

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО  
ОБРАЗОВАНИЯ «БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»  
(БГТУ им. В.Г.Шухова)**

Лабораторная работа №3  
дисциплина «Администрирование распределенных вычислительных сетей»  
по теме «Использование средств инструментария для управления Windows  
(WMI) в администрировании»

Выполнил: студент группы ВТ-41  
Проверил:

Макаров Д.С.  
Федотов Е.А.

Белгород 2020

# Лабораторная работа №3

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

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

### Ход работы

1. Просмотр набора классов в репозитории WMI.

Через меню “Выполнить” была вызвана команда wbemtest

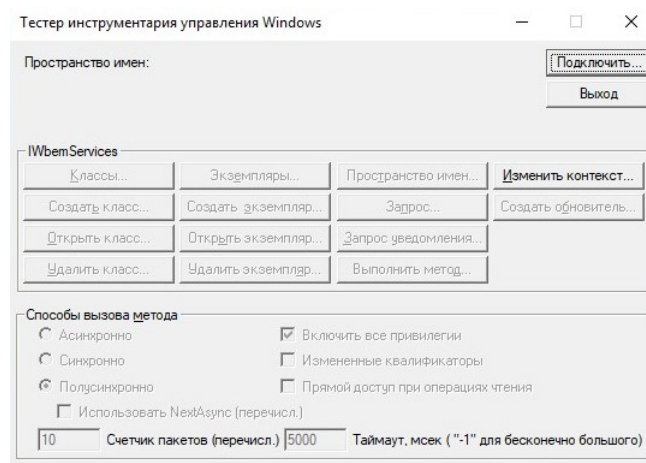


Рис. 1: Окно wbemtest

В списке всех классов WMI был найден класс Win32\_NTDomain и получен список всех его экземпляров.

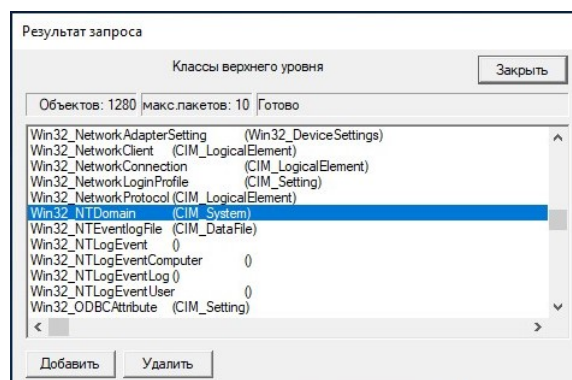


Рис. 2: Список классов

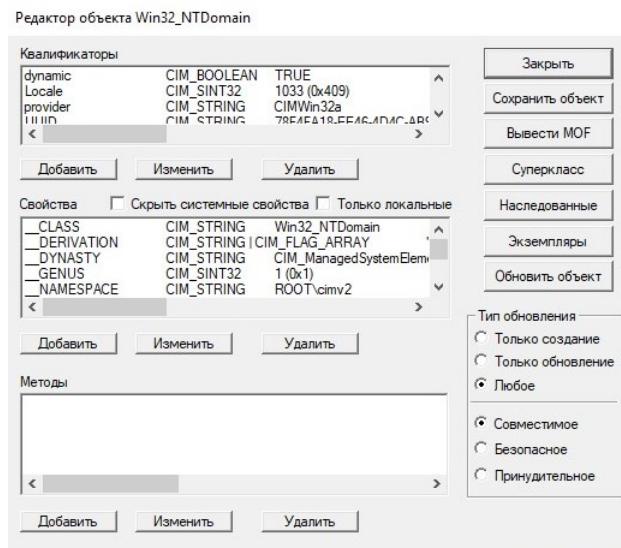


Рис. 3: Редактор объекта Win32\_NTDomain

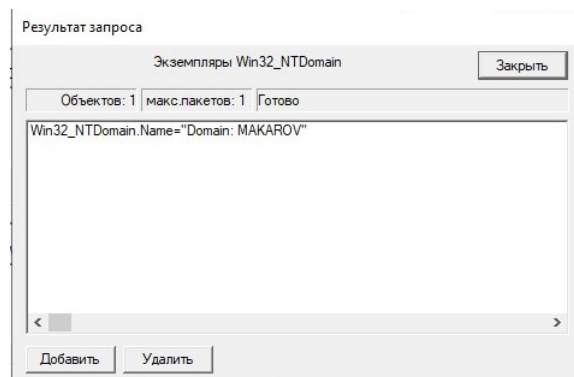


Рис. 4: Экземпляры класса Win32\_NTDomain

В окне списка соединителей был получен список групп домена и найдена группа "Sales Representative".

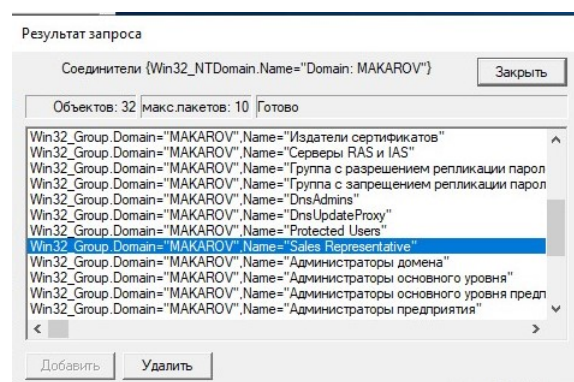


Рис. 5: Список групп

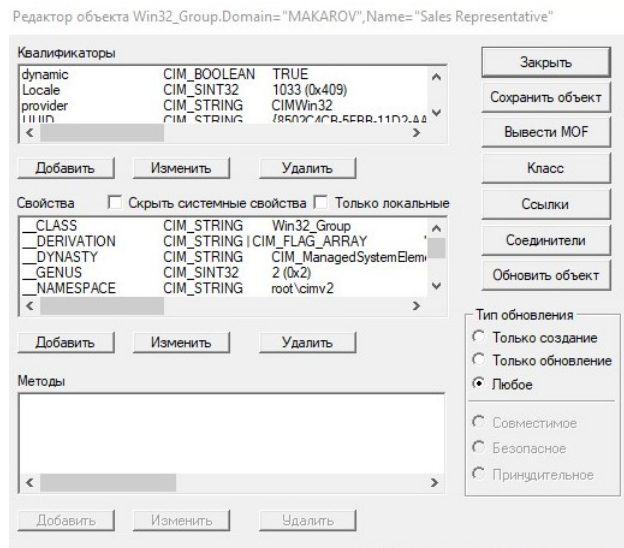


Рис. 6: Окно группы “Sales Representative”

В экземплярах класса учетных записей были найдены указанные пользователи, в атрибут *Disabled* установлены требуемые значения.

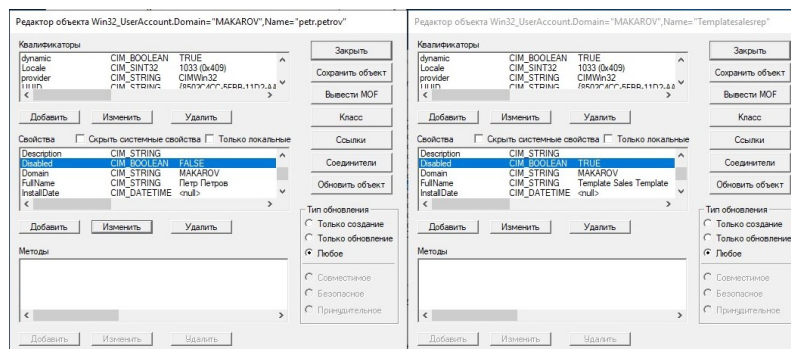


Рис. 7: Окна объектов пользователей

2. Был найден класс Win32\_UserAccount.

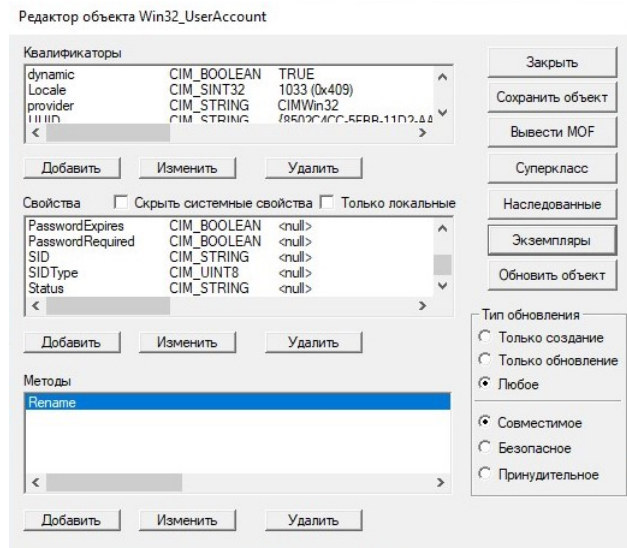


Рис. 8: Объект Win32\_UserAccount

В списке экземпляров класса был найден объект “petr.petrov”

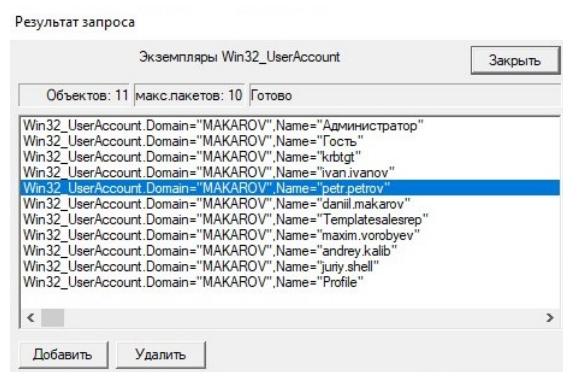


Рис. 9: Список экземпляров класса

В окне вызова метода был выбран метод Rename объекта “petr.petrov”, и установлены требуемые параметры.

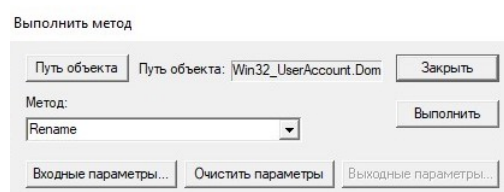


Рис. 10: Окно вызова метода

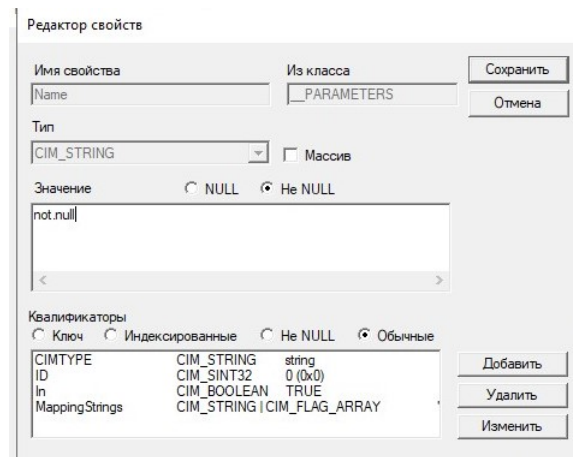


Рис. 11: Окно изменения аргументов метода

Метод был успешно выполнен но изменения не были внесены в поля объекта.

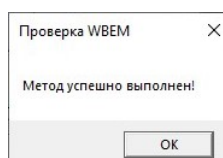


Рис. 12: Сообщение об успехе выполнения метода

### 3. Запросы WSL

В окне запросы, был выполнен WQL запрос

```
select * from Win32_UserInDomain
```

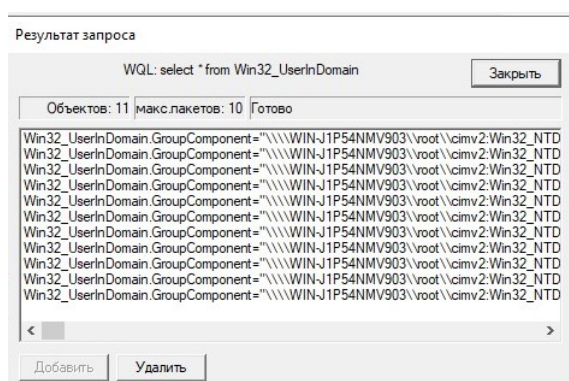


Рис. 13: Результат выполнения запроса

Запрос выводящий пользователей группы “Sales Representative”.

```
select * from Win32_GroupUser where
    GroupComponent = '
        Win32_Group.Domain    = "makarov",
        Name                   = "Sales Representative"
    ,
```

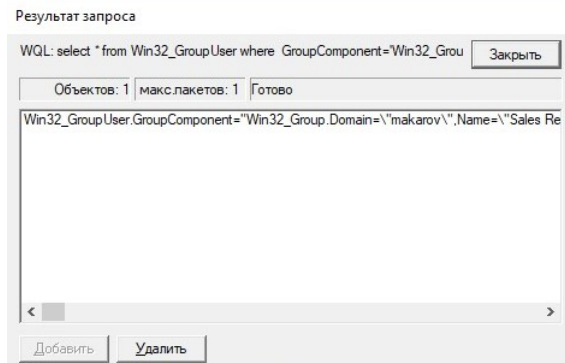


Рис. 14: Результат выполнения запроса

Запрос перечисляющие логические диски:.

```
select * from Win32_LogicalDisk
```

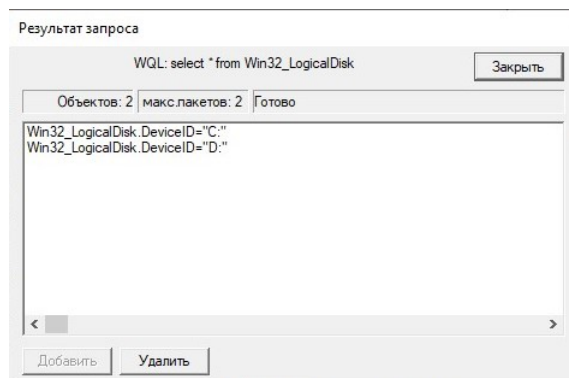


Рис. 15: Результат выполнения запроса

Запрос перечисляющие процессоры:.

```
select * from Win32_PerfRawData_PerfOS_Processor
```



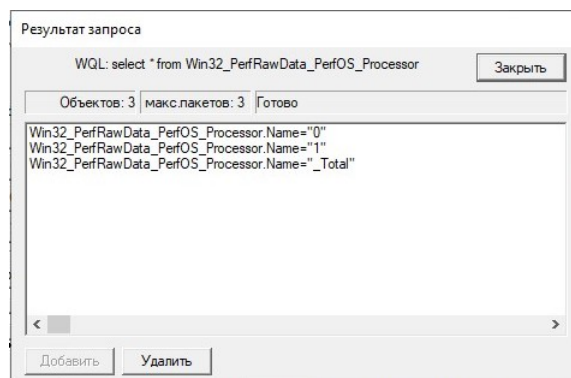


Рис. 16: Результат выполнения запроса

#### 4. Утилита wmic

Была запущена консоль powershell и в ней запущена консоль wmi. При просмотре списка команд, было указано что инструмент WMI является устаревшим и больше не поддерживается.

```
PS C:\Users\Администратор> wmic /?
Программа WMI устарела.

[глобальные параметры] <команда>

Имеются следующие глобальные параметры:
/namespace      Путь к пространству имен, с которым оперирует псевдоним.
/role            Путь к роли, содержащей определения псевдонимов.
/node           Серверы, с которыми будет работать псевдоним.
/implement       Уровень олицетворения для клиента.
/authlevel       Уровень проверки подлинности для клиента.
/locale          Код языка, который должен использовать клиент.
/privileges       Включает или исключает все привилегии.
/trace           Выводит отладочные данные в stderr.
/record          Записывает все вводимые команды и их выходные данные.
/interactive     Устанавливает или переустанавливает интерактивный режим.
/failfast        Устанавливает или переустанавливает режим failfast.
/user           Имя пользователя для сеанса.
/password       Пароль для входа в сеанс.
/output          Задаёт режим перенаправления выходных данных.
/append         Задаёт режим перенаправления выходных данных.
/aggregate       Устанавливает или переустанавливает режим совместного вывода.
/authority       Задаёт <тип полномочий> для подключения.
/?[<-BRIEF|FULL>] Сведения об использовании.

Для получения дополнительных сведений о конкретном глобальном параметре введите: <имя_параметра> /?

Для текущей роли доступны следующие псевдонимы:
ALIAS            - Доступ к псевдонимам, доступным на локальном компьютере
BASEBOARD        - Управление системной платой.
BIOS             - Управление BIOS.
BOOTCONFIG       - Управление конфигурацией загрузки.
CDROM            - Управление устройствами чтения компакт-дисков.
COMPUTERSYSTEM   - Управление компьютером.
CPU              - Управление ЦП.
CSPRODUCT        - Сведения о системе из SMBIOS.
DATAFILE         - Управление файлами данных.
DCOMAPP          - Управление приложениями DCOM.
DESKTOP          - Управление рабочим столом.
DESKTOPMONITOR   - Управление системой мониторинга рабочего стола.
DEVICEMEMORYADDRESS - Управление адресами памяти устройства.
DISKDRIVE        - Управление физическими дисками.
DISKQUOTA        - Использование дискового пространства для томов NTFS.
DMACHANNEL       - Управление каналами прямого доступа к памяти (DMA).
ENVIRONMENT      - Управление настройками системной среды.
FSDR             - Управление оглавлением файловой системы.
GROUP            - Управление учетными записями групп.
IDECONTROLLER    - Управление IDE-контроллерами.
IRQ              - Управление линиями запросов прерывания.
JOB              - Доступ к заданиям, запланированным с помощью службы расписания.
LOADORDER        - Управление системными службами, задающими зависимости при выполнении.
LOGICALDISK      - Управление локальными запоминающими устройствами.
LOGON            - Сеансы входа в систему.
MEMCACHE         - Управление кэш-памятью.
MEMORYCHIP       - Информация о микросхемах памяти.
MEMPHYSICAL      - Управление физической памятью компьютерной системы.
NETCLIENT        - Управление сетевыми клиентами.
NETLOGIN         - Управление данными входа в систему конкретных пользователей.
NETPROTOCOL      - Управление протоколами (и их сетевыми характеристиками).
NETUSE           - Управление активными сетевыми соединениями.
NIC              - Управление адаптерами сетевого интерфейса.
NICCONFIG        - Управление сетевыми адаптерами.
NTDOMAIN         - Управление доменами NT.
```

Рис. 17: Список команд WMI

Используя команду `wmic group where domain="makarov"` был выведен список всех групп домена.



```

Администратор: Windows PowerShell

Неверный формат IP-адреса. Требуется
развернутый формат, например, 11.11.12.13
Было введено "localhost"
PS C:\Users\Администратор> nbtstat -A 192.168.1.198

Ethernet:
Адрес IP узла: [192.168.1.198] Код области: []

Узел не найден.
PS C:\Users\Администратор>
PS C:\Users\Администратор> wmic
wmic:root\cli>
"/?" для вызова справки, QUIT для выхода.
wmic:root\cli>
"/?" для вызова справки, QUIT для выхода.
wmic:root\cli>group where domain="makarov"

Caption Description
makarov\Издатели сертификатов Члены этой группы могут публиковать сертификаты
makarov\Серверы RAS и IAS Серверы в этой группе могут полу
makarov\Группа с разрешением репликации паролей RODC Пароли членов данной группы могут реплицироваться на все ко
makarov\Группа с запретом репликации паролей RODC Пароли членов данной группы не могут реплицироваться на кон
makarov\Dsadmins Группа администраторов D
makarov\DnsUpdateProxy DNS-клиенты, которые раз
makarov\Protected Users Участниками этой группы о
makarov\Sales Representative Назначенные администраторы домена
makarov\Администраторы домена Члены этой группы могут выполнять административные де
makarov\Администраторы основного уровня Члены этой группы могут выполнять административные действия с ос
makarov\Администраторы предприятия Назначенные администраторы предприятия
makarov\Администраторы схемы Назначенные администраторы схемы
makarov\Владельцы-создатели групповой политики Члены этой группы могут изменять групповую политику для до
makarov\Гости домена Все гости домена
makarov\Клонируемые контроллеры домена Члены этой группы, являющиеся контроллерами домена,
makarov\Компьютеры домена Все рабочие станции и серверы, присоедин
makarov\Контроллеры домена Все контроллеры домена в домене
makarov\Контроллеры домена - только чтение Члены этой группы являются контроллерами доменов тольк
makarov\Контроллеры домена предприятия - только чтение Члены этой группы являются контроллерами доменов только для чте
makarov\Пользователи домена Все пользователи домена

```

Рис. 18: Результат работы команды

Используя команду `wmic group where domain="makarov"` был выведен список всех пользователей домена.

```

wmic:root\cli>where domain="makarov" list brief
where - псевдоним не найден.
wmic:root\cli>useraccountwhere domain="makarov" list brief
useraccountwhere - псевдоним не найден.
wmic:root\cli>useraccount where domain="makarov" list brief
AccountType Caption Domain FullName Name Name SID
512 MAKAROV\Администратор MAKAROV Администратор S-1-5-21-1205631921-172171058
512 MAKAROV\Гость MAKAROV Гость S-1-5-21-1205
512 MAKAROV\krbtgt MAKAROV krbtgt S-1
512 MAKAROV\ivan.ivanov MAKAROV Иван Иванов ivan.ivanov S-1-5-21-1205
512 MAKAROV\not_null MAKAROV Петр Петров not_null S-1-5-21-1205
512 MAKAROV\daniil.makarov MAKAROV Даниил Макаров daniil.makarov S-1-5-21-1205631
512 MAKAROV\Templatesalesrep MAKAROV Template Sales Template Templatesalesrep S-1
512 MAKAROV\maxim.vorobyev MAKAROV Максим Воробьев maxim.vorobyev S-1-5-21-12056319
512 MAKAROV\andrey.kalib MAKAROV andrey.kalib S-1
512 MAKAROV\juri.shell MAKAROV juri.shell S-1
512 MAKAROV\Profile MAKAROV Profile Account Profile S-1

```

Рис. 19: Результат работы команды

```

wmic:root\cli>group /?

GROUP - Управление учетными записями групп.

COBET. BNF при работе с псевдонимом.
(<псевдоним> [объект WMI] | <псевдоним> [<путь_WHERE>] | [<псевдоним> [<путь_WHERE>] [<предложение_команды>].

Использование:

GROUP ASSOC [<указатель_формата>]
GROUP CALL <имя_метода> [<список_фактических_параметров>]
GROUP CREATE <список_значений>
GROUP DELETE
GROUP GET [<список_свойств>] [<параметры_GET>]
GROUP LIST [<формат_LIST>] [<параметры_LIST>]

wmic:root\cli>
"/?" для вызова справки, QUIT для выхода.
wmic:root\cli>useraccount /?

USERACCOUNT - Управление учетными записями пользователей.

COBET. BNF при работе с псевдонимом.
(<псевдоним> [объект WMI] | <псевдоним> [<путь_WHERE>] | [<псевдоним> [<путь_WHERE>] [<предложение_команды>].

Использование:

USERACCOUNT ASSOC [<указатель_формата>]
USERACCOUNT CALL <имя_метода> [<список_фактических_параметров>]
USERACCOUNT CREATE <список_значений>
USERACCOUNT DELETE
USERACCOUNT GET [<список_свойств>] [<параметры_GET>]
USERACCOUNT LIST [<формат_LIST>] [<параметры_LIST>]
USERACCOUNT SET [<список_значений>]

```

Рис. 20: Список команд для group и useraccount

## 5. Сценарии с использованием WMI

Был создан сценарий с указанным исходным кодом

```

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="makarov" 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

```

Сценарий был исполнен при помощи консольной утилиты **cscript**.

Рис. 21: Результат работы сценария

## Вывод

В ходе выполнения данной лабораторной я ознакомился с утилитами использующими WMI, для взаимодействия с объектами домена. Так же я ознакомился с языком запросов WQL позволяющим, создавать SQL-подобные запросы, где вместо строк из таблиц с данными запрос возвращает объекты домена.

## Контрольные вопросы

1. Что такое WMI? Для чего она используется?

WMI – Windows Management Instrumentation, он же инструментарий для управления Windows. Представляет из себя набор интерфейсов для управления операционной системой через специальные компоненты, причем как локально, так и по сети. Позволяет использовать различные скриптовые языки для упрощения управления объектами Active Directory.

2. Перечислите средства работы с WMI для администратора.

- mofcomp.exe
- winmgmt.exe
- wmingmt.msc
- wbemtest.exe
- wmic.exe

### 3. Общая структура WMI.

Архитектура WMI состоит из 3 частей:

- ядро WMI (WMI infrastructure) - связующее звено архитектуры WMI, отвечающее за связность компонентов.
- управляющие программы (management applications)- потребителями сервисов WMI.
- управляемые объекты/ресурсы (managed resources) — любые логические или физические компоненты информационной системы, доступ к которым может быть получен с помощью WMI.

### 4. Опишите возможности программы WMIC.

Инструментарий WMI. Используется для получения сведений об оборудовании и системе, управления процессами и их компонентами, а также изменения настроек с использованием возможностей инструментария управления Windows.

### 5. Опишите возможности программы WBEMTEST.

Утилита предоставляющая графический интерфейс для доступа к ресурсам WMI, позволяющая получить списки классов, экземпляров классов, связи между ними, а так же выполнять методы классов и WQL запросы.

### 6. Использование WQL-запросов.

WQL запросы используют синтаксис SQL запросов, за исключением того что вместо связанных таблиц с данными выборка производится по классам домена, и вместо строк таблиц возвращаются объекты домена.