**1. Управление доступом Windows**

**1) Рассмотреть систему управления доступом к ресурсам Windows. Выписать и объяснить состав типов всех возможных субъектов безопасности, которым может быть предоставлен доступ к ресурсу**

Управление доступом – процесс авторизации субъектов Windows для доступа к объектам в сети или на компьютере. Основные понятия, составляющие управление доступом, — это разрешения, владение объектами, наследование разрешений, права пользователей и аудит объектов. Доступ к ресурсу проходит следующем образом: у каждого пользователя и группы есть свой SID, по которому можно узнать где состоит тот или иной субъект, а также какие назначены права и разрешения для них. У каждого ресурса есть владелец, который распоряжается разрешениями для участников безопасности, и система, проверяя эти права и разрешения, предоставляет доступ к ресурсу, учитывая, какие права они имеют к этому ресурсу. У участников безопасности есть права на чтение, изменение, чтение и запись и полный доступ к таким объектам, как файлы, папки, принтеры, разделы реестра и объекты доменных служб AD. Обычно владельцы объектов предоставляют права к ресурсам группам, а не отдельным пользователем и также предоставляют права не к отдельным ресурсам, а к контейнеру ресурсов для удобства управления доступом

Рассмотрим субъектов безопасности:

1. Локальные учетные записи. По умолчанию всегда имеются учетные записи Администратора и Гостя. Так как учетные записи локальные, то они доступны только тому компьютером, на котором они находятся
2. Локальные группы. Содержат группу пользователей в себе для упрощения управления доступа к ресурсам. Так же доступны только определенному компьютеру
3. Учетные записи AD. Учетной запись, которая используется внутри домена.
4. Группы AD. Содержат группы пользователей доменов в себе для упрощения управления доступа к ресурсам. Так же делятся на 3 типа, которые зависят от области применения
   1. Локальная в домене – используется для управления доступа к ресурсам внутри своего домена
   2. Глобальная – используется для управления доступа к ресурсам внутри своего домена, а также может управлять доступом к ресурсам любого другого домена, но это не рекомендуется делать
   3. Универсальная – используется для управления доступа к любым доменам

**2) Свести в таблицы перечень субъектов безопасности, доступных для конкретного узла, классифицировав по типам локальных и доменных учетных записей пользователей и групп.**

**Локальные учетные записи пользователей и группы.**

|  |  |  |
| --- | --- | --- |
| Локальные учетные записи | Локальные группы | Специальные группы |
| Администратор | Администраторы | Все |
| Гость | Пользователи | Прошедшие проверку |
| Система | Пользователи DCOM | Интерактивные |
|  | Пользователи журналов производительности | Консольный вход |
|  | Пользователи системного монитора | Анонимный вход |
|  | Пользователи удаленного рабочего стола | Все пакеты приложений |
|  | Опытные пользователи | Пользователь сервера терминалов |
|  | Гости | Служба |
|  | Репликатор | Local Service |
|  | Операторы архива | NT Service |
|  | Операторы печати | Права владельца |
|  | Операторы настройки сети | Сеть |
|  | Криптографические операторы | Создатель-владелец |
|  | Читатели журнала событий | Удаленный доступ |
|  | IIS\_IUSRS |  |
|  | Доступ DCOM службы сертификации |  |

**Доменные учетные записи пользователей и групп.**

|  |  |  |  |
| --- | --- | --- | --- |
| Учетные записи | Локальные группы | Универсальные группы | Глобальные группы |
| Администратор | Издатели сертификатов | Контроллеры домена предприятий | DNSUpdateProxy |
| Гость | Группа с разрешение репликации RODC | Администраторы схемы | Администраторы домена |
|  | Группа с запрещением репликации RODC | Администраторы предприятий | Владельцы – создатели групповой политики |
|  | Сервера RAS и IAS |  | Гости домена |
|  | DNSAdmins |  | Контроллеры домена |
|  |  |  | Компьютеры домена |
|  |  |  | Пользователи домена |

**3) Вывод**

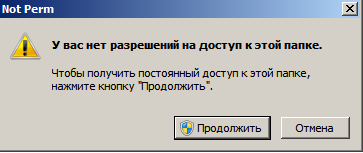
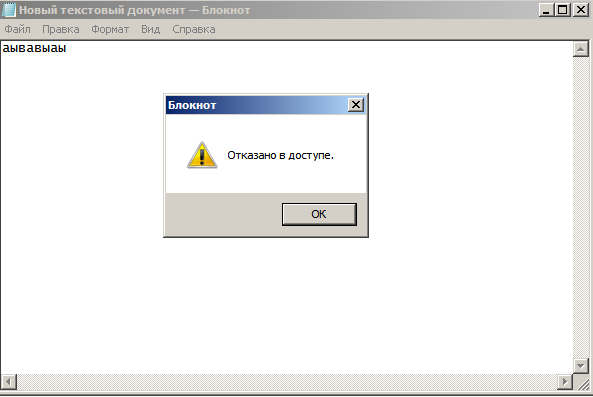
Была рассмотрена система управления Windows, перечислены субъекты безопасности, сведены в 2 таблицы перечни субъектов безопасности.

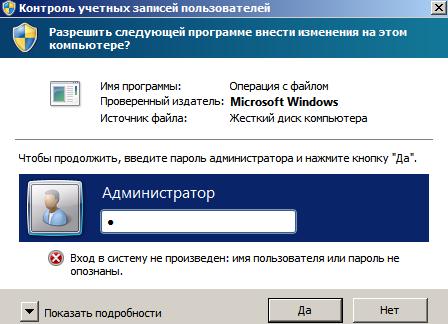
**2.** . **В каталоге \Student\Temp создать различные подкаталоги и файлы и назначить разрешения доступа для созданных пользователей. Войти в систему от имени пользователей и проверить их возможности доступа к объектам файловой системы.**

Создадим папку \Student\Temp и дадим для student полный доступ к ней. В ней, а также всех её подпапках отключим наследование разрешений, чтобы это функция не мешала менять нам разрешения для подкаталогов. Создадим 3 папки:

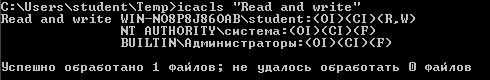
1. Not Perm – папка, для которой отсутствует доступ для student
2. Only Read – папка, для которой доступно только чтение для student
3. Read and Write – папка для которой доступно только чтение и запись для student

Зайдем в папку Temp от имени пользователя, и попробуем зайти в папку Not Perm, в которую у нас нет доступа. Из-за отсутствия доступа, когда мы заходим в папку, нам предлагают зайти от другого пользователя, так как нет разрешения на папку. Теперь посмотрим на папку Read. Зайдя в неё, мы видим ее файлы и можем их читать, но, когда мы пытаемся записать в него свой текст, нас предупреждают о том, что у нас нет доступа к ней. В папке Read and Write мы можем записывать изменения в файле, но не можем удалять или перемещать файл

** **

****

**2) Применить команду icacls для получения информации о разрешениях доступа на командном уровне.**

****

Применив команду icacls видим, что разрешения соответствуют тому, что мы задали

**3) Вывод**

Были опробованы различные разрешения для файлов и каталогов,изучен механизм запретов доступа, опробована команда icacls для получения информации о разрешениях доступа

**3. Соотнести различные варианты разрешений доступа к каталогам и файлам с допустимыми и запрещенными действиями над объектами файловой системы (создание, удаление, копирование, перемещение, изменение содержимого, получение информации о свойствах, смены владельца и др.)**. **Выполнить проверки для неочевидных комбинаций разрешений, назначенных на каталог и файлы в нем.**

**1) Сформировать таблицу результатов, в которой в строках перечислены варианты разрешений доступа, а в столбцах отмечены доступные операции.**

Пускай в таблице будут такие обозначения F – полный доступ (Full Permission), C – изменения (Changes), RE – чтение и выполнение (Read and Execution), R – чтение (Read) W – запись (Write).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Смена владельца | Выполнение | Удаление | Удаление подпапок и файлов | Перемещение | Чтение | Запись | Чтение разрешений |
| F | + | + | + | + | + | + | + | + |
| C | - | + | + | - | + | + | + | + |
| RE | - | + | - | - | - | + | - | + |
| W | - | - | - | - | - | - | + | - |
| R | - | - | - | - | - | + | - | + |

Также windows позволяет самому настроить доступные операции для групп и пользователей, отмечая разрешение доступа – Особые разрешения.

**2) Вывод**

Выполнить проверки для неочевидных комбинаций разрешений, назначенных на каталог и файлы в нем.

**4. Наследование**

**1) Рассмотреть свойства наследования разрешений доступа и опробовать варианты.**

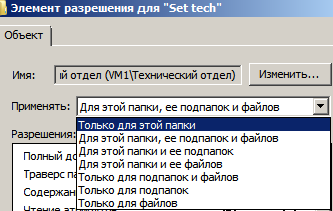
Есть 3 варианта наследования:

1. Наследование идет от родительского каталога, при этом родительский каталог сам унаследовал разрешение от своего родительского каталога.

2. Наследование идет от родительского каталога, но родительский каталог не наследует разрешения своего родительского каталога.

3. Дочерний каталог не наследует разрешения родительского каталога.

В параметрах разрешения можно указать наследование для каталога, задав ему направление

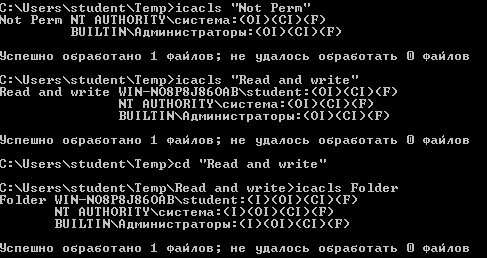


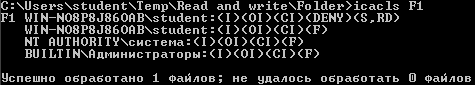
Смоделируем все 3 варианта в папке /Student/Temp

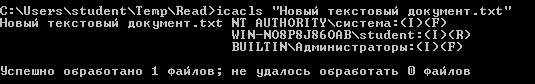
Используем папки и файлы, созданные во 2 пункте для рассмотрения наследования

В папке Not Perm создадим 231.txt файл и уберем у него наследование. Как видим icacls не вывел нам то, что файл наследуется.

(OI) - наследование объектами, (CI) - наследование контейнерами, (IO) - только наследование, (NP) - запрет на распространение наследования, (I) - наследование разрешений от родительского контейнера









Также можно наследовать запреты, комбинировать собственные разрешения с наследованными, передавать комбинацию своих и унаследованных разрешений.

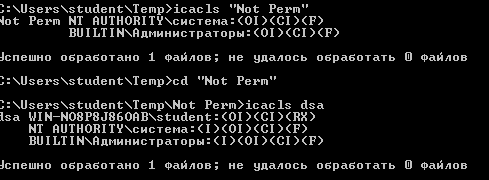
**2) Придумать примеры целесообразного и нецелесообразного применения наследования.**

Предположим, что у нас есть каталог, в котором находится информация для нескольких групп (структура какого-нибудь предприятия). В такой структуре есть ряд групп, которые не имеют доступ к некоторым подкаталогам. Для этой структуры для каждого подкаталога используется свои права и будет нецелесообразно унаследовать подкаталогам разрешения каталога, ведь разрешения перемешаются и надо будет настраивать запреты для каждого подкаталога, а так как в подкаталогах может быть целое дерево каталог, то наследование пойдет по цепочке и уйдет много времени на настройку запретов для всех подкаталогов подкаталога.

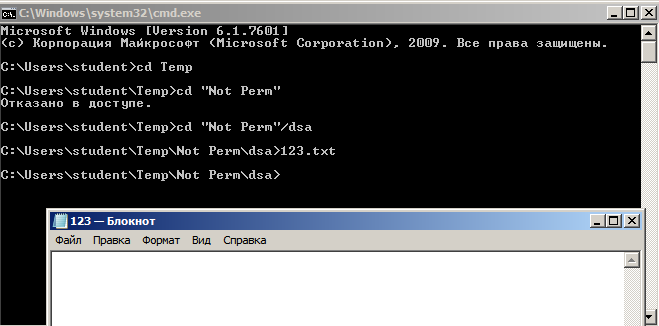
Из прошлого примера нецелесообразного наследования вытекает и целесообразное, а именно подкаталоги подкаталогов. Если к подкаталогу для пользователя включены определенные запреты или разрешения и надо предоставить такие же права всем подкаталогом подкаталога и далее, то наследование значительно упростит эту работу.

**3) На примере привилегии “Обход перекрестной проверки” показать преобладание привилегий над разрешениями.**

В папке Not Perm создадим папку dsa к которой у пользователя будет разрешения к ней и ее файлам



Теперь зайдем от пользователя Student и попытаемся открыть данные папки и файл. Как видно из консоли, попасть в папку Not Perm не удалось, однако открыть папку dsa, находящуюся в данном каталоге и файл получилось.



Это означает, что привилегии преобладают над разрешениями доступа. Также это подтверждает возможность администратора менять владельца папки или файла несмотря на отсутствие разрешения на это.

1. **Вывод**

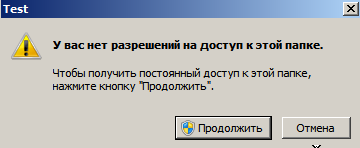
Были рассмотрены свойства и варианты наследования разрешений, были опробованы различные варианты наследования разрешений, приведены примеры целесообразного и нецелесообразного использования наследования разрешений, на примере привилегии «Обход перекрестной проверки» доказано преобладание привилегий над разрешениями доступа.

**5. Владельцы файлов**

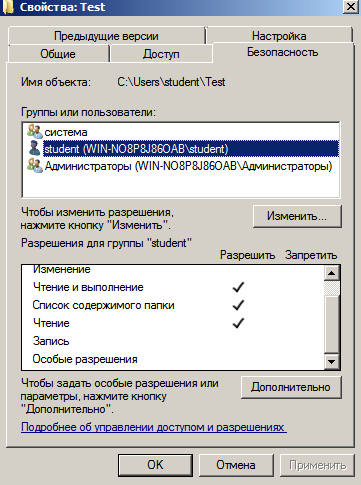
**1) Обосновать необходимость применения свойства владения объектом. Опробовать смену владельца объекта.**

Владелец объекта – важный объект в управлении объектов. Он в случае разных ошибок, всегда будет иметь доступ к разрешениям к папке, ведь из-за ошибки системы или вирусов могут удалится права разрешения на файл, и владелец как раз может в любом случае дать разрешение на операции с файлами. Чтобы сменить владельца, нужно иметь разрешение на смену владельца и обладать привилегией смены владельца.

Опробуем смену владельца. В папке student был файл Test, для которого разрешений у student не было, но мы сделали владельцем student

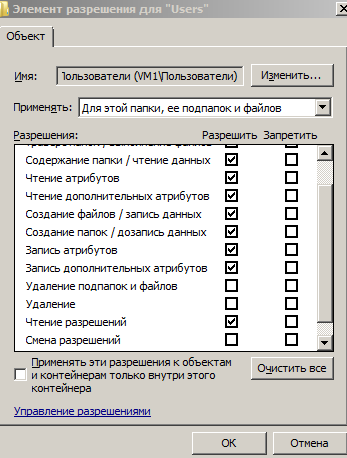
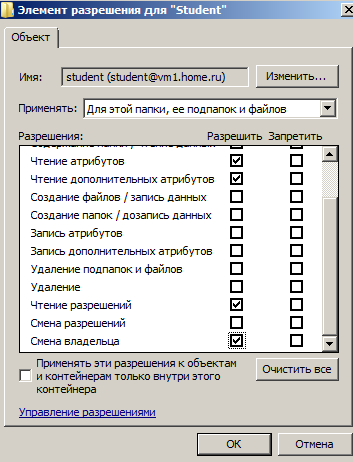


Теперь пользователь student может полностью распоряжаться разрешениями для папки, вплоть до того, чтобы дать себе и любому пользователю доступ к этой папке.



**2) Отформатировать сменный флэш-носитель в файловую систему NTFS, создать два каталога, на один назначить доступ группе Пользователи, на другой – конкретной учетной записи. Проверить и обосновать возможность доступа к каталогам носителя на другом компьютере, на котором есть группы и пользователи с теми же именами.**

Создадим в корне флэш-носителя папки Student и Users и оставим доступ к ним только доменному пользователю student и группе Пользователи соответственно. Чтобы убедиться в том, что мы пользуемся разрешениями доступа именно этих учетных записей и групп удалим разрешения всем остальным. Student мы дадим разрешение на чтение и смена владельца, а пользователям дадим доступ на запись и чтение

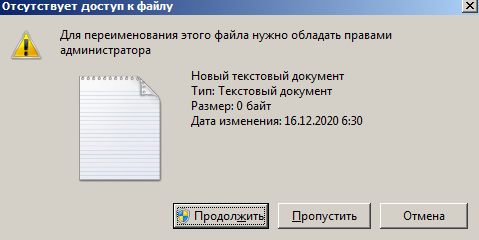
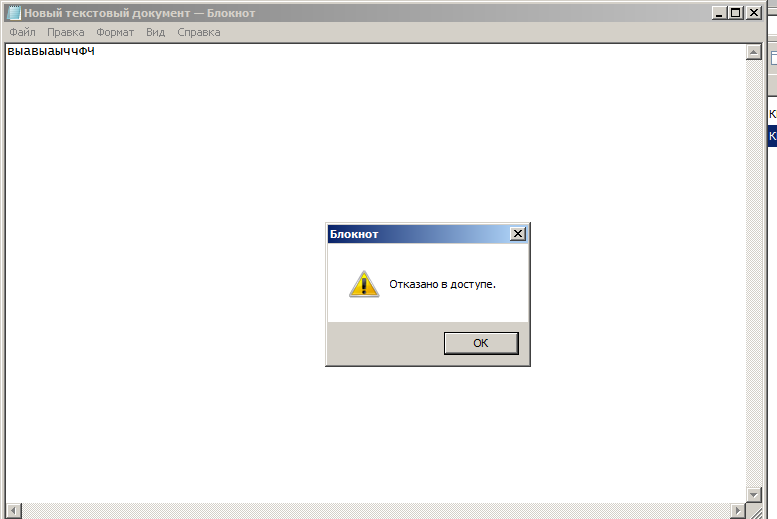
****

Попробуем 3 варианта входа:

1. Зайдем в учетную запись домена student с другого компьютера в домене
2. Зайдем в локальную учетную запись student с другого компьютера в домене
3. Зайдем в локальную учетную запись student с другого компьютера, не входящего в домен

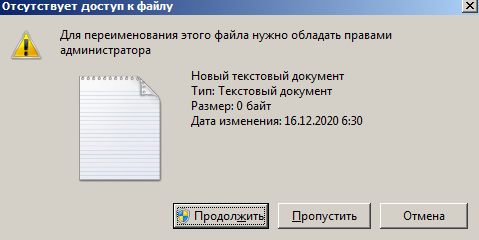
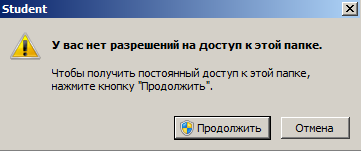
В первом случае мы смогли работать с папкой со всеми разрешениями, которые есть у группы Пользователе, это объясняется тем, что мы заходим в домен, имея тот же SID группы, так как мы в домене. В Student мы тоже попали беспрепятственно, ведь зашли мы от того же пользователя, которому давали доступ, а значит мы имеем тоже самое имя и тот же SID (ведь это та же самая учетная запись, только мы зашли в нее с другого компьютера



****

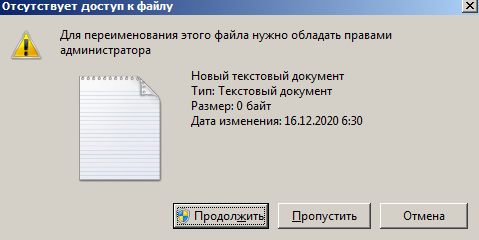
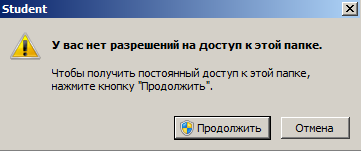
Во втором случае мы также смогли работать с папкой Users со всеми правами пользователя. Это объясняется тем, что мы находимся в домене, а вот с Student все обстоит не очень хорошо, ведь если и имена совпадают, но SID нет

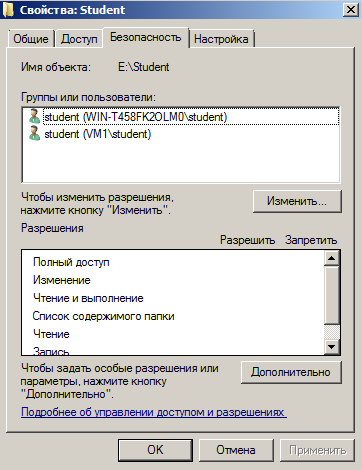
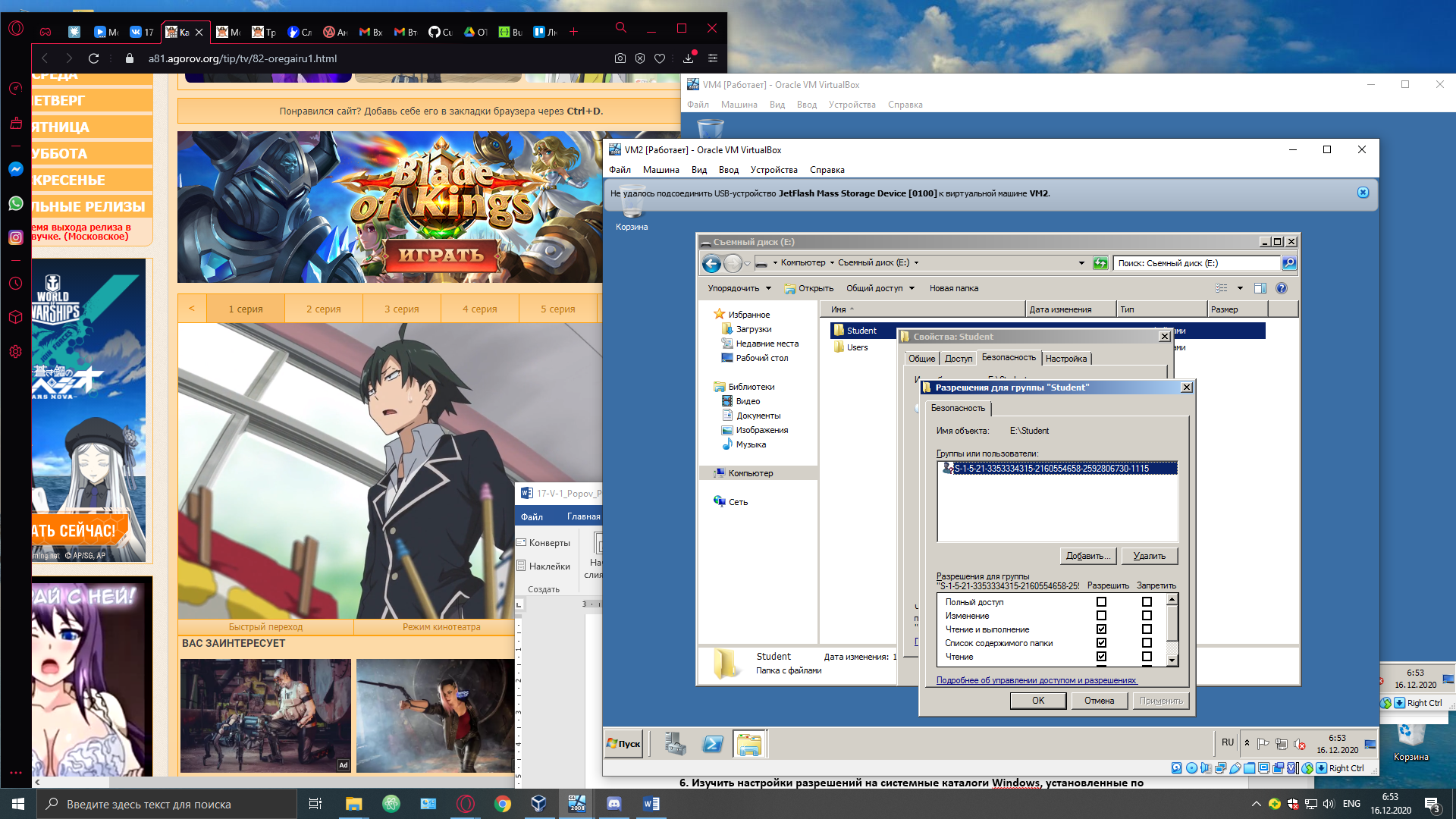
****

В третьем случае мы также смогли работать с папкой Users со всеми правами пользователя. Это объясняется тем, что группа Пользователи имеет фиксированный SID, который для большинства машин одинаков, и сама группа называется точно также. А вот с student все также, как и во втором случае. К сожалению, SID разные, а это значит, что это разные субъекты безопасности



****

Попробуем нажать продолжить, дадим полный доступ засчет прав Администратора и заметим интересное свойство, пользователи в домене друг друга опознали (в безопасности мы можем видеть имена), а вот компьютер, который не относится к домену вообще не распознал имя, а лишь распознал SID, это еще один аргумент к третьему случаю, ведь с точки зрения безопасности эти пользователи еще и имеют разные имена

****

**3) Вывод**

Была обоснована необходимость применения свойства владения объектом. Опробована смена владельца объекта. А также рассмотрена и опробована проверка доступа к каталогам на разных машинах, а также было замечено, что 2 компьютера, которые не знают друг друга, не могут распознать имена учетных записей, для которых расписаны разрешения в безопасности.

**6. Изучить настройки разрешений на системные каталоги Windows, установленные по умолчанию.**

**1)** **Для корневого каталога (C:\), каталогов \Windows, \Program Files, \Program Data, \Users с некоторыми показательными подкаталогами рассмотреть владельца, назначенные разрешения и передачу наследования. Результаты представить в виде иерархической схемы каталогов с приписанными в краткой форме свойствами безопасности.**

Условные обозначения: F — полный доступ, M — изменение, X — выполнение, RX — чтение и выполнение, R — чтение, RD – чтение данных, RA – чтение атрибутов, REA – чтение дополнительных атрибутов, Rc – чтение разрешений, W — запись, WD —запись данных, AD —дозапись данных, WA – запись атрибутов, WEA – запись дополнительных атрибутов, DC — удаление вложенных файлов, D – удаление, WDAC – смена разрешений, WO – смена владельца, S — синхронизация (RD + RA + REA + Rc = R, R + X = RX, WD + AD + WA + WEA = W, R + W + D + X= M), I - унаследованы

C:\

Владелец — TrustedInstaller

Разрешения:

System (F)

Администраторы (F)

Пользователи (RX, AD)

C:\Windows\

Владелец — TrustedInstaller

Разрешения:

TrustedInstaller (F)

System (M)

Администраторы (M)

Пользователи (RX)

C:\Windows\System32\

Владелец — TrustedInstaller

Разрешения:

TrustedInstaller (F)

System (M)

Администраторы (M)

Пользователи (RX)

C:\Windows\Microsoft.NET\

Владелец — TrustedInstaller

Разрешения:

TrustedInstaller (F)

System (M)

Администраторы (M)

Пользователи (RX)

C:\Program Files(x86)\

Владелец — TrustedInstaller

Разрешения:

TrustedInstaller (F)

System (M)

Администраторы (M)

Пользователи (RX)

C:\Program Files(x86)\Common Files

Владелец — TrustedInstaller

Разрешения:

TrustedInstaller (F)

System (M)

Администраторы (M)

Пользователи (RX)

C:\ProgramData\

Владелец —Администраторы

Разрешения:

System (F)

Администраторы (F)

Пользователи (M)

C:\ProgramData\Microsoft

Владелец — Администраторы

Разрешения:

System (F)

Администраторы (F)

Пользователи (RX)

Все (RX)

C:\Users\

Владелец — Администраторы

Разрешения:

System (F)

Администраторы (F)

Пользователи (RX)

Все (RX)

C:\Users\Default

Владелец — Администраторы

Разрешения:

System (F) (I)

Администраторы (F) (I)

Пользователи (RX) (I)

Все (RX) (I)

**2) Объяснить общий механизм защиты системы**

Администратор системы имеет полный доступ почти ко всем файлам и папкам за исключением большинства системных файлов и папок (у которых владельцем назначен TrustedInstaller для предотвращения внешних и внутренних угроз (вмешательств)), где он имеет право только на изменение файлов и папок. Пользователь имеет ограниченный доступ как к системны файлам и папкам, так и большинству обычных файлов и папок, а именно чтение и выполнение. Большинство разрешений назначаются администратором.

**3) Сопоставить роли в Windows субъектов безопасности Администратор и TrustedInstaller.**

Администратор — это встроенная учетная запись, которая обладает практически всеми привилегиями и может менять владельца любого (даже системного) объекта. Эта учетная запись нужна для того, чтобы пользователь мог при необходимости получить нужные привилегии.

TrustedInstaller — это служебная учетная запись для службы TrustedInstaller.exe. Данная служба ответственна за установку и обновление системы. Эта учетная запись обладает большими правами, чем Администратор, но обычный пользователь не может зайти под учетной записью TrustedInstaller. Данная учетная запись является владельцем множества системных каталогов и файлов, что не даёт обычным администраторам стать владельцем данных объектов, а значит удалить или изменить разрешения доступа объекта

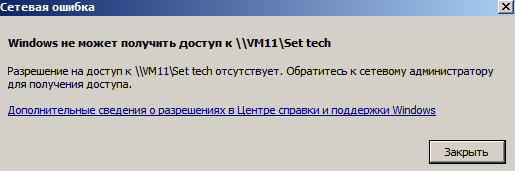
**4) Вывод**

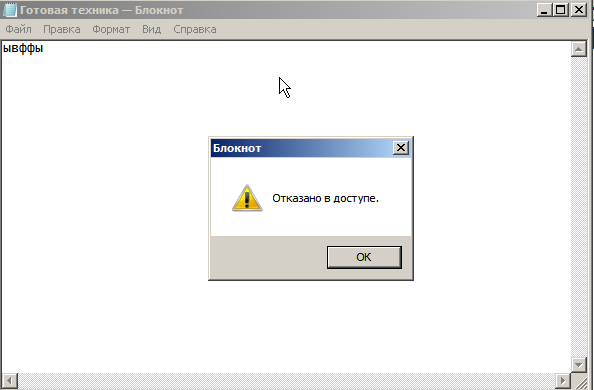
Были изучены настройки разрешений доступа на системные папки по умолчанию, объяснен общий механизм системы и сопоставлены роли Администратора и TrustedInstaller в системе.

**7. Реализовать сетевой доступ к общим файловым ресурсам.**

**1) Назначить разрешения доступа и проверить защищенность файловых ресурсов при доступе по сети.**

В 1 лабораторной работе уже была задействована схема, связанная с сетевым доступ. Там имелось 4 новых групп пользователей (Менеджеры, Операторы, Технический и Приемный отделы) Также в сети для них были созданы папки, в которых они должны работать. Проверим работу сети на примере пользователя Оператор, входящий в группу Операторы. Как видим к папке Set tech он не имеет никакого доступа, а также не можем записывать в файлы папки Rep tech.





**2)** **Результаты свести в таблицу, поясняющую смысл разрешений на каталог общего доступа.**

Папка Operators

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Смена владельца | Выполнение | Удаление | Удаление подпапок и файлов | Чтение | Запись | Чтение разрешений |
| Менеджеры | - | + | - | - | + | - | + |
| Операторы | + | + | + | + | + | + | + |
| Технический отдел | - | + | - | - | + | - | - |
| Приемный отдел | - | - | - | - | - | - | - |
| Пользователь | - | - | - | - | - | - | - |

Папка Set tech

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Смена владельца | Выполнение | Удаление | Удаление подпапок и файлов | Чтение | Запись | Чтение разрешений |
| Менеджеры | - | + | - | - | + | - | + |
| Операторы | - | - | - | - | - | - | - |
| Технический отдел | - | + | - | - | + | - | + |
| Приемный отдел | + | + | + | + | + | + | + |
| Пользователь | - | - | - | - | - | - | - |

Папка Rep tech

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Смена владельца | Выполнение | Удаление | Удаление подпапок и файлов | Чтение | Запись | Чтение разрешений |
| Менеджеры | - | + | - | - | + | - | + |
| Операторы | - | + | - | - | + | - | + |
| Технический отдел | + | + | + | + | + | + | + |
| Приемный отдел | - | - | - | - | - | - | - |
| Пользователь | - | - | - | - | - | - | - |

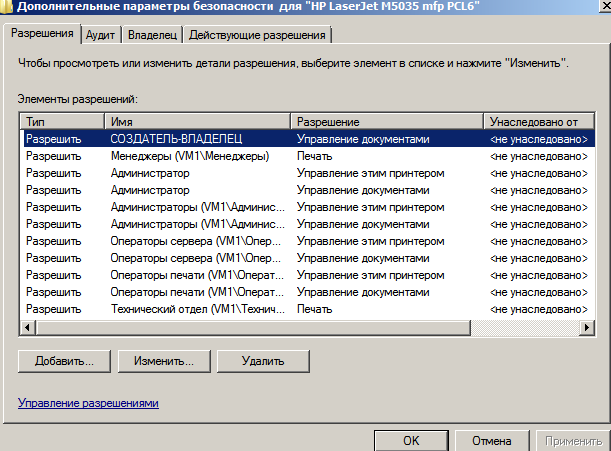
**3) Вывод**

Был реализован общий доступ к сетевым ресурсам, настроены разрешения для них и проверены доступы. Результаты были сведены в таблицу

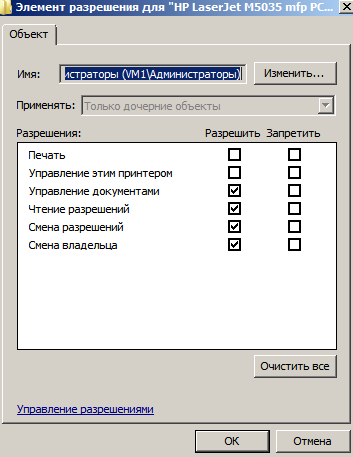
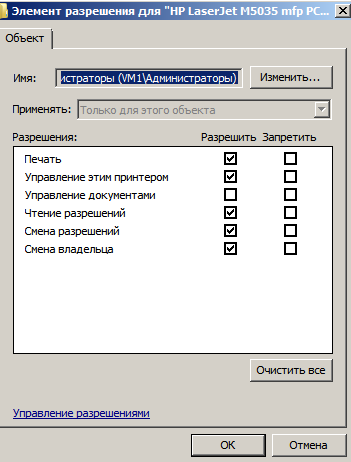
**8. Сервер печати**

**1) Определить состав разрешений доступа к устройству печати как объекту безопасности.**

Был установлен сервер печати, взятый из роли служб печати и документов, и добавлен в AD. Так как в данный момент я не имею принтеры, я добавил драйвер для случайного принтера через сервер печати (выбор пал на HP Laser Jet M5035) и после по драйверу подключен, как принтер в сервере печати. Рассмотрим разрешения и добавим разрешения печати для групп Менеджеры и Технический отдел

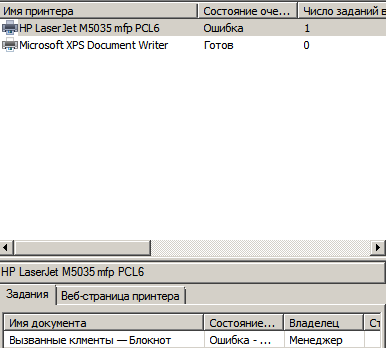
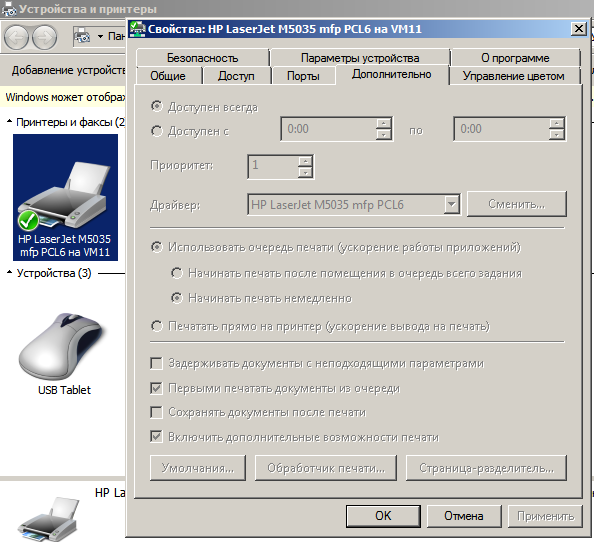
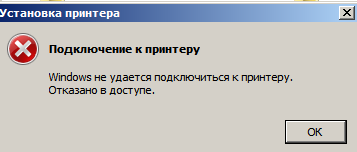


Как видим, Администратор имеет все права на принтер



**2) Реализовать сетевую печать и проверить разрешения доступа к принтеру**.

Администратор может полностью управлять принтером. Менеджеры и Технический отдел могут отправлять свои документы на печать (но так как принтера нет, то будет ошибка, но в очередь документ добавится), остальные же не имеют доступа к принтеру



**3) Вывод**

Был определен состав разрешений доступа для принтеров, реализована сетевая печать и проверена работа разрешений доступа к принтеру

**9. Реализовать план совместного использования прикладных программ и данных группой пользователей и защиты персональных данных каждого пользователя для модельной задачи администрирования, составленной в первой части работы.**

**1) Для управления доступом к приложениям применить политику ограниченного использования программ. Для защиты данных продумать структуру каталогов хранения прикладных данных разного типа доступа и назначить необходимые разрешения. (Возможно сравнить несколько вариантов). Представить схему безопасности данных.**

Имеется предприятие, в котором работают Менеджеры, Операторы, Технический отдел, Приемный отдел. Каждая группа имеет доступ к определенной БД (в нашем случае текстовым файлам).

Менеджеры могут читать БД всех для контроля, но изменять ничего не могут

Операторы имеют доступ к БД вызванные клиенты и право на чтения БД готовая техника

Технический отдел имеет доступ к БД готовая техника и документация и право на чтение БД принятая техника

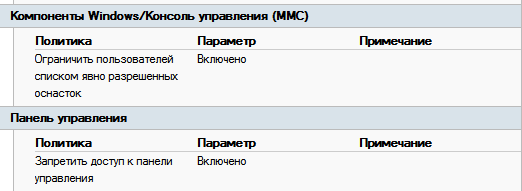
Приемный отдел имеет доступ к БД договоры и принятая техника

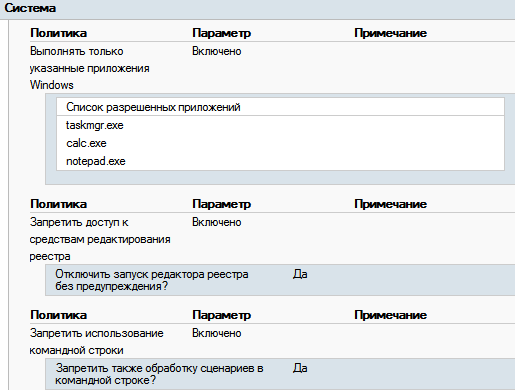
То есть все созданные группы могут относится к группе пользователя, но у каждого есть свои разрешения на папки и файлы.

В первой лабораторной работе мы уже ограничивали доступ к командной строке, реестру и Консоли управления всем добавленным группам (не имеет смысл писать политику безопасности для каждой группы, ведь они имеют разные права только на папки и файлы в них, а вот системный инструментарий можно и нужно отключить у каждого и для этого мы не будем создавать политику для каждого, а создадим одну общую). Также для защиты им нужно отключить доступ к панели управления. Для частоты эксперимента разрешим доступ только к диспетчеру задач, калькулятору и текстовому редактору (notepad.exe) (чтобы они во время работы использовали только необходимое ПО)

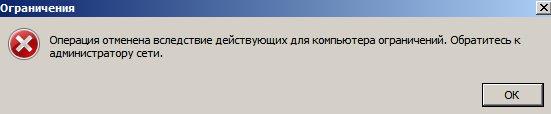
В итоге наша схема получилась простой и ненавязчивой:

Объект групповой политики (GPO) Zapret отвечает за такие группы пользователей, как Менеджеры, Операторы, Технический Отдел и Приемный отдел. Эти группы могут использовать лишь такие приложения, как калькулятор, текстовый редактор и диспетчер задач.





При попытке запуска paint.exe от пользователя Оператор получили ошибку



**2) Вывод**

Была рассмотрена оснастка Управление групповой политики (gpmc.msc) и разработана модель запретов и разрешений для схемы предприятия из первой лабораторной работы

**Вывод**

Были рассмотрены субъекты и объекты безопасности. Проведены проверки работы той или иной настройки безопасности (разрешения, групповые политики, сервер печати). Рассмотрели модель безопасности на примере предприятия.

**Исправления с первой лабораторной работы**

**5.4** **Составить полную схему связей учетных записей, глобальных, универсальных и локальных групп домена.** 