

Лабораторная работа 8. Дискреционный механизм разграничения доступа к файловым объектам

Цель лабораторной работы: практическое изучение дискреционного механизма разграничения доступа на основе встроенных средств операционной системы Windows XP Professional, позволяющих управлять доступом к файлам и папкам файловой системы NTFS.

Задачи лабораторной работы:

1. Основные права доступа к файловым объектам
2. Элементы разрешений на доступ
3. «Владелец» файла
4. Наследование прав доступа
5. Разграничение доступа к принтерам

Задание

Контрольные вопросы

Содержание лабораторной работы:

Войдите в операционную систему под учётной записью «Администратор».

Для применения правил разграничения доступа необходимо воспользоваться вкладкой «Безопасность». Так как она по умолчанию отключена, её необходимо активировать. Для этого необходимо в разделе «Свойства папки» отключить опцию «Использовать простой общий доступ к файлам» (рис. 1).

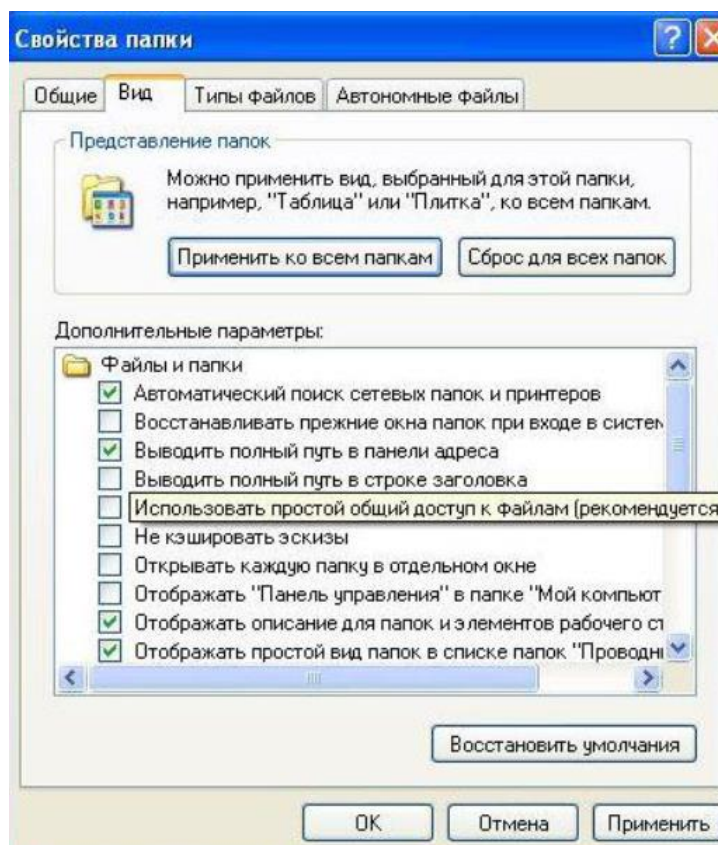


Рис. 1 - Раздел «Свойства папки»

1. Основные права доступа к файловым объектам

В NTFS все разрешения сводятся к шести стандартным разрешениям (Полный доступ, Изменить, Чтение и выполнение, Список содержимого папки, Чтение, Запись). Данные разрешения могут предоставляться пользователю (или группе пользователей) на доступ к объектам - каталогам и файлам. Право «Полный доступ» не только включает в себя все остальные разрешения, но и позволяет управлять разграничением доступа к данному объекту.

Назначение прав доступа пользователей осуществляется для каждого объекта. Назначить или изменить права доступа можно в «Свойствах» выбранного каталога или файла во вкладке «Безопасность». Сначала необходимо выбрать пользователя (или группу), которому будут назначаться разрешения.

Откройте вкладку «Безопасность» в «Свойствах» каталога <D:\Список содержимого папки>. Для изменения списка пользователей, имеющих право на доступ к объекту, нажмите на кнопку «Добавить» и выберите пользователя «user» (рис. 2).

Рис. 2 - Добавление нового пользователя

Установите пользователю «user» разрешение «Список содержимого папки» на доступ к текущему каталогу <D:\Список содержимого папки> (рис. 3).

Рис. 3 - Установка разрешения «Список содержимого папки»

Рис. 4 - Установка разрешения «Чтение»

Аналогично для пользователя «user» на каталоги «Чтение», «Чтение и выполнение», «Запись», «Изменение» и «Полный доступ» установите разрешения, соответствующие названиям этих каталогов (рис. 4-8).

Рис. 5 - Установка разрешения «Изменить»

Рис. 6 - Установка разрешения «Запись»

Рис. 7 - Установка разрешения «Чтение и выполнение»

Рис. 8 - Установка разрешения «Полный доступ»

Для проверки прав доступа, предоставленных пользователю при установке разрешений к заданным каталогам, войдите под учётной записью «user».

Разрешение «Список содержимого папки» предоставляет возможность просмотреть перечень объектов в данном каталоге. Войдите в соответствующий каталог и попытайтесь запустить исполняемый файл. Операционная система выдаст ошибку доступа к этому файлу (рис. 9). Попытайтесь открыть текстовый файл. Операционная система также выдаст ошибку доступа (рис. 10).

Рис. 9 - Ошибка доступа к исполняемому файлу

Рис. 10 - Ошибка доступа к текстовому файлу

Разрешение «Чтение» предоставляет возможность открывать в данном каталоге все файлы, кроме исполняемых. Войдите в соответствующий каталог и откройте текстовый файл. Измените текст в открытом файле и попытайтесь сохранить его. Операционная система выдаст ошибку доступа на создание файла (рис. 11). Попробуйте запустить исполняемый файл для проверки отказа в доступе.

Рис. 11 - Ошибка доступа на создание и сохранение изменённого текстового файла

Разрешение «Чтение и выполнение» предоставляет возможность открывать в данном каталоге все файлы. Войдите в соответствующий каталог и запустите исполняемый файл. Откройте текстовый файл, измените в нём текст и попытайтесь сохранить для проверки отказа в доступе на сохранение.

Разрешение «Запись» предоставляет возможность добавления файлов в данный каталог без права на доступ к вложенным в него объектам, в т.ч. на просмотр содержимого каталога. Попробуйте войти в соответствующий каталог. Операционная система выдаст ошибку доступа к каталогу (рис. 12). Для проверки возможности добавления файла создайте файл с именем «Запись» (например, на «Рабочем столе») и попытайтесь перетащить его в каталог «Запись». Операционная система выдаст ошибку копирования, т.к. файл с таким именем в каталоге существует. Переименуйте файл и повторно попытайтесь его перетащить - копирование выполнится (кроме того, наличие файла в каталоге можно проверить из под учётной записи «Администратор»).

Рис. 12 - Ошибка доступа к каталогу

Разрешение «Изменить» предоставляет возможность открывать и создавать (изменять) файлы в данном каталоге. Войдите в соответствующий каталог и запустите исполняемый файл. Откройте текстовый файл, измените в нём текст и сохраните его, создайте новый файл в каталоге. Откройте вкладку «Безопасность» у каталога «Изменение» или у любого вложенного файла и попытайтесь изменить права доступа к нему. Изменить права доступа нельзя (параметры включения разрешений неактивны), т.к. разрешение «Изменить» не включает возможность управления правами доступа (рис. 13).

Разрешение «Полный доступ» предоставляет все возможности для работы с каталогом и вложенными файлами, включая изменение разрешений. Для проверки откройте вкладку «Безопасность» у каталога «Полный доступ» или у любого вложенного файла и измените права доступа к нему.

Рис. 13 - Невозможность изменения разрешений на доступ

2. Элементы разрешений на доступ

Каждое стандартное разрешение состоит из нескольких элементов. Элементы разрешений позволяют более гибко настраивать права доступа пользователей. Войдите под учётной записью «Администратор».

Просмотреть элементы разрешений на доступ можно, нажав на кнопку «Дополнительно» во вкладке «Безопасность» и выбрав любой элемент разрешений (рис. 14). Наборы элементов, включаемых в стандартные разрешения, приведены на рис. 15-20.

Рис. 14 - Дополнительные параметры безопасности

Рисунок

Рис. 15 – Элементы разрешений для
«Списка содержимого папки»

Рис. 16 - Элементы разрешений для
«Чтения»

Рис. 17 - Элементы разрешений для
«Чтения и выполнения»

Рис. 18 - Элементы разрешений для
«Полного доступа»

Рис. 19 - Элементы разрешений для
«Изменить»

Рис. 20 - Элементы разрешений для
«Записи»

Использование возможностей элементов разрешений наиболее оправдано при разграничении доступа на удаление файла или каталога. Через элементы разрешений запретите пользователю «user» удаление каталога «Изменение», а также разрешите запись атрибутов на каталог «Чтение» (рис. 21-22).

Рис. 21 - Запрет удаления

Рис. 22 - Разрешение записи атрибутов

Для проверки установленных прав доступа войдите под учётной записью «user». Попытайтесь удалить файл из каталога «Изменение». Операционная система выдаст ошибку доступа на удаление файла (рис. 23).

Измените атрибуты файла в каталоге «Чтение» (например, атрибут «Скрытый» в свойствах файла). Примените сделанные изменения. Измените дополнительные атрибуты текстового файла в каталоге «Чтение» (например, автора документа во вкладке «Сводка» свойств файла). Попытайтесь применить сделанные изменения. Операционная система выдаст ошибку сохранения дополнительных атрибутов (рис. 24).

Рис. 23 - Ошибка доступа на удаление файла

Рис. 24 - Ошибка доступа на изменение дополнительных атрибутов

3. «Владелец» файла

В файловой системе NTFS у каждого объекта есть владелец. Владелец управляет назначением разрешений на доступ к объекту независимо от установленных разрешений. Создайте под учётной записью «user» в каталоге «Изменение» новый каталог (например, «test») и в нём текстовый файл (например, «test.txt»). Скопируйте в созданный текстовый файл информацию из файла «Изменение». Откройте вкладку «Владелец» файла «test.txt». В ней указывается текущий владелец объекта (рис. 25). Предоставьте полный доступ к созданному каталогу пользователю «user1» (рис. 26).

Рис. 25 - Вкладка «Владелец»

Рис. 26 - Предоставление прав пользователю «user1»

Войдите под учётной записью «user1».

Попытайтесь перейти в каталог «D:\Изменение\test» при помощи иерархического представления каталогов в «Проводнике». Переход невозможен, потому что у пользователя «user1» нет доступа к промежуточным каталогам. Попытайтесь перейти в тот же каталог, указав его полный путь в адресной строке «Проводника» (рис. 27). Откройте файл «test.txt». Таким образом, пользователь «user» может несанкционированно предоставить доступ пользователю «user1» к конфиденциальной информации.

Наличие полного доступа у пользователя «user1» к каталогу «test» позволяет ему изменять разрешения. Запретите доступ пользователя «Администратор» к файлу «test.txt» (рис. 28).

Рис. 27 - Доступ к каталогу через адресную строку

Рис. 28 - Запрет доступа к файлу

Дополнительно разрешение «Полный доступ» даёт возможность смены владельца файла. Смените владельца файла «test.txt» на пользователя «user1» (рис. 29).

Попытайтесь изменить владельца другого файла/каталога, к которому нет полного доступа (например, диска D:\). Операционная система выдаст ошибку изменения владельца (рис. 30).

Войдите под учётной записью «Администратор».

Попытайтесь получить доступ к файлу «test.txt». Несмотря на то, что «Администратор» не может получить доступ к файлу, он может сменить владельца. Измените владельца файла на группу «Администраторы». Закройте свойства файла. При повторном входе в свойства файла у пользователя появляется возможность устанавливать права доступа (рис.31). Пользователи и группы, имеющие право менять владельца, не обладая полным доступом к нему, перечисляются в групповых политиках в параметре «Овладение файлами и другими объектами» (рис.32).

Рис. 29 - Смена владельца файла

Рис. 30 - Ошибка смены владельца файла

Рис. 31 - Установка группы «Администраторы» в качестве владельца файла

Рис. 32 - Параметр «Овладение файлами и другими объектами»

4. Наследование прав доступа

NTFS поддерживает наследование разрешений, которое означает, что по умолчанию разрешения каталога распространяются на все его файлы и подкаталоги. Любые изменения разрешений на доступ к родительскому каталогу будут отражаться на его вложенных объектах.

Изменить унаследованные разрешения можно и со стороны вложенного объекта. Откройте вкладку «Разрешения» в дополнительных параметрах безопасности каталога «D:\Чтение\Чтение1» и отключите наследование (параметр «Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне»). При отключении наследования скопируйте текущие разрешения (рис. 33).

Рис. 33 - Выбор действия при отключении наследования

После отключения наследования каталогом разрешений от родительского в разделе «Унаследовано» у каждого элемента устанавливается значение «не унаследовано» (рис. 34). Описание изменений в разделе «Унаследовано».

Рис. 34 - Элементы разрешений при отключенном наследовании

Изменить действующие разрешения у вложенных объектов можно при помощи параметра «Заменить разрешения для всех дочерних объектов заданными здесь разрешениями, применимыми к дочерним объектам». Удалите учётную запись «user» из числа санкционированных пользователей каталога «Чтение1». В родительском для него каталоге «Чтение» установите изменение прав дочерних объектов (рис. 35). Проверьте восстановление учётной записи «user» в перечне санкционированных пользователей каталога «Чтение1».

При установке прав доступа на элементы можно выставлять не только разрешения, но и запреты. Запретите группе «Пользователи», членом которой является «user» (учётной записи «user» чтение разрешено) чтение файла «Чтение» (рис. 36). Войдите под учётной записью «user». Попробуйте открыть файл «Чтение». Невозможность открыть файл обусловлена тем, что запреты приоритетнее разрешений.

Рис. 35 - Включение принудительного наследования

Рис. 36 - Установка запрета на чтение

Действующие разрешения можно просмотреть в одноимённой вкладке Дополнительных параметров безопасности, выбрав интересующего пользователя или группу. Войдите под учётной записью «Администратор». Просмотрите действующие разрешения на файл «Чтение» для пользователя «user» (рис. 37). Удалите группу «Пользователи» из перечня разрешений. Повторно просмотрите действующие разрешения пользователя «user» (рис. 38). Таким образом, разрешения, предоставленные пользователю и группе, в которую он входит, суммируются. И после удаления элемента, запрещающего группе «Пользователи» чтение, у пользователя «user» остались только свои права.

Рис. 37 - Действующие разрешения пользователя

Рис. 38 - Действующие разрешения пользователя после изменения разрешений

При выставлении разрешений существует возможность указывать глубину наследования и типы объектов. Можно распространить установленные разрешения на данный каталог, только на вложенные объекты или на каталог и все его вложенные объекты, а также можно указать на вложенные каталоги или файлы будут распространяться разрешения.

Разрешите на каталог «Чтение» пользователю «user» создание папок только для подпапок, вложенных в этот каталог (рис. 39), т.е. в каталогах «Чтение» и «Чтение2» подпапки создавать будет запрещено, а в каталоге «Чтение1» (непосредственно вложенном в «Чтение») - разрешено. Войдите под учётной записью «user». Проверьте возможность создания папок во всех указанных каталогах.

Рис. 39 - Выбор глубины и типа объектов наследования

5. Разграничение доступа к принтерам

Под учётной записью «user» отправьте текстовый файл на печать при помощи принтера doPDF.

В разделе «Принтеры и факсы» меню «Пуск» попытайтесь изменить настройки принтера (рис. 40). Невозможность изменения настроек объясняется наличием у группы «Все» только права на «Печать» (отсутствием права на «Управление принтерами») (рис. 41).

Рис. 40 - Свойства принтера

Рис. 41 - Разграничение доступа к принтеру

Войдите под учётной записью «Администратор». Удалите из списка доступа к принтеру doPDF группу «Все».

Войдите под учётной записью «user».

Попытайтесь напечатать текстовый файл. Откройте раздел «Принтеры и факсы», в котором doPDF отсутствует, т.к. «user» не входит в список пользователей, имеющих право на работу с принтером.

Задание

Создайте каталоги «Общедоступно» и «Конфиденциально». В каждом из этих каталогов скопируйте исполняемый и текстовый файлы. Разграничьте доступ к принтеру, а также созданным каталогам и файлам в соответствии со своим вариантом.

Вариант 1

<i>Субъекты</i>	<i>Объекты</i>		
	<i>Общедоступно</i>	<i>Конфиденциально</i>	<i>Принтер</i>
Администратор	Полный доступ	Чтение	Полный доступ
user	Чтение	Изменить, кроме удаления	Печать Управление документами
User1	Изменить	Нет доступа	Печать

Вариант 2

<i>Субъекты</i>	<i>Объекты</i>		
	<i>Общедоступно</i>	<i>Конфиденциально</i>	<i>Принтер</i>
Администратор	Полный доступ	Чтение и выполнение	Полный доступ
user	Изменить	Чтение	Печать
user1	Чтение и выполнение	Изменить	Печать Управление документами

Вариант 3

<i>Субъекты</i>	<i>Объекты</i>		
	<i>Общедоступно</i>	<i>Конфиденциально</i>	<i>Текстовый файл в «Конфиденциально»</i>
Администратор	Полный доступ	Список содержимого	Нет доступа
user	Чтение	Изменить, кроме удаления	Изменить
user1	Изменить	Нет доступа	Нет доступа

Вариант 4

<i>Субъекты</i>	<i>Объекты</i>		
	<i>Общедоступно</i>	<i>Конфиденциально</i>	<i>Текстовый файл в «Конфиденциально»</i>
Администратор	Изменить	Чтение и выполнение	Нет доступа

user	Чтение	Изменить	Запрет удаления
user1	Полный доступ, кроме владельца смены	Запись	Нет доступа

Вариант 5

<i>Субъекты</i>	<i>Объекты</i>		
	<i>Общедоступно</i>	<i>Конфиденциально</i>	<i>Исполняемый файл в «Конфиденциально»</i>
Администратор	Полный доступ	Список содержимого	Выполнение
user	Чтение	Чтение и удаление	Выполнение, запрет удаления
user1	Изменить, кроме удаления	Запись	Нет доступа

Вариант 6

<i>Субъекты</i>	<i>Объекты</i>		
	<i>Общедоступно</i>	<i>Конфиденциально</i>	<i>Исполняемый файл в «Конфиденциально»</i>
Администратор	Полный доступ	Чтение	Изменить
user	Чтение и удаление	Список содержимого	Выполнение
user1	Изменить	Нет доступа	Нет доступа

Вариант 7

<i>Субъекты</i>	<i>Объекты</i>		
	<i>Общедоступно</i>	<i>Конфиденциально</i>	<i>Текстовый файл в «Конфиденциально»</i>
Администратор	Список содержимого	Полный доступ	Нет доступа
user	Изменить, кроме удаления	Чтение	Изменить
user1	Нет доступа	Изменить	Нет доступа

Вариант 8

<i>Субъекты</i>	<i>Объекты</i>		
	<i>Общедоступно</i>	<i>Конфиденциально</i>	<i>Текстовый файл в «Конфиденциально»</i>
Администратор	Чтение и выполнение	Изменить	Нет доступа
user	Изменить	Чтение	Изменить, запрет изменения дополнит. атрибутов
user1	Запись	Изменить, кроме удаления	Нет доступа

Вариант 9

<i>Субъекты</i>	<i>Объекты</i>		
	<i>Общедоступно</i>	<i>Конфиденциально</i>	<i>Исполняемый файл в «Конфиденциально»</i>
Администратор	Список содержимого	Полный доступ	Выполнение
user	Чтение и удаление	Чтение	Выполнение, запрет удаления
user1	Запись	Полный доступ	Нет доступа

Вариант 10

<i>Субъекты</i>	<i>Объекты</i>		
	<i>Общедоступно</i>	<i>Конфиденциально</i>	<i>Исполняемый файл в «Конфиденциально»</i>
Администратор	Чтение	Полный доступ	Изменить
user	Список содержимого	Чтение и удаление	Выполнение
user1	Нет доступа	Изменить	Нет доступа

Контрольные вопросы

1. Охарактеризуйте дискреционную модель управления доступом.
2. Перечислите стандартные права доступа к файловым объектам, существующие в файловой системе NTFS.
3. Объясните принцип работы разрешения «Запись».
4. Перечислите элементы разрешений.
5. Кто может стать владельцем объекта?
6. Раскройте понятие наследования разрешений.
7. Как отключить наследование разрешений?
8. Как реализовать принудительное наследование вложенными объектами установленных разрешений?
9. Перечислите приоритеты применения разрешений при определении действующих разрешений на доступ к файловым объектам.
10. Перечислите стандартные права доступа к принтерам, существующие в файловой системе NTFS.

Задание

Отчет по лабораторной работе выполняется по стандарту, описанному в методических указаниях

Рис.

Рис.

Рис.

