ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ

ВОРОНЕЖСКОЙ ОБЛАСТИ

государственное бюджетное профессиональное образовательное учреждение Воронежской области
«Воронежский государственный промышленно-гуманитарный колледж»
(ГБПОУ ВО «ВГПГК»)

Методические рекомендации по выполнению практических заданий по МДК.04.01 Организация администрирования информационных систем «ПМ.04 Эксплуатация и поддержка функционирования информационных систем»

Для студентов с инвалидностью по специальности 09.02.04 «Информационные системы», очной формы обучения

Часть 5

Воронеж

ББК 32.81.26-04.15
Е47

Печатается по решению методического совета
Воронежского государственного
промышленно-гуманитарного колледжа

Составители: Е. Н Рысцова, А.А. Руднева, А.Е.Овсянникова.

Е 47 **«МДК.04.01 Организация администрирования информационных систем «ПМ.04 Эксплуатация и поддержка функционирования информационных систем»: Методическое пособие по выполнению практических заданий** для студентов с инвалидностью по специальности 09.02.04 «Информационные системы» оч. формы обучения в 8-х частях / департамент образования, науки и молодеж. политики Воронеж. обл., Воронеж. гос. пром.-гуманитар. колледж ; [сост. Е. Н Рысцова, А.А. Руднева, А.Е.Овсянникова]. – Воронеж: ВГПГК, 2021. 14–с.

Изложены цели и задачи изучения МДК04.01; основные требования к практической работы; порядок выполнения, проверки и оценки; список основной и дополнительной рекомендуемой литературы.

ББК 32.81.26-04.15

Содержание

Практическая работа № 9

Тема: УЧЁТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ

ЦЕЛЬ РАБОТЫ: изучение возможностей управления учётными записями пользователей в ОС Windows Server 2003

ЗАДАЧИ РАБОТЫ

1. Изучить свойства учетных записей пользователей как средства назначения разрешений, сценариев регистрации, профилей и домашних каталогов.

2. Научиться создавать учетные записи пользователей и групп пользователей в ОС Windows Server 2003.

ПЕРЕЧЕНЬ ОБЕСПЕЧИВАЮЩИХ СРЕДСТВ

1. ПК.

2. Программное обеспечение: Oracle VirtualBox, ОС Windows Server 2003.

3.Учебно-методическая литература.

ОБЩИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Пользовательская учетная запись содержит имя и пароль для регистрации на локальном компьютере или в домене. В Active Directory (AD) учетная запись пользователя может также содержать дополнительную информацию, такую как полное имя пользователя, адрес электронной почты, номер телефона, отдел и физический адрес. Кроме того, учетная запись пользователя служит средством для назначения разрешений, сценариев регистрации, профилей и домашних каталогов.

В Windows Server 2003 определены пользовательские учетные записи двух типов: доменные учетные записи и локальные учетные записи.

Доменные учетные записи определены в Active Directory. Посредством системы однократного ввода пароля такие учетные записи могут обращаться к ресурсам во всем домене. Они создаются в консоли «Active Directory —пользователи и компьютеры».

Локальные учетные записи определены на локальном компьютере, имеют доступ только к его ресурсам и должны аутентифицироваться, прежде чем получат доступ к сетевым ресурсам. Локальные учетные записи пользователей создают в оснастке «Локальные пользователи и группы».

Локальные учетные записи пользователей и групп хранятся только на рядовых серверах и рабочих станциях. На первом контроллере домена они перемещаются в Active Directory и преобразуются в доменные учетные записи.

Все учетные записи пользователей распознаются по имени для входа в систему. В Windows Server 2003 оно состоит из двух частей:

- «имя пользователя» — текстовое имя учетной записи;

- «домен или рабочая группа», в которых находится учетная запись.

Например: для пользователя mask, учетная запись которого создана в домене is4.local, полное имя для входа в Windows Server 2003 выглядит так — mask@is4.local. Имя для предыдущих версий Windows — is4\ mask. При работе с Active Directory иногда требуется полное имя домена пользователя, состоящее из DNS-имени домена в сочетании с именами контейнера и группы. У пользователя is4.local \Users\ mask, is4.local — DNS-имя домена, Users – имя контейнера, а mask — имя пользователя.

С учетной записью пользователя могут сопоставляться пароль и открытый сертификат. В открытом сертификате сочетаются открытый и закрытый ключ для идентификации пользователя. Вход в систему по паролю проходит интерактивно. При входе в систему с открытым сертификатом используются смарт-карта и считывающее устройство.

Хотя для назначения привилегий и разрешений в Windows Server 2003 применяются имена пользователей, ключевым идентификатором u1091 учетной записи является генерируемый при создании уникальный идентификатор безопасности (SID). Он состоит из идентификатора безопасности домена и уникального относительного идентификатора, который был выделен хозяином относительных идентификаторов.

С помощью SID, ОС Windows Server 2003 способна отслеживать учетные записи независимо от имен пользователей. Благодаря наличию SID вы вправе изменять имена пользователей и удалять учетные записи, не беспокоясь, что кто-то получит доступ к ресурсам, создав учетную запись с тем же именем. Когда вы меняете имя пользователя, Windows Server 2003 сопоставляет прежний SID с новым именем. Когда вы удаляете учетную запись, Windows Server 2003 считает, что конкретный SID больше недействителен**.** Если вы затем создадите учетную запись с тем же именем, она не получит привилегий предыдущей записи, так как у нее иной SID.

Помимо учетных записей пользователей в Windows Server 2003 используются группы, позволяющие автоматически предоставлять разрешения схожим типам пользователей и упростить администрирование учетных записей. Если пользователь — член группы, которая вправе обращаться к ресурсу, то он тоже может к нему обратиться. Чтобы предоставить пользователю доступ к нужным ресурсам, вы просто включаете его в подходящую группу. Поскольку в разных доменах Active Directory могут быть группы с одинаковыми именами, на группы часто ссылаются по полному имени — домен\имя_группы.

В Windows Server 2003 используются группы трех типов:

- *локальные группы* определяются и используются только на локальном компьютере, создаются в оснастке «Локальные пользователи и группы»;

- *группы безопасности* располагают дескрипторами защиты и определяются в доменах посредством консоли «Active Directory — пользователи и компьютеры». Это те группы, для которых можно назначать права и разрешения. Права определяют, какая деятельность разрешается в домене члену подобной группы (пользователю или компьютеру), а разрешения определяют, к каким объектам в сети они будут иметь доступ. Группы безопасности можно использовать и для рассылки e-mail сообщений многим пользователям. Сообщение отсылается лишь один раз, но при этом его получают все члены группы. Для этого, впрочем, в сети должен быть установлен продукт Microsoft Exchange Server 2003. В этом случае группы безопасности ведут себя так же, как группы распространения;

- *группы распространения* используются как списки рассылки электронной почты, не имеют дескрипторов безопасности и определяются в доменах посредством консоли «Active Directory — пользователи и компьютеры». Эти группы предназначены только для рассылки

пользователям сообщений электронной почты. Для них не определяются права доступа к сетевым объектам.

Группы безопасности имеют все свойства групп распространения, но не наоборот. Но дело в том, что некоторые приложения могут работать только с ними, а не с группами безопасности.

У групп возможны разные области действия — локальная доменная, встроенная локальная, глобальная и универсальная. От этого зависит, в какой части сети они действительны.

Локальные доменные группы предоставляют разрешения в одном домене, В состав локальных доменных групп входят лишь учетные записи (и пользователей, и компьютеров) и группы из домена, в котором они определены.

Встроенные локальные группы обладают особыми разрешениями в локальном домене. Для простоты их часто также называют локальными доменными группами, но в отличие от обычных групп, встроенные локальные группы нельзя создать или удалить — можно лишь изменить их состав. Как правило, говоря о локальных доменных группах, имеется в виду и обычные, и встроенные локальные группы, если не указано обратное.

Глобальные группы используются для назначения разрешений на доступ к объектам в любом домене дерева или леса. В глобальную группу входят только учетные записи и группы из домена, в котором они определены.

Универсальные группы управляют разрешениями во всем дереве или лесе; в них входят учетные записи и группы из любого домена в дереве или лесе домена. Универсальные группы доступны только в Active Directory в основном режиме Windows 2000 или в режиме Windows Server 2003.

Универсальные группы очень полезны на больших предприятиях, имеющих несколько доменов. Состав универсальных групп не должен часто меняться, так как любое изменение надо реплицировать во все глобальные каталоги в дереве или лесе. Чтобы уменьшить количество изменений, включайте в универсальную группу только группы, а не сами учетные записи.

В Windows Server 2003 учетные записи групп, как и учетные записи пользователей, различаются по уникальным идентификаторам безопасности. Это значит, что нельзя удалить учетную запись группы, а затем создать группу с тем же именем, чтобы у нее появились прежние разрешения и привилегии. У новой группы будет новый SID, и все разрешения и привилегии старой группы будут утеряны.

Для каждого сеанса пользователя в системе Windows Server 2003 создает маркер безопасности, содержащий идентификатор учетной записи пользователя и SID всех групп безопасности, к которым относится пользователь. Размер маркера растет по мере того, как пользователь добавляется в новые группы безопасности. Это приводит к следующим последствиям:

- чтобы пользователь вошел в систему, маркер безопасности должен быть передан процессу входа в систему. Поэтому по мере увеличения членства пользователя в группах безопасности процесс входа требует все больше времени;

- чтобы выяснить разрешения доступа, маркер безопасности пересылается на каждый компьютер, к которому обращается пользователь. Поэтому чем больше маркер безопасности, тем выше сетевой трафик.

Сведения о членстве в группах распространения не передаются в маркере безопасности, поэтому состав этих групп не влияет на размер маркера.

ЗАДАНИЕ

1. Создать учётную запись пользователя.

2. Изучить свойства созданной учётной записи.

3. Создать группу безопасности и группу распространения, включить учётную запись пользователя в эти группы.

4. Создать шаблон учетной записи.

ТРЕБОВАНИЯ К ЗАЧЕТУ

1. К зачету необходимо предоставить результаты выполненной работы.

2. Отчет с подробным описанием выполненных работ.

3. Подготовить ответы на вопросы.

ТЕХНОЛОГИЯ ВЫПОЛНЕНИЯ РАБОТЫ

Создание доменной учетной и1079 записи

1. На сервере запустить консоль «Active Directory — пользователи и компьютеры».

2. Перед созданием учетной записи пользователя необходимо создать новое подразделение. Для этого в левом окне консоли щелкнуть правой кнопкой мыши по значку домена и из контекстного меню выбрать «Создать» - «Подразделение».

3. В появившемся диалоговом окне ввести имя подразделения, например: «*student*».

4. После создания подразделения приступить к созданию учётной записи пользователя. Для этого требуется щелкнуть правой кнопкой мыши по созданному подразделению «*student*» и из контекстного меню выбрать «Создать» - «Пользователь».

5. В диалоговом окне «Новый объект - Пользователь». Заполнить пункты «Имя» и «Фамилия».

6. В поле «Имя входа пользователя» ввести «*User1*». Это же регистрационное имя будет автоматически введено и в поле «Имя входа в систему пользователя (пред-Windows 2000)». Данное значение можно изменить вручную, но это не рекомендуется. Нажмите «Далее».

Рекомендуется избегать использования в регистрационном имени символы кириллицы, поскольку не на каждом компьютере можно переключиться на русскую раскладку в ходе регистрации.

7. Заполните поля «Пароль» и «Подтверждение».

При этом необходимо придумать и ввести сложный пароль, удовлетворяющий следующим минимальным требованиям:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
- пароль должен состоять не менее чем из семи символов;

 в пароле должны присутствовать символы трех категорий из числа следующих четырех: прописные буквы английского алфавита от A до Z, строчные буквы английского алфавита от a до z, десятичные цифры (от 0 до 9), неалфавитные символы (например, !, $, #, %).

8. При необходимости установить флажок «Требовать смену пароля при следующем входе в систему».

9. После проверки информации о новом пользователе завершить создание учетной записи нового пользователя.

Изучение свойств созданной учётной записи.

1. Открыть свойства созданной учетной записи u1087 пользователя.

2. Изучить все вкладки.

3. Заполнить вкладки «Общие», «Адрес», «Организация».

4. Сделать учетную запись членом группы «Администраторы домена». Для этого следует на вкладке «Член групп» выполнить команду «Добавить».

5. В появившемся диалоговом окне выполнить команды «Дополнительно» - «Поиск».

6. Из результатов поиска выбрать группу «Администраторы домена».

7. Задать основную группу - «Администраторы домена»

8. Исключить учетную запись из группы «Пользователи домена».

Включение учётной записи пользователя в созданные группы.

Для создания новой группы требуется выполнить следующее:

1. Щелкнуть правой кнопкой мыши по подразделению «*student*» и из контекстного меню выбрать «Создать» - «Группа».

2. В появившемся диалоговом окне заполнить поля «Имя группы» и «Имя группы (пред-Windows 2000)» в соответствие с правилами, например: «*security*» .

3. Установить область действия «Глобальная» и «Тип группы» - «Группа безопасности».

4. Создать группу «*extending*». Установив «Область действия группы» - «Универсальная», «Тип группы» - «Группа распространения».

5. Включить вашу учетную запись в созданные группы.

Создание шаблона

Последовательность действий по созданию шаблона состоит из следующих этапов:

1. Запустить консоль «Active Directory — пользователи и компьютеры» и создать пользователя с именем *«mask»*.

2. В окне свойств вновь созданной записи заполнить все необходимые поля на вкладках «Адрес» и «Организация».

3. Используя вкладку «Учетная запись» установить время входа для пользователя с понедельника по субботу с 8:00 до 18:00.

4. Далее нужно щелкнуть по созданной записи правой кнопкой мыши и из контекстного меню выбрать команду «Отключить учетную запись».

Создание учетной записи по шаблону

1. Щелкнуть по шаблону *«mask»* правой кнопкой мыши и из контекстного меню выбрать команду «Копироватьu187 ».

2. В появившемся окне ввести регистрационное имя *«mask1»*, в качестве имени и фамилии тоже *«mask1».*

3. Задать пароль для первого входа в систему и снять флажок «Отключить учетную запись».

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что содержит пользовательская учетная запись?

2. Какие типы учетных записей определены в Windows Server 2003?

3. Из каких частей состоит имя для входа в систему Windows Server 2003?

4. Что такое SID?

5. Для чего создаются группы пользователей?

6. Какие три типа групп используются в ОС Windows Server 2003?

7. Можно ли удалив учетную запись группы, создать заново группу с таким же именем с тем, чтобы у нее появились прежние разрешения и привилегии? Ответ объяснить.

8. Что содержит маркер безопасности, который создает ОС Windows Server 2003 для каждого сеанса пользователя?

9. Объясните, почему, чем больше маркер безопасности, тем выше сетевой трафик.

Практическая работа № 10

Тема: РАЗГРАНИЧЕНИЕ ПРАВ ДОСТУПА К РЕСУРСАМ СЕРВЕРА

ЦЕЛЬ РАБОТЫ: изучение основ разграничения доступа пользователей к

ресурсам сервера.

ЗАДАЧИ РАБОТЫ

1. Изучить возможности серверного программного обеспечения по разграничению доступа пользователей системы.

2. Научиться предоставлять и разграничивать доступ к ресурсам сервера (файлам и папкам) для пользователей сети.

ПЕРЕЧЕНЬ ОБЕСПЕЧИВАЮЩИХ СРЕДСТВ

1. ПК.

2. Программное обеспечение: Oracle VirtualBox, ОС Windows Server 2003.

3. Учебно-методическая литература.

ОБЩИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Учетная запись пользователя имеет две функции. Первая это возможность зарегистрироваться на локальном компьютере или в домене. Другой функцией является возможность регулировать уровень прав доступа к объектам в сети.

Такими объектами могут быть принтер, файл, папка, учетная запись и т.д. В разделах, отформатированных файловой системой NTFS, можно ограничить доступ к файлам и папкам для отдельных пользователей или групп при помощи разрешений NTFS.

Существует пять стандартных разрешений NTFS для файлов и шесть для папок.

Таблица 11.1 Таблица стандартных разрешений NTFS и папок.

Разрешение	*Допускаемые действия*
Полный доступ	Разрешается все, в том числе возможность становиться u1074 владельцем файла или папки и заново назначать разрешения Изменить Разрешается все, что предусмотрено разрешениями «Запись» и «Чтение и выполнение» плюс удаление файла или папки
Чтение и выполнение	То же, что «Чтение», плюс возможность запуска, если файл исполняемый. Для папки разрешается доступ к файлам в подпапках, даже если нет доступа к самой папке

Список содержимого папки	Разрешается просмотр списка файлов и подпапок *Примечание: Доступно только в свойствах папки*
Чтение	Разрешается чтение файла и просмотр его свойств: имени владельца, разрешений и атрибутов. Для папки разрешается просмотр вложенных файлов и подпапок
Запись	Разрешается перезапись файлам изменение его атрибутов. Для папки разрешается добавление файлов и подпапок, а также изменение атрибутов папки
Особые разрешения	Задает набор специальных (нестандартных) разрешений Каждое стандартное разрешение складывается из нескольких специальных разрешений.

Неограниченное право доступа к файлу (папке) имеет его владелец. Первоначально владельцем становится пользователь, который создал данный файл.

Он имеет возможность изменять разрешения на этот файл для себя и для других. Новым владельцем файла может стать либо тот пользователь, которому предыдущий владелец предоставил такое разрешение, либо член группы локальных администраторов. В ОС Windows Server 2003 владелец может передать право собственности на файл другому пользователю.

По умолчанию разрешения наследуются от родительской папки. Если вы хотите изменить разрешения на файл, то первым делом нужно отменить наследование для этого файла.

Права доступа к сетевой папке определяются как разрешениями NTFS на эту папку, так и разрешениями, установленными при открытии доступа к данной папке по сети. В результате пользователь получает наименьшее из этих разрешений.

Таблица 11.2 Таблица результатов взаимодействия прав доступа для пользователя User1(пользователь не входит в группу администраторов).

Разрешения NTFS для пользователя User1	*Право доступа к общей папке*	*Результат*
«Чтение» «Все»	«Чтение»	«Чтение»
«Полный доступ» Администраторы	«Полный доступ»	Нет доступа
«Чтение», «Запись» «Все»	«Чтение»	«Чтение»

«Чтение» «Все»	«Полный доступ»	«Чтение»
«Полный доступ» «Все»	«Чтение»	«Чтение»

Если права, предоставленные ему файловой системой NTFS больше, то воспользоваться ими он сможет только тогда, когда зарегистрируется на том компьютере, на котором физически расположена сетевая папка.

Самым надежным местом для хранения личных документов пользователя является папка «Мои документы», входящая в его профиль. С точки зрения администратора домена такое размещение оптимально, потому что все папки «Мои документы» можно разместить на сервере, что обеспечит как доступ к ним с любой рабочей станции, так и регулярное резервное копирование.

ЗАДАНИЕ

1. Создать папку на локальном диске сервера

2. Предоставить доступ к этой папке для других пользователей.

3. Создать хранилище.

ТРЕБОВАНИЯ К ЗАЧЕТУ

1. К зачету необходимо предоставить результаты выполненной работы.

2. Отчет с подробным описанием выполненных работ.

3. Подготовить ответы на вопросы.

ТЕХНОЛОГИЯ ВЫПОЛНЕНИЯ РАБОТЫ

Создание папки на локальном диске сервера

1. Создать папку на диске «C:».

2. В новой папке создать два текстовых файла: file1.txt и file2.txt.

3. Щелкнуть правой кнопкой мыши по новой папке и из контекстного меню выбрать команду «Свойства».

4. В диалоговом окне свойств перейдите на вкладку «Безопасность».

5. В верхней части окна отметить группу «Пользователи» и нажмите «Удалить». Появится сообщение, что эту группу удалить нельзя, так как разрешения унаследованы от родительской папки.

6. Нажать кнопку «Дополнительно» и появившемся диалоговом окне «Дополнительные параметры безопасности» снять флажок «Разрешить наследование от родительского объекта к этому объекту и его дочерним объектам, добавляя их к разрешениям, явно заданным в этом окне». После этого в окне сообщения «Безопасность» нажать кнопку «Удалить» и закрыть окно дополнительных параметров, нажав кнопку «ОК».

Предоставление доступа к папке

Теперь необходимо u1088 разрешить доступ к новой папке группе локальных администраторов и созданному вами пользователю. Локальные администраторы должны иметь полный доступ ко всем ресурсам данного компьютера на тот случай, если он будет отключен от домена. При нормальной работе в домене управлять доступом к локальным ресурсам имеет право член группы администраторов домена, который всегда входит в группу локальных администраторов.

1. Щелкнуть на новой папке правой кнопкой мыши и из контекстного меню выбрать команду «Общий доступ и безопасность».

2. На вкладке «Доступ» установить переключатель «Открыть общий доступ к этой папке».

3. Нажать кнопку «Разрешения». Проверить, что группы пользователей «Все» установлен флажок доступа «Чтение/Разрешить».

4. Закрыть окно разрешений и в окне свойств перейти на вкладку «Безопасность»

5. Нажать кнопку «Добавить» для отображения диалогового окна «Выбор: Пользователи, Компьютеры или Группы».

6. В поле «Введите имена выбираемых объектов» указать группу «*Администратор*» и нажать кнопку «Проверить имена». Выберите из списка нужную группу администраторов.

7. На вкладке «Безопасность» в области разрешения для групп установите флажок «Разрешить/Полный доступ".

8. Подобным образом, созданному вами пользователю дополнительно назначить разрешение «Запись» .

Разрешения, предоставленные пользователю «User1» на новую папку, действительны и для ее дочерних объектов. Чтобы убедиться в этом, нужно закрыть окно свойств папки и вызвать окно свойств файла file1. txt. Удалить разрешения на этот файл вам не удастся, пока вы не снимете флажок «Разрешить наследование от родительского объекта к этому объекту и его дочерним объектам, добавляя их к разрешениям, явно заданным в этом окне».

Для проверки назначенных прав доступа пользователя «User1» выполните следующие действия:

1. Зарегистрироваться на сервере как пользователь «User1».

2. Перейти в папку «Новая папка» и открыть файл file1.txt.

3. Записать в него какую либо информацию и сохранить файл.

4. Удалить файл file1.txt.

Создание структуры хранилища

1. Зарегистрироваться на сервере как администратор.

2. Запустить консоль «Управление компьютером». Развернуть ветвь «Служебные программы» - «Общие папки».

3. Правой кнопкой мыши щелкнуть по папке «Общие ресурсы» и из контекстного меню выбрать команду «Новый общий ресурс». Запуститься мастер создания общих ресурсов.

4. Затем следует нажать на кнопку «Далее» и в поле «Путь к папке» задать путь «C:\Library». После нажатия на кнопку «Далее» появится сообщение об отсутствии заданной папки с запросом на ее создание. Нажать «Да» подтвердив создание папки.

5. В окне «Разрешения» установить значение «У всех пользователей доступ только для чтения».

6. Завершите работу мастера, нажав кнопку «Готово».

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие функции имеет учетная запись пользователя?

2. Какие стандартные разрешения NTFS существует для файлов и папок?

3. Может ли владелец передать право собственности на файл другому пользователю в ОС Windows Server 2003?

4. Какими разрешениями определяются права доступа к сетевой папке?

5. Какие действия необходимо выполнить для предоставления доступа к папке?

6. Действительны ли разрешения, предоставленные пользователю на новую папку, для ее дочерних объектов?

7. Как создается структура хранилища?