МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

|  |
| --- |
| Белгородский государственный технологический университет  им. В.Г. Шухова |

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

Утверждено

научно-методическим советом

университета

**АДМИНИСТРИРОВАНИЕ ПРОГРАММНЫХ**

**И ИНФОРМАЦИОННЫХ СИСТЕМ**

Методические указания к выполнению лабораторных работ

для студентов для студентов специальности 230105 –

Программное обеспечение вычислительной техники

и автоматизированных систем

УДК 004.4 (07)

ББК 32.973 я7

А 31

Составители: ст. преп. *Е. А. Федотов*

ст. преп. *А. И. Гарибов*

Рецензент канд. техн. наук, доц. *В. Г. Синюк*

|  |  |
| --- | --- |
| А 31 | **Администрирование** программных и информационных систем: методические указания к выполнению лабораторных работ / сост.: Е. А. Федотов, А. И. Гарибов. – Белгород: Изд-во БГТУ, 2014. –70 с. |

В методические указания включены требования и рекомендации к выполнению лабораторных работ по дисциплине “Администрирование программных и информационных систем”.

Методические указания предназначены для студентов специальности 230105 – Программное обеспечение вычислительной техники и автоматизированных систем.

Данное издание публикуется в авторской редакции.

**УДК 004.4 (07)**

**ББК 32.973. я7**

|  |  |
| --- | --- |
| © | Белгородский государственный технологический университет (БГТУ) им. В.Г. Шухова, 2017 |

Оглавление

[Лабораторная работа №1 4](#_Toc498024232)

[Установка и настройка Windows Server 2012 с использованием виртуальных машин 4](#_Toc498024233)

[Лабораторная работа №2 9](#_Toc498024234)

[Создание объектов пользователей и управление ими 9](#_Toc498024235)

[Лабораторная работа №3 21](#_Toc498024236)

[Использование средств инструментария для управления Windows (WMI) в администрировании 21](#_Toc498024237)

[Лабораторная работа №4 27](#_Toc498024238)

[Группы. Настройка политик и событий 27](#_Toc498024239)

[Лабораторная работа №5 33](#_Toc498024240)

[Присоединение компьютера к домену Active Directory 33](#_Toc498024241)

[Лабораторная работа №6 45](#_Toc498024242)

[Обеспечение безопасности ресурсов с помощью разрешений NTFS 45](#_Toc498024243)

[Лабораторная работа №7 57](#_Toc498024244)

[Архивация и восстановление данных 57](#_Toc498024245)

[Библиографический список 69](#_Toc498024246)

# Лабораторная работа №1

# Установка и настройка Windows Server 2012 с использованием виртуальных машин

**Цель работы:** Получение навыков установки и настройки виртуальных машин. Использование виртуальных машин для инсталляции и запуска операционных систем Windows Server 2012 и Windows 10. Настройка компьютера для работы под управлением Windows Server 2012. Настройкасервера в роли контроллера домена.

**Порядок выполнения работы**

1. Изучить теоретический материал.
2. Выполнить практические задания.
3. Сделать выводы на основании проделанной работы

**Теоретические сведения**

**Виртуализация операционных систем**

Виртуализация операционных систем представляет собой процесс создания так называемого “виртуального компьютера” на физическом (хостовом) компьютере, в который устанавливается своя собственная операционная система. На одном хостовом компьютере виртуальных машин может быть несколько со своими виртуальными аппаратными компонентами такими как оперативную память, процессоры, винчестеры, сетевые адаптеры и т.д. Эти ресурсы используются виртуальной машиной за счет физических ресурсов аппаратного обеспечения хостового компьютера.

**Настройка Windows Server 2012**

После установки и активации Windows можно настроить сервер при помощи страницы *Управление данным сервером.* Стандартные роли, для выполнения которых можно сконфигурировать сервер следующие:

* Файловый сервер;
* Сервер печати;
* Сервер приложений;
* Почтовый сервер;
* Сервер терминалов;
* Сервер удаленного доступа или VPN-сервер;
* Контроллер домена Active Directory;
* DHCP-сервер;
* Сервер потоков мультимедиа;
* WINS-сервер.

**Служба каталогов Active Directory**

*Рабочая группа* – это логическое объединение сетевых компьютеров, которые совместно используют общие ресурсы (файлы, папки и принтеры).

Рабочую группу также называют *одноранговой сетью,* т.к. все компьютеры в ней могут использовать общие ресурсы на равных условиях, без выделения сервера.

*Домен* - это логическое объединение компьютеров в сети, которые совместно используют центральную базу данных каталога.

*База данных каталога* содержит учетные записи пользователя и информацию о политиках безопасности для домена. Эту базу данных называют каталогом, и она представляет собой часть базы данных службы Active Directory — службы каталогов Windows 2012.

Домены Active Directory с разными корневыми доменами образуют несколько деревьев. Они объединяются в самую большую структуру Active Directory — *лес*. Лес Active Directory содержит все домены в рамках службы каталогов. Лес может состоять из нескольких доменов в нескольких деревьях или только из одного домена. Когда доменов несколько, глобальный каталог Active Directory позволяет клиентам одного домена получать информацию об объектах, расположенных в других доменах леса. В глобальном каталоге может быть лишь часть информации об объекте, но этого достаточно, чтобы найти более подробные сведения. Ресурсы организации представлены в Active Directory в виде объектов или записей в БД. Каждый объект характеризуется рядом атрибутов или свойств. Создав контроллер домена, администратор заполняет его объектами. Служба Active Directory способна хранить миллионы объектов, включая пользователей, группы, компьютеры, принтеры, общие папки, сайты, связи сайтов, объекты групповой политики (ОГП), зоны DNS и записи узлов. Для объединения компьютеров и пользователей используются организационные подразделения (ОП). Групповая политика позволяет централизованно управлять практически любыми конфигурационными изменениями системы.

**Консоли MMC**

Консоль ММС (Microsoft Management Console) - главный административный инструмент Windows Server 2012. Она консолидирует и организует наиболее часто используемые утилиты. Консоли ММС можно настраивать и приспосабливать под конкретные потребности, поэтому ряд задач можно делегировать другим пользователям. Консоль ММС предоставляет стандартный интерфейс для одного или нескольких прикладных модулей, называемых *оснастками*, которые применяются для конфигурирования параметров среды. Эти оснастки приспособлены для решения конкретных задач, их можно упорядочивать и группировать в рамках консоли MMC.

**Службы терминалов**

Службы терминалов устанавливаются по умолчанию вместе с ОС. На основе сервера с Windows Server 2012 можно создать сервер служб терминалов. Службы терминалов позволяют совместно использовать приложения с помощью таких инструментов, как Дистанционное управление рабочим столом, Удаленный помощник и Сервер терминалов. Компьютер может параллельно обрабатывать до двух одновременных подключений удаленного рабочего стола без приобретения дополнительных лицензий. Добавив компонент *Сервер терминалов* и настроив соответствующую лицензию множество пользователей смогут запускать приложения на сервере.

**Задания к работе**

* 1. Установить виртуальную машину MS Virtual PC на хостовом компьютере.
  2. Установить Windows Server 2012 в виртуальной машине. Настроить сетевое взаимодействие между хостовой и виртуальной машинами.
  3. Настроить сервер в качестве первого контроллера в домене с именем уникальным в пределах группы (например, фамилия\_студента.com).
  4. Определить NetBIOS–имя домена тремя различными способами (графический пользовательский интерфейс, интерфейс командной строки, сценарий VBScript).
  5. Создать и сохранить консоль MMC. Создать свою оснастку с консолью *Просмотр событий.*
  6. Добавить компьютер для удаленного управления. Для активации серверной части приложения необходимо на вкладке *Удаленное использование* окна *Система* выбрать переключатель *Разрешить удаленный доступ к этому компьютеру*. Осуществить подключение к удаленному рабочему столу. Подробно изучить данную возможность.
  7. Установить службу терминалов и выполнить удаленное администрирование сервера. Настроить сервер в качестве сервера терминалов. Изучить возможности *Удаленного помощника* и механизма управления. Изучить все параметры программы *Удаленное подключение к рабочему столу*.
  8. Удаленная помощь средствами Windows Messenger. Для получения удаленной помощи клиент должен создать приглашение и послать его эксперту как сообщение Windows Messenger. Для отправки приглашений через службу Windows Messenger имя эксперта должно быть в списке контактов Windows Messenger. Личный запрос удаленной помощи возможен, только когда эксперт подключен к сети.

**Содержание отчета**

1. Название работы
2. Цель работы
3. Выполненные задания. Необходимо сопровождать все проделанные действия скриншотами и описаниями к ним.
4. Выводы.

**Контрольные вопросы**

1. Каковы преимущества использования виртуальных машин?
2. Каковы недостатки использования виртуальных машин?
3. Перечислите роли, для выполнения которых можно сконфигурировать сервер.
4. Дайте определение домена.
5. Что такое NetBIOS-имя домена? Перечислите способы его определения.
6. Для чего нужны консоли ММС? Определение оснастки.
7. Для чего нужны службы терминалов. Средства удалённого администрирования.
8. Сколько одновременных подключений удаленного рабочего стола может параллельно обрабатывать компьютер.

# Лабораторная работа №2

# Создание объектов пользователей и управление ими

**Цель работы:** научиться создавать и управлять объектами пользователей, а также познакомиться с консолью *Active Directory — пользователи и компьютеры* и служебными программами, запускаемыми из командной строки.

**Порядок выполнения работы**

1. Изучить теоретический материал.
2. Выполнить практические задания.
3. Сделать выводы на основании проделанной работы

**Теоретические сведения**

**Подразделения**

Службы каталогов, в основу которых положен протокол LDAP, в том числе и Active Directory, хранят данные в контейнерах, организованных в виде иерархиче­ской структуры, которая называется *деревом информации каталога*. Каждый контейнер может содержать другие контейнеры и узлы-листья, являющиеся конечными точками иерархии. Двумя самыми рас­пространенными типами контейнеров в Active Directory являются *подразделение,* или *организационное подразделение* (Organizational Unit, OU), и обыкновенный *объект-контейнер.*

Организационное подразделение можно создать при помощи следующего сценария:

' ----- SCRIPT CONFIGURATION --------

strOrgUnit = "<имя\_подразделения>" 'например: Tools

strOrgUnitParent = "<ОИ\_род\_контейнера>" 'например: ou=Engineering.dc=povtas.dc=com

strOrgUnitDescr = "<имя\_подразделения>" 'например: Tools Users

' ----- END CONFIGURATION -----------

set objDomain = GetObject("LDAP://" & strOrgUnitParent)

set objOU = objDomain.Create("organizationalUnit", "OU=" & strOrgUnit)

objOU.Put "description",strOrgUnitDescr

objOU.SetInfo

WScript.Echo "Successfully created " & objOU.Name

ОП можно удалить при помощи следующего сценария:

set objOU = GetObject("LDAP://<ОИ\_подразделения>")

objOU.DeleteObject(0)

**Учетные записи пользователей**

Active Directory требует, чтобы перед разрешением доступа к ресурсам проводилась проверка подлинности пользователя на основе его учетной записи, которая содержит имя для входа в систему, пароль и уникальный идентификатор безопасности (security identifier, SID). В процессе входа в систему Active Directory проверяет подлинность имени и пароля. После этого подсистема безопасности может создать маркер доступа, представляющий этого пользователя. В маркере доступа содержатся SID учетной записи пользователя и SID всех групп, к которым относится пользователь. При помощи этого маркера можно проверить назначенные пользователю права, в том числе право локально входить в систему, а также разрешить или запретить доступ к ресурсам, защищенным *таблицами управления доступом* (access control list, ACL).

Учетная запись пользователя интегрирована в объект пользователя в Active Directory. Ее можно создать при помощи следующего сценария:

Const ADS\_UF\_NORMAL\_ACCOUNT = 512

Set objParent = GetObject("LDAP://OU=Employees, DC=povtas, DC=com")

Set objUser = objParent.Create("user","cn=Сидор Сидоров")

objUser.Put "sAMAccountName", "sidor"

objUser.Put "userPrincipalName","sidor@povtas.com"

objUser.Put "givenName","Сидор"

objUser.Put "sn","Сидоров"

objUser.Put "displayName","Сидор Сидорович"

objUser.SetInfo

objUser.Put "userAccountControl",ADS\_UF\_NORMAL\_ACCOUNT

objUser.SetPassword("we34gJk89N\_\_cvd3")

objUser.AccountDisabled = FALSE

objUser.SetInfo

Сценарий перемещения учетной записи пользователя из одного контейнера в другой:

strUserDN = "<ОИ\_пользователя>"

'Например: cn=petr.cn=users.dc=povtas.dc=com

strOUDN = "<ОИ\_нового\_род\_контейнера>"

'Например: ou=Sales.dc=povtas.dc=com

Set objUser = GetObject("LDAP://" & strUserDn)

Set objOU = GetObject("LDAP://" & strOUDN)

objOU.MoveHere objUser.ADsPath, objUser.Name

Сценарий разблокирования объекта пользователя:

strUsername = "<имя\_пользователя>" 'Например: petr

strDomain = "<NetBIOS-имя\_домена>" 'Например: POVTAS

set objUser = GetObject("WinNT://" & strDomain & "/" &strUsername)

if objUser.IsAccountLocked = TRUE then

objUser.IsAccountLocked = FALSE

objUser.SetInfo

WScript.Echo "Account unlocked"

else

WScript.Echo "Account not locked"

end if

Свойства объекта пользователя разбиты на несколько основных категорий:

* **Свойства учетной записи: вкладка Учетная запись.** Некоторые из этих свойств настраиваются при создании объекта пользователя, в том числе имена для входа пароль и управляющие флаги учетной записи.
* **Личная информация: вкладки Общие, Адрес, Телефоны и Организация.** На вкладке **Общие** перечислены свойства учетного имени, которые настраивают при создании объекта пользователя.
* **Управление настройками пользователя: вкладка Профиль.** Здесь можно указать путь к профилю пользователя, сценарий входа и местоположение домашних папок.
* **Членство в группах: вкладка Член групп.** Можно добавить и удалить группы пользователей, а также выбрать основную группу для пользователя.
* **Службы терминалов: вкладки Профиль служб терминалов, Среда, Удаленное управление и Сеансы.** Здесь можно настраивать и управлять работой пользователя во время сеанса служб терминалов.
* **Удаленный доступ: вкладка Входящие звонки.** Предназначена для включения и настройки разрешения на удаленный доступ.
* **Приложения: вкладка СОМ+.** Назначает пользователю наборы разделов Active Directory СОМ+. Эта новая функция Windows Server 2003 помогает управлять распределенными приложениями.

**Команда CSVDE**

CSVDE — это средство командной строки, позволяющее импортировать и экспортировать объекты в Active Directory из/в текстовый файл с разделителями — запятыми, формат которого широко распространен и читается такими программами, как Блокноти Microsoft Excel. Эта команда представляет собой мощный инструмент для быстрой генерации объектов. Ее базовый синтаксис следующий:

Csv -{}-de [ - i j [-f имя-файла] [-k], где:

- i — включает режим импорта; если не указан, по умолчанию включается режим экспорта;

- f *имя-файла —* указывает имя импортируемого файла;

- k — во время импорта игнорирует ошибки, в том числе *объект уже существует, нарушение ограничения* и *атрибут или значение уже существует,* и продолжает обработку.

**Профили пользователей**

*Профиль пользователя* — это набор папок и файлов данных, содержащих элементы среды рабочего стола конкретного пользователя. Профиль состоит из:

* ярлыков в меню **Пуск,** на рабочем столе и на панели быстрого запуска;
* документов на рабочем столе и, если не настроена переадресация, в папке **Мои документы;**
* избранных страниц и файлов «cookie» в Internet Explorer;
* сертификатов (если они внедрены в сети);
* специальных файлов приложений, например пользовательского словаря, шаблонов и списка автотекста в Microsoft Office;
* содержимого папки **Сетевое окружение;**
* параметров отображения рабочего стола, например его вида, фона и заставки.

Эти элементы у каждого пользователя свои. Желательно, чтобы они не изменялись между входами в систему, были доступны, если пользователю потребуется войти в другую систему, и их можно было восстановить в случае, если система даст сбой и ее потребуется переустановить.

**Задания к работе**

* + - 1. Создать организационное подразделение (ОП) Employees с помощью консоли Active Directory и создать ОП Temp с помощью сценария.
      2. Создать пользователей в ОП Employees со следующей информацией:

|  |  |
| --- | --- |
| Поле | Ввести |
| Имя | Иван |
| Фамилия | Иванов |
| Имя входа пользователя | ivan.ivanov |
| Имя входа пользователя (пред-Windows 2000) | ivan.ivanov |

* + - 1. Создать второй объект пользователя со следующими свойствами:

|  |  |
| --- | --- |
| Поле | Ввести |
| Имя | Петр |
| Фамилия | Петров |
| Имя входа пользователя | petr.petrov |
| Имя входа пользователя (пред-Windows 2000) | petr.petrov |

* + - 1. Создать объект пользователя для себя с помощью *сценария*, следуя тем же соглашениям для имен входа, что и для двух предыдущих объектов.
      2. Задать свойства вашего объекта пользователя на вкладках Общие, Адрес, Профиль, Телефоны и Организация. Изучить остальные свойства, связанные с вашим объектом пользователя, но пока не изменять их.
      3. Изменить свойства нескольких объектов пользователей. Выделить объекты пользователей Иван Иванов и Петр Петров. В меню Действие нужно выбрать Свойства. Изучите свойства, доступные при выборе нескольких объектов, но не изменяйте их. Задайте следующие свойства для двух объектов пользователей:

|  |  |  |
| --- | --- | --- |
| Вкладка | Поле | Ввести |
| Общие | Описание | Обучает администрированию серверных ОС |
| Общие | Номер телефона | (4722) 55-03-05 |
| Общие | Веб-страница | pv.bstu.ru |
| Адрес | Улица | Костюкова |
| Адрес | Город | Белгород |
| Адрес | Область/Край | Белгородская |
| Адрес | Почтовый индекс | 308000 |
| Организация | Должность | старший преподаватель |
| Организация | Организация | БГТУ им. В.Г. Шухова |

Удостоверьтесь, что свойства, которые вы задали, действительно были применены к объектам.

* + - 1. При помощи команды Найти осуществите поиск пользователя Иван Иванов в вашем домене. При помощи команды Переместить переместите его в ОП Temp. Переместите объект пользователя обратно в ОП Employees с помощью *сценария*.

С помощью *сценария* удалите ОП Temp.

* + - 1. Создать учетную запись пользователя со следующими данными:

|  |  |
| --- | --- |
| Поле | Ввести |
| Имя | Template |
| Фамилия | Sales Template |
| Имя входа пользователя | Template.sales.rep |
| Имя входа пользователя (пред-Windows 2000) | Templatesalesrep |

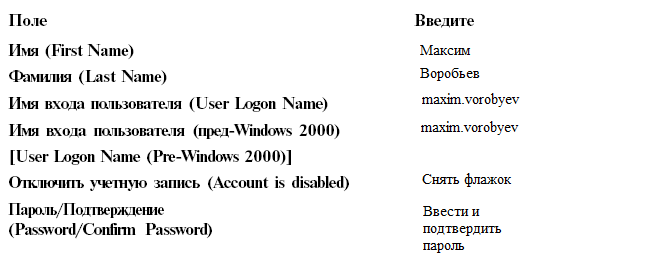
Завершите создание шаблона без изменения остальных параметров. Отключите созданную учётную запись пользователя с помощью *сценария.*

Раскройте свойства объекта Template Sales Representative. Настройте глобальную группу безопасности с именем Sales Representative ОП Security Groups. Задайте следующие свойства для шаблонной учетной записи:

|  |  |  |
| --- | --- | --- |
| Вкладка | Поле | Ввести |
| Член групп | Член групп | Sales Representative |
| Учетная запись | Время входа | Понедельник - пятница с 9-00 до 17-00 |
| Учетная запись | Истекает | 3 месяца от текущей даты |
| Организация | Организация | Povtas |
| Профиль | Путь к профилю | \\Server1\Profiles\ %Username% |

* + - 1. Создать объекты пользователей путем копирования шаблона.

В меню Действие объекта Template Sales Representative щелкните Копировать. Создайте новую учетную запись пользователя со следующими данными:



Удостоверьтесь, что информация, заданная для шаблона на вкладках свойств Член групп, Учетная запись и Организация, была скопирована в новый объект.

Так как эта учетная запись понадобится для других упражнений, измените значения двух свойств: на вкладке Учетная запись дли параметра Срок действия учетной записи задайте значение Не ограничен, а параметр Время входа настройте так, чтобы вход в систему был разрешен в любое время.

* + - 1. Создайте CSV-файл, из которого будут импортированы два объекта user:

DN,objectClass,sAMAccountName,sn,givenName,userPrincipalName

"CN=Андрей Калиберда,OU=Employees,DC=povtas,DC=com",user,andrey.kalib,Калиберда,Андрей,andrey.kalib@povtas.com

"CN=Юрий Шелаев,OU=Employees,DC=povtas,DC=com",user,juriy.shell,Шелаев,Юрий,juriy.shell@povtas.com

* + - 1. Создав файл в п. 10, импортируйте его содержимое, выполнив команду cvsde:

> csvde -i -f <имя\_файла>.csv

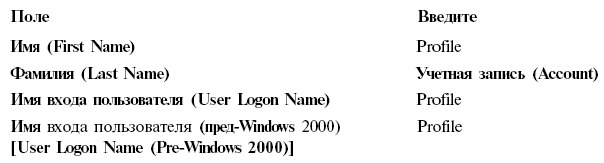
Если команда выдаст подтверждение об успешном выполнении, раскройте *Active Directory — пользователи и компьютеры,* чтобы убедиться, что объекты были созданы. Если команда выдает сообщение об ошибках, раскройте файл USERS.CSV в *Блокноте* и внесите исправления. Так как пользователи были импортированы без паролей, их нужно назначить и включить учетные записи. Сделайте это при помощи соответствующего *сценария* с использованием средств LDAP.

* + - 1. Из командной строки исполните следующую команду:

dsquery user "OU=Employees, DC=povtas, DC=com" - stalepwd 7

Теперь необходимо, чтобы при следующем входе найденных пользователей в систему требовалась смена пароля. Сделайте это с помощью *сценария.*

* + - 1. В контейнере Builtin консоли *Active Directory — пользователи и компьютеры* раскройте окно свойств группы *Операторы печати*. На вкладке Члены группы добавьте группу *Пользователи домена*.
      2. На диске С: создайте папку Profiles. Разрешите Полный доступ к данной папке.
      3. Создайте учетную запись пользователя, которая будет применяться исключительно для создания шаблонов профилей, по следующим данным:



* + - 1. Войдите в систему под учетной записью Profile. Настройте рабочий стол. Настройте рабочий стол при помощи приложения Экран (Display) из Панели управления.
      2. Войдите в систему как Администратор. В Панели управления дважды щелкните Система. На вкладке Дополнительно в области Профили пользователей щелкните Параметры. Выберите профиль, который вы настроили для учетной записи Profile, скопируйте его на \рrofiles\petr.petrov. В области Разрешить использование щелкните Изменить, введите petr.petrov.

Откройте папку C:\Profiles и убедитесь, что папка профиля petr.petrov создана.

Откройте свойства объекта пользователя Петр Петров в дереве консоли *Active Directory — пользователи и компьютеры.* На вкладке Профиль в поле Путь к профилю введите \profiles\%username%.

Проверьте, что преднастроенный перемещаемый профиль пользователя работает правильно.

* + - 1. В *Панели управления* откройте *Система*. На вкладке Дополнительно в области Профили пользователей щелкните Параметры. Выберите профиль, который вы настроили для учетной записи Profile, скопируйте его на \profiles\sales. В области Разрешить использование щелкните Изменить на Users.

Откройте папку C:\Profiles и убедитесь, что папка профиля Sales создана.

Раскройте папку C:\Profiles\Sales и переименуйте скрытый файл Ntuser.dat в Ntuser.man. Этот профиль станет обязательным.

В ОП Employees выберите объекты: Петр Петров, Андрей Калиберда, Юрий Шелаев. В меню Действие выберите Свойства. Перейдите на вкладку Профиль и установите флажок Путь к профилю, введите \profiles\sales.

Проверьте, что преднастроенный перемещаемый профиль пользователя настроен правильно. (не получилось сделать)

Удостоверьтесь, что профиль обязательный, изменив вид рабочего стола. Вы сможете внести изменения, но они не сохранятся для будущих сеансов.

Выйдите из системы и войдите как Калиберда Андрей. Так как профиль обязательный, вы не увидите изменений, сделанных на предыдущем шаге.

Выйдите из системы и войдите как Петр Петров. Должен появиться рабочий стол без изменений.

**Содержание отчета**

1. Название работы
2. Цель работы
3. Выполненные задания. Необходимо сопровождать все проделанные действия скриншотами и описаниями к ним.
4. Выводы.

**Контрольные вопросы**

1. Что такое учетная запись пользователя?
2. Какими способами можно создавать учетные записи?
3. Перечислите свойства объекта пользователя.
4. Какие свойства учетной записи можно одновременно изменить для нескольких объектов пользователей?
5. Перечислите средства командной строки Active Directory.
6. Профили пользователя. Виды профилей.

# Лабораторная работа №3

# Использование средств инструментария для управления Windows (WMI) в администрировании

**Цель работы:** познакомиться со структурой объектов WMI, способами доступа к ним, а такженаучиться работать с WMI через сценарии и утилиты **WBEMTEST** и **WMIC**.

**Порядок выполнения работы**

1. Изучить теоретический материал.
2. Выполнить практические задания.
3. Сделать выводы на основании проделанной работы

**Теоретические сведения**

**Windows Management Instrumentation** (Инструментарий для Управления Windows) — набор интерфейсов для управления операционной системой через специальные компоненты, причем как локально, так и по сети.

WMI позволяет использовать скриптовые языки, такие как [VBScript](http://ru.wikipedia.org/wiki/VBScript) или [Windows PowerShell](http://ru.wikipedia.org/wiki/Windows_PowerShell) для управления персональными компьютерами и серверами, работающими под управлением [Microsoft Windows](http://ru.wikipedia.org/wiki/Microsoft_Windows).

По своей сути WMI – это расширенная и адаптированная компанией Microsoft реализация стандарта WBEM, в основе которого лежит идея создания универсального интерфейса мониторинга и управления к различным системам и компонентам распределенной информационной среды предприятия с использованием объектно-ориентированной идеологии и широко распространенных веб-технологий представления информации: протоколов XML и HTTP.

В основе структуры представления данных в стандарте WBEM лежит CIM (Common Information Model – модель информации общего типа), реализующая объектно-ориентированный подход к представлению компонентов систем как классов со своим набором свойств и методов, а также принципов наследования.

Основное средство для описания новых элементов модели CIM – это синтаксис языка Managed Object Format (MOF), который является текстовым и легко понятным человеку.

Любое приложение или драйвер в операционной системе может добавить к системной модели CIM свой набор классов. Такое расширение модели позволяет легко интегрировать в единую систему мониторинга и управления новые приложения. Для этого приложение должно зарегистрировать свои классы в существующей модели CIM и обеспечить стандартные вызовы встроенных процедур для создания объектов этих классов и наполнения их свойствами и методами. Набор этих процедур оформляется как WMI Provider – специальная библиотека, являющаяся мостом между любым приложением и ядром службы WMI.

* *Провайдеры WMI* скрывают детали внутренней реализации управляемых объектов, позволяя Менеджеру объектов обращаться к ним, используя API-функции.
* *Менеджер объектов CIM* (Common Information Model Object Manager, CIMOM) обеспечивает обработку всех запросов конечных приложений к WMI и доставку информации от WMI к конечным приложениям.
* *Репозиторий* (хранилище классов) *CIM*, объекты-экземпляры которых создаются провайдером WMI по запросу потребителя.
* *Библиотека поддержки сценариев* (WMI scripting library), которая располагается в файле *wbemdisp.dll* в каталоге %SystemRoot%\System32\Wbem\.

**Задания к работе**

1. Просмотр набора классов в репозитории WMI.

Щелкните Пуск\Выполнить, введите wbemtest.

Установите флажок «Включить все привилегии».

Нажмите Подключить.

В окне подключения введите в поле Пространство имен \\Server01\root\cimv2 и нажмите Подключить.

Затем нажмите кнопку «Классы…», выберите «Рекурсивно», не заполняйте поле суперкласса и нажмите «Ok». В результате вы получите список классов, определенный в вашем репозитории WMI, в пространстве имен CIMv2.

Найдите класс Win32\_NTDomain и щелкните на нем дважды левой кнопкой мыши.

В открывшемся окне редактора нажмите кнопку Экземпляры, чтобы увидеть список экземпляров.

Найдите свой домен и зайдите в окно свойств для данного экземпляра.

Нажмите кнопку Соединители.

Используя утилиту wbemtest, получите список экземпляров групп домена.

Найдите в списке группу «Sales Representatives» и ознакомьтесь со значениями параметров этой группы.

Найдите в экземплярах класса учетных записей пользователей Templatesalesrep и petr.petrov. Убедитесь, что свойство Disabled у первого установлено в True, а у второго – в False. Измените значение Disabled у petr.petrov.

2. Найдите класс Win32\_UserAccount.

В окне методов этого класса значится метод Rename.

Найдите экземпляр petr.petrov, скопируйте в буфер обмена значение его свойства \_RELPATH.

В главном окне wbemtest нажмите кнопку Выполнить метод (Execute Method).

В появившемся окне введите в поле Object Path содержимое буфера обмена и нажмите ОК.

Вы получили доступ к методу Rename для этого экземпляра. Задайте входные параметры для метода (свойство Name) и выполните метод.

Убедитесь в Active Directory Users and Computers, что в свойствах аккаунта изменилось имя. Измените его обратно на petr.petrov.

С помощью выполнения соответствующего метода осуществите перезагрузку системы (класс Win32\_OperatingSystem).

3. Запросы WQL.

Нажмите на кнопку Query в окне утилиты wbemtest.

Убедитесь, что в качестве типа запроса выбран WQL.

В поле ввода напишите запрос.

select \* from Win32\_UserInDomain

Результатом выполнения запроса будет список пользователей.

Составьте и выполните запрос, выводящий список пользователей своего домена, являющихся членами группы Sales Representative.

Составьте и выполните запрос, выводящий список заблокированных учетных записей пользователей.

Составьте и выполните запросы, перечисляющие логические диски, процессоры, видеокарты, принтеры в составе системы, а также выполняющиеся на сервере в данный момент процессы. Ознакомьтесь со свойствами экземпляров классов.

1. Утилита Wmic.

Запустите интерпретатор командной строки cmd.exe и в строке приглашения наберите WMIC. После этого появится приглашение консоли WMI.

Просмотрите весь список команд и псевдонимов при помощи команды wmic /? (wmic:root\cli>/?).

Используя команду wmic group where domain=”<Имя\_домена>”, получите список групп домена.

Выполните команду:



Просмотрите возможные команды для useraccount и group.

Создайте новую группу в своем домене.

Создайте в этой группе пользователя, задав его имя, полное имя, и требование изменения пароля при следующем заходе в систему.

Убедитесь, что группа и пользователь созданы при помощи утилиты wmic.

Удалите группу и пользователя в ней, используя команду Delete.

Запросите параметры домена (ntdomain).

Разблокируйте аккаунт Templatesalesrep.

Убедитесь в том, что аккаунт был разблокирован, при помощи соответствующего запроса.

1. Сценарии с использованием WMI
   1. Просмотр списка процессов при помощи сценария

Откройте блокнот и наберите следующий текст:

On error Resume Next

strComputer="server01"

Set objWMIService = GetObject("winmgmts:\\" & strComputer &"\root\cimv2")

Set colItems=objWMIService.ExecQuery("Select \* from Win32\_UserAccount")

For each objItem in colItems

if ObjItem.domain="POVTAS" then

Wscript.echo "Caption "&ObjItem.caption

Wscript.echo "Name: "&ObjItem.name

Wscript.echo "Full name: "&ObjItem.fullname

Wscript.echo "Disabled: "&ObjItem.disabled

Wscript.echo "------------------------------"

end if

Next

Сохраните файл, сменив расширение на \*.vbs.

Запустить сценарий на выполнение можно просто двойным щелчком на файле, тогда результаты будут выводиться в виде сообщений.

Однако, в данном случае это неудобно, поэтому воспользуйтесь возможностью запуска сценариев в режиме консоли.

Запустите командную строку и выполните команду cscript <имя\_файла\_сценария.vbs>.

Просмотрите полученную информацию.

Разберите текст сценария, чтобы уяснить принцип его составления.

* 1. Управление объектами с помощью сценариев WMI

Выведите список групп, присутствующих в домене.

Напишите сценарий, при помощи которого объект пользователя будет перемещен из одной группы в другую.

Создайте сценарий, выводящий список групп и учетных записей пользователей, входящих в эти группы с основными параметрами по каждому объекту в текстовый файл.

Создайте сценарии синхронного и асинхронного отслеживания подключений пользователей домена.

**Содержание отчета**

1. Название работы
2. Цель работы
3. Выполненные задания. Необходимо сопровождать все проделанные действия скриншотами и описаниями к ним.
4. Выводы.

**Контрольные вопросы**

1. Что такое WMI? Для чего она используется?
2. Перечислите средства работы с WMI для администратора.
3. Общая структура WMI.
4. Опишите возможности программы WMIC.
5. Опишите возможности программы WBEMTEST.
6. Использование WQL-запросов.
7. Каковы виды обработки событий WMI?

# Лабораторная работа №4

# Группы. Настройка политик и событий

**Цель работы:** получить навыки создания групп и работы с ними при помощи сценариев и команды LDIFDE, а также настройки политик и событий.

**Порядок выполнения работы**

1. Изучить теоретический материал.
2. Выполнить практические задания.
3. Сделать выводы на основании проделанной работы

**Теоретические сведения**

Группы Active Directory — это гибкие структуры, которые могут включать объекты практически любых типов и используются для самых разных целей, в том числе для управления доступом пользователей к ресурсам и определения фильтров в случае применения групповых политик. Кроме того, группы Active Directory можно использовать в качестве списков рассылки сообщений электронной почты.

Каждая группа имеет определенную область действия и относится к одному из двух типов: *безопасности* или *распространения*. Группы безопасности исполь­зуются для ограничения доступа к ресурсам, а группы распространения — просто как механизм группировки объектов. Область действия группы может быть *гло­бальной*, *универсальной* или *локальной доменной*. Она определяет, в какой части леса располагаются включаемые в группу объекты и в какой части леса группа используется в списках контроля доступа. Члены универсальных и локальных доменных групп могут относиться к любым доменам леса, но при этом первым разрешения обычно предоставляются в любом домене леса, а вторым — только в локальном. Глобальные группы включают пользователей из того же домена, к которому относится группа, но зато им могут быть предоставлены разрешения в любом домене леса.

**Смена паролей пользователей**

Если пользователь забыл пароль, необходима смена пароля. Для этого не требуется знать старый пароль пользователя. Просто щелкните объект пользователя и в меню **Действие** выберите **Смена пароля**.Дважды введите новый пароль, чтобы подтвердить изменение. Кроме того, общепринятая практика в таких случаях — установить флажок *Требовать смену пароля при следующем входе в систему.*

Очень часто может потребоваться отключение, включение и переименование объектов пользователей. Эти действия выполняются схожим образом. Щелкните объект пользователя и в меню *Действие* выберите нужную команду:

* **отключение и включение** — если пользователю в течение длительного периода времени не требуется доступ к сети, отключите его учетную запись, а когда пользователю снова потребуется войти в сеть, включите ее. В зависимости от текущего состояния объекта в меню *Действие*вы увидите только одну из команд: *Отключить* или *Включить*;
* **удаление** — если пользователь уволился, а замены в скором времени не ожидается, нужно удалить его объект. Удалив пользователя, вы удалите сведения о его членстве в группах и (из-за удаления SID) его права и разрешения. Если вы затем создадите объект пользователя с тем же именем, у него будет другой SID, и вам потребуется переназначить права, разрешения и группы;
* **переименование** — объект пользователя потребуется переименовать, если он изменил фамилию или уволился, но для него планируется замена, и нужно сохранить права, разрешения, сведения о членстве в группах и большинство свойств.

**Задания к работе**

1. Создание и изменение группы.

В консоли *Active Directory — пользователи и компьютеры* раскройте контейнер Users и создайте в нем глобальную группу распространения Agents и выберите Свойства.

Можете ли вы изменить область действия и тип этой группы? Почему?

Если вы не можете изменить тип и область действия группы, ваш домен работает в смешанном режиме Windows 2000 или в промежуточном режиме Windows Server 2012. Чтобы изменить тип или область действия группы, необходимо перевести домен в основной режим Windows 2000 или в режим Windows Server 2012.

1. Напишите сценарии, которые позволят выполнить операции:
2. Создание трех локальных групп в ОП Groups: Group1, Group2 и Group3.
3. Изменение области действия созданных групп на глобальную (сначала на универсальную, а затем на глобальную).
4. Создание трех учетных записей пользователей: User1, User2 и User3.
5. Добавление User1, User2 и User3 в группу Group1.
6. Просмотр членов группы Group1.
7. Перемещение Group1 в группу Group2.

Какие группы теперь можно преобразовать в универсальные? Проверьте свои теоретические знания (вы должны без проблем преобразовать две из трех этих групп).

1. Управление учетными записями групп с помощью команды LDIFDE
   1. Вывести список доступных параметров команды LDIFDE
   2. Экспорт сведений о пользователях из одного ОП.

В домене создайте ОП Marketing. Добавьте в ОП Marketing двух или трех пользователей. Дайте им произвольные имена. Экспортируете содержимое ОП Marketing из состава вашего домена.

* 1. Создание группы командой LDIFDE

С помощью команды LDIFDE добавить группу Management в ОП Marketing из состава вашего домена.

В консоли *Active Directory — пользователи и компьютеры* проверьте, что новая группа создана.

1. Работа с политиками

4.1. Настройка политик

В консоли *Active Directory* — *пользователи и компьютеры* щелкните узел домена и выберите его свойства.

На вкладке Групповая политика выберите Default Domain Policy и щелкните *Изменить*. Раскройте узлы Конфигурация компьютера, Конфигурация Windows, Параметры безопасности, Политики учетных записей и Политика блокировки учетной записи.

Дважды щелкните политику Блокировка учетной записи на. Установите флажок Определить следующий параметр политики.

Установите продолжительность периода в 0. Убедитесь, что значение политики Блокировка учетной записи на — 0, пороговое значение — 5 и сброс политики счетчика произойдет через 30 минут.

Щелкните контейнер Контроллеры домена, расположенный по иерархии ниже узла домена и выберите Свойства.

На вкладке Групповая политика выберите Default Domain Controllers Policy и щелкните Изменить.

Раскройте узлы Конфигурация компьютера, Конфигурация Windows, Параметры безопасности, Локальные политики и Политика аудита.

Дважды щелкните политику Аудит событий входа в систему.

Выберите Определить следующий параметр политики, установите флажки Успех и Отказ.

Дважды щелкните политику Аудит входа в систему. Выберите Определить следующий параметр политики, установите флажки Успех и Отказ.

Дважды щелкните политику Аудит управления учетными записями. Выберите Определить следующий параметр политики, установите флажок Успех.

4.2. Генерация событий входа в систему

Завершите сеанс на Server1.

Сгенерируйте два события неудачного входа в систему, дважды попытавшись войти с именем пользователя petr.petrov и неверным паролем.

Войдите в систему правильно (как пользователь petr.petrov).

Выйдите из системы.

4.3. Генерация событий управления учетными записями

Войдите в систему как Администратор.

Откройте консоль Active Directory — пользователи и компьютеры и выберите ОП Employees.

Выберите объект пользователя Петр Петров и раскройте меню Действие, в котором выберите команду Смена пароля.

Введите и подтвердите новый пароль для Петр Петров.

4.4. Анализ событий безопасности, сгенерированных проверкой подлинности

Откройте консоль *Управление компьютером* из группы Администрирование.

Раскройте узел Просмотр событий и щелкните Безопасность.

Расширьте столбец Категория, чтобы видеть типы зарегистрированных событий.

Изучите события, сгенерированные действиями, которые вы только что выполнили.

Обратите внимание на события неудачного и удачного входа в систему, а также на смену пароля для пользователя Петр Петров.

**Содержание отчета**

1. Название работы
2. Цель работы
3. Выполненные задания. Необходимо сопровождать все проделанные действия скриншотами и описаниями к ним.
4. Выводы.

**Контрольные вопросы**

1. Что такое группы Active Directory? Типы групп.
2. Перечислите политики паролей. Что они определяют?
3. Перечислите политики блокировки учетной записи. Что они определяют?
4. Что такое аудит? Перечислите политики аудита.
5. Что содержит журнал событий безопасности?
6. Для чего необходима возможность отключения, включения и переименования объектов пользователей?

# Лабораторная работа №5

# Присоединение компьютера к домену Active Directory

**Цель работы:** получить навыки создания учетных записей компьютеров, присоединения компьютеров к домену.

**Порядок выполнения работы**

1. Изучить теоретический материал.
2. Выполнить практические задания.
3. Сделать выводы на основании проделанной работы

**Теоретические сведения**

В стандартной конфигурации Windows Server 2012 и всех ОС Microsoft Windows компьютер принадлежит какой-либо *рабочей* *группе* (workgroup). В рабочей группе компьютер на базе Windows NT (включая Windows NT 4, 2000, XP и Windows Server 2012) может проверять подлинность пользователей только из своей локальной БД *диспетчера учетных записей безопасности* (Security Accounts Manager, SAM). Такая система автономна во всех смыслах. Принадлежность к рабочей группе позволяет лишь видеть список компьютеров своей группы в *Проводнике.* Хотя пользователь такого компьютера и может подсоединяться к общим ресурсам на других машинах в рабочих группах или доменах, он на самом деле не входит в систему под доменной учетной записью.

Чтобы пользователь входил в систему под доменной учетной записью, компьютер должен принадлежать какому-нибудь домену: необходимо создать учетную запись компьютера и настроить его для присоединения к домену по этой учетной записи.

Учетная запись компьютера, как и учетная запись пользователя, содержит имя, пароль и *идентификатор безопасности* (security identifier, SID). Эти свойства встроены в класс объекта компьютера в Active Directory. Подготовка к включению компьютера в домен, таким образом, очень похожа на подготовку объекта пользователя для добавления в домен: вам нужно создать в Active Directory объект компьютера.

**Создание учетных записей компьютеров**

Для создания объекта компьютера в Active Directory необходимо быть членом групп *Администраторы* (Administrators) или *Операторы учета* (Account Operators) на контроллерах домена. Члены групп *Администраторы домена* (Domain Admins) и *Администраторы предприятия* (Enterprise Admins) по умолчанию являются участниками группы *Администраторы* (Administrators). Также можно делегировать административные права, чтобы другие пользователи или группы могли создавать объекты компьютеров.

Скрипт создания объекта computer:

' ----- SCRIPT CONFIGURATION ------------

strBase = "<имя\_род\_конт\_компьютера>" 'Например: cn=Computers,dc=povtas,dc=com

strComp = "<имя\_компьютера>" 'Например: ivan-pc

strDescr = "<описание>" 'Например: ivan's Windows XP workstation

' ----- END CONFIGURATION ---------------

'Из перечисления ADS\_USER\_FLAG\_ENUM

Const ADS\_UF\_WORKSTATION\_TRUST\_ACCOUNT = &h1000

set objCount = GetObject("LDAP://" & strBase)

set objComp = objCont.Create("computer","cn=" & strComp)

objComp.Put "sAMAccountName", strComp & "$"

objComp.Put "description", strDesc

objComp.Put "userAccountControl", ADS\_UF\_WORKSTATION\_TRUST\_ACCOUNT

objComp.SetInfo

Wscript.Echo "Computer account for " & strComp & " created"

**Создание учетной записи компьютера командой NETDOM**

Программа **NETDOM** входит в комплект средств поддержки и устанавливается из каталога Support\Tools компакт-диска Windows Server 2003. Эта программа также содержится на компакт-дисках Windows 2000 и XP. Используйте версию, подходящую для вашей платформы. Команда NETDOM позволяет выполнять из командной строки множество операций, связанных с учетными записями доменов и безопасностью.

Чтобы создать в домене учетную запись компьютера, введите следующую команду:

netdom add имя\_компьютера / domain:имя\_домена /userd:пользователь /

PasswordD:пapoль\_пoльзoвaтeля [/ou:DN\_ОП]

Эта команда создает учетную запись для компьютера *имя\_компьютера* в домене *имя\_домена* от имени *пользователя* домена с паролем *пароль\_пользователя.* Параметр /ou приводит к созданию объекта в ОП с различающимся именем *DN\_ОП.* Если имя целевого ОП не указано, по умолчанию учетная запись компьютера создается в контейнере Computers.

**Сценарий присоединения компьютера к домену:**

' ------- SCRIPT CONFIGURATION --------------

strComputer ="<имя\_компьютера>" 'Например:ivan-pc

strDomain ="<имя\_домена>" 'Например:povtas.com

strDomainUser ="<UPN-имя\_пользователя>" 'Например:administrator@povtas.com

strDomainPassword ="<пароль\_пользователя\_домена>"

strLocalUser ="<администратор\_компьютера>" 'Например:administrator

strLocalPasswd ="<пароль\_пользователя\_компьютера>"

' ------- END CONFIGURATION -----------------

'Константы

Const JOIN\_DOMAIN = 1

Const ACCT\_CREATE = 2

Const ACCT\_DELETE = 4

Const WIN9X\_UPGRADE = 16

Const DOMAIN\_JOIN\_IF\_JOINED = 32

Const JOIN\_UNSECURE = 64

Const MACHINE\_PASSWORD\_PASSED = 128

Const DEFERRED\_SPN\_SET = 256

Const INSTALL\_INVOCATION = 262144

'Подключение к компьютеру

set objWMILocator = CreateObject("WbemScripting.SWbemLocator")

objWMILocator.Security\_.AuthenticationLevel = 6

set objWMIComputer = objWMILocator.ConnectServer(strComputer,

"root\cimv2",

strLocalUser,

strLocalPasswd)

set objWMIComputerSystem = objWMIComputer.Get(

"Win32\_ComputerSystem.Name='"&

strComputer & "'")

'Присоединение к домену

rc = objWMIComputerSystem.JoinDomainOrWorkGroup(strDomain,

strDomainPasswd,

strDomainUser,

vbNullString,

JOIN\_DOMAIN)

if rc<>0 then

WScript.Echo "Join failed with error: " & rc

else

WScript.Echo "Successfully joined " & strComputer & " to " & strDomain

end if

**Сценарий перемещение объекта computer:**

' Этот код перемещает компьютер в заданный контейнер или подразделение

' --------- SCRIPT CONFIGURATION -----------

strCompDN = "<ОИ\_компьютера>" 'Например:cn=ivan-xp,cn=users,dc=povtas,dc=com

strOUDN = "<ОИ\_нового\_род\_контейнера>" 'Например:ou=workstations,dc=povtas,dc=com

' --------- END CONFIGURATION --------------

set ObjComp = GetObject("LDAP://" & strCompDN)

set objOU = GetObject("LDAP://" & strOUDN)

objOU.MoveHere objComp.ADsPath, objComp.Name

**Сценарий переименование компьютера:**

'Этот код переименовывает компьютер и записывает его новое имя в каталог Active Directory

' ------- SCRIPT CONFIGURATION --------------

strComputer ="<имя\_компьютера>" 'Например:ivan-pc

strNewComputer ="<новое\_имя\_компьютера>" 'Например:ivan-xp

strDomainUser ="<UPN-имя\_пользователя>" 'Например:administrator@povtas.com

strDomainPassword ="<пароль\_пользователя\_домена>"

strLocalUser ="<администратор\_компьютера>" 'Например:administrator

strLocalPasswd ="<пароль\_пользователя\_компьютера>"

' ------- END CONFIGURATION -----------------

'Подключение к компьютеру

set objWMILocator = CreateObject("WbemScripting.SWbemLocator")

objWMILocator.Security\_.AuthenticationLevel = 6

set objWMIComputer = objWMILocator.ConnectServer(strComputer,

"root\cimv2",

strLocalUser,

strLocalPasswd)

set objWMIComputerSystem = objWMIComputer.Get(

"Win32\_ComputerSystem.Name='"&

strComputer & "'")

'Переименование компьютера

rc = objWMIComputerSystem.Rename(strNewComputer,

strDomainPasswd,

strDomainUser)

if rc<>0 then

WScript.Echo "Rename failed with error: " & rc

else

WScript.Echo "Successfully renamed " & strComputer & " to " & strNewComputer

end if

WScript.Echo "Rebooting..."

set objWSHShell = WScript.CreateObject("WScript.Shell")

objWSHShell.Run "shutdown.exe /r"

**Сценарий переустановки учетной записи компьютера:**

' Этот код переустанавливает учетную запись компьютера, назначая ей пароль, используемый по умолчанию. После выполнения данного действия нужно повторно присоединить компьютер к домену

set objComputer = GetObject("LDAP://<ОИ\_компьютера>")

objComputer.SetPassword "<имя\_компьютера>"

**Задания к работе**

1. В консоли *Active Directory* — *пользователи и компьютеры* в ОП Servers создайте объект для компьютера с именем SERVER02. Задайте только имя компьютера. Не меняйте значения других параметров по умолчанию.
2. Создайте учетную запись компьютера командой DSADD.
3. Создайте при помощи сценария учетную запись компьютера desktop04 в Servers.
4. В Active Directory переместите компьютер desktop03 из ОП Servers в ОП Domain Controllers.

Выполните аналогичные действия с компьютером desktop04, используя сценарий. Перетащите значок server02 из контейнера Servers в Computers. Убедитесь, что server02 появился в нужном месте. Переместите объект компьютера desktop04 обратно в ОП Servers. Проверьте, что этот компьютер снова находится в ОП Servers.

1. Присоединение компьютера к домену.

Здесь нужен второй компьютер, подключенный к server01. Кроме того, нужно правильно сконфигурировать DNS, чтобы для server01 была создана запись ресурса службы (SRV). На втором компьютере DNS должна быть сконфигурирована так, чтобы он мог находить server01 как контроллер домена.

Войдите в систему на этом компьютере. Чтобы изменять членство этого компьютера в домене, нужно войти в систему под учетной записью локальной группы *Администраторы*.

Откройте вкладку Имя компьютера. Для этого дважды щелкните Система в *Панели управления* или в папке Сетевые подключения, в меню Дополнительно выберите Сетевая идентификация.

Щелкните Изменить.

Установите переключатель в положение домена и введите DNS-имя домена.

По запросу введите имя и пароль учетной записи администратора домена.

Будет предложено перезагрузить систему. Щелкайте ОК в ответ на все сообщения и закройте все диалоговые окна. Перезагрузите систему.

1. Управление учетными записями компьютеров

Переименуйте созданный ранее desktop04 в desktop05, пользуясь *сценарием*.

Откройте консоль *Active Directory* — *пользователи и компьютеры*. Выберите ОП Security Groups и создайте глобальную группу безопасности с именем Deployment. Выберите ОП Desktops.

Создайте учетную запись для компьютера desktop04. На первой странице окна Новый объект — Компьютер щелкните Изменить ниже строки Присоединить к домену этот компьютер могут пользователь или группа пользователей, указанные ниже. Введите Deployment в окне Выбор: «Пользователь» или «Группа».

Завершите создание объекта компьютера desktop04.

1. Поиск неактивных объектов в Active Directory с помощью командной строки

Найдите учетные записи компьютеров, не подключавшихся к Active Directory в течение заданного времени. Выполните это с помощью интерфейса командной строки.

Осуществите поиск компьютеров, которые были не активны в течение 2 недель.

Удалить учетные записи всех компью­теров, которые не подключались к домену в течение 12 и более недель с помощью командной строки.

Скорректируйте условия запроса таким образом, чтобы поиск осуществлялся только в контейнере Desktops.

8. Поиск объектов в Active Directory

В консоли *Active Directory — пользователи и компьютеры* на панели инструментов щелкните значок Поиск объектов в службе каталогов Active Directory.

В списке Найти выберите Компьютеры, а в списке в — Целиком Active Directory.

В поле Имя компьютера введите server и щелкните Найти.

9. Изменение свойств объекта компьютера.

Откройте окно свойств компьютера server01 и перейдите на вкладку Размещение.

Введите Headquarters Server Room (Серверная в головном офисе).

Перейдите на вкладку Управляется и щелкните кнопку Изменить.

Введите Иван. Заметьте: отображается имя этого пользователя и его контактная информация.

Перейдите на вкладку Операционная система (Operating System). Заметьте: отображается версия используемой ОС и уровень пакета обновления.

10. Устранение неполадок с учетной записью компьютера.

Нужно устранить неполадку в реалистичной ситуации. Пользователь в домене povtas.com жалуется: при входе в систему на компьютере desktop03 выдается сообщение об ошибке:

«Не удалось подключиться к домену, либо потому, что контроллер домена не работает или недоступен по другой причине, либо потому, что учетная запись этого компьютера не найдена. Повторите попытку спустя некоторое время. Если это сообщение продолжает появляться, обратитесь за помощью к системному администратору».

Пользователь подождал, снова попробовал войти в систему, получил то же сообщение, подождал еще и получил это сообщение в третий раз. На попытки входа в систему он потерял уже 20 минут. Пользователь обращается к вам за помощью.

Определите наиболее вероятную причину проблемы пользователя:

1. Пользователь ввел неверное имя;
2. Пользователь ввел неверный пароль;
3. Пользователь выбрал неверный домен из списка Вход на (Log On To);
4. Безопасный канал связи компьютера с доменом разорван;
5. Реестр данного компьютера поврежден;
6. На компьютере установлена политика, запрещающая данному пользователю интерактивный вход в систему.

Перечислите, какие действия из следующего списка необходимо предпринять для устранения проблемы. Определите порядок действий. Не обязательно использовать все перечисленные шаги.

1. Включить учетную запись этого компьютера.
2. Присоединить компьютер desktop03 к домену contoso.com.
3. Определить, существует ли данная учетная запись компьютера в Active Directory.
4. Переустановить эту учетную запись компьютера или создать ее снова.
5. Включить desktop03 в какую-либо рабочую группу.
6. Удалить учетную запись этого компьютера.
7. Отключить учетную запись этого компьютера.

10.2. Устранение проблем с учетной записью компьютера

В консоли *Active Directory* — *пользователи и компьютеры*  найдите компьютер desktop03.

Убедившись, что эта учетная запись компьютера существует, переустановите ее.

Утилитой dsmod переустановите пароль компьютера. После этого компьютер следует повторно присоединить к домену.

Переустановите учетную запись desktop03 еще раз, пользуясь командой netdom.

**Содержание отчета**

1. Название работы
2. Цель работы
3. Выполненные задания. Необходимо сопровождать все проделанные действия скриншотами и описаниями к ним.
4. Выводы.

**Контрольные вопросы**

1. Для чего нужна учетная запись компьютера?
2. Какими способами можно создавать учетные записи компьютеров?
3. Перечислите свойства объекта компьютера.
4. Для чего необходима возможность удаления, отключения и переустановки учетных записей компьютеров?
5. Каковы правила при устранении неполадок с учетными записями компьютеров?
6. Почему учетная запись компьютера создается в домене до присоединения компьютера к домену?

# Лабораторная работа №6

# Обеспечение безопасности ресурсов с помощью разрешений NTFS

**Цель работы:** получить навыки обеспечения безопасности ресурсов с помощью разрешений NTFS.

**Порядок выполнения работы**

1. Изучить теоретический материал.
2. Выполнить практические задания.
3. Сделать выводы на основании проделанной работы

**Теоретические сведения**

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, размещенных 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, АСЕ), для этого пользователя или группы, к которой он принадлежит. Эта запись назначит запрашиваемый тип доступа (например, **Чтение**) пользователю. Если в ACL нет соответствующей АСЕ, то пользователь не получит доступ к ресурсу.

**Множественные разрешения NTFS**

Можно установить несколько разрешений пользователю и всем группам, членом которых он является. Для этого нужно 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.

**Приоритет разрешений для файлов над разрешениями для папок**

В NTFS разрешения для файлов имеют больший приоритет, чем разрешения для папок. Если у вас есть разрешение на доступ к файлу и право **Обход перекрестной проверки**, то вы сможете воспользоваться доступом к этому файлу, даже если у вас нет доступа к папке, в которой содержится файл. Вы можете получить доступ к тем файлам, для которых у вас есть разрешения, воспользовавшись UNC-именем файла или локальным путем для открытия файла из соответствующего приложения. Это возможно, даже если папка, в которой находится файл, невидима и у вас нет соответствующего разрешения для данной папки. Другими словами, если у вас нет разрешения на доступ к папке, содержащей нужный вам файл, для доступа к файлу вам необходимо обладать правом **Обход перекрестной проверки** и знать полный путь к файлу.

**Приоритет запрещения над разрешениями**

Можно запретить доступ к файлу пользователю или группе, хотя этот метод контроля ресурсов нельзя назвать предпочтительным. Запрет имеет больший приоритет, чем разрешение на всех уровнях, на которые он распространяется. Даже если у группы, в которую входит пользователь имеется разрешение на доступ к файлу или папке, запрет на доступ для пользователя блокирует все имеющиеся разрешения.

**Задания к работе**

1. Начните сеанс работы, используя учетную запись члена группы **Администраторы**, и создайте учетные записи пользователей по данным следующей таблицы.

|  |  |
| --- | --- |
| **Учетная запись пользователя** | **Тип** |
| Userl | Ограниченная учетная запись |
| User2 | Ограниченная учетная запись |
| User3 | Ограниченная учетная запись |
| User4 | Ограниченная учетная запись |

Создайте следующие папки:

* C:\Public;
* C:\Public\Library.

1. Определить устанавливаемые по умолчанию разрешений NTFS для папки Public.
2. Проверка разрешений, установленных для папки Public. Войдите в систему, используя учетную запись User1, затем запустите Проводник.

Перейдите в папку Public, создайте текстовый документ, назовите его User1. Введите следующий текст:

*The first four letters in the alphabet are a, b, c, and d.*

Выделите значок папки Public в древовидной структуре папок. В пункте меню Файл выберите Создать, затем щелкните Текстовый документ для создания нового документа.

Операция прошла успешно? Почему?

Попытайтесь выполнить следующие операции с созданным файлом:

* откройте файл;
* измените файл;
* удалите файл.

Какие действия вы смогли успешно совершить и почему?

В папке Public снова создайте текстовый документ User1.

Завершите сеанс.

Войдите в систему, используя учетную запись User2.

Попытайтесь выполнить следующие операции с текстовым документом User1:

* откройте файл;
* измените файл;
* удалите файл.

Какие действия вы смогли успешно совершить и почему?

1. Установить разрешения NTFS для папки Public.

При этом необходимо соблюдать следующие правила:

* все пользователи должны иметь возможность читать документы и файлы в папке Public;
* все пользователи должны иметь возможность создавать документы в папке Public;
* все пользователи должны иметь возможность изменять содержание, свойства и разрешения для создаваемых ими документов в папке Public;
* пользователь User2 несет ответственность за подержание папки Public и должен иметь возможность изменять и удалять все файлы в папке Public.

Основываясь на полученной в упражнении 1 информации, определите, как следует изменить разрешения для соответствия этим четырем критериям? Почему?

В настоящее время ваша регистрационная запись — User2. Можете ли вы изменить разрешения, установленные для пользователя User2, пока вы подключены как User2? Почему?

1. Установка разрешений NTFS для папки.

Войдите в систему, используя учетную запись пользователя, который является членом группы Администраторы. Затем откройте Проводник.

Выберите папку Public, затем пункт меню Свойства.

Перейдите на вкладку Безопасность диалогового окна свойств папки.

На вкладке Безопасность щелкните кнопку Изменить.

На вкладе *Разрешение для группы* щелкните кнопку *Добавить*

В текстовом поле Введите имена выбираемых объектов введите User2, затем щелкните кнопку Проверить имена.

В текстовом поле Введите имена выбираемых объектов должна появиться надпись “имя компьютера”\User2. Теперь пользователь User2 включен в список Группы или пользователи диалогового окна свойств папки Public.

Какие разрешения установлены для пользователя User2?

Щелкните кнопку Дополнительно. Вы увидите, что пользователь User2 (“имя компьютера”\User2) включен в список Элементы разрешений.

Убедитесь, что строка User2 выделена, и щелкните кнопку Изменить. Вы увидите в текстовом поле Имя учетную запись пользователя User2 (“имя компьютера”\User2).

В колонке Разрешить щелкните Полный доступ.

Теперь в колонке Разрешить установлены все флажки.

1. Проверка разрешений NTFS для папки.

Войдите в систему, используя учетную запись User2.

Запустите Проводник.

Откройте диск С:, затем откройте папку Public.

Попытайтесь совершить следующие действия с текстовым документом User1:

* измените файл;
* удалите файл.

Какие действия вы смогли совершить и почему?

1. Проверка разрешений NTFS.

Войдите в систему, используя учетную запись User1, затем запустите Проводник.

В Проводнике откройте папку Public\Library.

Создайте текстовый документ User1 в папке Library.

Завершите сеанс.

1. Проверка разрешений для папки Library с использованием подключения с учетной записью User2.

Зарегистрируйтесь в системе, используя учетную запись User2, затем запустите Проводник.

Откройте папку Public\Library.

Попытайтесь совершить следующие действия с текстовым документом User1

* открыть файл;
* изменить файл;
* удалить файл.

Какие действия вы смогли совершить и почему?

Завершите работу.

1. Смена владельца файла.

Подключитесь, используя учетную запись пользователя, который является членом группы Администраторы.

В папке Public создайте текстовый документ и назовите его OWNER.

Щелкните правой кнопкой мыши значок документа OWNER, затем выберите пункт меню Свойства.

Перейдите на вкладку Безопасность для просмотра разрешений, установленных для файла OWNER. Щелкните кнопку Дополнительно. Откроется диалоговое окно Дополнительные параметры безопасности для Owner с активной вкладкой Разрешения. Посмотрите кто является текущим владельцем файла OWNER?

1. Установка разрешения, позволяющего пользователю сменить владельца.

В диалоговом окне Дополнительные параметры безопасности для Owner перейдите на вкладку Разрешения.

Щелкните кнопку Добавить Откроется диалоговое окно Выбор: пользователи или группы.

Убедитесь, что в текстовой поле Размещение, которое расположено вверху диалогового окна, выбрано имя вашего компьютера.

В текстовом поле Введите имена выбираемых введите User1, затем щелкните кнопку Проверить имена.

В списке Введите имена выбираемых объектов должна появиться запись “имя компьютера”\User1. Это означает, что учетная запись пользователя Userl найдена на компьютере с именем “имя компьютера” и является действительной учетной записью.

В списке разрешений установите флажок Разрешить для разрешения Сменить владельца.

1. Смена владельца файла.

Зарегистрируйтесь в системе, используя учетную запись User1, затем запустите Проводник.

Разверните папку Public. Измените владельца на User1.

Кто теперь является владельцем файла OWNER?

1. Проверка разрешений для файла в качестве владельца.

Установите разрешение Полный доступ пользователю User1 к текстовому документу OWNER.

Щелкните кнопку Дополнительно и нажмите *Отключение наследования,* преобразовывая разрешения к явно заданным в этом окне.

В диалоговом окне Безопасность щелкните кнопку Удалить.

Удалите текстовый документ OWNER.

1. Создание папки при подключении с учетной записью пользователя.

Под учетной записью User1, в Проводнике, в корневой папке диска С, создайте папку с именем Temp1.

Какие разрешения установлены для этой папки?

Кто является владельцем папки? Почему?

Закройте все приложения и закончите работу.

1. Создание папки при подключении с учетной записью члена группы Администраторы.

Подключитесь с учетной записью Администратор или как пользователь, который является членом группы Администраторы, и запустите Проводник.

В корневой папке диска С: создайте папки Теmр2 и Теmр3.

Каковы разрешения для папок Теmр2 и Теmр3, которые вы только что создали?

Кто является владельцем папок Теmр2 и Теmр3? Почему?

Установите разрешения для папок Теmр2 и Теmр3. Нажмите *Отключение наследования,* преобразовывая разрешения к явно заданным в этом окне В открывшемся диалоговом окне щелкните Удалить для удаления всех разрешений, кроме указанных явно.

|  |  |
| --- | --- |
| Папка | Установите следующие разрешения |
| Теmр2 | Администраторы: Полный доступ  Пользователи: Чтение и выполнение |
| Теmр3 | Администраторы: Полный доступ  Операторы архива: Чтение и выполнение  Пользователи: Полный доступ |

1. Копирование папки в другую папку на одном и том же томе NTFS

Под учетной записью члена группы Администраторы, в Проводнике, скопируйте папку C:\Temp2 в папку C:\Templ. Для этого выделите значок папки C:\Temp2 и, удерживая нажатой клавишу CTRL, перетащите мышью C:\Temp2 в C:\Templ.

Так как была произведена операция копирования, должны существовать обе папки: C:\Temp2 и C:\Templ\Temp2.

Выделите C:\Templ\Temp2, затем сравните разрешения и права владельца с папкой C:\Temp2.

Кто владелец папки C:\Templ\Temp2 и какие разрешения для нее установлены? Почему?

1. Перемещение папки на одном и том же томе.

Зарегистрируйтесь в системе как пользователь User1.

В Проводнике выделите значок папки C:\Temp3, затем переместите ее в папку C:\Templ.

Что произошло с разрешения и владельцем для папки C:\Templ\ Теmр3? Почему?

Закройте все окна и завершите сеанс работы.

1. В папке C:\Temp1\Temp3 создайте текстовый документ с именем NOACCESS. Запретите для группы Пользователи разрешение Полный доступ для текстового документа NOACCESS.
   1. Просмотрите результаты запрета разрешения Полный доступ к папке Теmр3.

Как предотвратить удаление пользователями, имеющими разрешение Полный доступ к папке, файла в этой папке, для которого установлен запрет на разрешение Полный доступ?

**Содержание отчета**

1. Название работы
2. Цель работы
3. Выполненные задания. Необходимо сопровождать все проделанные действия скриншотами и описаниями к ним.
4. Выводы.

**Контрольные вопросы**

1. Какое из следующих утверждений правильно описывает разрешения NTFS для папок и файлов?
   * Система безопасности NTFS эффективна только в том случае, если пользователь получает доступ к файлу или папку при работе в сети.
   * Система безопасности NTFS эффективна, если пользователь получает доступ к файлу или папке на локальном компьютере.
   * Разрешения NTFS явно указывают, какие пользователи и группы могут получить доступ к файлам и папкам, и какие действия можно совершать с содержимым этих файлов и папок.
   * Разрешения NTFS могут быть использованы для всех файловых систем, совместимых с Windows XP Professional/
2. Какое из следующих разрешений NTFS для папок позволяет вам удалить папку?

* **Чтение**.
* **Чтение и выполнение**.
* **Изменение**.
* **Администрирование**.

1. Какое разрешение NTFS для файлов следует установить для файла, если вы позволяете пользователям удалять файл, но не позволяете становиться владельцем файла?
2. Что такое список управления доступом (ACL)? Чем ACL отличается от элемента списка управления доступом (ACE)?
3. Что такое эффективные разрешения пользователя для ресурса?
4. Какие объекты по умолчанию наследуют разрешения, установленные для родительской папки?
5. Какое разрешение устанавливается для группы Все при форматировании тома?
6. Какие разрешения рекомендуется устанавливать при установке разрешений для папок общего доступа для группы Пользователи, а какие для группы Создатель-Владелец?
7. Кто может устанавливать разрешения для отдельных пользователей и групп? (Выберите все правильные ответы.)

* Члены группы Администраторы.
* Члены группы Опытные пользователи.
* Пользователи, обладающие разрешением **Полный доступ**.
* Владельцы файлов и папок.

1. Какой из следующих вкладок диалогового окна свойств файла или папки следует воспользоваться для установки или изменения разрешения NTFS для файла или папки?

* **Дополнительно**.
* **Разрешения**.
* **Безопасность**.
* **Общие**.

1. Каково назначение особого разрешения **Обзор папок/Выполнение файлов**?
2. Чем отличается разрешение **Удаление** от разрешения **Удаление подпапок и фалов**?
3. Какое из следующих утверждений о копировании файла или папки верно? (Выберите все правильные ответы.)

* При копировании фала из одной папки в другую на одном томе разрешения для файла не изменяются.
* При копировании файла из папки на томе NTFS в другую папку на томе NTFS разрешения для файла не изменяются.
* При копировании файла из одной папки на томе NTFS в другую папку на другом томе NTFS разрешения для файла совпадают с разрешениями для папки, в которую файл копируют.
* При копировании файла из папки на томе NTFS в другую папку на томе FAT разрешения для файла утрачиваются.

1. Какое из следующих утверждений о перемещении файла или папки верно? (Выберите все правильные ответы.)

* При перемещении файла из одной папки в другую на одном томе разрешения для файла не изменяются.
* При перемещении файла из папки на томе NTFS в другую папку на томе FAT разрешения для файла не изменяются.
* При перемещении файла из одной папки на томе NTFS в другую папку на другом томе NTFS разрешения для файла совпадают с разрешениями для папки, в которую файл перемещают.
* При перемещении файла из одной папки в другую на томе NTFS разрешения для файла не совпадают с разрешениями для папки, в которую файл перемещают.

1. С какими ограничениями следует устанавливать разрешения при установке разрешений NTFS?
2. Если вы хотите, чтобы пользователь или группа не имела доступа к определенной папке или файлу, следует ли запретить разрешения для этой папки или файла?

# Лабораторная работа №7

# Архивация и восстановление данных

**Цель работы:** изучить типы архивирования, освоить программу архивации данных, изучить методы архивации и восстановления данных.

**Порядок выполнения работы**

1. Изучить теоретический материал.
2. Выполнить практические задания.
3. Сделать выводы на основании проделанной работы

**Теоретические сведения**

Успех любой процедуры резервного копирования зависит от правильного выбора средств и планирования. В состав Windows Server 2003 входит надежная, гибкая служебная программа Ntbackup. Она поддерживает большинство функций, которые встречаются в средствах сторонних разработчиков, включая возможность составления расписания архивации и взаимодействия со *Службой теневого копирования тома* (Volume Shadow Copy Service, VSS) и системой RSM (Removable Storage Management).

**Определение стратегии архивации**

Выбрав файлы для архивации и указав размещение резервной копии, нужно выбрать тип архива, определяющий, какие именно из выбранных файлов будут копироваться на целевой носитель.

Каждый тип архива так или иначе связан с атрибутом, который есть у каждого файла, — **Архивный**.Атрибут архивирования — это флаг, который устанавливается при создании или изменении файла. Для уменьшения размера и продолжительности заданий резервного копирования большинство типов архивации записывают на носитель только те файлы, у которых установлен атрибут архивирования. Чаще всего недоразумения возникают из-за терминологии. Например, фраза «Файл помечен как заархивированный», на самом деле означает, что атрибут архивирования сброшен после очередного задания архивации. Следующее задание архивации не будет копировать этот файл на носитель. Однако, если этот файл изменится, атрибут архивирования снова будет установлен, и файл запишется на носитель при следующем резервном копировании.

При изучении типов архивации обратите внимание, как атрибут архивирования используется и воспринимается каждым из них. Запомните преимущества и недостатки каждого типа, способы полного восстановления структуры данных в зависимости от реализованной процедуры резервного копирования.

**Обычная архивация**

Архивируются все выбранные файлы и папки. Атрибут **Архивный** сбрасывается. Обычная архивация не учитывает атрибут архивирования при определении файлов, подлежащих резервному копированию; все выбранные ресурсы записываются на целевой носитель. Каждая стратегия начинается с обычной архивации, которая по существу создает базовую линию, копируя все файлы в задании архивации.

По сравнению с другими типами обычная архивация выполняется дольше и требует больше места на носителе. Но, поскольку создается полная резервная копия данных, обычная архивация обеспечивает самую высокую скорость восстановления системы. Вам не придется восстанавливать несколько заданий. Обычная архивация сбрасывает атрибут архивирования у всех выбранных файлов.

**Добавочная архивация**

На целевой носитель копируются только выбранные файлы с установленным атрибутом архивирования, и флаг сбрасывается. Если добавочная архивация выполняется на следующий день после обычной или другой добавочной архивации, копируются только созданные или измененные за последний день файлы.

Добавочная архивация самая быстрая и формирует архив минимального размера. Тем не менее, она не так эффективна, как обычная, поскольку требует восстановления сначала обычного архива, а затем всех последующих добавочных архивов в порядке их создания.

**Разностная архивация**

Копируются только выбранные файлы с атрибутом архивирования, и флаг не сбрасывается. Поскольку разностная архивация учитывает атрибут архивирования, копируются только файлы, созданные или измененные с момента последней обычной или добавочной архивации. Атрибут архивирования не сбрасывается, поэтому разностные архивы содержат не только созданные или измененные файлы, но и все файлы, скопированные при предыдущей разностной архивации. В результате резервные копии становятся больше, а сама разностная архивация длится дольше, чем добавочная, но меньше, чем обычная.

Разностная архивация, однако, значительно эффективнее добавочной в плане восстановления: требуется восстановить только обычный и последний разностный архивы.

**Копирующая архивация**

Архивируются все выбранные файлы и папки. Атрибут архивирования не учитывается. Копирующая архивация не применяется для обычного или планового резервного копирования. Ее удобно использовать для перемещения данных между системами или создания архивной копии данных на некоторый момент времени без вмешательства в стандартные процедуры резервного копирования.

**Ежедневная архивация**

Копируются все выбранные файлы и папки, измененные в течение дня с момента последней ежедневной архивации (на основе даты изменения файла). Атрибут архивирования не используется и не сбрасывается. Если вам нужно создать резервную копию файлов и папок, измененных за день, не составляя расписание, используйте ежедневную архивацию.

**Совмещение типов резервного копирования**

Хотя создание обычного архива каждую ночь обеспечивает возможность восстановления данных на следующий день с помощью одного задания, обычная архивация требует слишком много времени, и ночное задание может продлиться до утра, снижая производительность в рабочие часы. Чтобы выбрать оптимальную стратегию резервного копирования, необходимо учесть продолжительность и размер задания архивации, а также скорость восстановления системы в случае сбоя. Есть *два типичных решения.*

* **Обычная и разностная архивация.** В воскресенье выполняется обычная архивация, а с понедельника по пятницу — разностная. Разностная архивация не сбрасывает атрибут архивирования, поэтому каждая операция копирует все изменения, произошедшие с понедельника. В случае сбоя данных в пятницу придется восстановить только обычный архив от воскресенья и разностный от четверга. Такая стратегия требует больше времени для резервного копирования, особенно если данные изменяются часто, но восстановление происходит быстрее и удобнее, поскольку набор архивации занимает меньше дисков или лент.
* **Обычная и добавочная архивация.** В воскресенье выполняется обычная архивация, а с понедельника по пятницу — добавочная. Последняя сбрасывает атрибут архивирования, поэтому каждая операция архивации включает только файлы, изменившиеся со времени последнего резервного копирования. В случае сбоя данных в пятницу придется восстановить обычный архив, сделанный в воскресенье, и все добавочные архивы с понедельника по пятницу. Такая стратегия требует меньше времени на резервное копирование, но больше на восстановление.

**Восстановление данных**

Вместе со стратегией архивации вы должны создать и проверить процедуры восстановления данных и убедиться, что соответствующий персонал обладает необходимыми знаниями и навыками. В данной лабораторной работе обсуждаются процессы и параметры, доступные для восстановления данных с помощью программы *Архивация данных.*

**Параметры восстановления**

Windows Server 2012 поддерживает несколько параметров, определяющих ход восстановления файлов. Чтобы их настроить, запустите программу *Архивация данных* и в меню **Сервис** выберите **Параметры:**

* **Не заменять файл на компьютере.** Файлы, которые уже находятся в целевом расположении, пропускаются; этот параметр используется по умолчанию. Например, такой способ восстановления подходит, когда некоторые (но не все) файлы удалены из папки, куда идет восстановление. Тогда отсутствующие файлы будут восстановлены из архива.
* **Заменять файл на компьютере, только если он старее.** Существующие файлы заменяются, только если они старее файлов из набора архивации. Идея в том, что более свежий файл, который находится в целевой папке, может содержать информацию, которую вы не хотите перезаписывать.
* **Всегда заменять файл на компьютере.** Все файлы заменяются версией из архива независимо от даты их последнего изменения. Вы потеряете данные в файлах, которые изменились после архивации. Тем не менее, в целевом размещении останутся все файлы, которых нет в наборе архивации.

**Теневые копии общих папок**

Windows Server 2012 предлагает администраторам и пользователям еще один способ быстрого восстановления поврежденных файлов и папок. Используя VSS, Windows Server 2012 автоматически кэширует копии файлов по мере их изменения. Если пользователь удаляет, перезаписывает или нежелательно изменяет файл, вы можете просто восстановить его предыдущую версию. Тем не менее, эта важная функция не исключает архивацию. Она обеспечивает быстрое восстановление при решении простых, повседневных проблем, но не предназначена для восстановления больших объемов потерянных данных.

**Задания к работе (в методичке под сервер 2008 другое задание)**

1. Создание данных для примера.

Откройте *Блокнот* и введите следующий текст.

md c:\Data

net share data=C:\Data

md c:\Data\Finance

cd c:\data\Finance

echo Historical Financial Data > Historical.txt

echo Current Financials > Current.txt

echo Budget > Budget.txt

echo Financial Projections > Projections.txt

Сохраните файл как «C:\createfiles.bat».

Откройте окно командной строки и исполните команду cd с:\.

Исполните команду createfiles.bat.

В *Проводнике* откройте каталог C:\Data\Finance.

Если столбец Атрибуты не отображается, щелкните заголовки столбцов, например, Изменен правой кнопкой и выберите Атрибуты. Появится столбец с атрибутами файлов.

1. Запустите программу Архивация данных командой Ntbackup.exe, либо в меню Пуск\Программы\Стандартные\Служебные выберите Архивация данных.

Снимите флажок Всегда запускать в режиме мастера.

Щелкните Расширенный режим и перейдите на вкладку Архивация.

Раскройте узел Мой компьютер, диск С:, папку Data, затем щелкните каталог Finance.

В меню Задание выберите Сохранить выделенные.

Сохраните список выбранных файлов под именем Finance Backup.bks.

В поле Носитель архива или имя файла введите c:\backup-normal.bkf.

Щелкните кнопку Архивировать, а затем Дополнительно.

Убедитесь, что в списке Тип архива выбрано Обычный.

Щелкните Затереть данные носителя этим, а затем Архивировать.

Откроется диалоговое окно Ход архивации. После завершения архивации щелкните кнопку Отчет.

Просмотрите отчет. Он не должен содержать ошибок.

Заметьте, что в *Проводнике* столбец Атрибуты теперь не содержит атрибуты архивирования.

1. Разностная архивация

Откройте файл C:\Data\Finance\current.txt и добавьте в него любой текст. Сохраните и закройте файл.

Изучите папку C:\Data\Finance в *Проводнике.* Для каких файлов отображается атрибут архивирования?

Запустите программу *Архивация данных* и перейдите на вкладку Архивация.

В меню Задание выберите Загрузить выделенные, чтобы загрузить список Finance Backup.

В поле Носитель архива или имя файла введите c:\backup-diff-day1.bkf.

Щелкните Архивировать.

Щелкните Дополнительно и выберите тип архива Разностный.

Запустите резервное копирование и убедитесь, что оно выполнилось без ошибок.

Посмотрите на папку в *Проводнике*.Для каких файлов установлен атрибут архивирования?

Откройте файл Budget и внесите какие-либо изменения. Сохраните и закройте файл. Убедитесь, что теперь атрибут архивирования для него установлен.

Повторите вышеописанные шаги, чтобы создать резервную копию c:\backup-diff-day2.bkf. Не забудьте просмотреть отчет архивации. Сколько файлов было скопировано в ходе архивации?

1. Добавочная архивация

Запустите программу *Архивация данных* и перейдите на вкладку Архивация.

В меню Задание выберите Загрузить выделенные, чтобы загрузить список Finance Backup.

В поле Носитель архива или имя файла введите путь c:\backup-inc-day2.bkf.

Щелкните Архивировать.

Щелкните кнопку Дополнительно и выберите тип архива Добавочный.

Запустите резервное копирование и после завершения убедитесь, что оно выполнилось без ошибок.

Посмотрите на папку в *Проводнике*.Для каких файлов установлен атрибут архивирования?

Откройте файл Projections и внесите какие-либо изменения. Сохраните и закройте файл. Для этого файла в *Проводнике* должен появиться атрибут архивирования.

Повторите вышеописанные шаги, чтобы создать резервную копию c:\backup-inc-day3.bkf.

1. Восстановление данных

5.1. Проверка процедур архивации и восстановления

Запустите программу *Архивация данных*.

Перейдите на вкладку Восстановление и управление носителем.

Щелкните знак «+», чтобы раскрыть файл.

Щелкните знак «+», чтобы раскрыть файл Backup-normal.bkf.

Установите флажок, чтобы выбрать диск С:.

Последовательно раскройте узлы С:, Data и Finance. Заметьте: после выбора папки и С: будут отмечены ее вложенные папки и файлы.

В списке Восстановить файлы в выберите Альтернативное размещение.

В поле Альтернативное размещение введите путь C:\TestRestore.

Щелкните Восстановить.

После завершения задания восстановления щелкните кнопку Отчет и изучите журнал операции восстановления.

Откройте папку C:\TestRestore и убедитесь, что структура папки и файлы восстановлены правильно.

Повторите вышеописанные шаги для восстановления файла backup-diff-day2.bkf.

После завершения задания восстановления щелкните кнопку Отчет, чтобы просмотреть журнал операции восстановления. Если вы случайно закрыли окно состояния задания, в меню Сервис щелкните Отчет, выберите последний отчет и щелкните Просмотр.

Изучите отчет по последнему заданию восстановления. Сколько файлов было восстановлено?

Таких файлов нет. Почему? Причина в параметрах восстановления.

В меню Сервис выберите Параметры и перейдите на вкладку Восстановление. Теперь вы можете выявить проблему. По умолчанию программа архивации не заменяет файлы на компьютере. Поэтому при восстановлении из разностного архива файлы, обновленные после обычной архивации, не были перезаписаны.

Выберите Всегда заменять файл на компьютере.

Еще раз восстановите файл backup-diff-day2.bkf. Отчет должен подтверждать восстановление двух файлов.

Итак, вы проверили процедуры архивации и восстановления, научились изменять параметры восстановления. Удалите папку C:\TestRestore.

1. Дополнительные возможности архивации и восстановления

6.1. Составление расписания архивации

Запустите программу *Архивация данных* и перейдите на вкладку Архивация.

В меню Задание загрузите файл выбора Finance Backup.

В поле Носитель архива или имя файла введите путь C:\Backup-Everyday.bkf.

Щелкните Архивировать.

Щелкните Дополнительно и выберите тип архива Добавочный.

Щелкните Расписание.

Назовите задание «Daily Incremental Backup» (Ежедневная добавочная архивация).

Щелкните Свойства. Настройте задание для ежедневного запуска. Настройте время на две минуты вперед, чтобы сразу увидеть результаты этого задания.

Завершите настройку запланированного задания. Вам будет предложено ввести пароль в окне Указание учетной записи.

Откройте диск С: в *Проводнике* и подождите две минуты. Вы увидите, как появится задание архивации.

Запустите программу *Архивация данных*, в меню Сервис выберите Отчет и просмотрите последний журнал архивации, чтобы проверить состояние вашего задания. Количество скопированных файлов может быть равно нулю, если вы не изменяли файлы.

Если задание выполняется неправильно, откройте консоль *Просмотр событий* из группы программ Администрирование. Изучите журнал *Приложение* и определите источник проблемы.

6.2. Запуск программы *Архивация данных* из командной строки

Запустите программу *Архивация данных* и перейдите на вкладку Запланированные задания.

Щелкните значок в календаре, соответствующий запланированному заданию.

Щелкните Свойства.

Выделите команду в поле Выполнить и нажмите Ctrl+C, чтобы ее скопировать.

Откройте окно командной строки.

Щелкните меню окна (значок в левом верхнем углу окна командной строки) и в меню Изменить выберите Вставить. В командную строку будет вставлен вызов Ntbackup со всеми параметрами. Нажмите Enter. Задание архивации будет выполнено.

Сейчас рекомендуется удалить запланированное задание архивации, чтобы было легче работать с дополнительными заданиями архивации, которые вы запланируете далее. Запустите программу *Архивация данных*,перейдите на вкладку Запланированные задания и в календаре щелкните значок, соответствующий запланированному заданию. Щелкните Удалить.

6.3. Включение теневого копирования

Убедитесь, что к папке C:\Data открыт общий доступ и группа *Все* обладает для нее разрешением общего ресурса *Полный доступ*.

Откройте папку Мой компьютер.

Щелкните правой кнопкой диск С: и выберите Свойства.

Перейдите на вкладку Теневые копии.

Выберите том С: и щелкните Включить.

6.4. Имитация изменений сетевых файлов

Откройте папку C:\Data\Finance, а затем файл Current.txt. Измените содержимое файла, сохраните и закройте его.

Удалите файл C:\Data\Finance\Projections.txt.

6.5. Восстановление файлов с помощью вкладки *Предыдущие версии*

Откройте общий ресурс: в меню Пуск выберите Выполнить и исполните команду \\server01\data.

При обращении к общей папке важно использовать UNC, а не локальный путь. Вкладка Предыдущие версии доступна только при подключении к общей папке по сети.

Откройте папку Finance.

Щелкните файл Current.txt правой кнопкой и выберите Свойства.

Перейдите на вкладку Предыдущие версии.

Выберите предыдущую версию файла Current.txt.

Щелкните Копировать, выберите Рабочий стол в качестве целевого размещения и снова щелкните Копировать.

Откройте файл Current.txt на вашем рабочем столе. Вы увидите, что данная его версия не содержит изменений, сделанных в упражнении 6.4.

Вернитесь к папке \\Server01\Data. В этот раз не открывайте папку Finance.

Чтобы восстановить удаленный файл Projections.txt, щелкните папку Finance правой кнопкой и выберите Свойства.

Перейдите на вкладку Предыдущие версии.

Выберите предыдущую версию папки Finance и щелкните Показать.

Щелкните файл Projections.txt правой кнопкой и выберите Копировать.

Перейдите к окну, где отображается текущее состояние папки \\server01\data.

Откройте папку Finance.

Вставьте файл Projections.txt в эту папку. Теперь вы восстановили предыдущую версию файла Projections.txt.

**Содержание отчета**

1. Название работы
2. Цель работы
3. Выполненные задания. Необходимо сопровождать все проделанные действия скриншотами и описаниями к ним.
4. Выводы.

**Контрольные вопросы**

1. Для чего нужна архивация данных?
2. Перечислите типы архивации.
3. Каковы основные стратегии архивации?
4. Перечислите параметры восстановления файлов.
5. Каковы дополнительные возможности архивации и восстановления данных?
6. Для чего необходимо планирование заданий архивации?
7. С какой целью используют теневые копии папок

# Библиографический список

Закер, Крейг. Официальный учебный курс Microsoft: Управление и поддержка среды Microsoft Windows Server 2003 (70-290) / К. Закер; пер. с англ. - М.: ЭКОМ; БИНОМ. Лаборатория знаний, 2006. - 447 с.: ил.

Клейменов, С.А. Администрирование в информационных системах: учеб. пособие для студ. высш. учеб. заведений / С.А. Клейменов, В.П. Мельников, А.М. Петраков; под ред. В.П. Мельникова. - М.: Издательский центр «Академия», 2008. - 272 с.

Коробко, И. В. Администрирование сетей Windows с помощью сценариев / И.В. Коробко. - СПб.: БХВ-Петербург, 2007.

Коробко, И. В. Справочник системного администратора по программированию Windows/ И.В. Коробко. - СПб.: БХВ-Петербург, 2009. - 576 с.: ил.

Макин, Дж. С. Внедрение, управление и поддержка сетевой инфраструктуры Microsoft Windows Server 2003. Учебный курс Microsoft / Дж. С. Макин, Йен Маклин. Пер.с англ. — 2-е изд., испр. - М. : «Русская Редакция»; СПб.: Питер, 2008. - 624 стр.: ил.

Самойленко, А. Виртуальные машины на платформе Microsoft Virtual PC 2007 / А. Самойленко [Электронный ресурс] - Режим доступа: <http://www.windowsfaq.ru/content/view/566>

Семенов, Ю.А. Протокол LDAP (Lightweight Directory Access Protocol) / Ю.А. Семенов [Электронный ресурс] - Режим доступа: http://book.itep.ru/4/45/ldap.htm

Хенриксон, Х. IIS 6.0. Полное руководство. Справочник профессионала. /Х. Хенриксон, С. Хофман. Пер. с англ., - М.: Издательство «СП ЭКОМ», 2004. - 672 с.: ил.

Холме, Дэн. Управление и поддержка Microsoft Windows Server 2003. Учебный курс MCSA/MCSE / Холме Дэн, Томас Орин. Пер. с англ. — М.: Издательско-торговый дом «Русская Редакция», 2008. — 448 стр.: ил.

Чекмарев, А. Н. Microsoft Windows Server 2003. Русская версия / Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Под общ. ред. А.Н. Чекмарева. - СПб.: БХВ-Петербург, 2008. - 1120 с.: ил.