Лабораторная работа № 7
Управление доступом к данным ОС.

Цель работы: Освоение навыков управления доступом пользователей к файлам и папкам с целью защиты информации от несанкционированного доступа.

Оборудование: ПК, ОС Windows.

Время выполнения: 90 минут.

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

Файловые системы современных операционных систем при соответствующей настройке эффективно обеспечивают безопасность и надежность хранения данных на дисковых накопителях. Для операционных систем Windows стандартной является файловая система NTFS.

Устанавливая для пользователей определенные разрешения для файлов и каталогов (папок), администраторы могут защитить информацию от несанкционированного доступа. Каждый пользователь должен иметь определенный набор разрешений на доступ к конкретному объекту файловой системы. Кроме того, он может быть владельцем файла или папки, если сам их создает. Администратор может назначить себя владельцем любого объекта файловой системы, но обратная передача владения от администратора к пользователю невозможна.

Назначение разрешений производится для пользователей или групп. Так как рекомендуется выполнять настройки безопасности для групп, то необходимо, чтобы пользователь был членом хотя бы одной группы на компьютере или в домене.

Разрешения могут быть установлены для различных объектов компьютерной системы, однако в этой работе будут рассмотрены разрешения для файлов и папок. Другие задачи, например разрешения для принтеров, решаются аналогичным образом.

Назначения разрешений для файла или папки администратор выбирает данный файл или папку и при нажатии правой кнопки мыши использует команду Свойства и в появившемся окне переходит на вкладку Безопасность. Пример для папки с именем Авиатор приведен на рисунке 1.1.

В зоне Имя имеется список групп и пользователей, которым уже назначены разрешения для данного файла или папки.

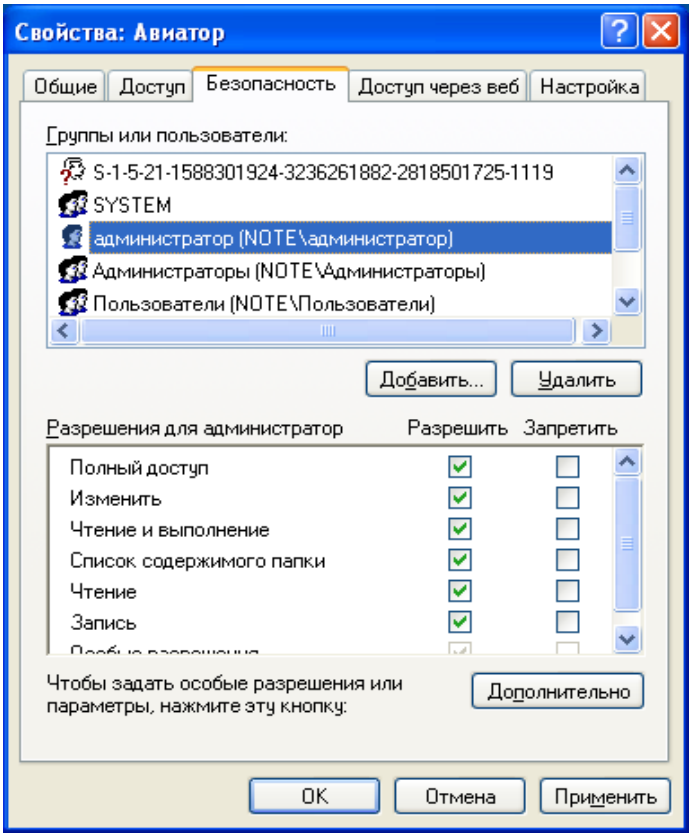

Рисунок 1.1 Вкладка Безопасность окна свойств папки Авиатор

Для добавления пользователя или группы нажмите кнопку Добавить или Удалить. При добавлении появится диалог Выбор: Пользователи, Компьютеры или Группы. Добавив пользователя или группу, мы увидим этот объект в зоне Имя и выделив его, можем задать необходимые разрешения с помощью установки флажков Разрешитьили Запретить в зоне Разрешения.

Стандартные разрешения для файлов:

- Полный доступ;
- Изменить;
- Чтение и выполнение;
- Чтение;
- Запись.

Стандартные разрешения для папок:

- Полный доступ;
- Изменить;
- Чтение и выполнение;
- Список содержимого папки
- Чтение;
- Запись.

Разрешение Чтение позволяет просматривать файлы и папки и их атрибуты.

Разрешение Запись позволяет создавать новые файлы и папки внутри папок, изменять атрибуты и просматривать владельцев и разрешения.

Разрешение Список содержимого папки позволяет просматривать имена файлов и папок.

Разрешение Чтение и выполнение для папок позволяет перемещаться по структуре других папок и служит для того, чтобы разрешить пользователю открывать папку, даже если он не имеет прав доступа к ней, для поиска других файлов или вложенных папок. Разрешены все действия, право на которые дают разрешения Чтение и Список содержимого папки. Это же разрешение для файлов позволяет запускать файлы программ и выполнять действия, право на которые дает разрешение Чтение.

Разрешение Изменить позволяет удалять папки, файлы и выполнять все действия, право на которые дают разрешения Запись и Чтение и выполнение.

Разрешение Полный доступ позволяет изменять разрешения, менять владельца, удалять файлы и папки и выполнять все действия, на которые дают право все остальные разрешения NTFS.

Разрешения для папок распространяются на их содержимое: подпапки и файлы.

При назначении пользователю или группе разрешения на доступ к файлу или папке руководствуются тем уровнем доступа, который достаточен для данной группы или пользователя при выполнении им своих рабочих обязанностей.

Рассмотренные разрешения относятся к пользователям данного компьютера, совершившим вход локально непосредственно на данную машину. Такие разрешения называются разрешениями файловой системы.

Так как файловая система WindowsназываетсяNTFS, то разрешения файловой системы дляWindowsназывают разрешениямиNTFS.

Разрешения для пользователей, получившим доступ к папке или файлу через сеть, регулируются отдельно с помощью так называемых разрешений общего доступа. Эти разрешения распространяются только на папки, к которым предоставлен общий доступ через сеть и действуют только для пользователей, обращающихся к папке через сеть. Возможности пользователя задаются разрешениями, представленными ниже:

- Полный доступ;
- Изменить;
- Чтение;

Доступ к средствам настройки разрешений общего доступа выполняется через свойства папки, предоставленной в общий доступ (рисунок 1.2)

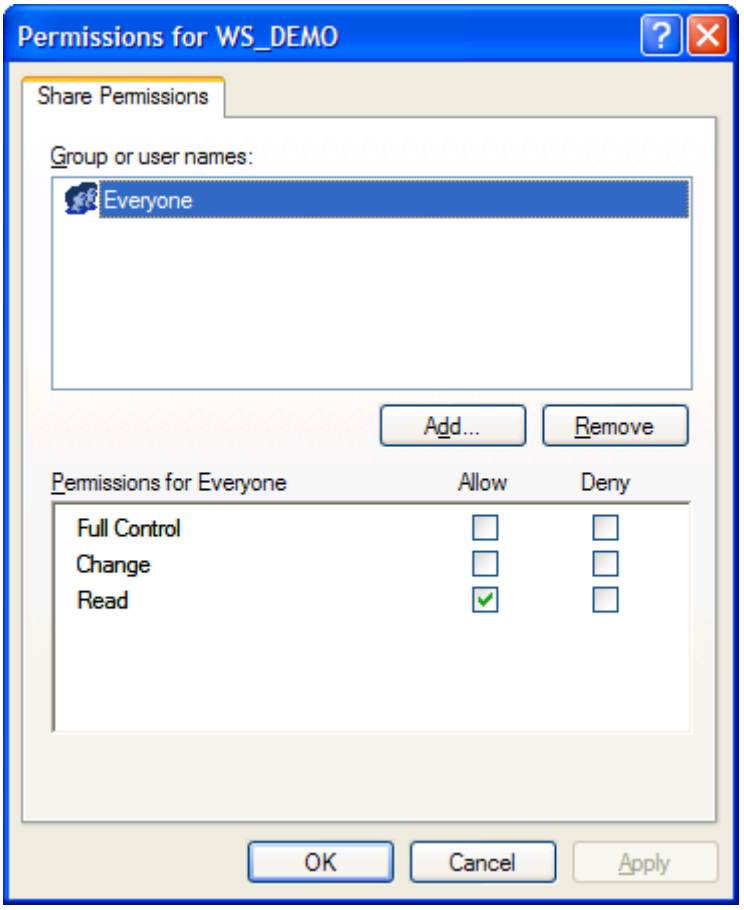

Рисунок 1.2 Разрешения общего доступа для папки WS_DEMO

Разрешения общего доступа являются средством обеспечения безопасности данных при коллективной работе с документами и поэтому должны устанавливаться очень тщательно и обоснованно. При этом администратору рекомендуется действовать следующим образом.

- Для каждого ресурса общего доступа определить, каким группам пользователей необходим доступ к нему и какой требуется уровень доступа;
- Для упрощения администрирования назначайте разрешения группам, а не отдельным пользователям;
- Устанавливайте максимально строгие разрешения, которые, однако, должны позволять пользователям совершать необходимые действия;
- Организуйте ресурсы общего доступа таким образом, чтобы папки с одинаковым уровнем требований безопасности находились в одной папке. Затем установите общий доступ только к ней, все вложенные папки наследуют настройки безопасности;
- Для папок общего доступа применяйте интуитивно понятные пользователям имена, корректно отображаемые всеми клиентскими операционными системами, используемыми на предприятии.
- Если в общих папках предполагается хранить программы-приложения, то целесообразно поместить их в одну папку – единое место хранения и обновлении я приложений;

Несколько общих папок, доступных членам группы Администраторы, так называемые скрытые Административные общие папки, создаются операционной системой автоматически. Имена этих папок заканчиваются знаком $. Это корневые каталоги каждого тома на жестком диске (C$,D$ и т.д.), папкаAdmin$ для доступа к системному каталогу, папкаPrint$ для доступа к файлам драйверов принтеров.

Кроме того, скрытую папку с общим доступом можно создать с целью доступа к ней только тех пользователей, которые будут знать имя скрытой папки.

Получить доступ к общим папкам других компьютеров можно используя компоненты Сетевое окружение, Мой компьютер, Мастер добавления в сетевое окружении и команду выполнить (Run).

Соединение с общей папкой через Сетевое окружение выполняется двойным щелчком по ресурсу, к которому необходимо получить доступ. Если общий ресурс отсутствует в списке доступных, выберите значок Добавить новый элемент в сетевое окружение и укажите адрес подключаемого ресурса.

Соединение с общей папкой через компонент Мой компьютер выполняется через меню Сервис этого компонента в пункте Подключить сетевой диск при указании пути к общему ресурсу. Если необходимо пользоваться этим соединением постоянно, нужно чтобы флажок Восстанавливать при входе в систему был установлен. Соединение будет доступно в разделе Сетевые диске окна Мой компьютер.

Для соединения с общей папкой с помощью команды Выполнить щелкните Пуск, затем Выполнить и введите путь к папке в формате UNC(\\имя_ компьютера\имя_общей папки).

Рассмотрим, как пользоваться средствами установки разрешений файловой системы и общего доступа.

После выбора объекта, для которого будет выполняться настройка разрешений файловой системы, в диалоговом окне свойств файла или папки необходимо выбрать вкладку Безопасность, показанную на рисунке 1.3.

В данном случае показано, что для папки Авиатор для группы Администраторы установлены разрешения уровня Полный доступ, а для группы Все разрешения ограничены на уровне Чтение.

При установке разрешений в списке групп можно заметить имена так называемых встроенных системных групп, невидимых при использовании оснасток для управления группами и пользователями. Эти группы не имеют определенных членств, которые можно назначить или изменить, но в них система включает различных пользователей в различное время, в зависимости от того, каким образом пользователь получает доступ к системе или ресурсам.

Разрешения можно не только устанавливать, но запрещать. Запрет имеет больший приоритет, чем разрешение. Запрет разрешений как метод контроля ресурсов Microsoftприменять не рекомендует, и он используется, в основном, для дополнительной настройки разрешений конкретным пользователям, в отличие от разрешений для других пользователей группы.

Рассмотренные разрешения называются стандартными и позволяют решить большинство задач, связанных с регулированием уровня доступа групп к ресурсам.

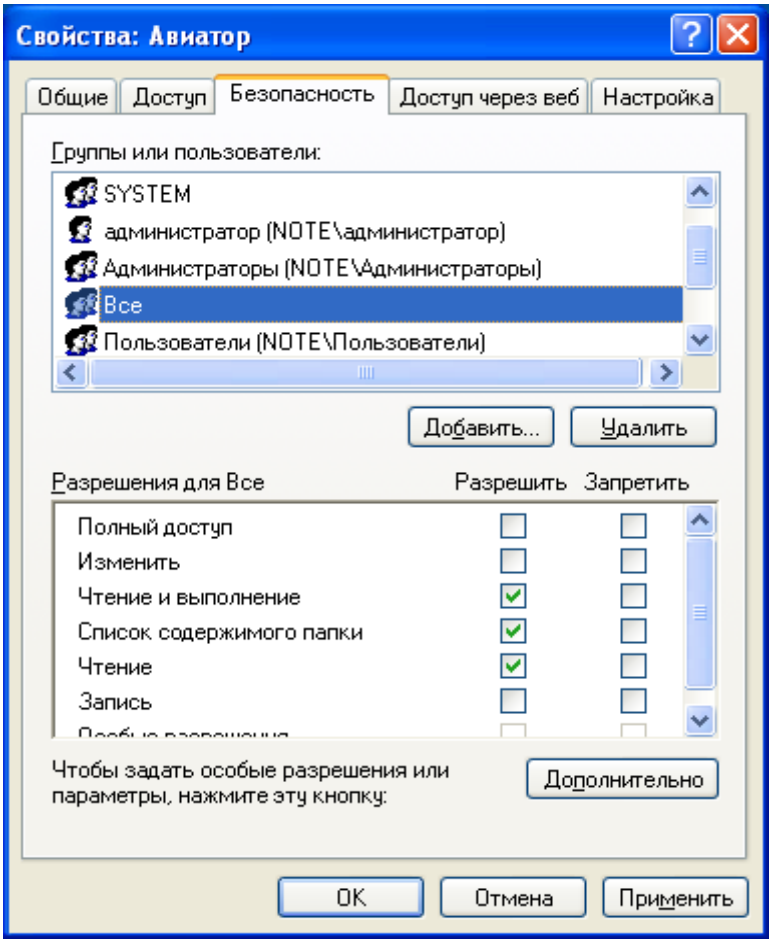

Рисунок 1.3 Установка разрешений для группы Все

Кнопка Дополнительно служит для задания специальных разрешений. Каждое стандартное разрешение состоит из нескольких специальных, например, стандартное разрешение Запись состоит из шести специальных разрешений: создание файлов/запись данных, Создание папок/запись данных, запись атрибутов, Запись дополнительных атрибутов, чтение разрешений, синхронизация. Специальные разрешения можно использовать для более тонкой настройки в нестандартных ситуациях.

В окне специальных разрешений имеются закладки Аудит, Владелец и Эффективные разрешения.

Аудит - это процесс, позволяющий фиксировать события, происходящие в системе и имеющие отношения к безопасности. На данной вкладке производится выбор пользователя или группы, для которых данная папка (или файл) будет объектом аудита. Аудит изучается в лабораторной работе № 6.

Закладка Владелец обеспечивает такое свойство безопасности, как право владения объектом файловой системы. Администратор всегда может стать владельцем любого объекта файловой системы, любой пользователь является владельцем созданных им объектов и, если локальные или доменные политики безопасности разрешат, пользователь может назначать себя владельцем других файлов и папок.

Подробное рассмотрение вопросов владения выходит за рамки данного пособия, однако отметим, что многие операции с файлами и папками, например: смена разрешений, шифрование и дешифрование привязаны к факту владения данным объектом.

Список управления доступом (ACL) хранится на дискеNTFSдля каждого файла или папки. В нем перечислены пользователи и группы, для которых установлены разрешения для файла или папки, а также сами назначенные разрешения.

Каждому пользователю или группе могут быть установлены множественные разрешения через участие в нескольких группах с разным набором разрешений. В этом случае действуют эффективные разрешения – пользователь обладает всеми назначенными ему разрешениями.

Действует приоритет разрешений для файлов над разрешениями для папок и приоритет запрещения над разрешением.

Разрешения, назначенные родительской папке, по умолчанию наследуются всеми подпапками и файлами, содержащимися в папках. Однако есть возможность предотвратить наследование для любой вложенной папки и в этом случае эта папка сама становится родительской для вложенных в нее папок.

Если папка предоставлена для общего доступа, то на нее распространяются разрешения двух видов:

- разрешения файловой системы, установленные для пользователей данного компьютера;
- разрешения общего доступа, объявленные для пользователей, получивших доступ через сеть.

Обычно для папок общего доступа задают разрешения полного доступа, а ограничения вводят установкой разрешений NTFS.

В этом случае действует объединение разрешений NTFSи разрешений для общей папки, при котором наиболее строгое разрешение имеет приоритет над другими.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

Задание 1. Создать новую учетную запись (Имя учетной записи: ISИмя) с правами обычного доступа.

Задание 2. Создать на диске С папку Share (в пользователи Admin), внутри папки создать еще две папки: Документы и Личное.

Задание 3. В папку Документы поместить:

- Блокнот (Скопировать в блокнот «Основные сведения» с сайта aktt.org)
- В сети Интернет найти базу данных (БД) и поставить на нее пароль (Можно использовать свою БД)
- Архив с паролем, содержимое архива – блокнот и БД.

Задание 4.В папку Личное поместить:

- Word-документ (Поместить внутрь документа любимое стихотворение/ рассказ и в интернете найти подходящую картинку)
- 2-3 картинки из интернета.

Задание 5.

1. На созданный ранее файл Блокнот для пользователя «Студент» поставить «полный доступ», для пользователя «ISИмя» - «Запретить полный доступ».
2. Файл с БД для пользователей «Студент» и «IS Имя», предоставить права «Чтение».
3. Для Архива всем пользователям предоставить права «Изменения».
4. Экспериментально проверьте доступ и функции к этим файлам с разных пользователей ПК.

Задание 6.

1. На папку Личное для всех пользователей поставить полный запрет, кроме пользователя «ISИмя» (Для этого пользователя предоставить «полный доступ»).
2. Экспериментально проверьте доступ и функции к этим файлам с разных пользователей ПК.

Задание 7. При попытке изменить, открыть или удалить папку/файл в Windows возможно получить данное сообщение «Нет доступа к папке»/ «Запросите разрешение на изменение этой

папки» и аналогичные. Есть несколько способов этого решения: стать владельцем данной информации, использование командной строки для получения владельца и использование стороннего ПО.

Примечание: для всех действий необходимо иметь права администратора.

Командная строка.

А) Для того, чтобы изменить владельца папки или файла с помощью командной строки, имеются две команды, первая из них — takeown.

Для ее использования, запустите командную строку от имени Администратора (в Windows 8 и Windows 10 это можно сделать из меню, вызываемого правым кликом по кнопке Пуск, в Windows 7 — с помощью правого клика по командной строке в стандартных программах).

В командной строке, в зависимости от того, владельцем какого объекта вам нужно стать, введите одну из команд:

- takeown /F “полный путь к файлу” — стать владельцем указанного файла. Чтобы сделать всех администраторов компьютера владельцами, используйте параметр /A после пути к файлу в команде.
- takeown /F “путь к папке или диску” /R /D Y — стать владельцем папки или диска. Путь к диску указывается в виде D: (без слэша), путь к папке — C:\Folder (также без слэша).

Б) Еще одна команда, которая позволяет получить доступ к папке или файлам (изменить их владельца) — icacls, использовать которую следует так же, в командной строке, запущенной от имени администратора.

Пути указываются аналогично предыдущему способу. Если требуется сделать владельцами всех администраторов, то вместо имени пользователя используйте Администраторы (или, если не сработает, Administrators).

Дополнительная информация: помимо того, чтобы стать владельцем папки или файла, вам может потребоваться также получить разрешения для изменения, для этого вы можете использовать следующую команду (дает полные права пользователю для папки и вложенных объектов): ICACLS «%1» /grant:r «имя_пользователя»:(OI)(CI)F

В) Есть и другие способы решить проблему «отказано в доступе» и быстро стать владельцем, например, с помощью сторонних программ, встраивающих пункт «Стать владельцем» в контекстное меню проводника. Одна из таких программ — TakeOwnershipPro, бесплатная и, насколько я могу судить, без чего-то потенциально нежелательного. Аналогичный пункт в контекстное меню можно добавить и путем редактирования реестра Windows.

При помощи данной информации изменить владельца какого-либо файла. (Использовать все способы)

Задание 8.

1. Для папки Share предоставить «общий доступ» для пользователей локальной сети.
2. Экспериментально проверьте доступ к этим файлам и возможные действия с этими файлами.

Задание 9. Создайте еще одну папку C:\\Share\asd. Объединитесь со студентами за соседним ПК и через локальную сеть в папку asd перенесите все ранее созданные документы, которые сможете.

Контрольные вопросы:

1. Какие файловые системы вам известны?

1. Какое разрешение NTFS позволяет вам удалят папки?
2. Какой вкладкой диалогового окна «Свойства» файла или папки следует воспользоваться для установки или изменения разрешений NTFS.
3. Можно ли запретить администратору системы доступ к какому – либо файлу? Может ли он обойти это ограничение?
4. Как изменить владельца объекта в среде Windows?
5. В чем различие между избирательным и обязательным управлением доступом? Какой из этих подходов более надежен?

Литература:

1. А.В. Батаев, Н.Ю. Налютин, С.В. Синицын. Операционные системы и среды. -М. : Издательский центр «Академия», 2017.-272с.

2. Танэнбаум Э., Бос Х. Современные операционные системы. 4-е изд.- СПБ.: Питер 2015.- 1120с.

3. Назаров С.В. Операционные системы . - М. : КНОРУС, 2016. -376с.