

Лабораторная работа № 1

Тема: Использование приёмов работы с файловой системой NTFS. Назначение разрешений доступа к файлам и папкам.

Цель: *Научиться устанавливать разрешения NTFS для файлов и для папок для отдельных пользователей и групп в операционной системе Windows (XP,7,8), а также устранять проблемы доступа к ресурсам.*

Содержание работы и последовательность ее выполнения

1. Теоретические сведения

Общие сведения об использовании разрешений NTFS

Разрешения NTFS позволяют явно указать, какие пользователи и группы имеют доступ к файлам и папкам и какие операции с содержимым этих файлов или папок им разрешено выполнять. Разрешения NTFS применимы только к томам, отформатированным с использованием файловой системы NTFS. Они не предусмотрены для томов, использующих файловые системы FAT или FAT32. Система безопасности NTFS эффективна независимо от того, обращается ли пользователь к файлу или папке, размещенным на локальном компьютере или в сети.

Разрешения, устанавливаемые для папок, отличаются от разрешений, устанавливаемых для файлов. Администраторы, владельцы файлов или папок и пользователи с разрешением «Полный доступ» имеют право назначать разрешения NTFS пользователям и группам для управления доступом к этим файлам и папкам.

Список управления доступом

В NTFS хранится **список управления доступом** (access control list -**ACL**) для каждого файла и папки на томе NTFS. В этом списке перечислены пользователи и группы, для которых установлены разрешения для файла или папки, а также сами назначенные разрешения. Чтобы пользователь получил доступ к ресурсу, в ACL должна быть запись, называемая **элемент списка управления доступом** (access control entry - **ACE**) для этого пользователя или группы, к которой он принадлежит. Эта запись назначит запрашиваемый тип доступа (например, **Чтение**) пользователю. Если в ACL нет соответствующей ACE, то пользователь не получит доступ к ресурсу.

Множественные разрешения NTFS

Вы можете установить несколько разрешений пользователю и всем группам, членом которых он является. Для этого вы должны иметь представление о правилах и приоритетах, по которым в NTFS назначаются и объединяются множественные разрешения и о наследовании разрешений NTFS.

Эффективные разрешения. Эффективные разрешения пользователя для ресурса - это совокупность разрешений NTFS, которые вы назначаете отдельному пользователю и всем группам, к которым он принадлежит. Если у пользователя есть разрешение «Чтение» для папки, и он входит в группу, у которой есть разрешение «Запись» для той же папки, значит, у этого пользователя есть оба разрешения.

Установка разрешений NTFS и особых разрешений

Вы должны руководствоваться определенными принципами при установке разрешений NTFS. Устанавливайте разрешения согласно потребностям групп и пользователей, что включает в себя *разрешение или предотвращение наследования* разрешений родительской папки подпапками и файлами, содержащимися в родительской папке.

Если вы уделите немного времени на планирование ваших разрешений NTFS и будете соблюдать при планировании несколько принципов, то обнаружите, что разрешениями легко управлять.

- Для упрощения процесса администрирования сгруппируйте файлы по папкам следующих типов: папки с приложениями, папки с данными, личные папки. Централизуйте общедоступные и личные папки на отдельном томе, не содержащем файлов операционной системы и других приложений. Действуя таким образом, вы получите следующие преимущества:

- сможете устанавливать разрешения только папкам, а не отдельным файлам;
- упростите процесс резервного копирования, так как вам не придется делать резервные копии файлов приложений, а все общедоступные и личные папки находятся в одном месте.

- Устанавливайте для пользователей только необходимый уровень доступа. Если необходимо чтение файла, установите пользователю разрешение Чтение для этого файла. Это уменьшит вероятность случайного изменения файла или удаления важных документов и файлов приложений пользователем.

- Создавайте группы согласно необходимому членам группы типу доступа, затем установите соответствующие разрешения для группы. Назначайте разрешения отдельным пользователям только в тех случаях, когда это необходимо.

- При установке разрешений для работы с данными или файлами приложений установите разрешение Чтение и выполнение для групп **Пользователи** и **Администраторы**. Это предотвратит случайное удаление файлов приложений или их повреждение вирусами или пользователями.

- При установке разрешений для папок с общими данными назначьте разрешения Чтение и выполнение и Запись группе Пользователи и разрешение Полный доступ для группы Создатель-владелец. По умолчанию пользователь, создавший документ, также является его владельцем. Владелец файла может дать другому пользователю разрешение на владение файлом. Пользователь, который принимает такие права, в этом случае становится владельцем файла. Если вы установите разрешение Чтение и выполнение и Запись группе Пользователи и разрешение Полный доступ группе Создатель-владелец, то пользователи получат возможность читать и изменять документы, созданные другими пользователями, а также читать, изменять и удалять файлы и папки, создаваемые ими.

- Запрещайте разрешения, только если необходимо запретить отдельный тип доступа определенному пользователю или группе.

- Поощряйте пользователей в установке разрешений для файлов и папок, которые они создают, и научите их это делать самостоятельно.

Администраторы, пользователи с разрешением Полный доступ и владельцы файлов и папок могут устанавливать разрешения для отдельных пользователей и групп.

Можно получить доступ к дополнительным возможностям поиска, включая возможность поиска удаленных учетных записей пользователей, учетных записей с неустаревшими паролями и учетных записей, по которым не подключались определенное количество дней.

Назначение или запрещение особых разрешений

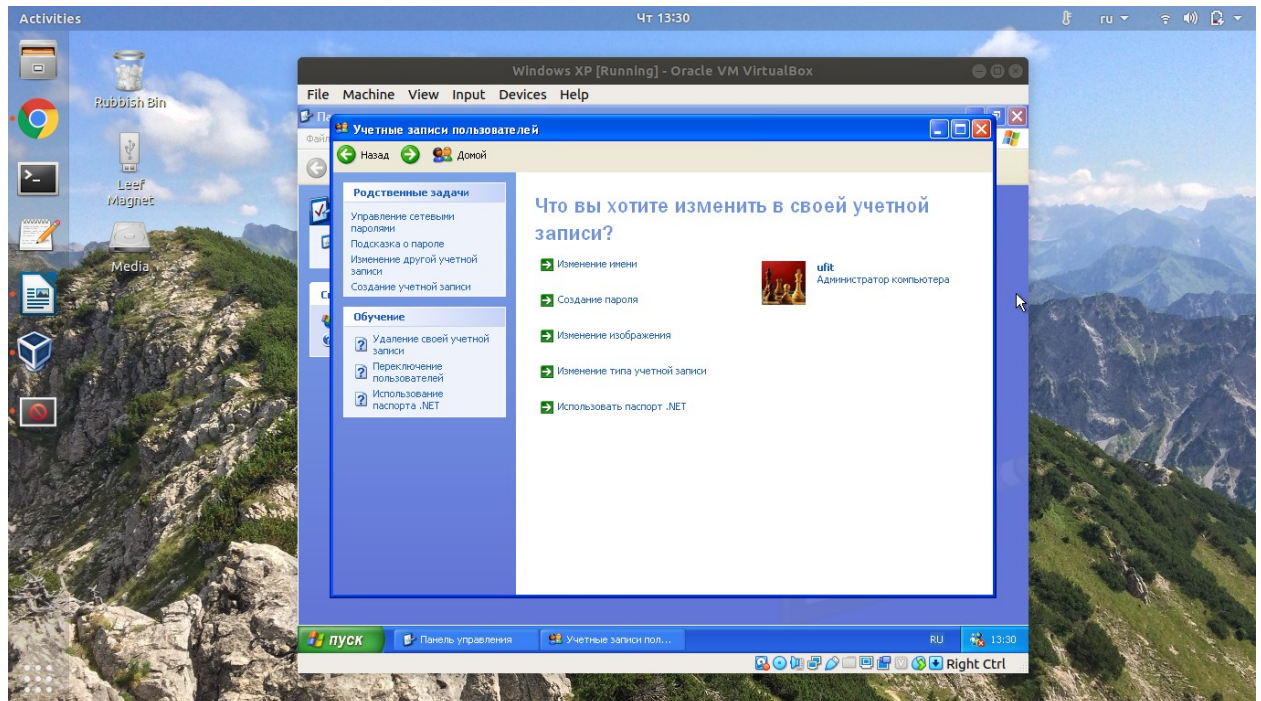
Щелкните кнопку **Дополнительно**, чтобы открыть диалоговое окно **Дополнительные параметры безопасности**, где перечислены группы и пользователи и установленные для них разрешения для этого объекта. В поле **Элементы разрешений** также указано, от какого объекта разрешения унаследованы и к каким объектам применимы. Вы можете воспользоваться диалоговым окном **Дополнительные параметры безопасности** для изменения разрешений, установленных для пользователя или группы. Для изменения разрешений, установленных для пользователя или группы, выделите пользователя и щелкните кнопку **Изменить**. Откроется диалоговое окно **Элемент разрешения для**. Затем выделите или отмените определенные разрешения, которые вы хотите изменить.

2. Задание для самостоятельной работы

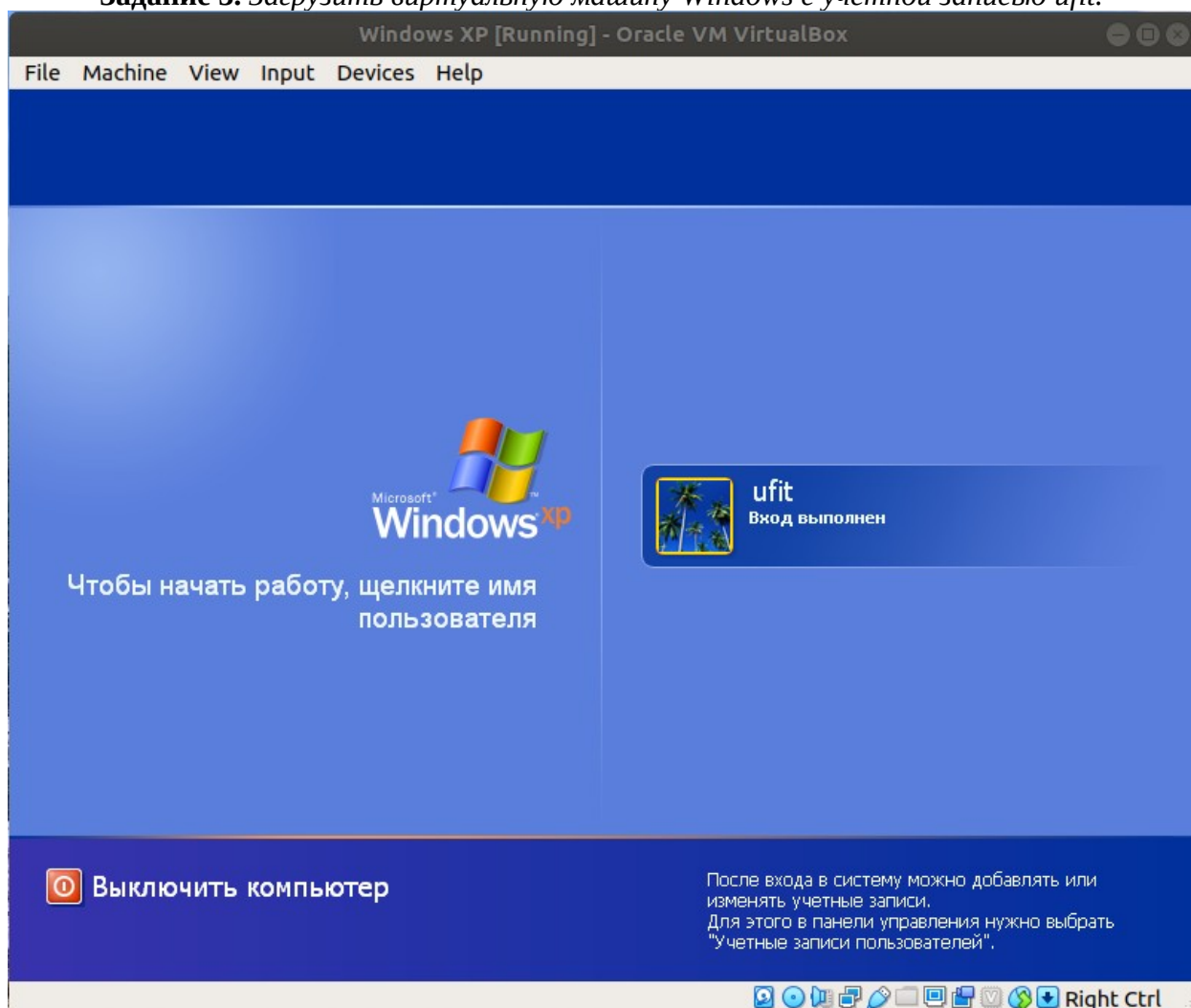
Задание 1. Открыть Sun Virtual Box.



Задание 2. Загрузить виртуальную машину Windows (XP или 7,8) и создать новую учетную запись ufit (с правами администратора).



Задание 3. Загрузить виртуальную машину Windows с учетной записью ufit.



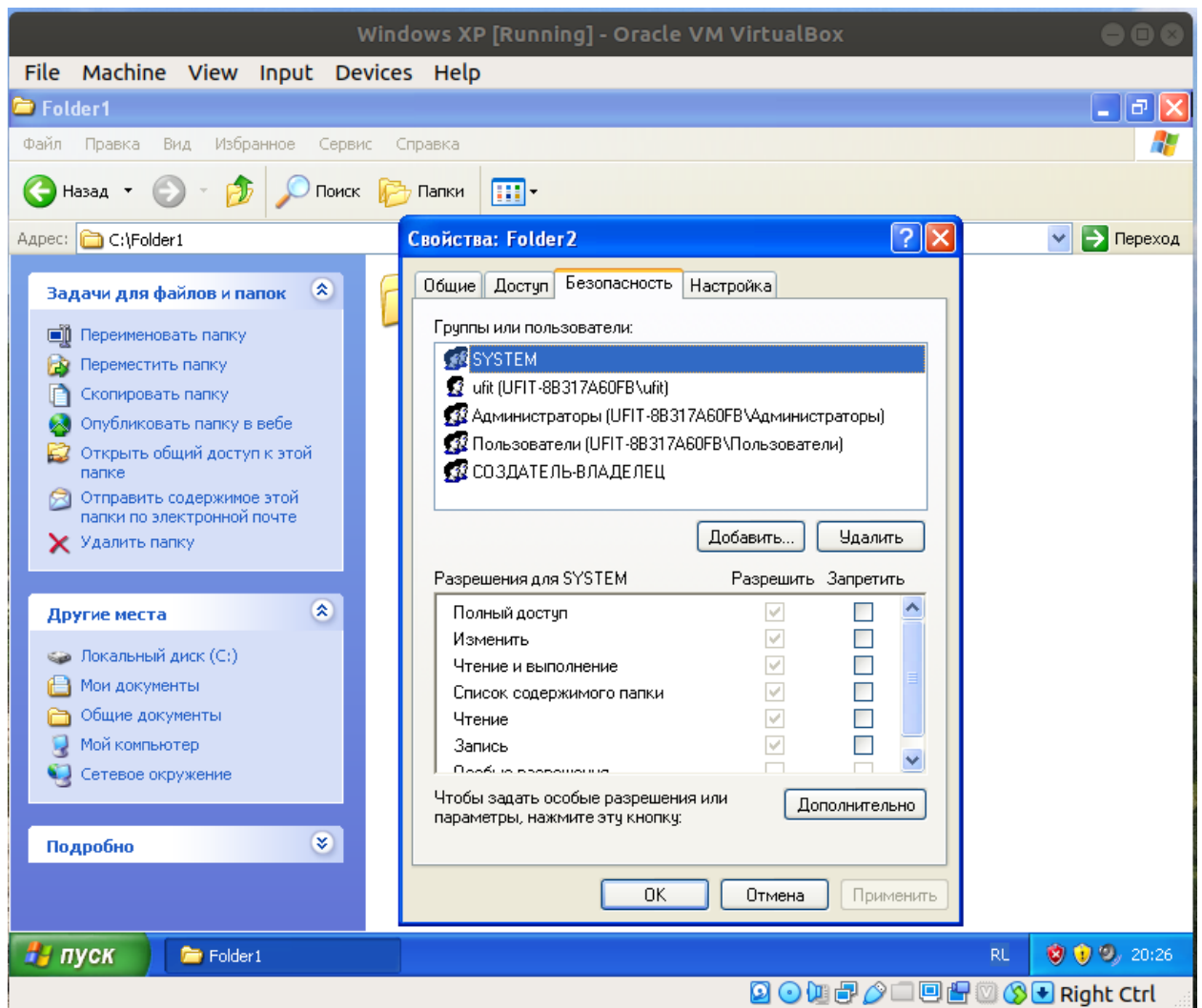
Задание 4. Определение разрешений NTFS по умолчанию для только что созданной папки.

Запустить **Проводник**, создать папки **C:\FoIder1** и **C:\FoIder1\Folder2**. Просмотреть разрешения, установленные для созданных папок, щелкнув по вкладке **Безопасность** диалогового окна свойств папки. Обратит внимание на наследование разрешений папкой **Folder2** от родительской папки **Folder 1**.

Если на экране не видна вкладка **Безопасность**, вам следует уточнить два вопроса:

1) Раздел вашего диска отформатирован как NTFS или как FAT? Только на разделах NTFS используются разрешения NTFS, и, таким образом, только на разделах NTFS видна вкладка **Безопасность**.

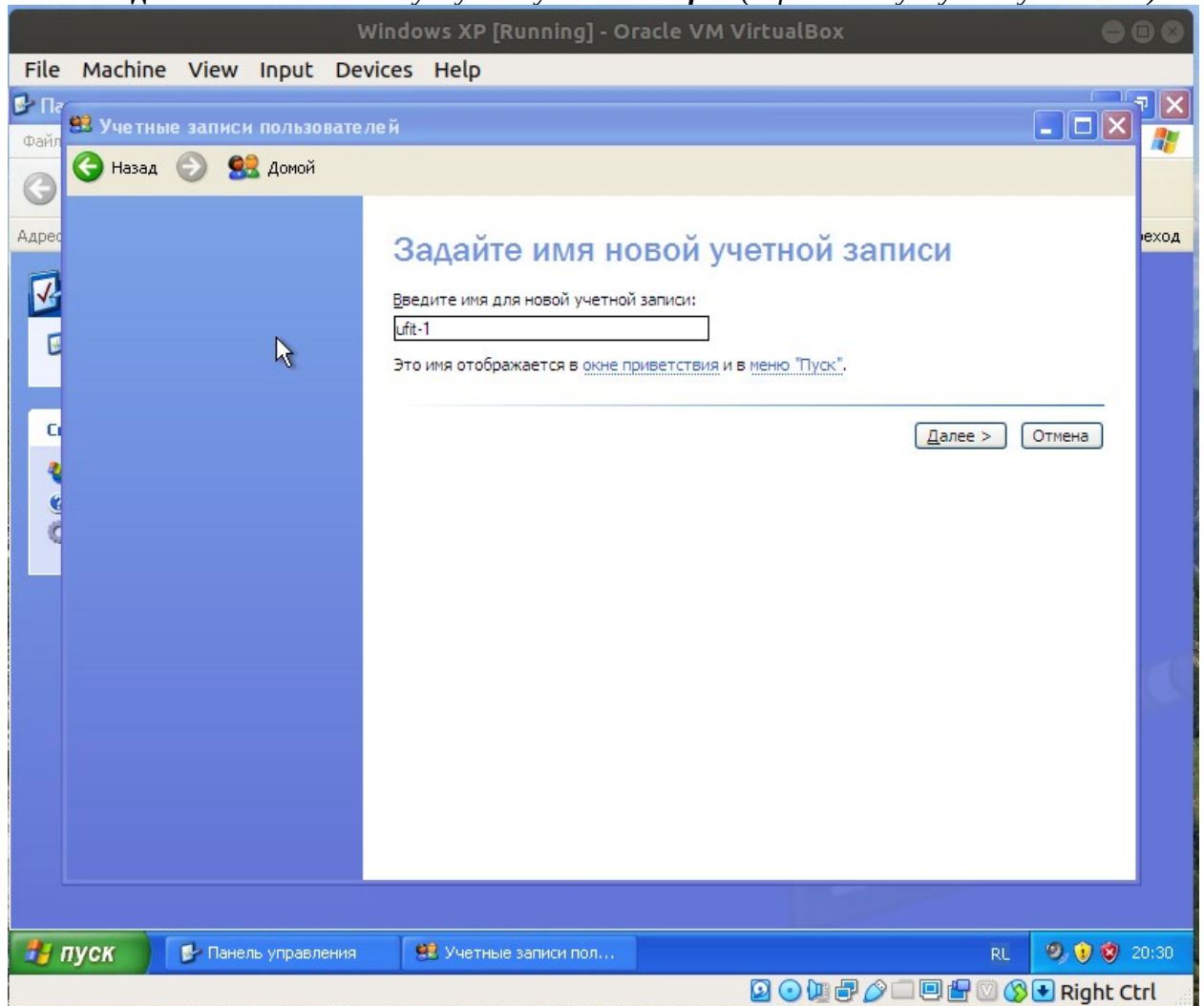
2) Используете вы простой общий доступ к файлам или нет? Щелкните кнопку **Отмена**, чтобы закрыть диалоговое окно свойств папки. В пункте меню **Сервис** выберите пункт **Свойства папки**. В диалоговом окне **Свойства папки** перейдите на вкладку **Вид**. В списке **Дополнительные параметры** снимите флажок **Использовать простой общий доступ к файлам (рекомендуется)** и щелкните **ОК**.

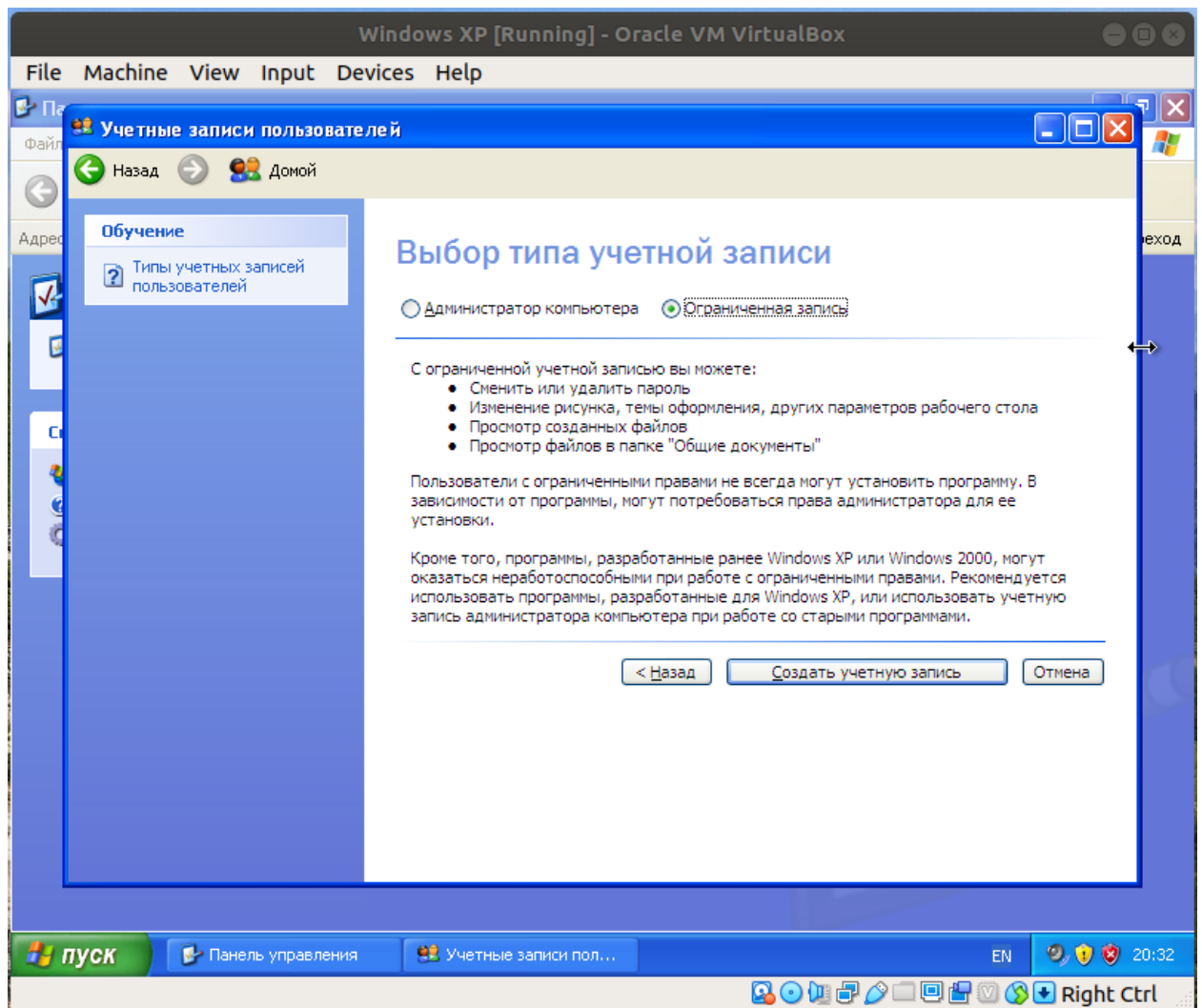


Определить для какой группы установлены особые разрешения. Щелкнуть кнопку **Дополнительно**, выделить эту группу и просмотреть установленные разрешения.

Закрыть диалоговое окно свойств папки. Закрыть окно **Проводник** и завершить сеанс.

Задание 5. Создать новую учетную запись **ufit-1**(ограниченную учетную запись).





Задание 6. Войти в систему с учетной записью **ufit-1**. Запустить **Проводник**, войти в папку **C:\Folder1**. Создать два текстовых документа, присвоив им имена **file 1** и **file 2**

Попытаться выполнить следующие операции с **файлом file1**: открыть файл; изменить файл; удалить файл. Какие действия вы смогли успешно совершить и почему?

Все действия получилось проделать успешно, потому что файл был создан учетной записью **ufit-1**, от лица которой потом файл был изменен, а потом и удален.

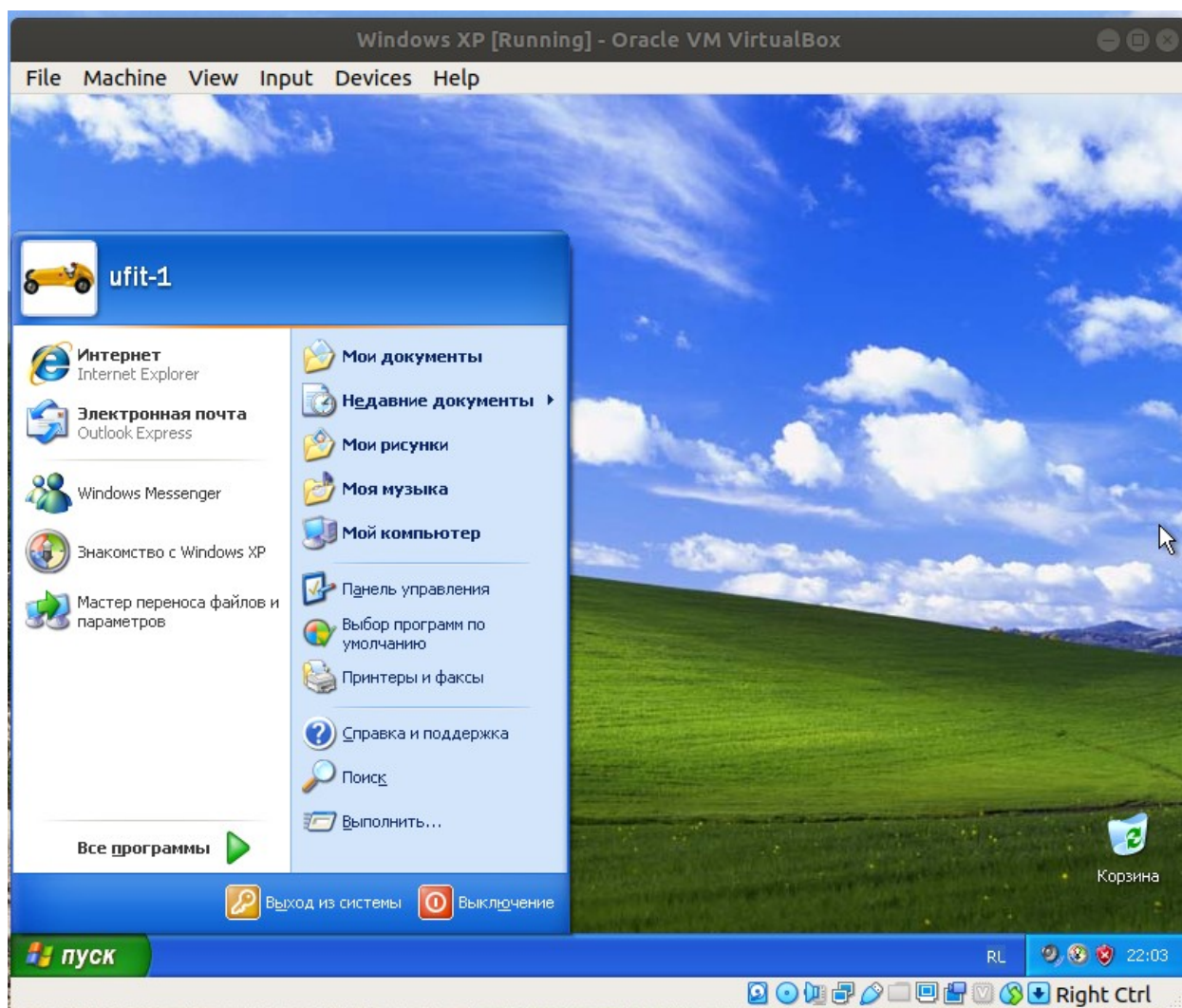
Создать учетную запись **ufit-2** (ограниченную). Завершить сеанс работы и войти в систему, используя учетную запись **ufit-2**. Запустить **Проводник**, войти в папку **C:\Folder1**. Попытаться выполнить следующие операции с файлом **file2**: открыть файл; изменить файл; удалить файл. Какие действия вы смогли успешно совершить и почему?

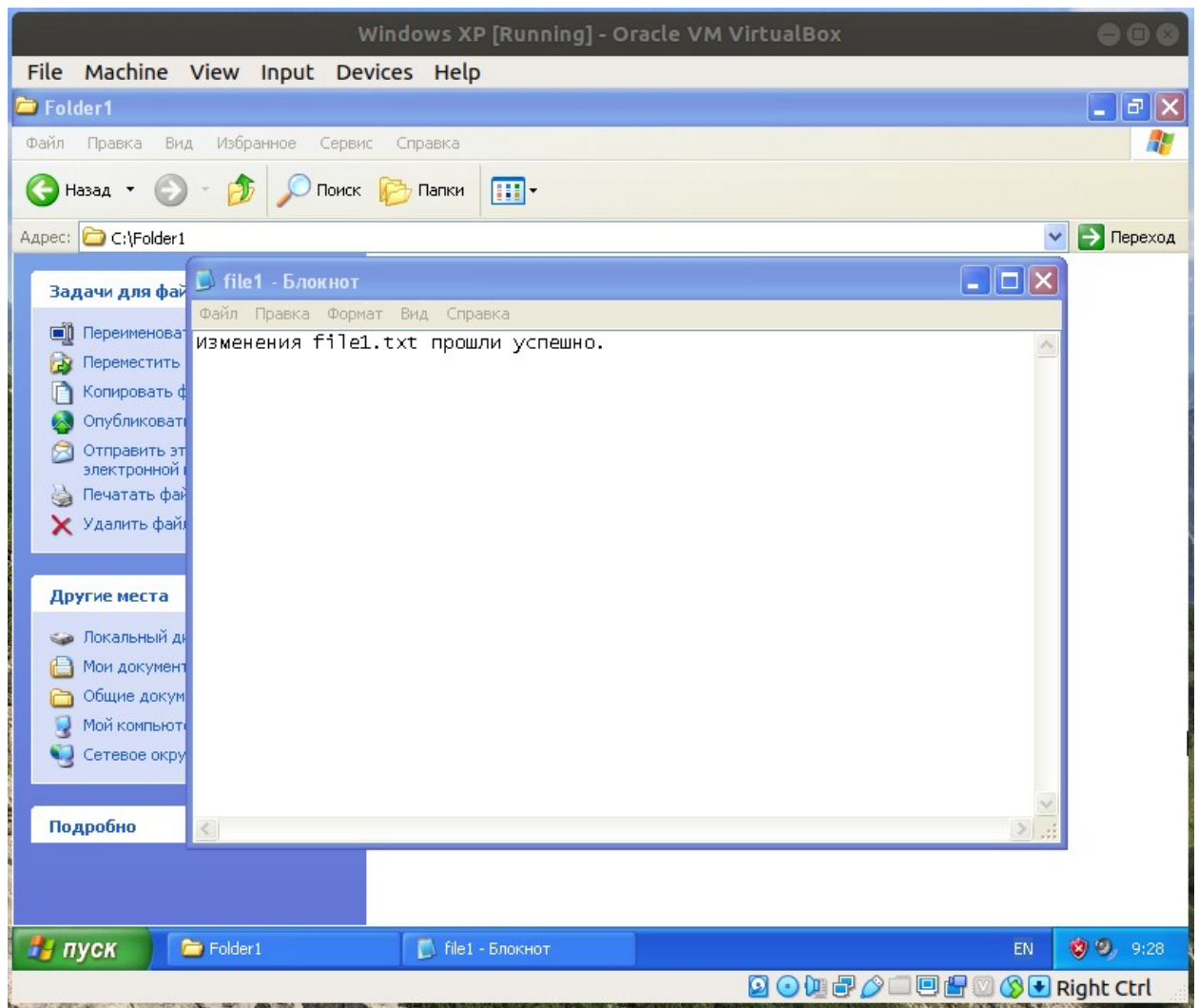
Файл получилось открыть, но не изменить и удалить, потому что файл был создан ограниченной учетной записью **ufit-1**, а попытки изменить и удалить файл были произведены от имени другой ограниченной учетной записи.

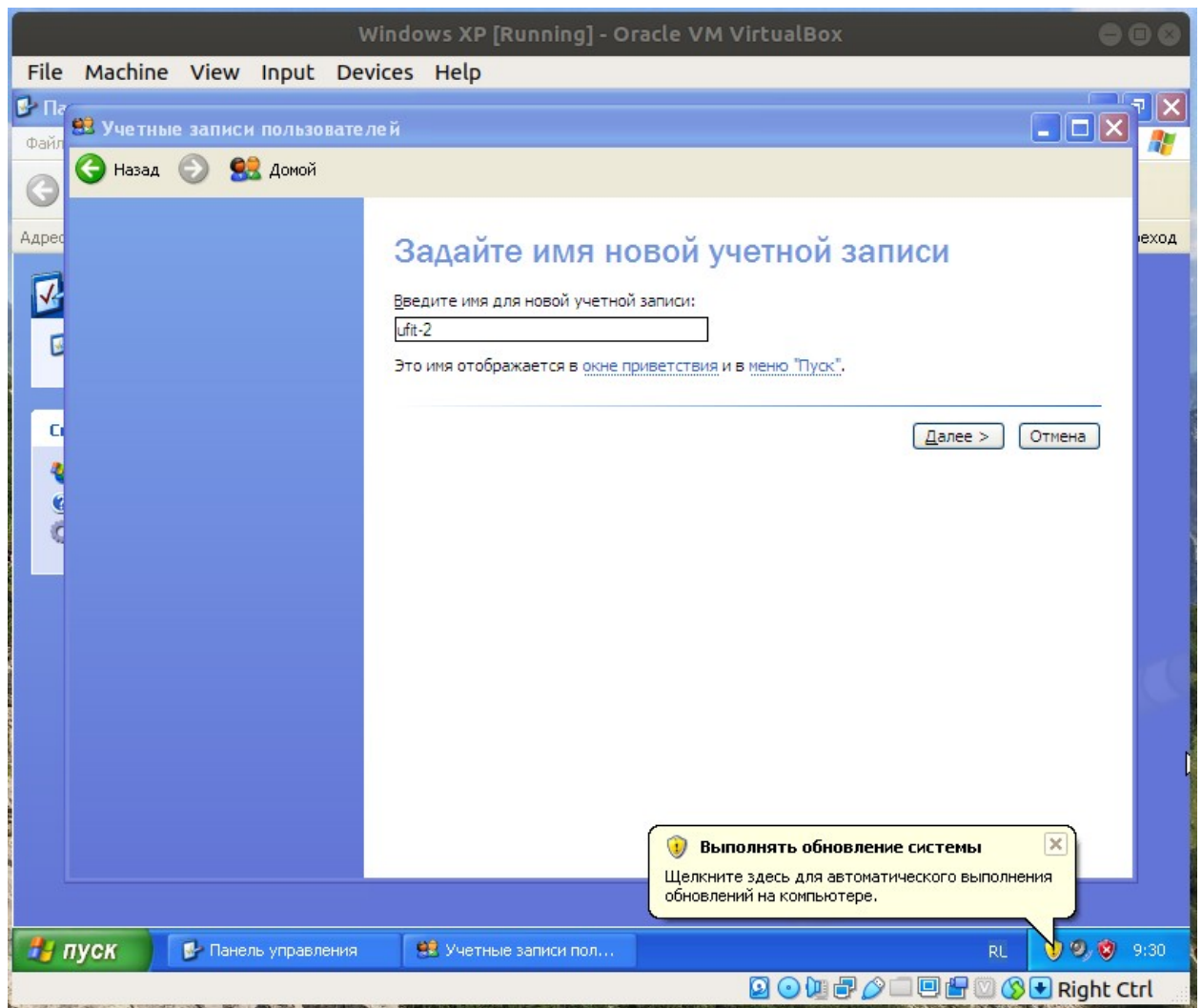
В настоящее время ваша регистрационная запись - **ufit-2**. Можете ли вы изменить разрешения, установленные для пользователя, пока вы подключены как **ufit-2**? Почему? От имени ограниченной учетной записи **ufit-2** можно устанавливать разрешения можно

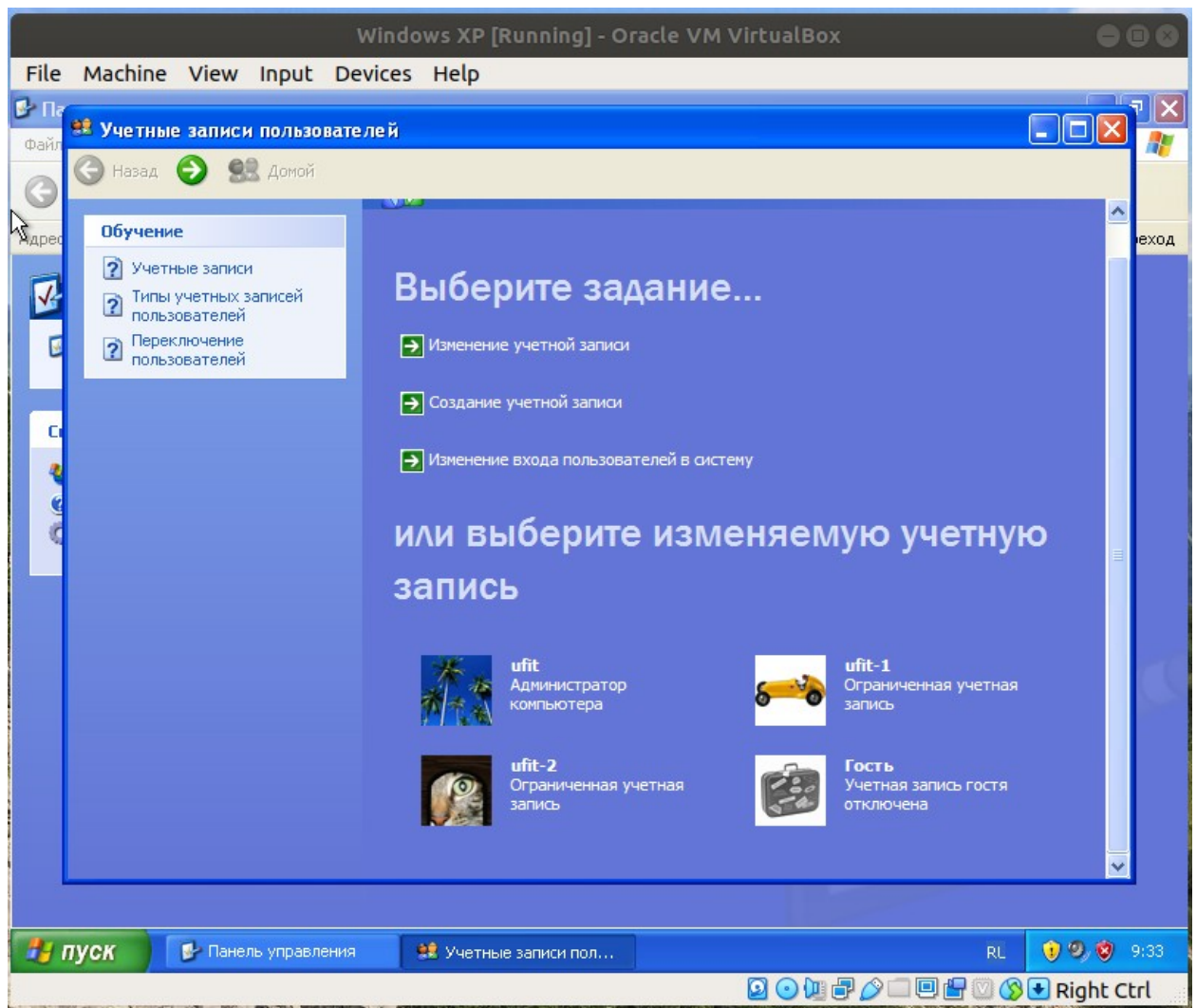
только для тех файлов, которые были созданы от имени ограниченной учетной записи ufit-2.

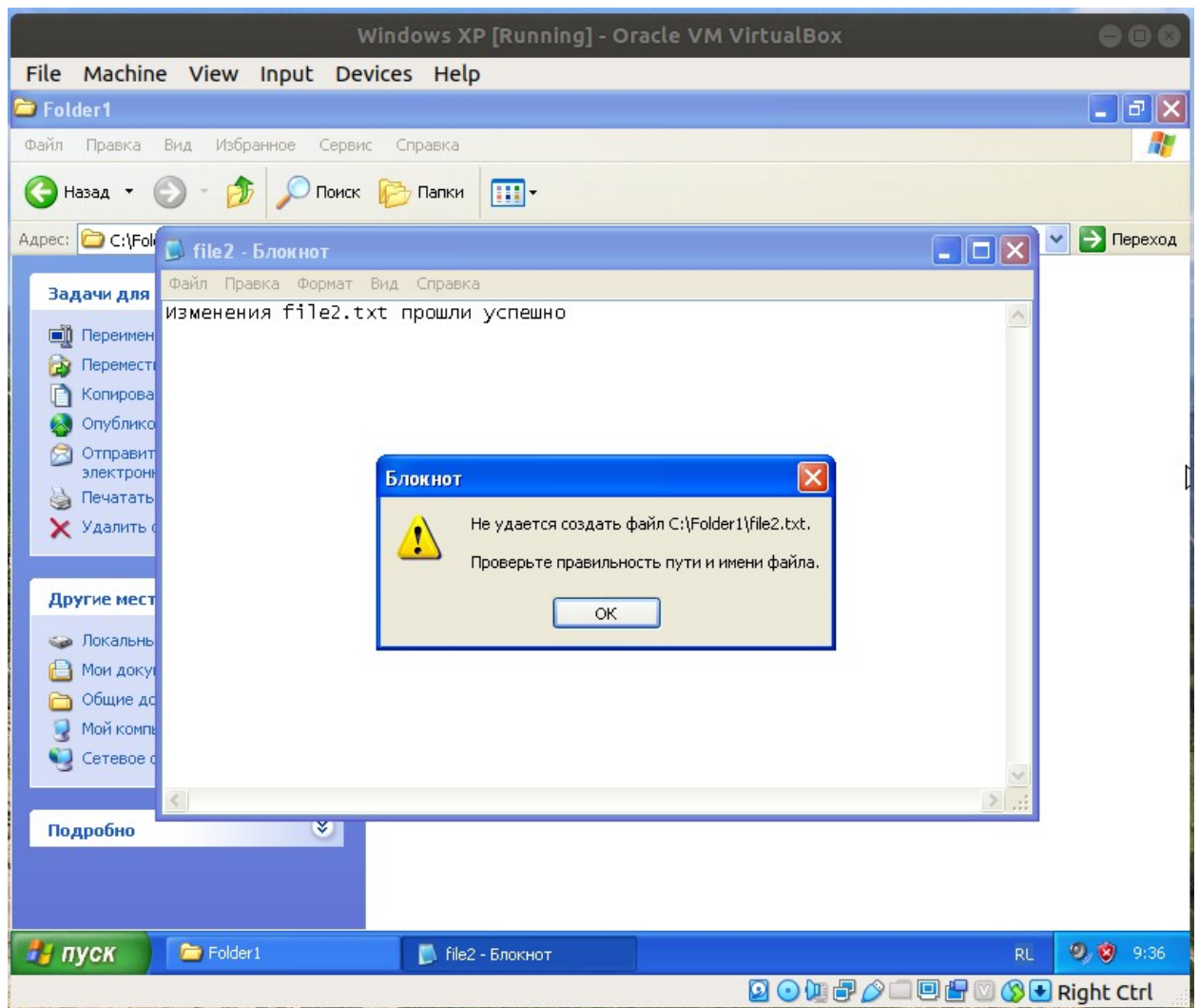
Завершить сеанс.







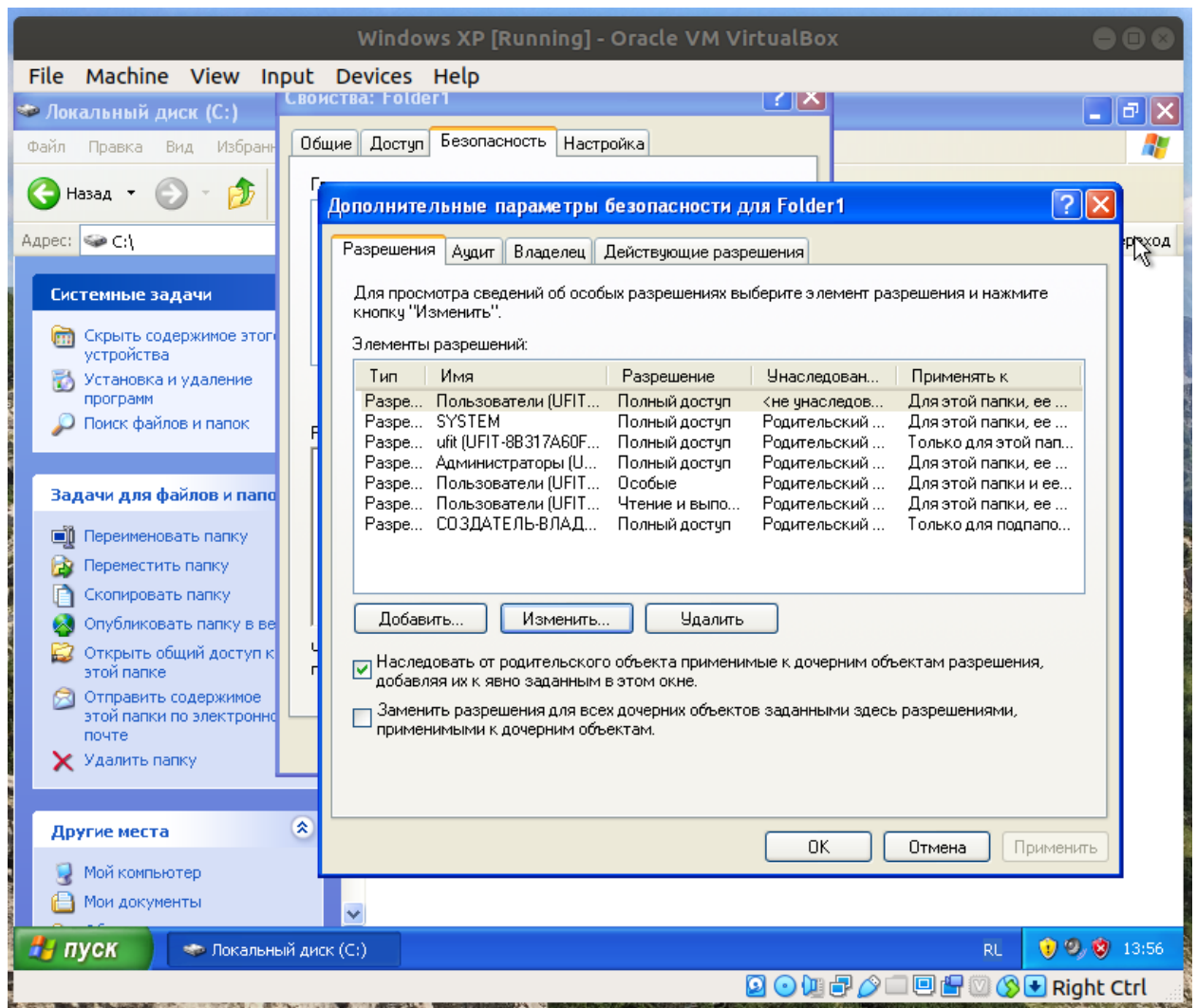


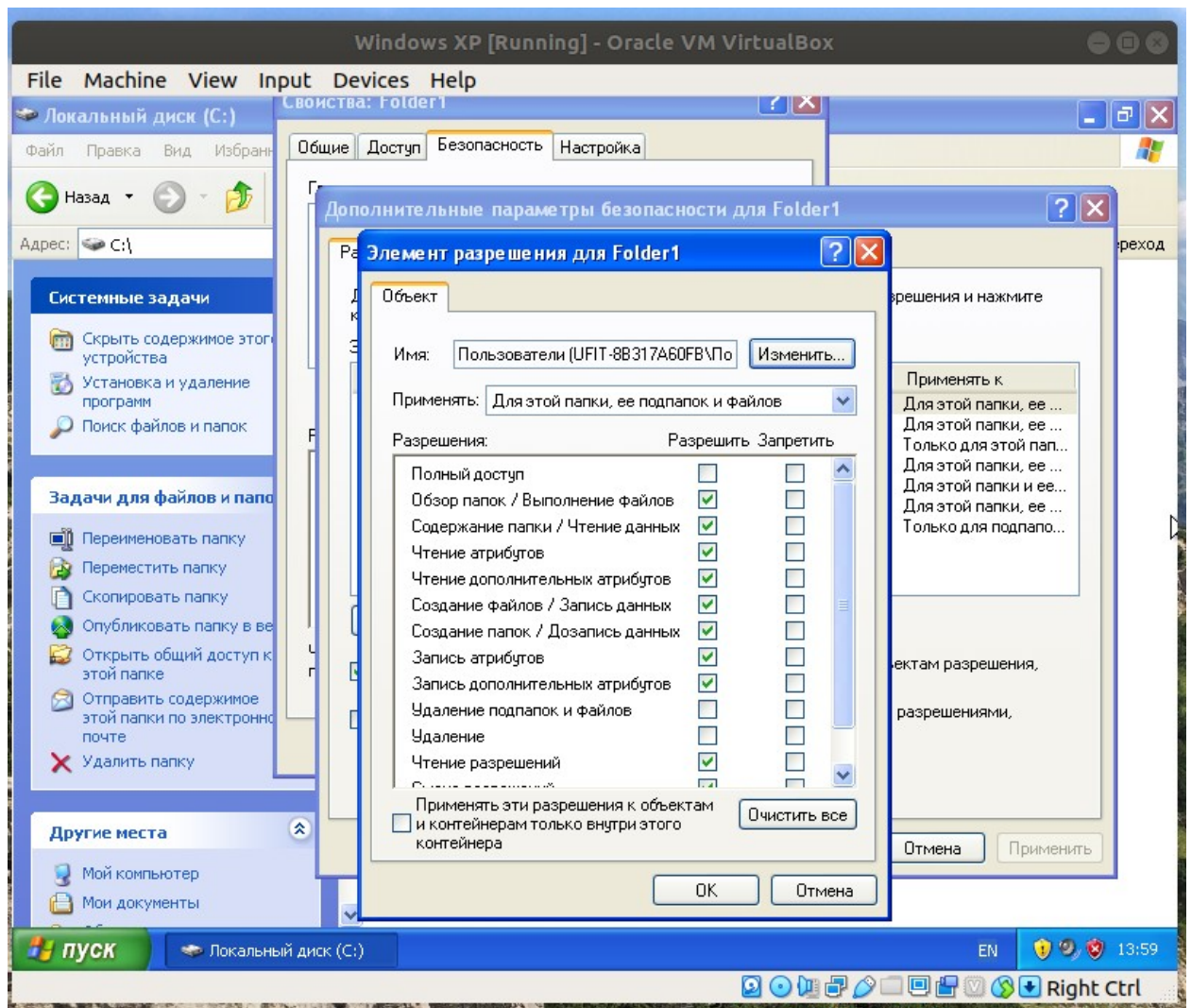


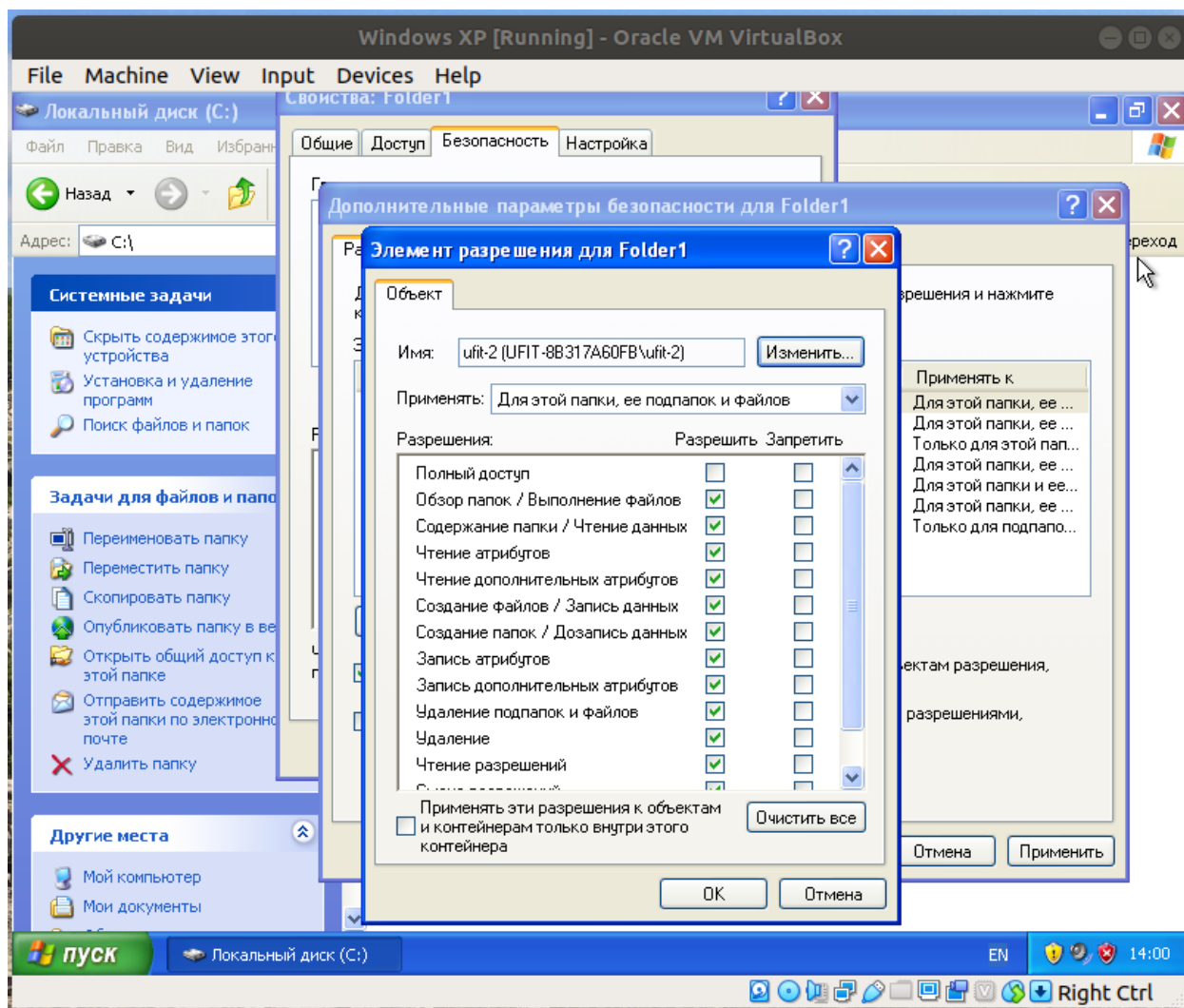
Задание 7. Установить разрешения NTFS для папки C:\Folder1. При этом необходимо соблюдать следующие правила:

- 1) все пользователи должны иметь возможность читать документы и файлы в папке **Folder1**;
- 2) все пользователи должны иметь возможность создавать документы в папке **Folder1**;
- 3) все пользователи должны иметь возможность изменять содержание, свойства и разрешения для создаваемых ими документов в папке **Folder1**;
- 4) пользователь **ufit-2** несет ответственность за содержимое папки **Folder1** и должен иметь возможность изменять и удалять все файлы в папке **Folder1**.

Основываясь на полученной информации, определить, как следует изменить разрешения для соответствия этим четырем критериям?







Войти в систему, используя учетную запись **ufit**. Открыть Проводник. Открыть папку **Folder1**. Щелкнуть правой кнопкой мыши значок папки **Folder1**, затем выбрать пункт меню Свойства. Перейти на вкладку **Безопасность** диалогового окна свойств папки. На вкладке **Безопасность** щелкнуть кнопку **Добавить**. Откроется диалоговое окно **Выбор: Пользователи или Группы**

В текстовом поле **Введите имена выбираемых объектов** ввести **ufit-2**, затем щелкнуть кнопку **Проверить имена**. В текстовом поле **Введите имена выбираемых объектов** должна появиться надпись **<имя компьютера>\ufit-2**. Это свидетельствует, что Windows обнаружила пользователя **ufit-2** на компьютере **<имя компьютера>** и что это действительная учетная запись пользователя. Щелкнуть **ОК**, чтобы закрыть диалоговое окно **Выбор: Пользователи или Группы**. Теперь пользователь **ufit-2** включен в список Группы или пользователи диалогового окна свойств папки **Folder1**. Какие разрешения установлены для пользователя **ufit-2**?

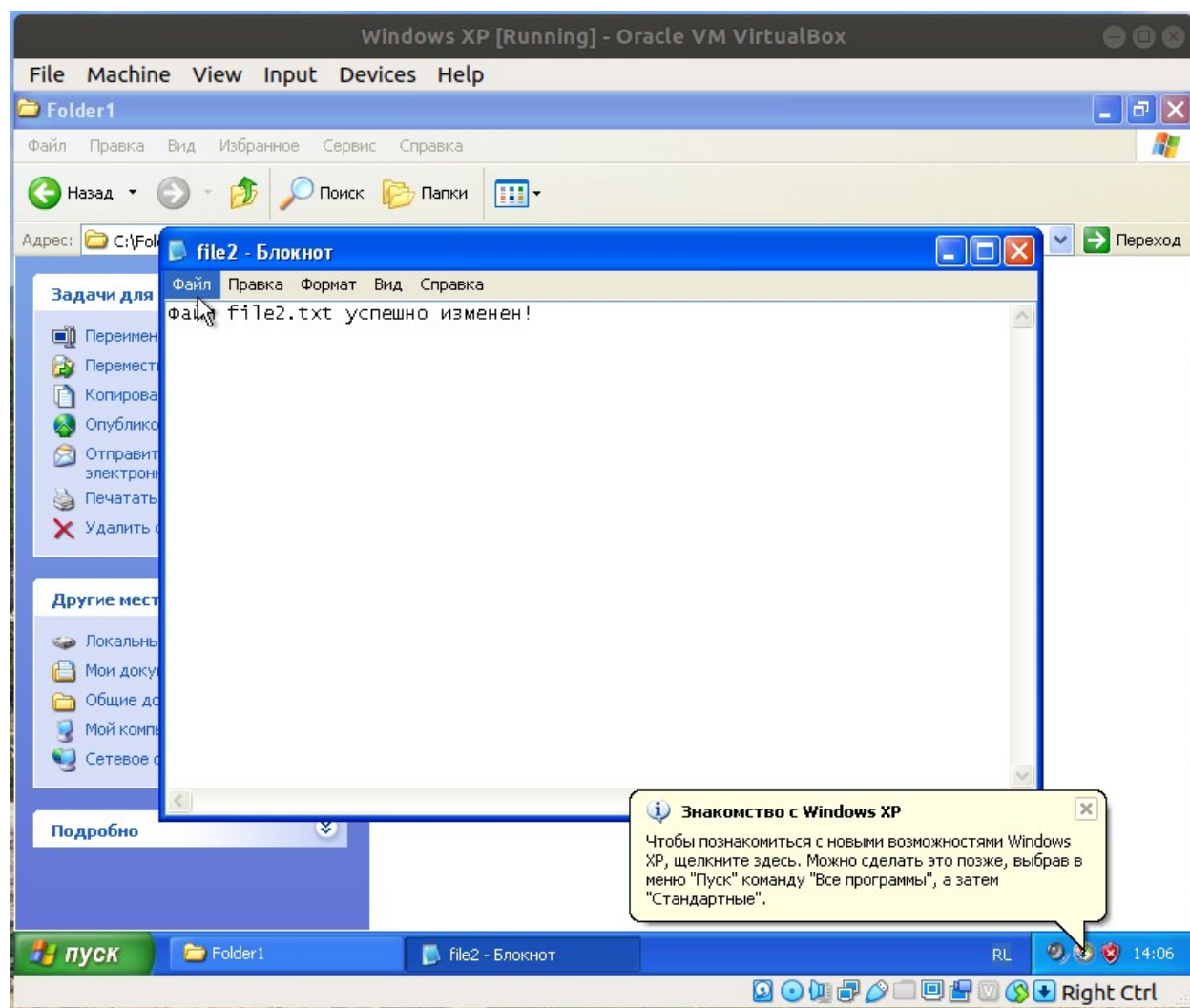
Щелкнуть кнопку **Дополнительно**. Откроется диалоговое окно **Дополнительные параметры безопасности** для **Folder1**, и вы увидите, что пользователь **ufit-2** включен в список **Элементы разрешений**. Убедиться, что строка **ufit-2** выделена, и щелкнуть кнопку **Изменить**. Откроется диалоговое окно **Элемент разрешения** для **Folder1**, и вы увидите в текстовом поле **Имя** учетную запись пользователя **ufit-2**.

В колонке **Разрешить** щелкнуть **Полный доступ**. Теперь в колонке **Разрешить** установлены все флажки. Щелкнуть **ОК**, чтобы закрыть диалоговое окно **Элемент разрешения** для **Folder1** и щелкнуть **ОК**, чтобы закрыть диалоговое окно **Дополнительные параметры безопасности** для **Folder 1**. Щелкнуть **ОК**, чтобы закрыть диалоговое окно свойств папки **Folder 1**.

Закрыть **Проводник** и завершить сеанс Windows

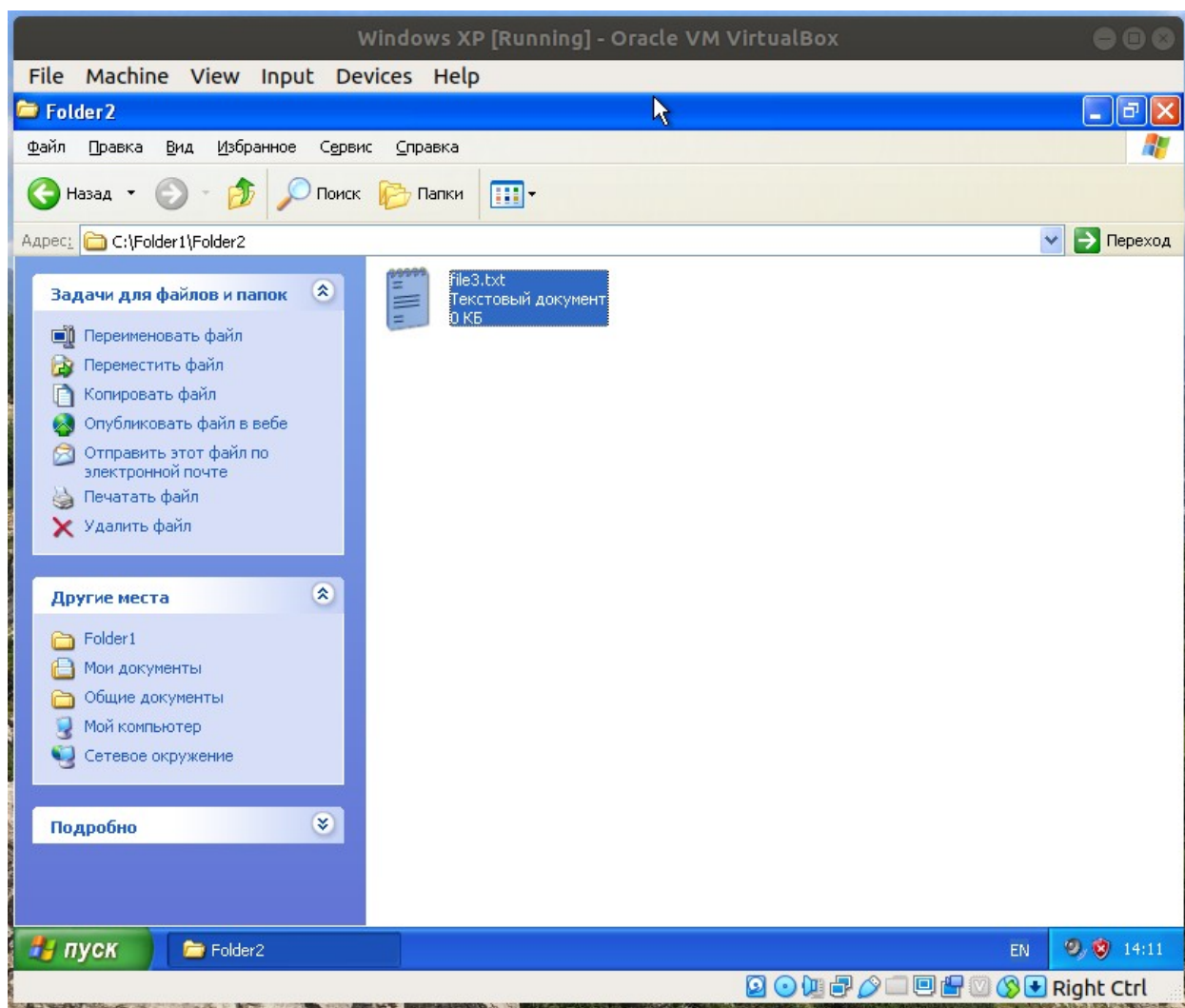
Войти в систему, используя учетную запись **ufit-2**. Запустить **Проводник**, войти в папку **C:\Folder1**. Попытаться выполнить следующие операции с файлом **file2**: изменить файл; удалить файл. Какие действия вы смогли успешно совершить и почему? Завершить сеанс Windows.

Все действия проведены успешно, потому что ограниченной учетной записи **ufit-2** были предоставлены права на выполнения этих действий.



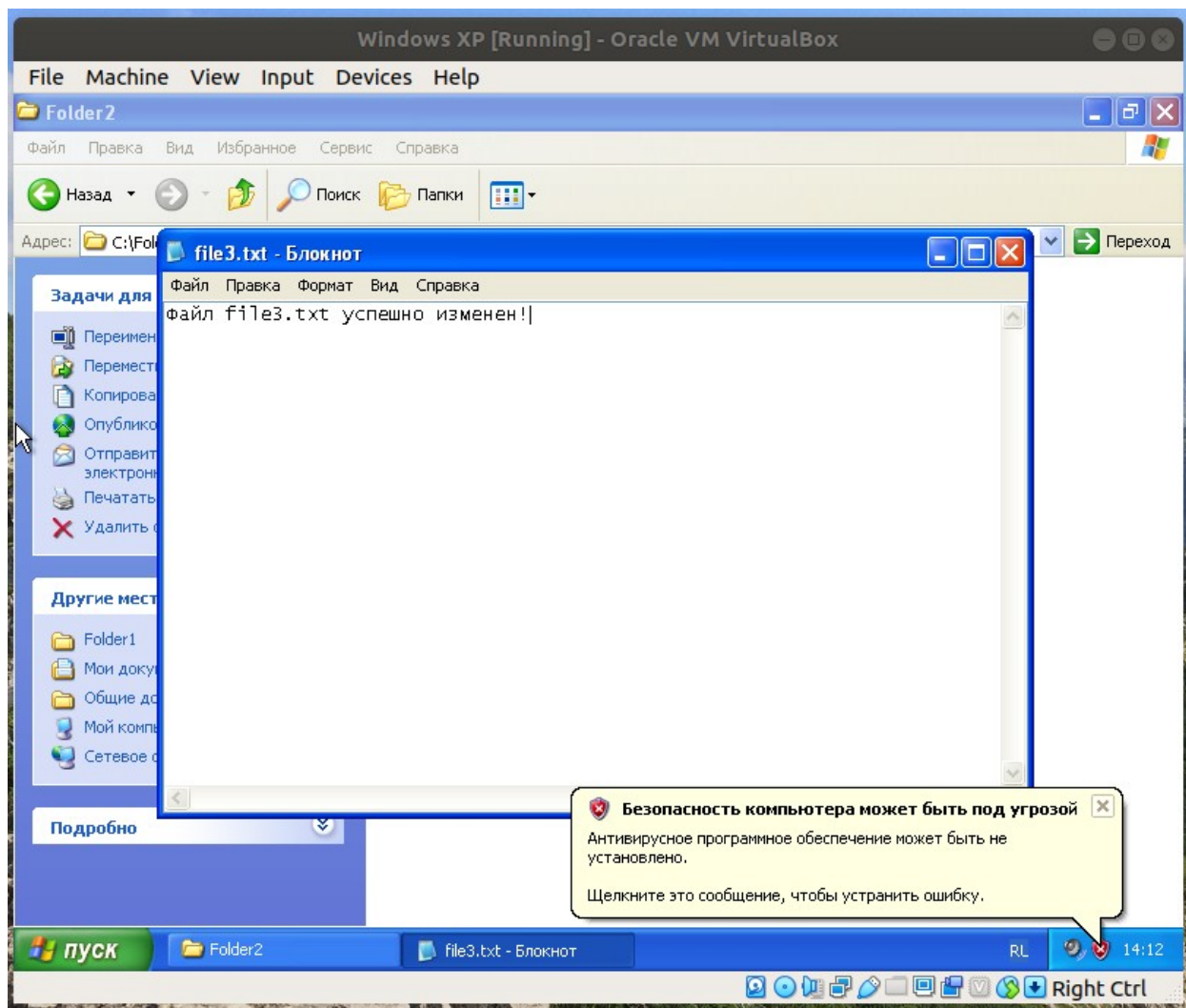
Задание 8. Проверить, как разрешения NTFS наследуются в иерархии папок.

Войти в систему, используя учетную запись **ufit-1**. Запустить **Проводник**, войти в папку **C:\Folder1\Folder2**. Создать текстовый файл с именем **file3** в папке. Завершить сеанс Windows XP Professional.



Войти в систему, используя учетную запись **ufit-2**. Запустить **Проводник**, войти в папку **C:\Folder1\Folder2**. Попытаться выполнить следующие операции с файлом **file3**: открыть файл; изменить файл; удалить файл. Какие действия вы смогли совершить и почему? Завершить сеанс Windows.

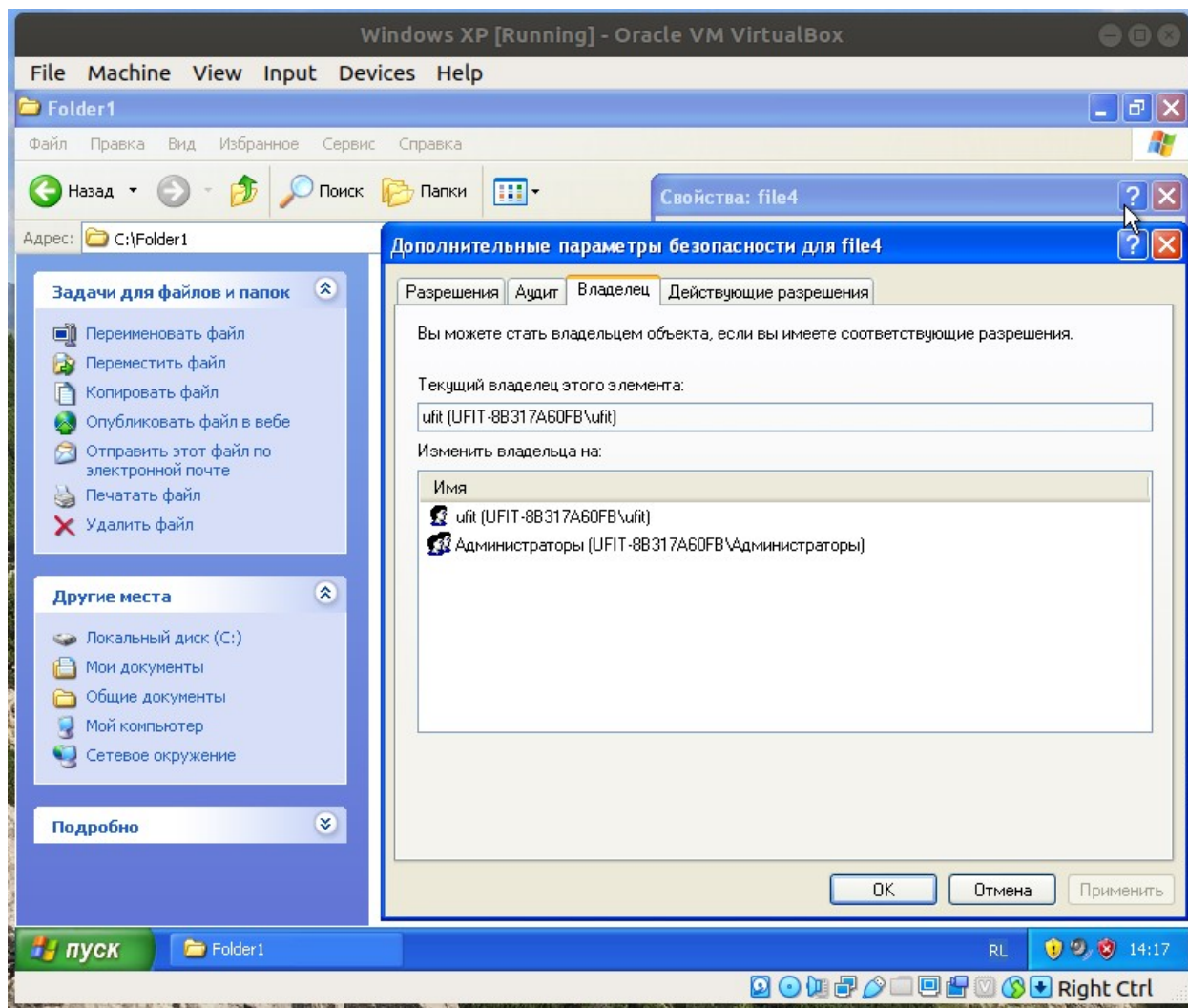
Получилось выполнить все действия, потому что все разрешения учетным записям, которые были назначены папке Folder1 были унаследованы папкой Folder2.



Задание 9. Изучить результаты смены владельца файла.

Войти в систему, используя учетную запись **ufit**. В папке **C:\Folder1** создать текстовый файл **file4**.

Щелкнуть правой кнопкой мыши значок документа **file4**, затем выбрать пункт меню **Свойства**. Откроется диалоговое окно **Свойства: file4** с активной вкладкой **Общие**. Перейти на вкладку **Безопасность** для просмотра разрешений, установленных для файла **file4**. Щелкнуть кнопку **Дополнительно**. Откроется диалоговое окно **Дополнительные параметры безопасности для file4** с активной вкладкой **Разрешения**. Перейти на вкладку **Владелец**. Кто является текущим владельцем файла **file4**?



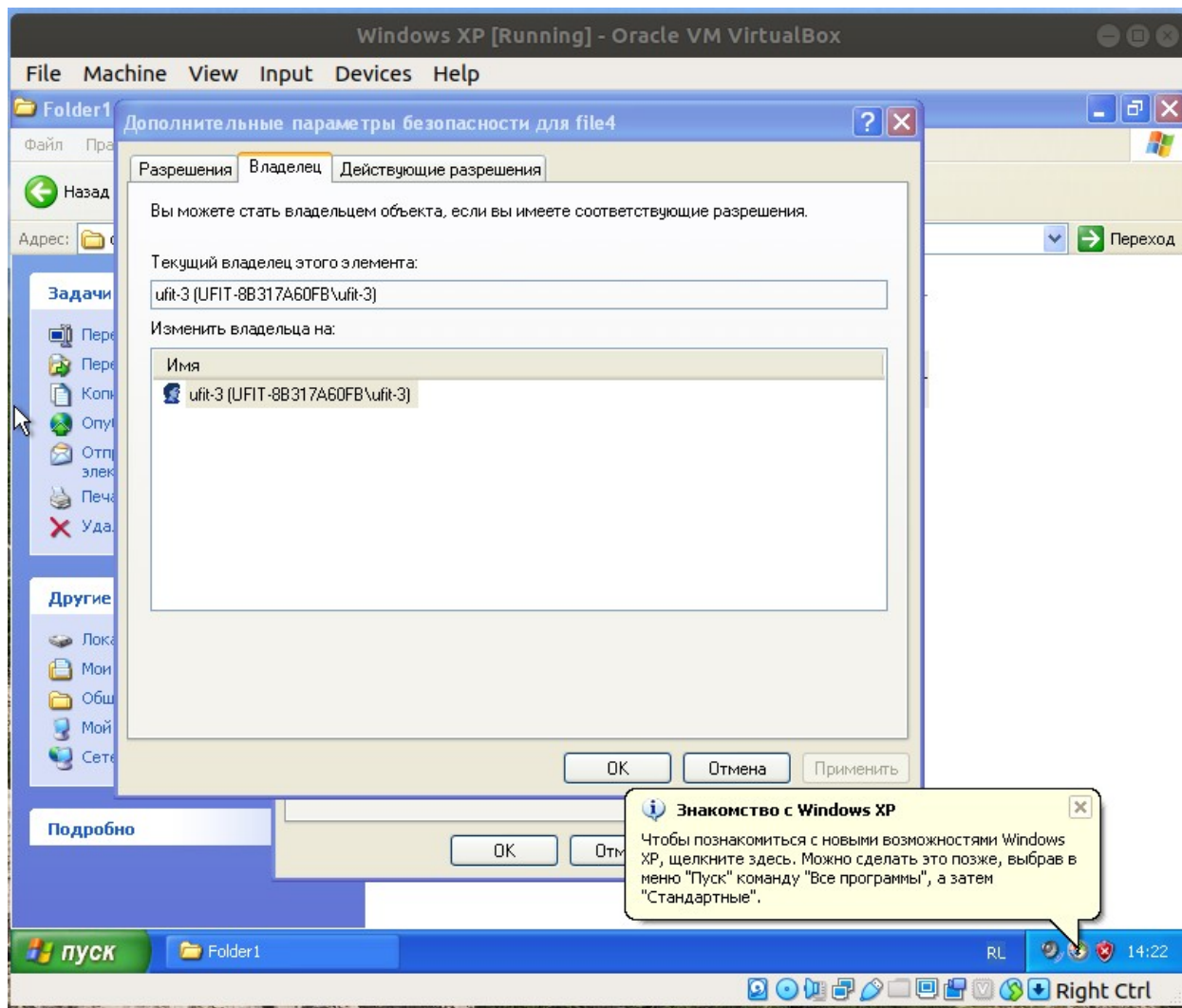
Установка разрешения, позволяющего пользователю сменить владельца.

В диалоговом окне **Дополнительные параметры безопасности для file4** перейти на вкладку **Разрешения**. Щелкнуть кнопку **Добавить**. Откроется диалоговое окно **Выбор: Пользователи или Группы**. Убедиться, что в текстовом поле **Размещение**, которое расположено вверху диалогового окна, выбрано имя вашего компьютера. В текстовом поле **Введите имена выбираемых объектов** ввести **ufit-3**, затем щелкните кнопку **Проверить имена**. Щелкнуть **ОК**.

Станет активным диалоговое окно **Элемент разрешения для file4**. Обратить внимание на то, что все элементы разрешений для пользователя **ufit-3** не отмечены. В колонке **Разрешения** установить флажок **Разрешить** для разрешения **Сменить**

владельца. Щелкнуть **ОК.** Щелкнуть **ОК** для того, чтобы вернуться к диалоговому окну свойств файла **file4.** Щелкнуть **ОК** для сохранения изменений и закрыть диалоговое окно свойств файла **file4.** Закрыть **Проводник** и выйти из системы. Смена владельца файла.

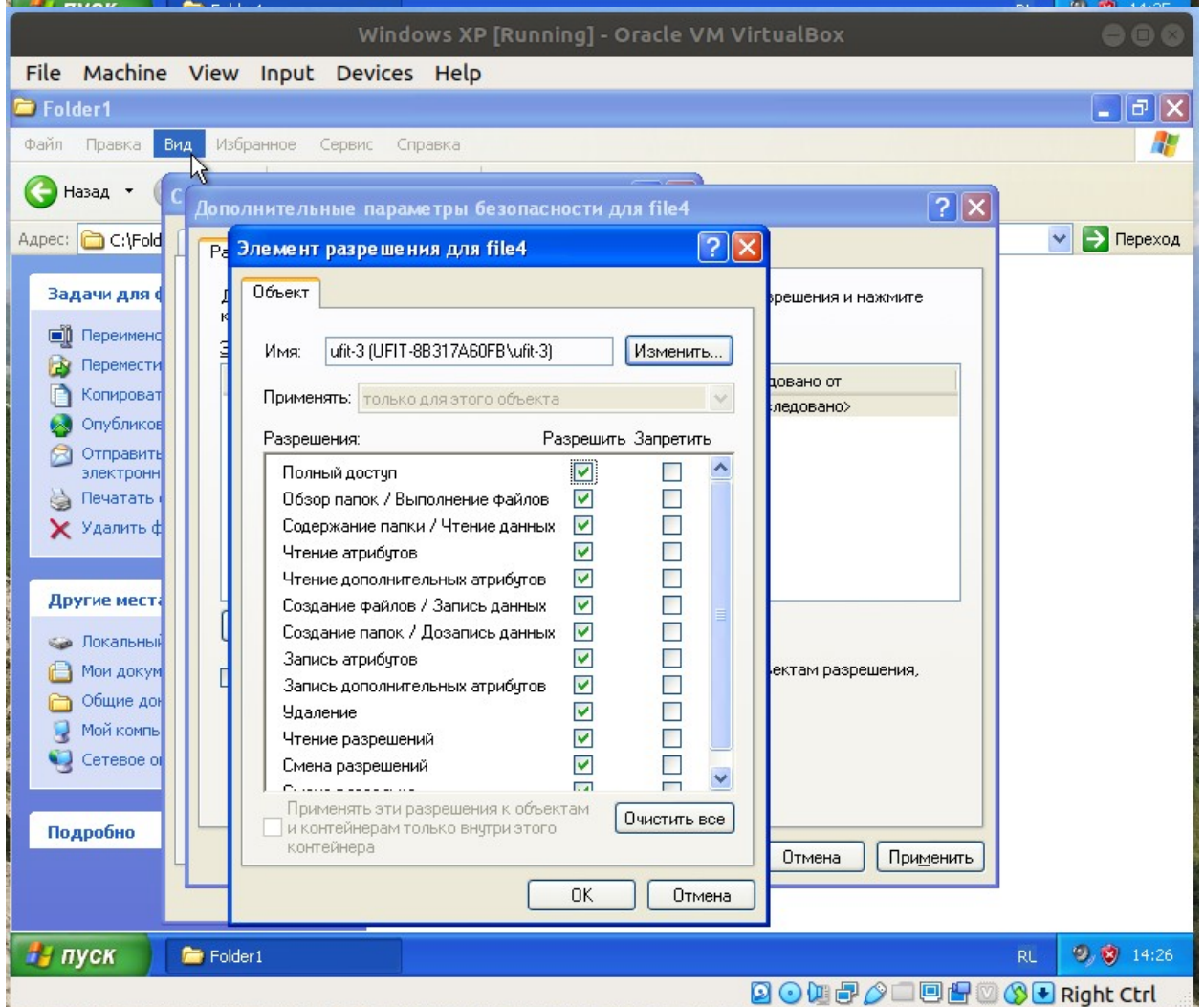
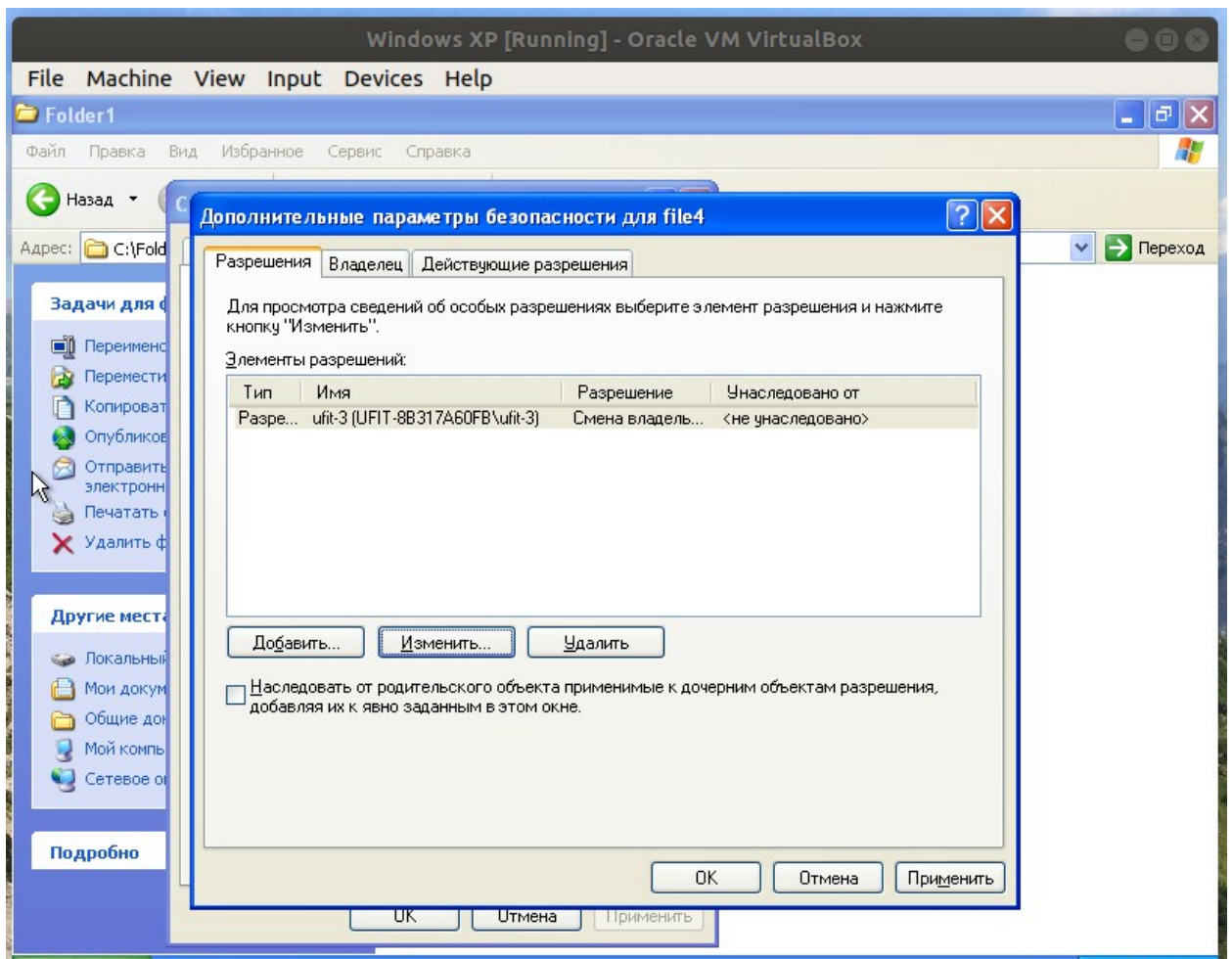
Войти в систему, используя учетную запись **ufit-3.** Запустить **Проводник**, войти в папку **C:\Folder1.** Щелкнуть правой кнопкой мыши значок файла **file4** и выбрать пункт меню **Свойства.** Перейти на вкладку **Безопасность** для просмотра разрешений для файла. Щелкнуть **Дополнительно** и перейти на вкладку **Владелец.** В колонке **Изменить владельца** на выбрать **ufit-3**, затем щелкнуть кнопку **Применить.** Кто теперь является владельцем файла **file4?**



Щелкнуть **ОК**, чтобы закрыть диалоговое окно **Дополнительные параметры безопасности для file4.**

Проверка разрешений для файла в качестве владельца.

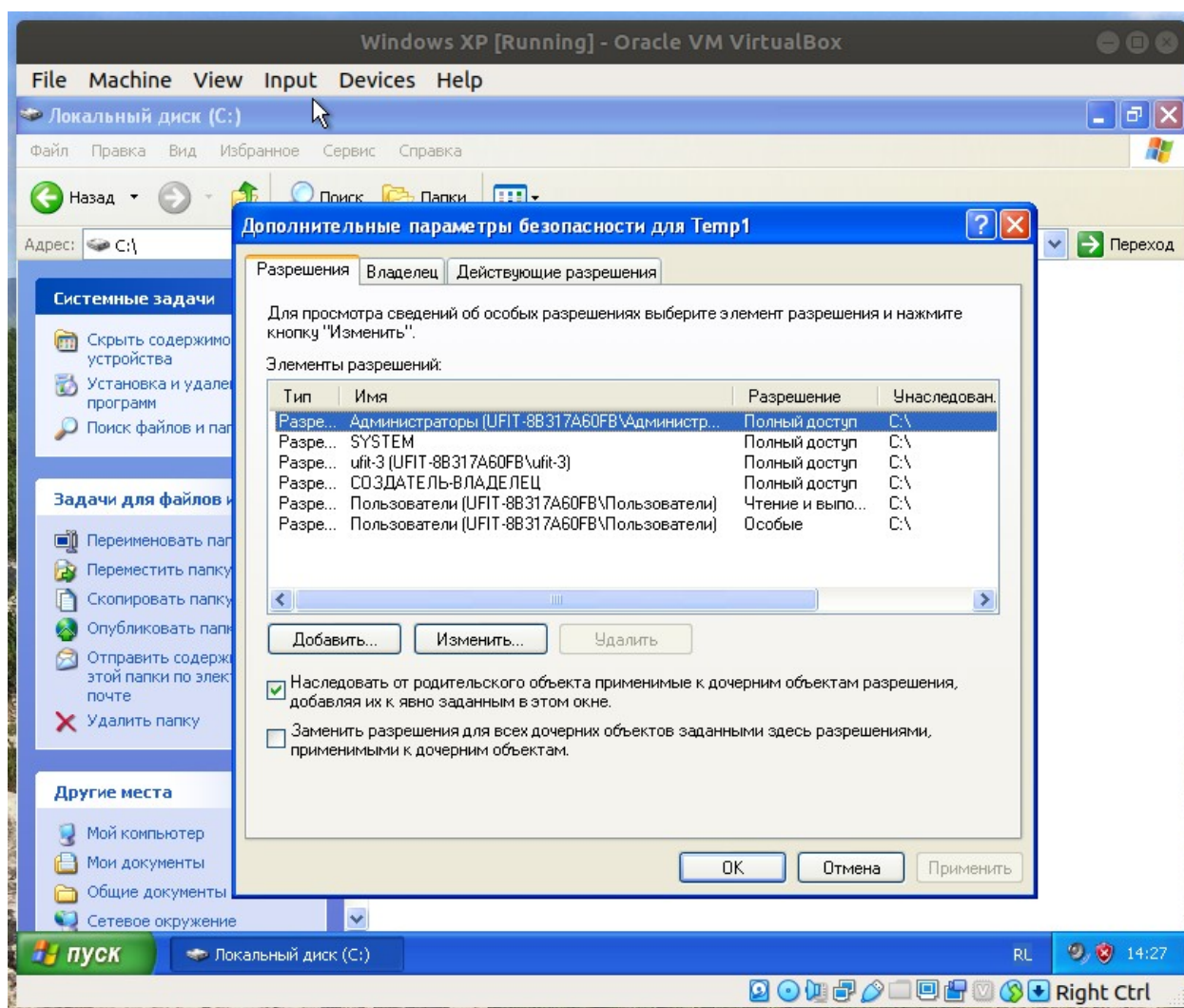
Щелкнуть кнопку **Дополнительно** и снять флажок **Наследовать от родительского объекта применимые к дочерним объектам разрешения**, добавляя их к явно заданным в этом окне. Установить разрешение **Полный доступ к текстовому документу file4** и нажать кнопку **Применить.** Щелкнуть **ОК**, чтобы закрыть диалоговое окно **Дополнительные параметры безопасности для file4.** Щелкнуть **ОК**, чтобы закрыть диалоговое окно свойств файла **file4.**

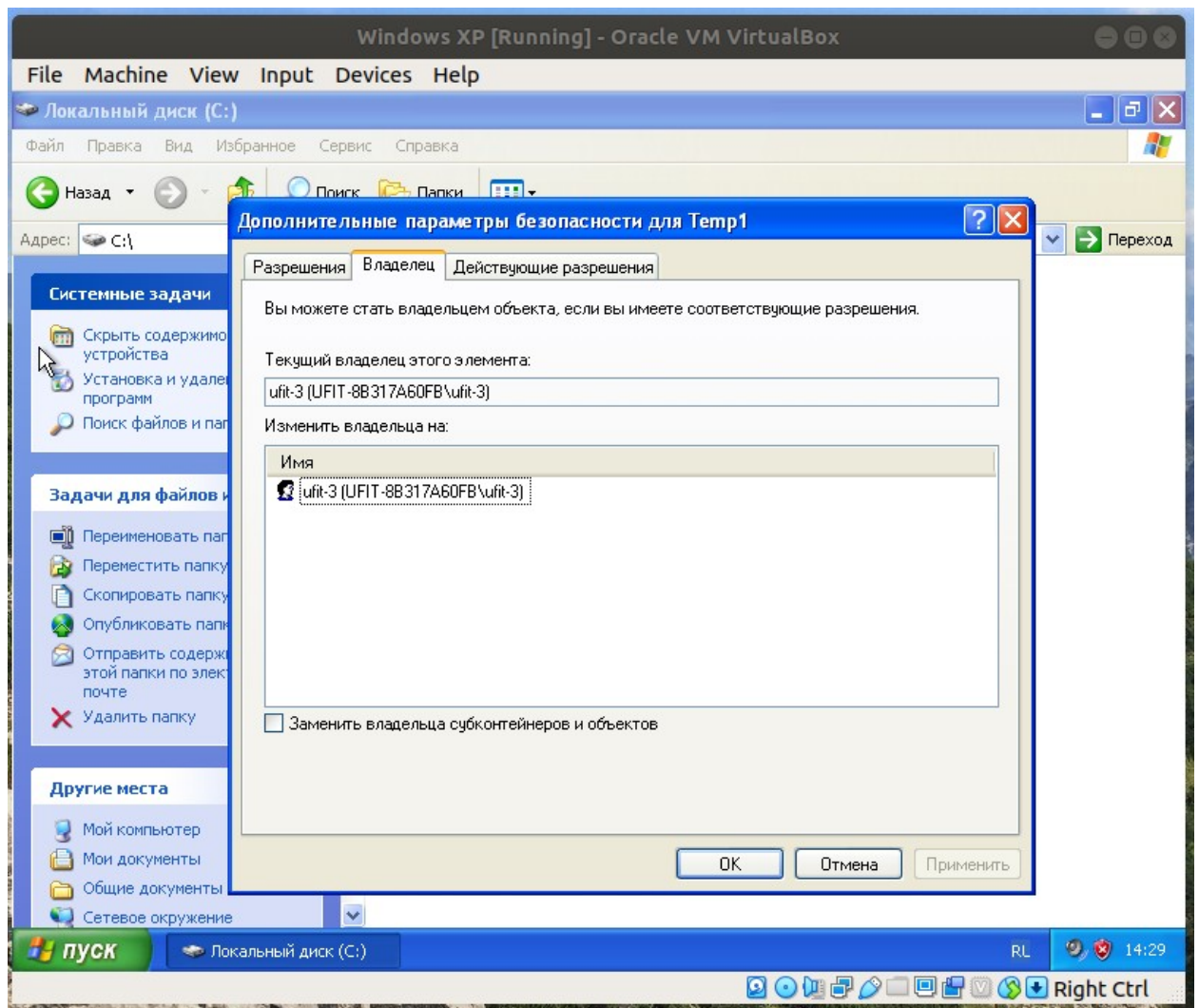


Задание 10. Изучить изменение разрешений и прав владельца при копировании и перемещении папок.

Создание папки при подключении с учетной записью пользователя.

Пока вы зарегистрированы в системе под учетной записью **ufit-3** создать папку с именем **Temp1** в корневой папке диска **C:**. Какие разрешения установлены для этой папки? Кто является владельцем папки?

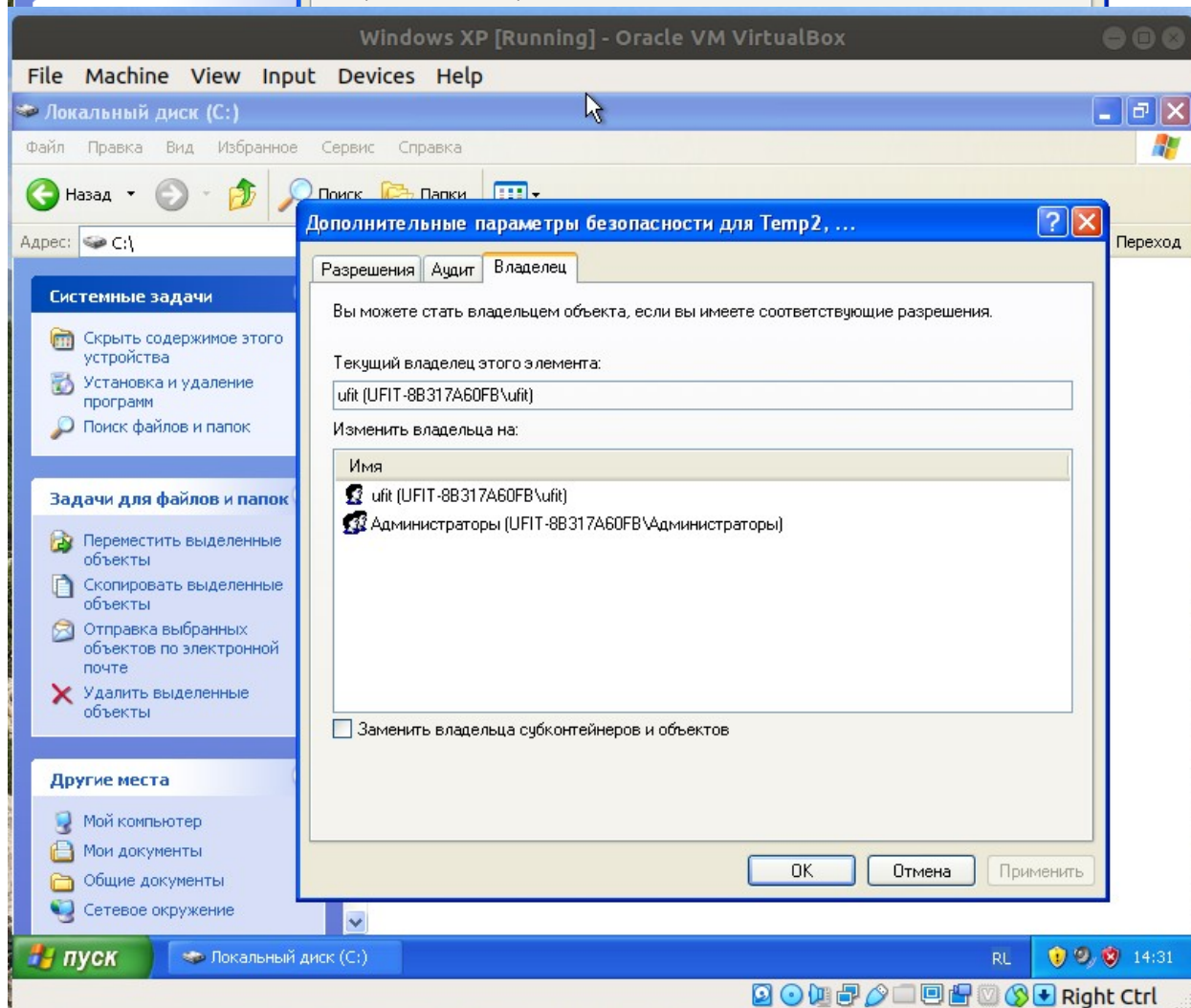
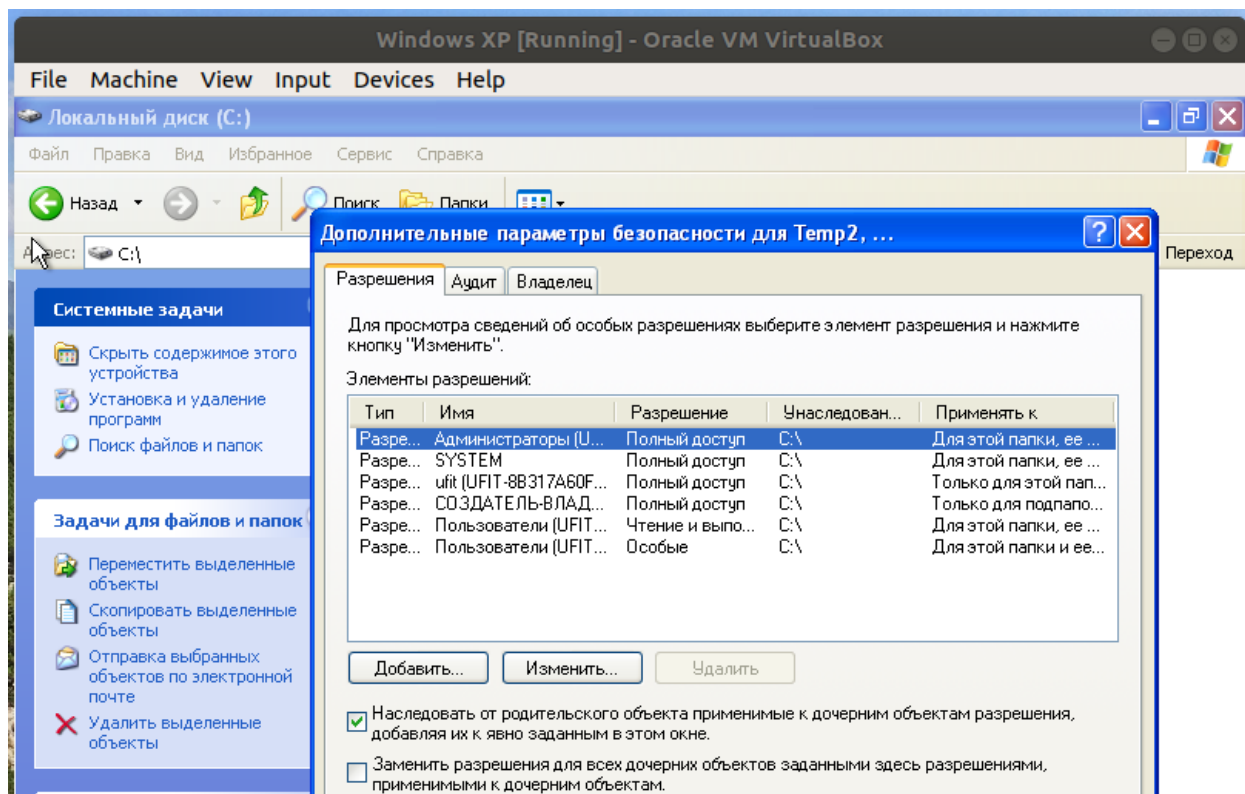




Создание папок при подключении с учетной записью члена группы **Администраторы**.

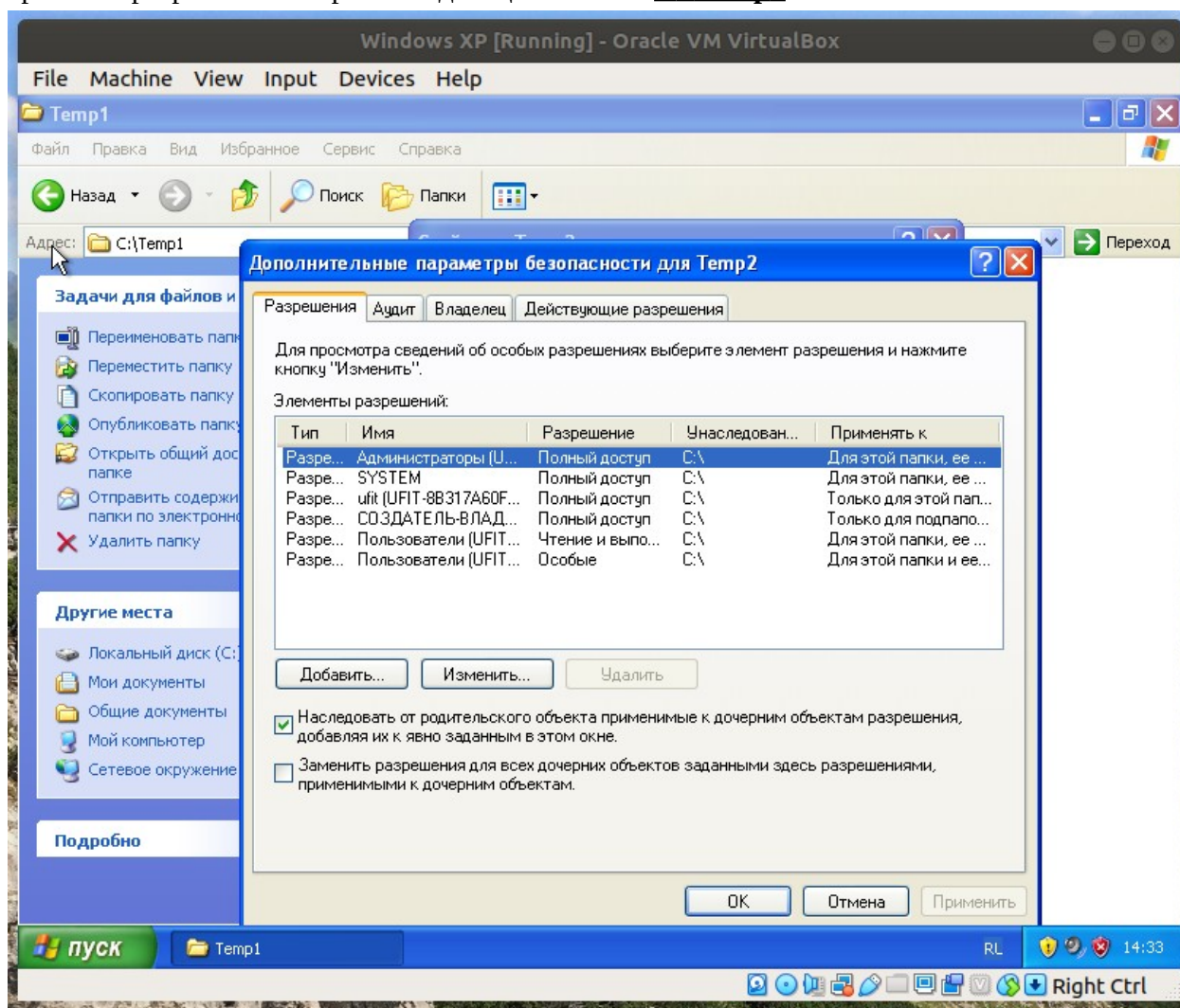
Подключитесь с учетной записью **ufit** и создайте папки **Temp2** и **Temp3** в корневой папке диска **C:**.

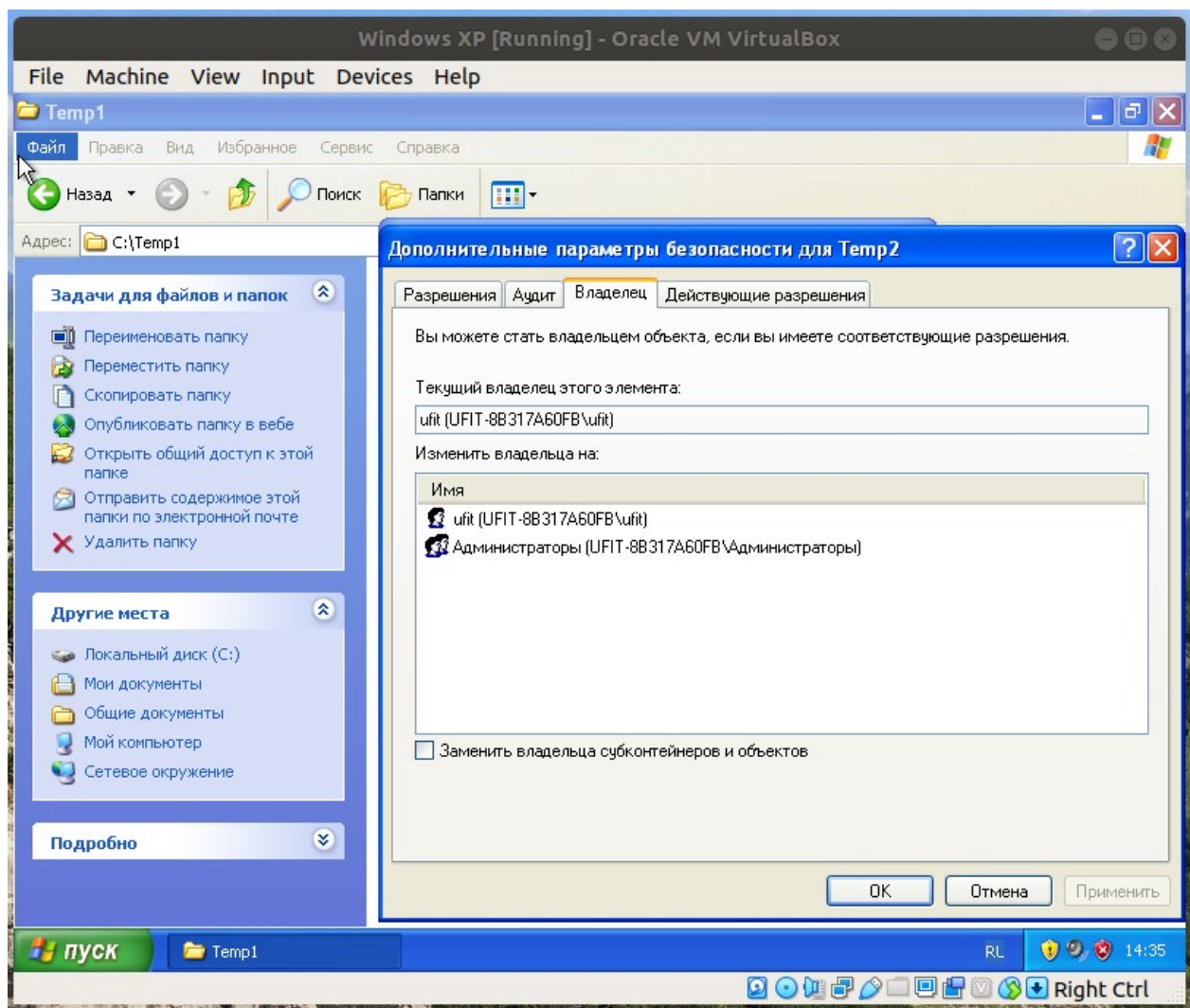
Каковы разрешения для папок, которые вы только что создали? Кто является владельцем папок **Temp2** и **Temp3**?

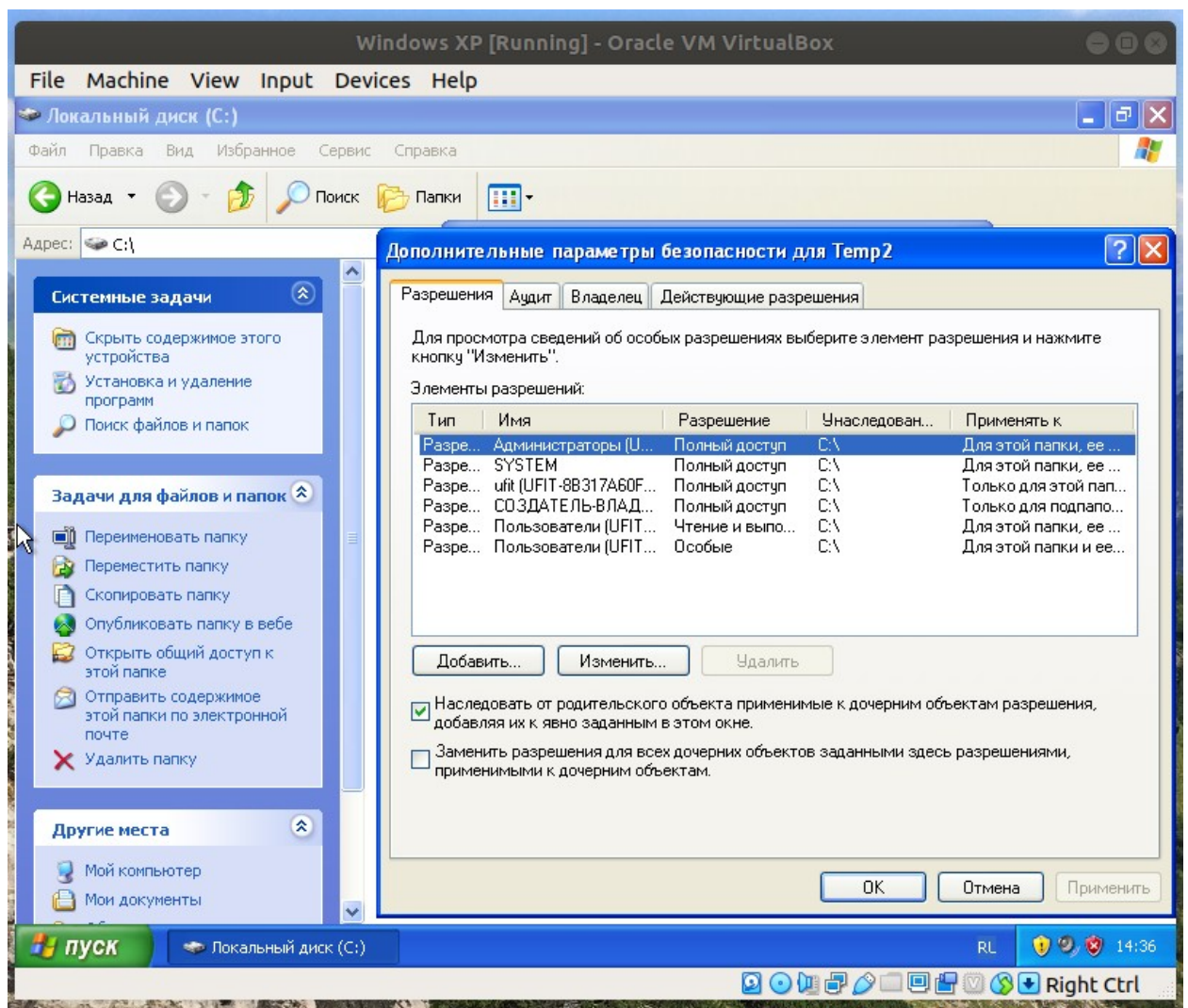


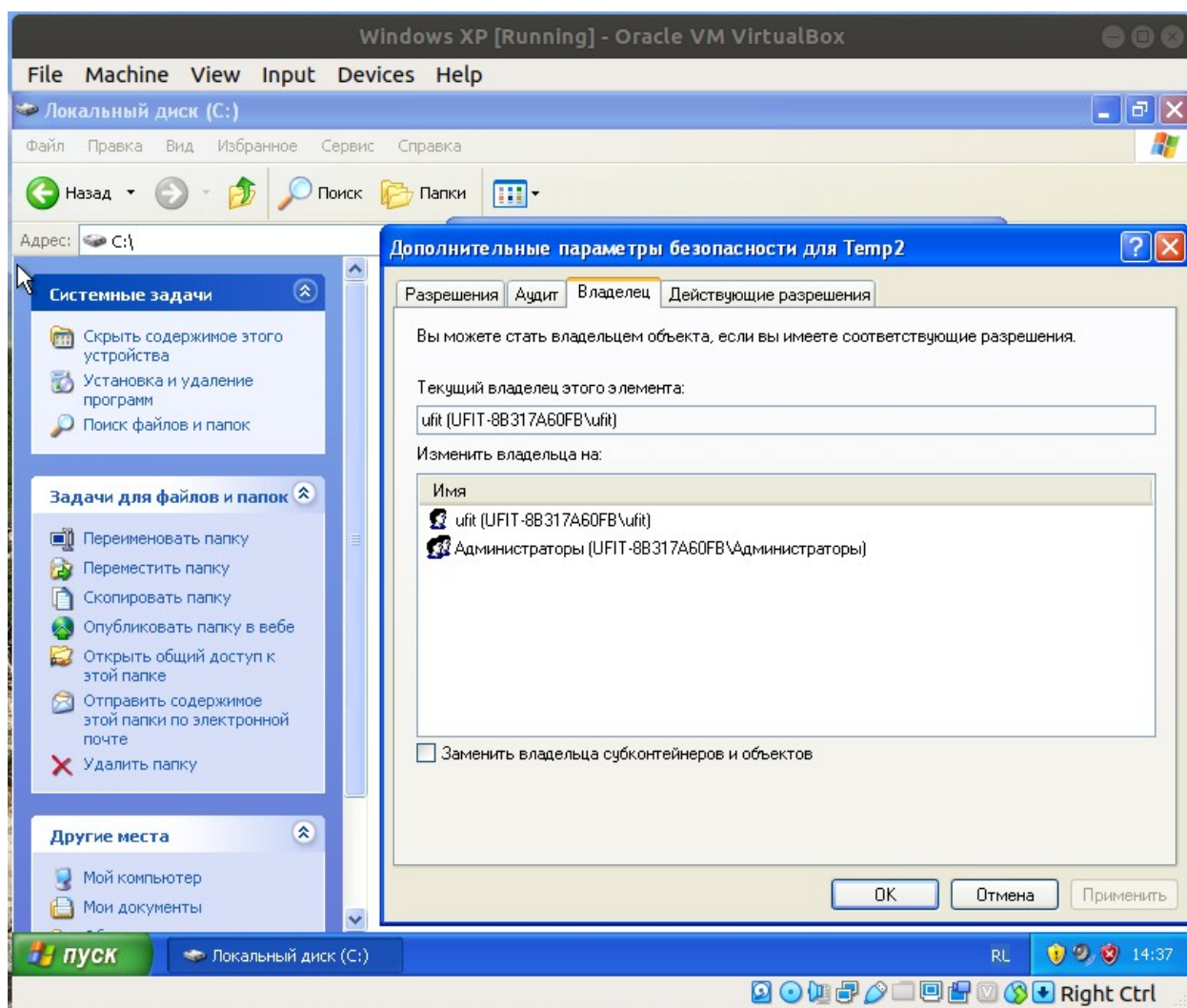
Пока вы находитесь в системе под учетной записью **ufit**, скопировать папку **C:\Temp2** в папку **C:\Temp1**. Для этого выделить значок папки **C:\Temp2** и, удерживая нажатой клавишу **CTRL**, перетащить мышью **C:\Temp2** в **C:\Temp1**.

Выделив **C:\Temp1\Temp2**, просмотреть разрешения и права владельца, затем сравнить разрешения и права владельца с папкой **C:\Temp2**.









Перемещение папки на одном и том же томе NTFS.

Войти в систему с учетной записью **ufit-3**. В **Проводнике** выделить значок папки **C:\Temp3**, затем переместить ее в папку **C:\Temp1**. Что произошло с разрешениями и владельцем для папки **C:\Temp1\Temp3**?

Владелец папки изменился. Владелцем **C:\Temp3** является ufit, а владельцем **C:\Temp1\Temp3** — ufit-3.

Задание 11. *Самостоятельно определить: как предотвратить удаление пользователями, имеющими разрешение **Полный доступ** к папке, файла в этой папке, для которого установлен запрет на разрешение **Полный доступ**?*

Запретить наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным.