) нажать кнопку «Изменить» и в появившемся окне выбрать нужные разрешения (рис. 4). Дважды нажать кнопку «ОК» (возвращаясь по окнам), а затем «Применить» и «ОК».

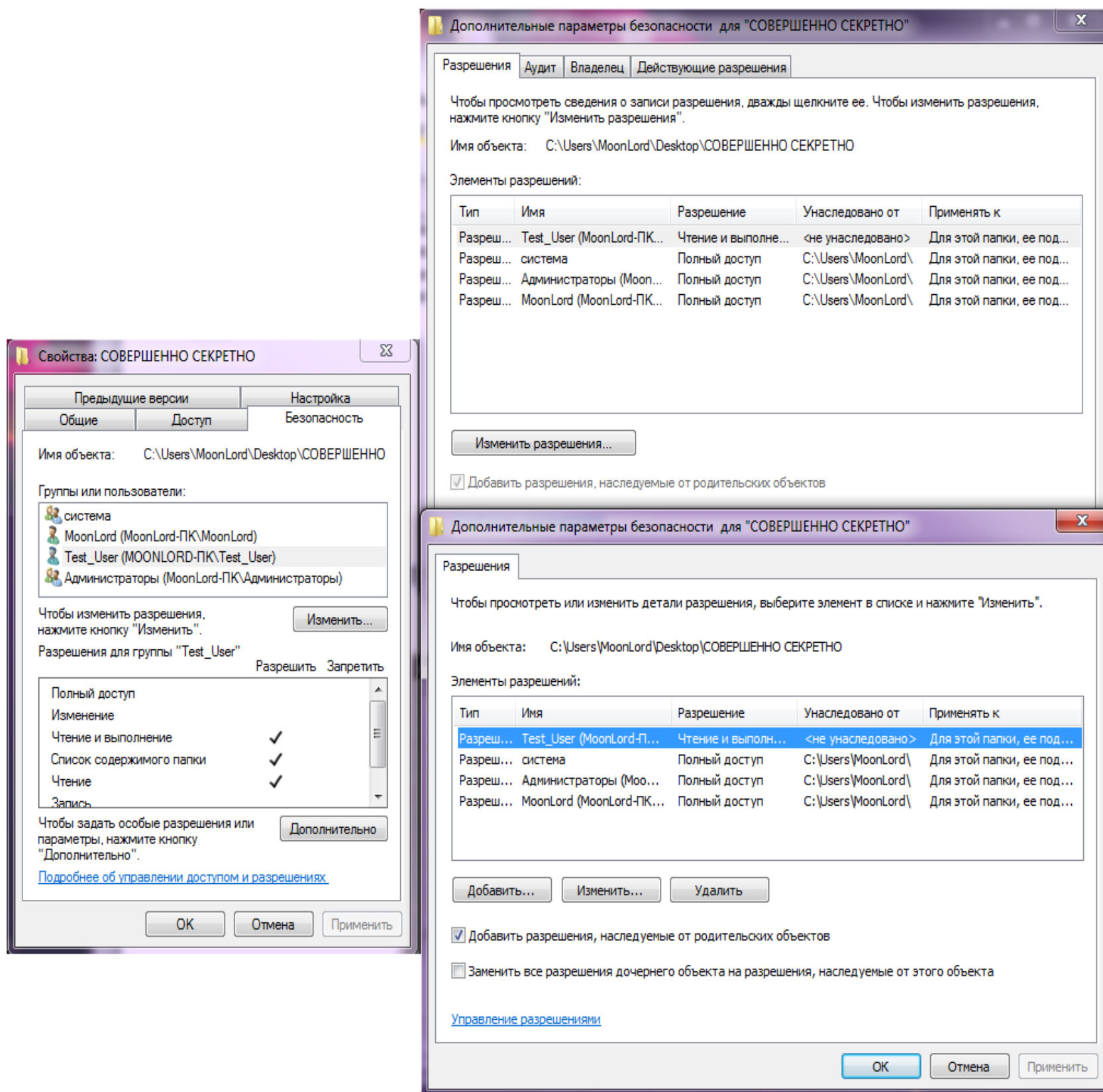


Рис. 3

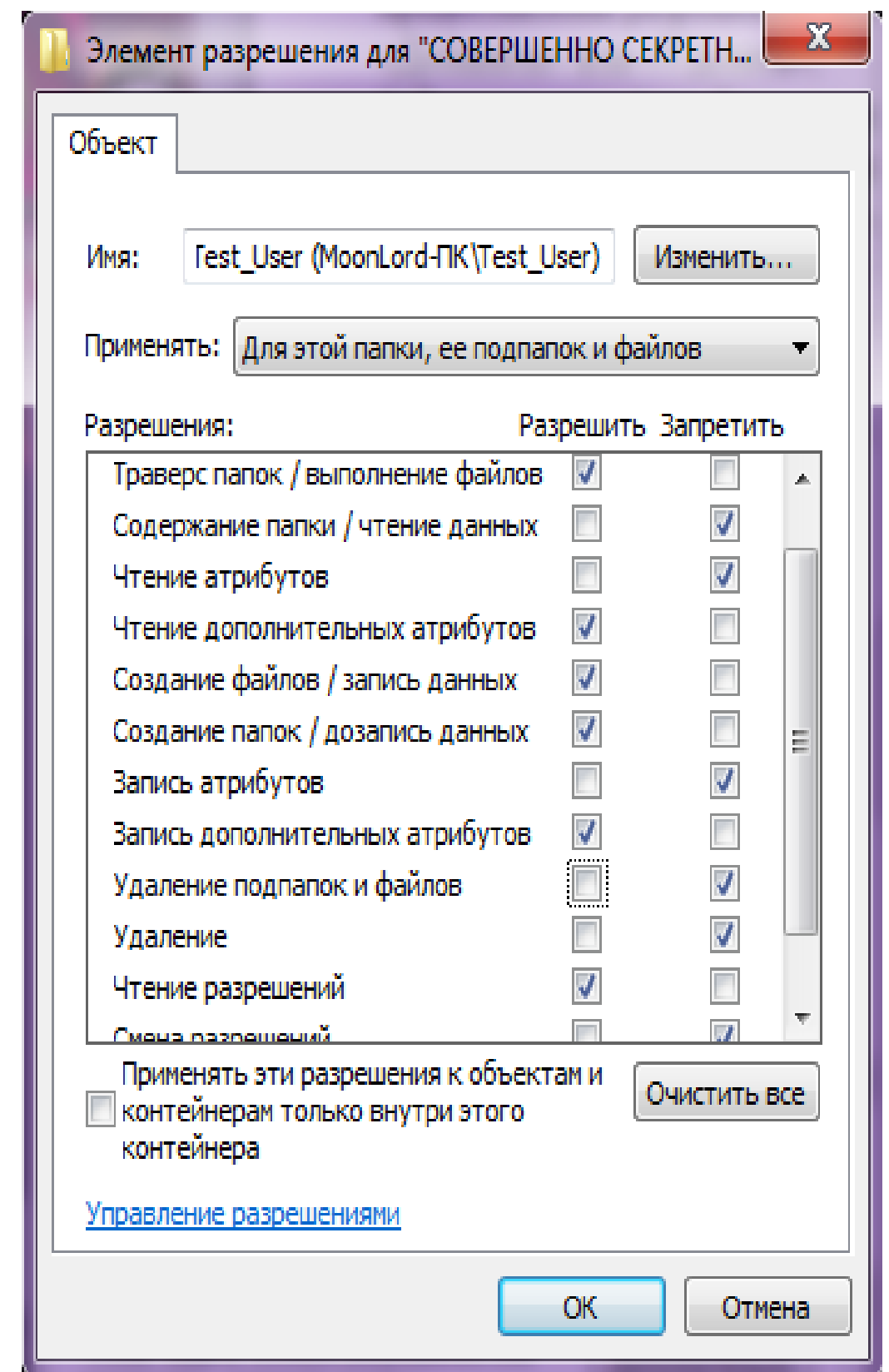


Рис. 4

Пояснение: *Траверс папок* – разрешение на «проход» сквозь вложенные папки, т.е. если у пользователя нет разрешения «Траверс папок» на папку, то пользователь, открыв папку, его содержимого не увидит. Но! К папкам, которые являются «невидимыми», но пользователь знает, что они существуют, можно получить доступ по прямой ссылке (путь к папке).

Атрибут файла – метаданные, которые описывают файл.

Смена разрешений (и чтение) – разрешение или запрет на чтение или смену разрешений к папке («Чтение», «Запись», «Удаление», «Полный доступ»).

Следует иметь в виду, что если для пользователя установлен запрет на «Удаление», то файлы, находящиеся внутри папок, удалить все равно можно, если у пользователя установлено разрешение «Удаление подпапок и файлов».

Практическая часть Передача права владения

Пользователь может назначить себя владельцем какого-либо объекта файловой системы, если у него есть необходимые права. Для передачи владения или просмотра текущего владельца файла (папки), нужно открыть окно «Свойства», перейти на вкладку «Безопасность» и нажать кнопку «Дополнительно». В появившемся окне перейти на вкладку «Владелец». Текущий владелец виден в поле «Текущий владелец» этого элемента (нашего дополнительного пользователя необходимо добавить в список «Другие пользователи и группы...»). Провести те же действия, как на рис. 2). В списке «Изменить...» перечислены пользователи, имеющие право получения владения данным объектом. Нужно выбрать нужного пользователя и нажать кнопку «Применить» и затем «ОК» (рис. 5).

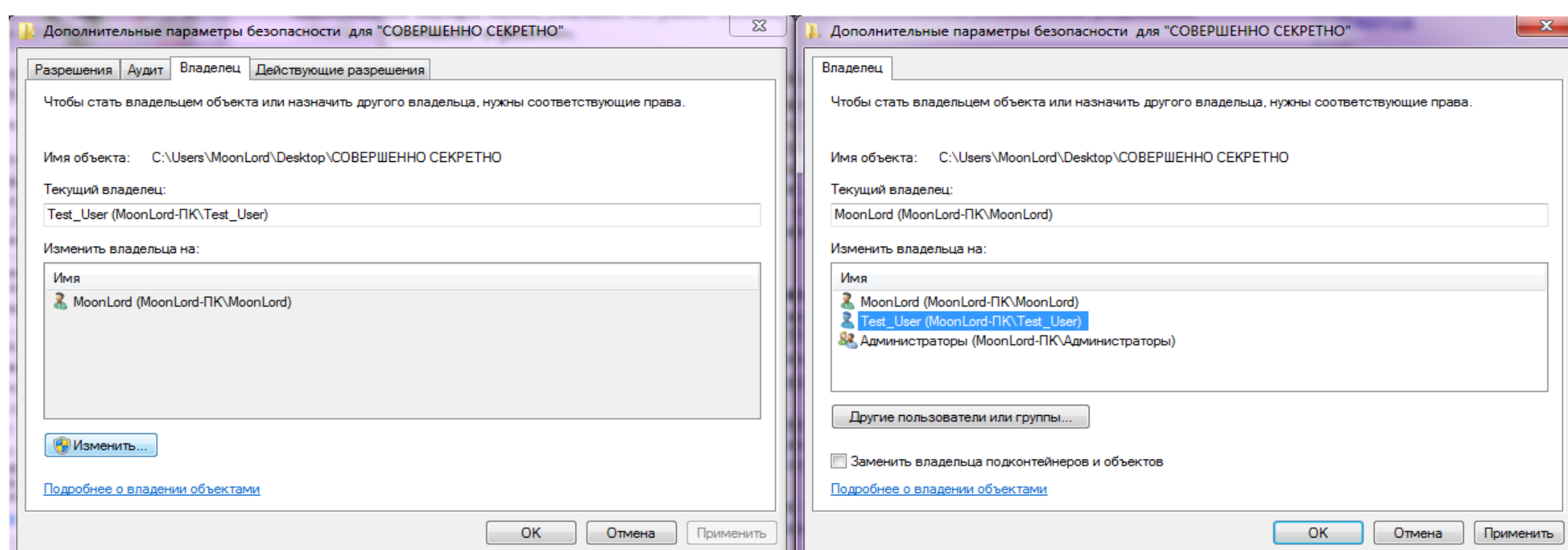


Рис. 5

Точки соединения NTFS

Точки соединения (аналог монтирования в UNIX) позволяют отображать целевую папку (диск) в пустую папку, находящуюся в пространстве имен файловой системы NTFS 5.0 локального компьютера. Целевой папкой может служить любой допустимый путь Windows 2000. Точки соединений (поддерживаются только в NTFS 5.0) прозрачны для приложений, это означает, что приложение или пользователь, осуществляющий доступ к локальной папке NTFS, автоматически перенаправляется к другой папке.

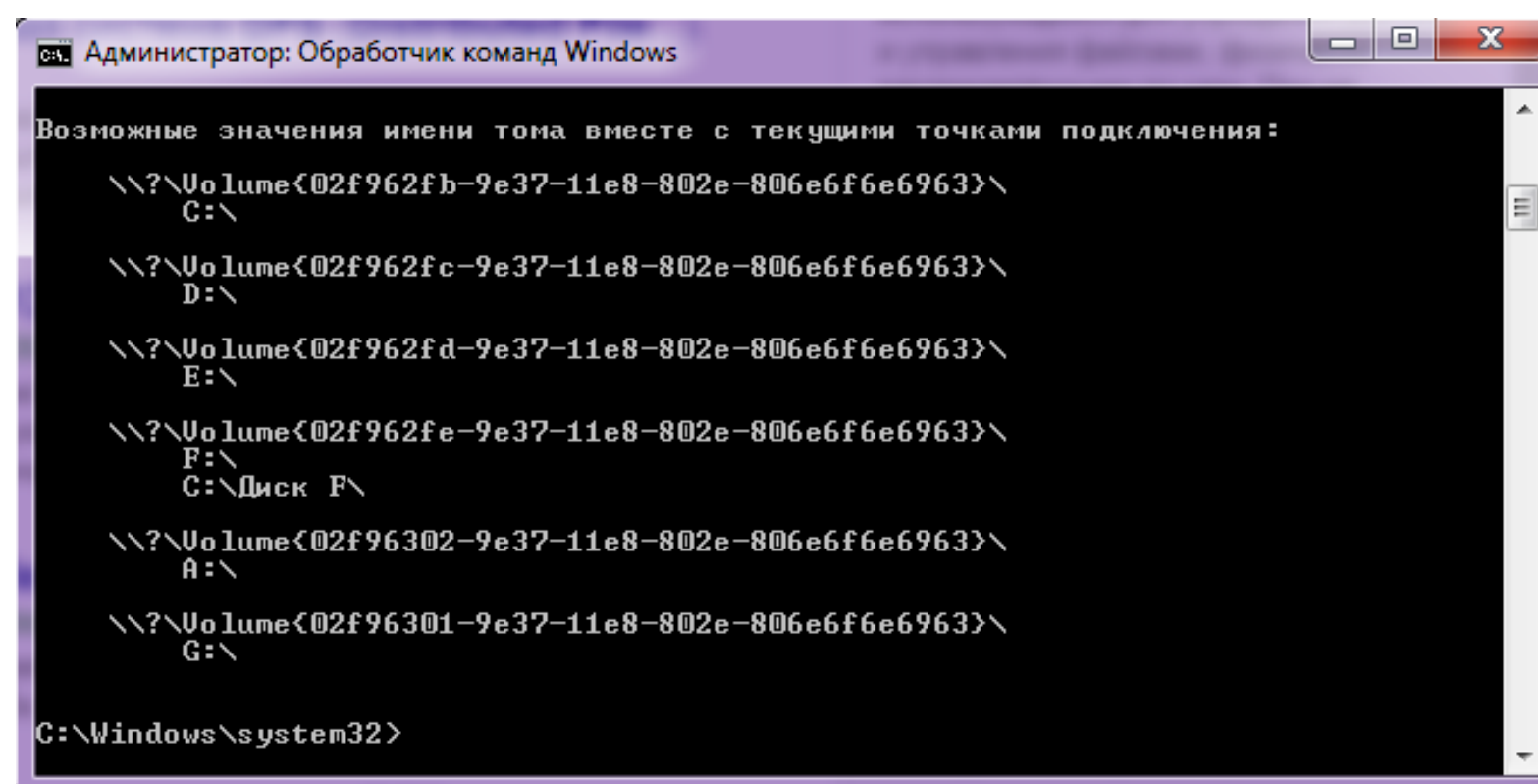
Точки соединения NTFS (New Technology File System – стандартная файловая система для семейства операционных системы Windows, которая поддерживает хранение метаданных) отличаются от точек соединения распределенной файловой системы DFS (Distributed File System – компонент Microsoft Windows: используется для упрощения доступа к файлам и их управления). Точки соединения DFS отображают общий ресурс сети, управляемый DFS. Таким ресурсом может быть любой допустимый общий ресурс сети. Однако оба средства служат для создания общего пространства имен хранения информации.

Для работы с точками соединения на уровне томов можно использовать стандартные средства системы — утилиту «Mountvol.exe» (вызов из командной строки) и оснастку «Управление дисками».

С помощью утилиты «Mountvol» можно выполнить следующие действия:

- ❖ Отобразить корневую папку локального тома в некоторую целевую папку NTFS, т.е. подключить или монтировать том;
- ❖ Вывести на экран информацию о целевой папке точки соединения NTFS, использованной при подключении тома;
- ❖ Просмотреть список доступных для использования томов файловой системы;
- ❖ Уничтожить точки подключения томов.

Параметры утилиты Mountvol можно получить, введя в командной строке ее имя (рис. 6).

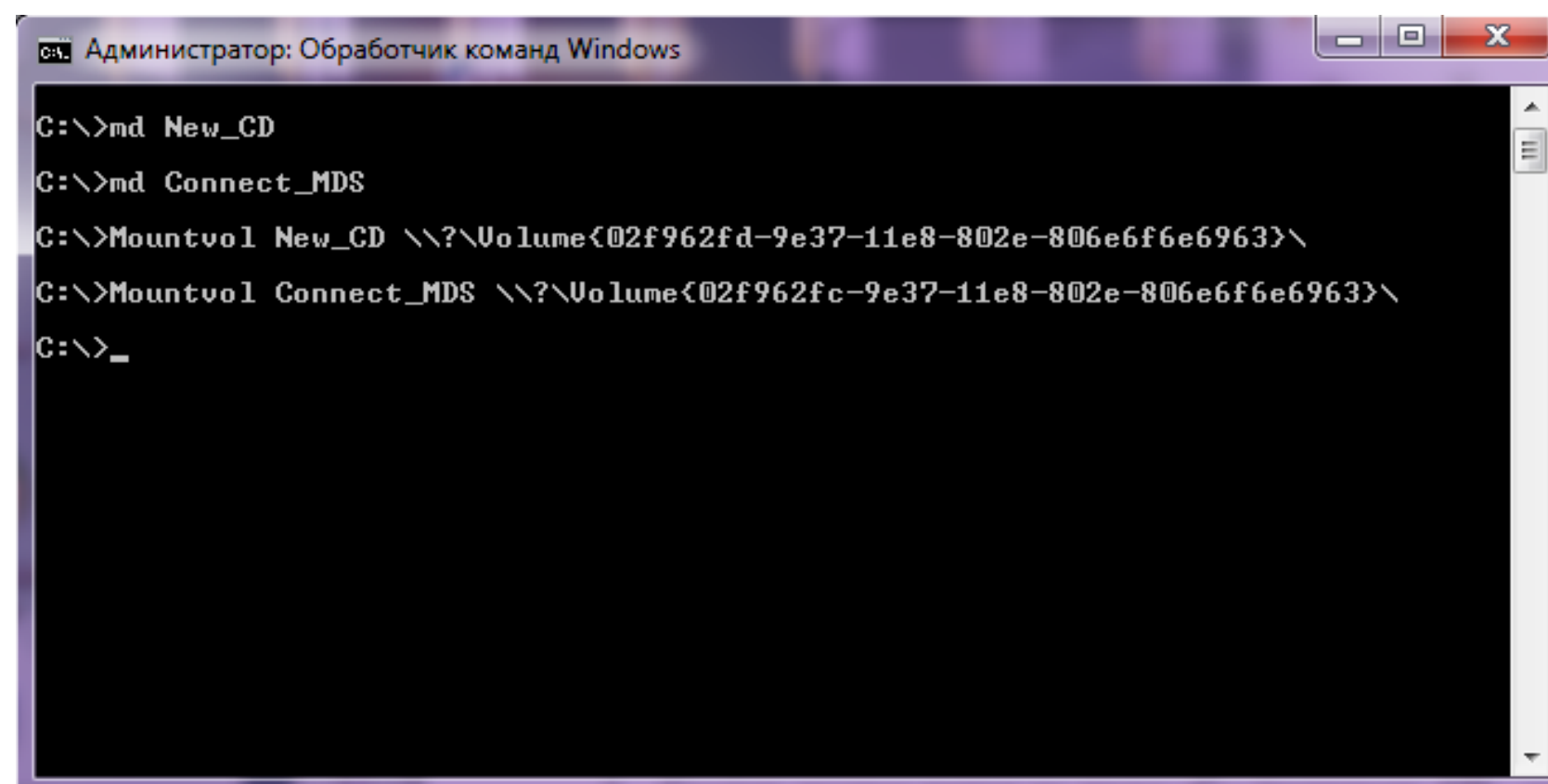


```
Администратор: Обработчик команд Windows
Возможные значения имени тома вместе с текущими точками подключения:
\\?\Volume{02f962fb-9e37-11e8-802e-806e6f6e6963}\
C:\
\\?\Volume{02f962fc-9e37-11e8-802e-806e6f6e6963}\
D:\
\\?\Volume{02f962fd-9e37-11e8-802e-806e6f6e6963}\
E:\
\\?\Volume{02f962fe-9e37-11e8-802e-806e6f6e6963}\
F:\
C:\Диск F\
\\?\Volume{02f96302-9e37-11e8-802e-806e6f6e6963}\
A:\
\\?\Volume{02f96301-9e37-11e8-802e-806e6f6e6963}\
G:\
C:\Windows\system32>
```

Рис. 6

Пусть на компьютере установлено два тома (C: и D:), флэш-память (F:) и устройство CD-ROM (E:). Том «C:» отформатирован под NTFS 5.0, поэтому на нем можно расположить несколько точек соединения. Для монтирования некоторого тома нужно выполнить следующие действия:

1. В окне командной строки запустить утилиту Mountvol и просмотреть список имен устройств компьютера (см. рис. 6);
2. Создать пустые папки на диске «C:» (например, CD - для подключения устройства CD-ROM и MoreDisrSpace — для подключения MoreDisrSpace диска «D:»), как это показано на рис. 7. С помощью утилиты Mountvol подключить подключение диска D: и CD-ROM'а выглядит следующим образом:



```
Администратор: Обработчик команд Windows
C:\>md New_CD
C:\>md Connect_MDS
C:\>Mountvol New_CD \\?\Volume{02f962fd-9e37-11e8-802e-806e6f6e6963}\
C:\>Mountvol Connect_MDS \\?\Volume{02f962fc-9e37-11e8-802e-806e6f6e6963}\
C:\>_.
```

Рис. 7

3. Открыв папку «Мой компьютер», можно увидеть папки «CD» и «MoreDisrSpace» в корневом каталоге диска «C:», которыми можно пользоваться точно так же, как ранее дисками «E:» и «D:» (рис. 8);

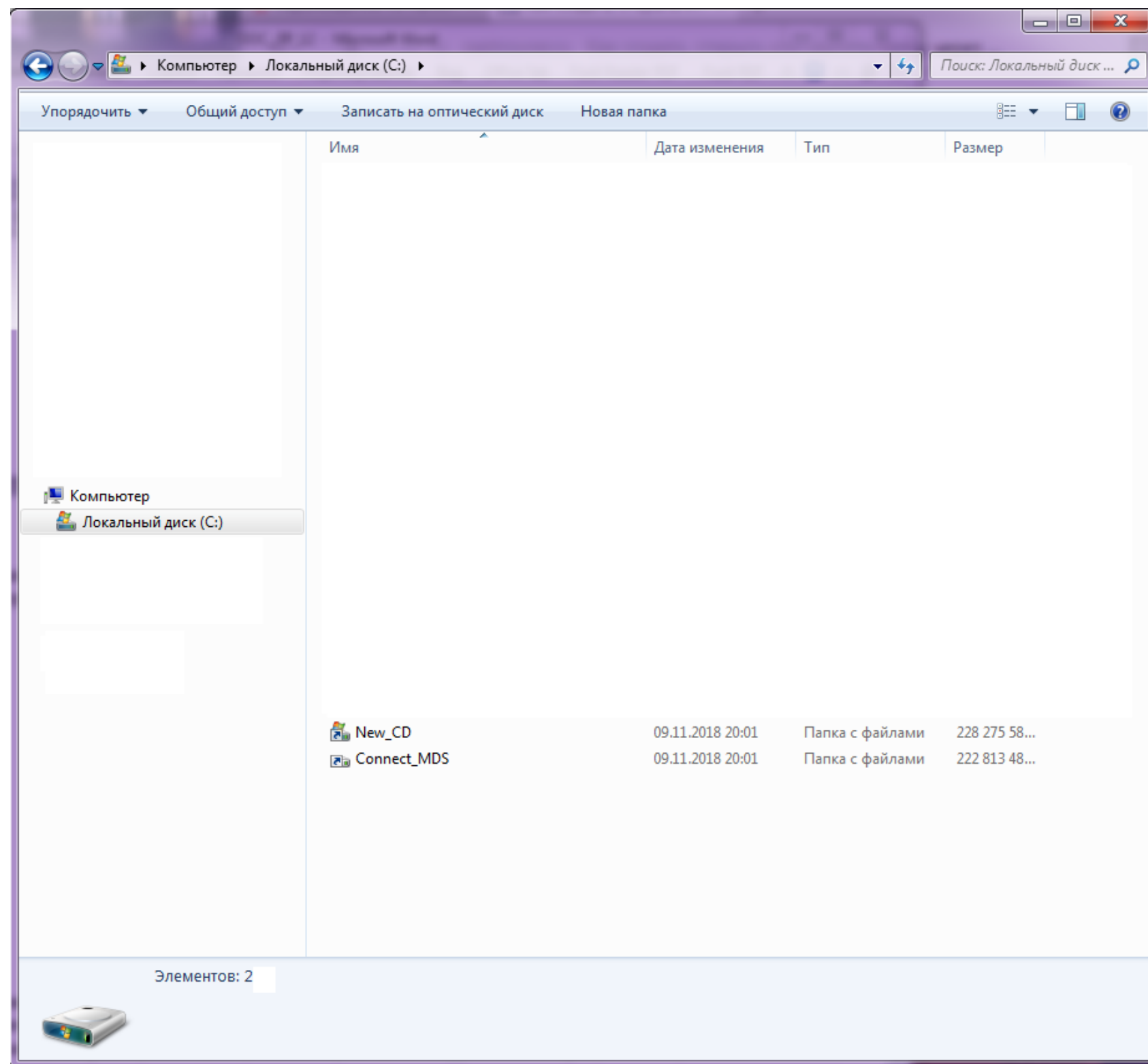


Рис. 8

Оснастка «Управление дисками» позволяет создать точки соединения для дисков компьютера. В качестве примера рассмотрим подключение съемного диска с файловой системой FAT. Для этого нужно запустить оснастку «Управление дисками», выбрать нужный диск (в нашем случае диск «F:») и нажать правую кнопку мыши. В контекстном меню выбрать команду «Изменение буквы и пути диска» (рис. 9). В открывшемся окне нажать кнопку «Добавить». Откроется окно диалога «Добавление новой буквы диска или пути диска». Нажать кнопку «Обзор» и в новом окне выбрать диск («Точку соединения»), например «C:». Нажать кнопку «Создать папку» и ввести ее имя, например «Новый Диск F», вместо слов «Новая папка». Нажать «ОК» (рис. 10). Все окна диалога закроются, кроме оснастки «Управление компьютером». Если теперь открыть окно «Мой компьютер», то в корневом каталоге можно увидеть папку «Новый Диск F» (т.е. в диске «C:»).

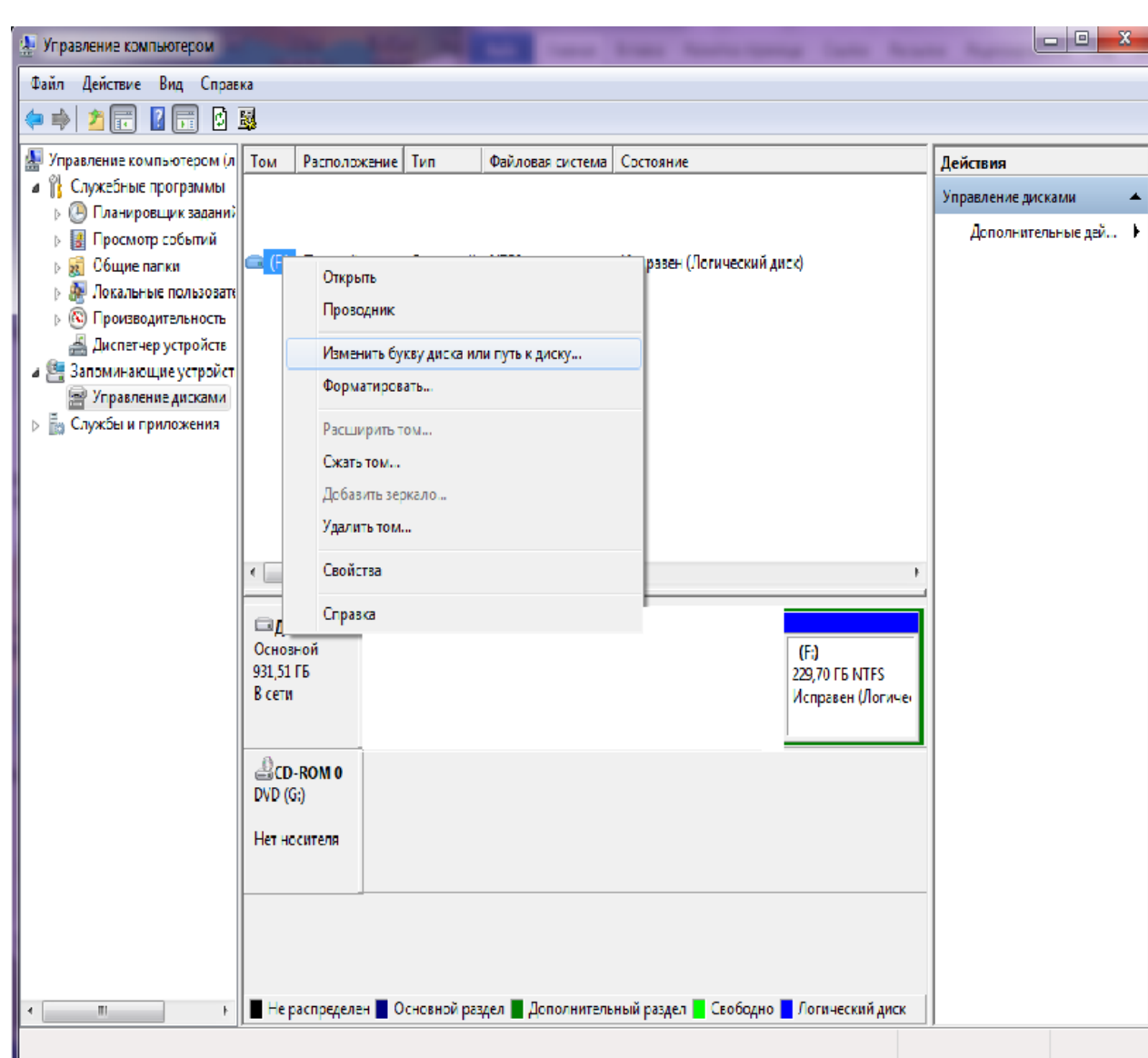


Рис. 9

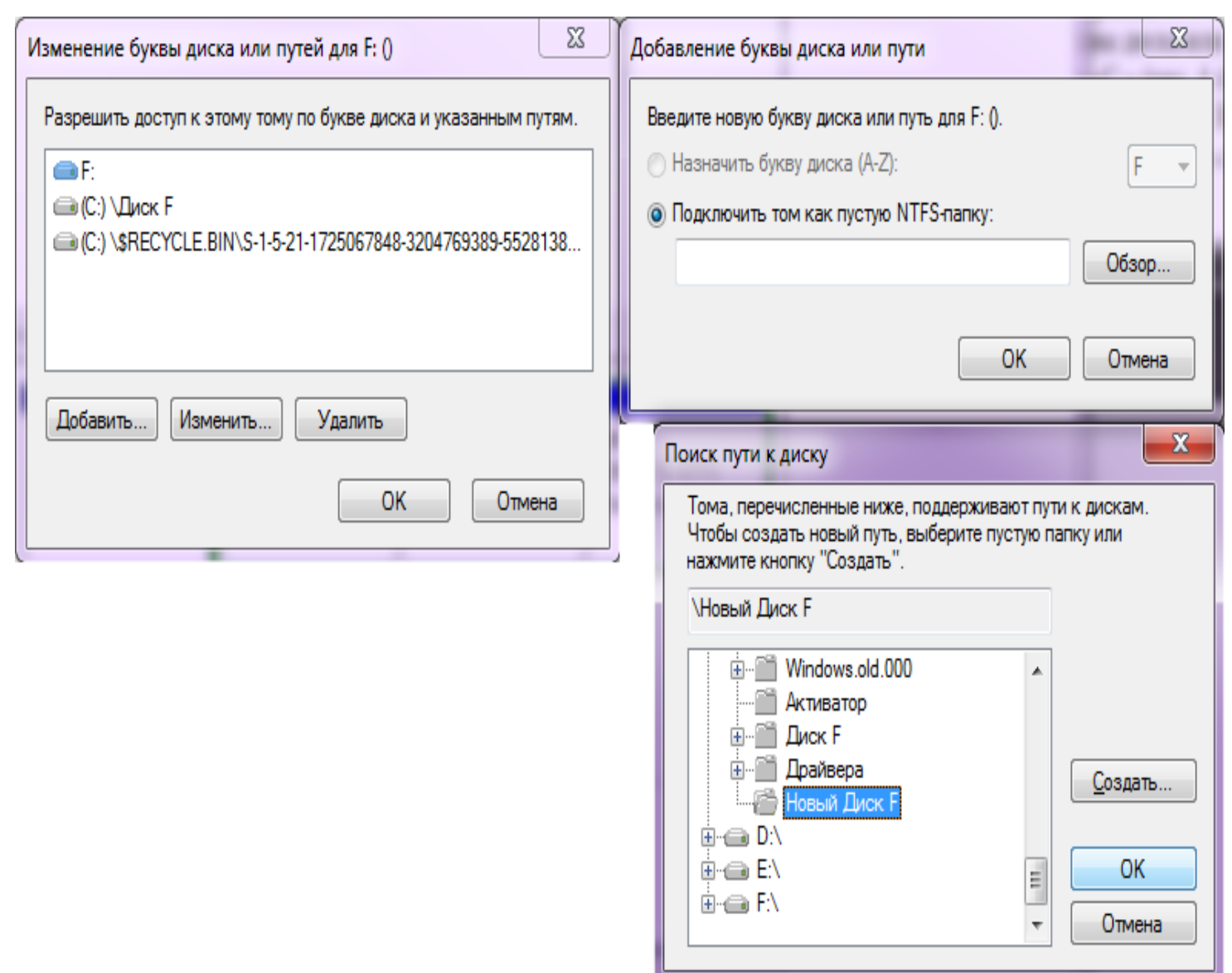


Рис. 10

Для удаления точки соединения запустить оснастку «Управление дисками», указать нужный том файловой системы и нажать правую кнопку мыши. Выбрать команду «Изменить буквы диска и пути диска». В открывшемся окне выбрать нужный путь и нажать кнопку «Удалить».

Шифрующая файловая система EFS

Поскольку шифрование и дешифрование выполняются автоматически, пользователь может работать с файлом так же, как и до установки его криптозащиты. Все остальные пользователи, которые попытаются получить доступ к зашифрованному файлу, получают сообщение об ошибке доступа, поскольку они не владеют необходимым личным ключом, позволяющим им расшифровать файл.

Шифрование информации задается в окне свойств файла или папки. В окне свойств файла на вкладке «Общие» (ПКМ по папке – «Свойства») нужно нажать кнопку «Другие». Появится окно диалога «Дополнительные атрибуты». В группе «Атрибуты сжатия и шифрования» установить флажок «Шифровать содержимое для защиты данных» и нажать кнопку «ОК» (рис. 11).

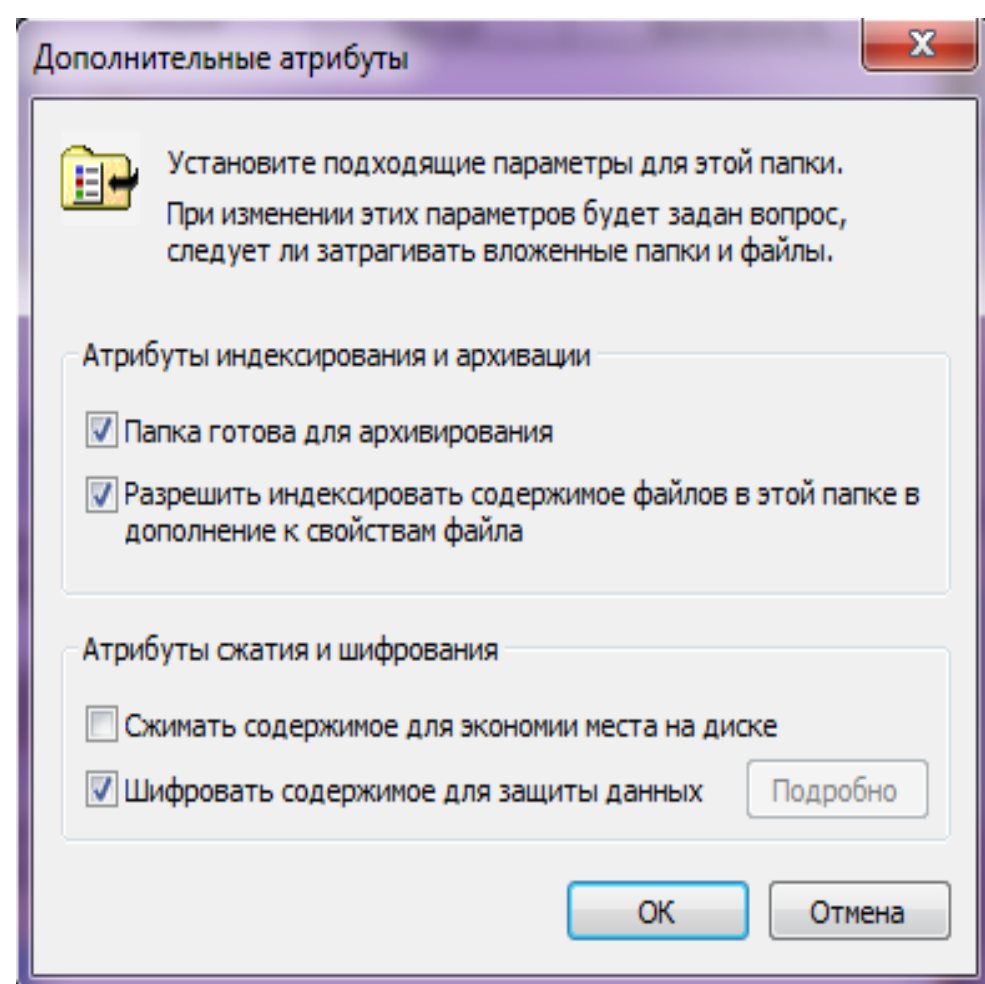


Рис. 11

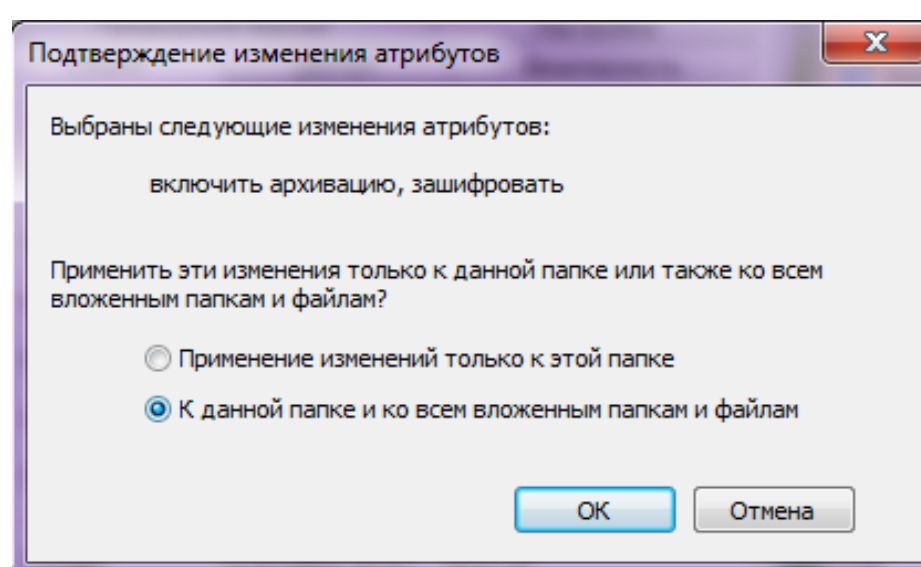


Рис. 12

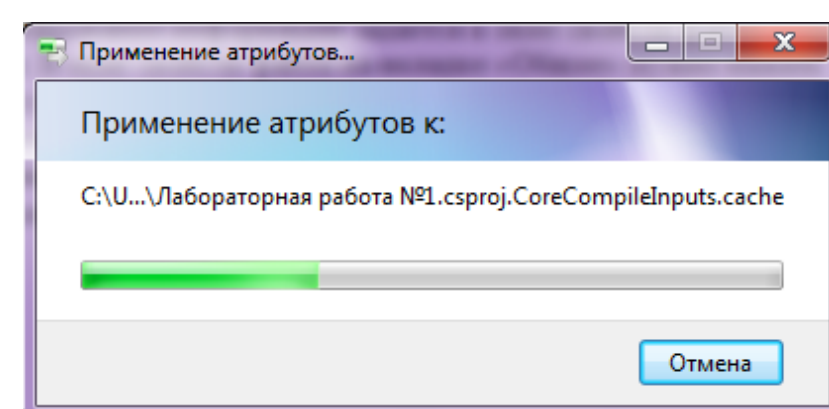


Рис. 13

Появится окно (рис. 12), в котором надо указать режим шифрования. При шифровании папки можно указать следующие режимы применения нового атрибута: «Применение изменений только к этой папке» или «К этой папке и ко всем вложенным папкам и файлам» (рис. 12). Нажать кнопку «ОК». Начнет процесс применения атрибутов (рис. 13). Для дешифрования файла или папки на вкладке «Общие» окна свойств соответствующего объекта нажать кнопку «Другие», и в открывшемся окне сбросить флажок «Шифровать содержимое для защиты данных».

В процессе шифрования файлов и папок система **EncryptingFileSystem (EFS)** – шифрованная файловая система – реализует шифрование на уровне файлов в ОС семейства Windows) формирует специальные атрибуты (**DataDecryptionField** - поле дешифрования данных), содержащие список зашифрованных ключей (**FEK - FileEncryptionKey**), что позволяет организовать доступ к файлу со стороны нескольких пользователей. Для шифрования файла FEK используется открытая часть пары ключей каждого пользователя. Информация, требуемая для дешифрования, привязывается к самому файлу. Секретная часть ключа пользователя используется при дешифровании FEK. Она хранится в безопасном месте, например на смарт-карте или в устройстве высокой степени защищенности.

Файл FEK применяется для создания ключей восстановления, которые хранятся в другом специальном атрибуте - «Поле восстановления данных» (**DataRecoveryField - DRF**). Сама процедура восстановления выполняется довольно редко (при уходе пользователя из организации или забывании секретной части ключа).

Система EFS имеет встроенные средства восстановления зашифрованных данных в условиях, когда неизвестен личный ключ пользователя. Пользователи, которые могут восстанавливать зашифрованные данные в условиях утраты личного ключа, называются «агентами восстановления данных». Они обладают сертификатом (X.509 v.3) на восстановление данных и личным ключом, с помощью которого выполняется операция восстановления зашифрованных данных.

Контрольные вопросы

1. Что такое NTFS? Что такое DFS?
2. Опишите основные преимущества файловой системы NTFS.
3. Расскажите о точках соединения.
4. Подумайте, что представляет собой устройство MoreDisrSpace?

Содержание отчета

В отчет о выполненной работе включить следующие материалы:

1. Тему и цель работы.
2. Результаты выполнения заданий: исследуемые схемы, полученные таблицы переходов.
3. Анализ полученных результатов.

4. Ответы на контрольные вопросы.
5. Выводы по работе.