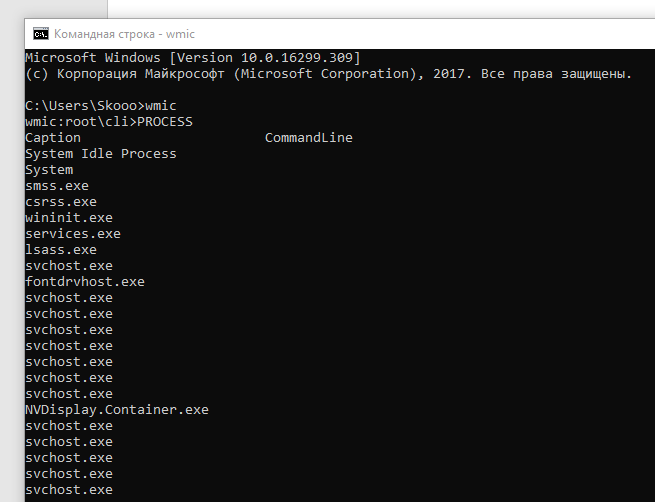
**Лабораторная работа 14**

**Доступ к WMI из командной строки. Командная оболочка WMIC**

**Запуск WMIC. Использование встроенной справки**

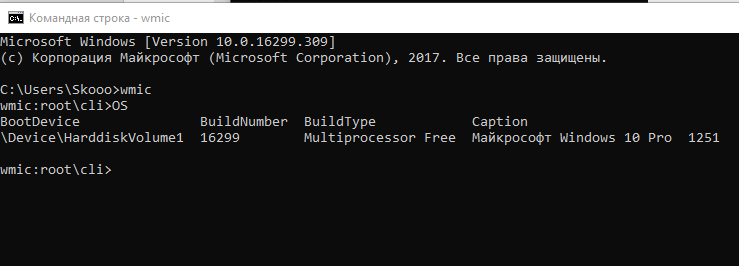
Для запуска WMIC в интерактивном режиме необходимо выполнить команду wmic в стандартном интерпретаторе команд cmd.exe или в диалоговом окне Выполнить (Run) в меню Пуск (Start). После этого на экран выводится стандартное приглашение WMIC, wmic:root\cli>.

После этого можно вводить с клавиатуры команды WMIC (регистр символов значения не имеет), которые запускаются после нажатия клавиши <Enter>. Например, если набрать в командной строке WMIC слово PROCESS и нажать <Enter>, то на экран выведется список всех процессов, запущенных в данный момент в системе:



Если же ввести в командной строке WMIC слово OS, то мы увидим на экране свойства операционной системы, установленной на компьютере:

wmic:root\cli>OS



Выполнив теперь команду PROCESS CALL /?, мы получим краткое описание методов, которые могут быть вызваны при работе с процессами:

wmic:root\cli>PROCESS CALL /?

Вызов методов.

Использование:

CALL <имя метода> [<список фактических параметров>]

ЗАМЕЧАНИЕ. <список фактических параметров> ::= <факт. парам.> |

<факт. парам.>, <

Для псевдонима доступны следующие команды и методы:

Вызов [ Ввод/Вывод ]Параметры и тип Состояние

==== ===================== ======

AttachDebugger (null)

Create [UNKNOWN]CommandLine(STRING) (null)

[UNKNOWN]CurrentDirectory(STRING)

[UNKNOWN]ProcessStartupInformation(OBJECT)

[UNKNOWN]ProcessId(UINT32)

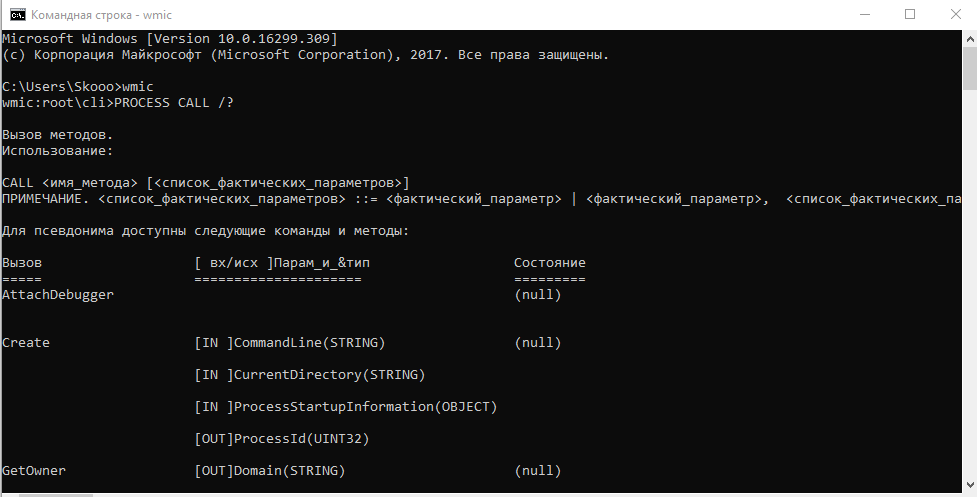
GetOwner [UNKNOWN]Domain(STRING) (null)

[UNKNOWN]User(STRING)

GetOwnerSid [UNKNOWN]Sid(STRING) (null)

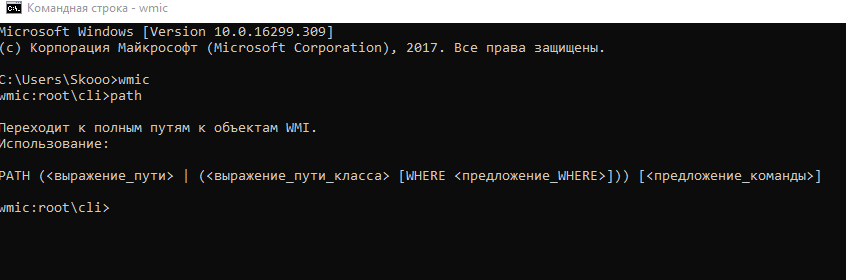
SetPriority [IN ]Priority(SINT32) (null)

Terminate [UNKNOWN]Reason(UINT32) (null)



**Команда PATH**

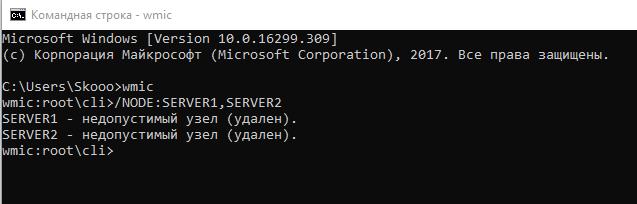
Команда PATH применяется для прямого доступа к одному или нескольким экземплярам классов WMI, без указания псевдонимов WMIC. Команда PATH особенно полезна, если для нужного класса WMI не существует псевдонима WMIC.



**Параметр /NODE**

В параметр /NODE записываются разделяемые запятыми имена компьютеров, к которым будет обращаться WMIC при поиске классов WMI, соответсвующих вводимым в командной строке псевдонимам. Например:

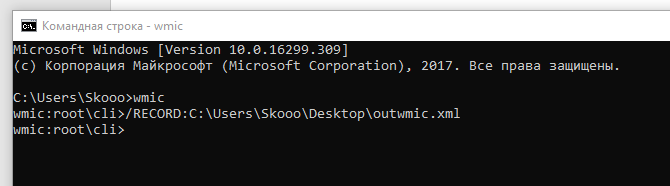
/NODE:SERVER1,SERVER2

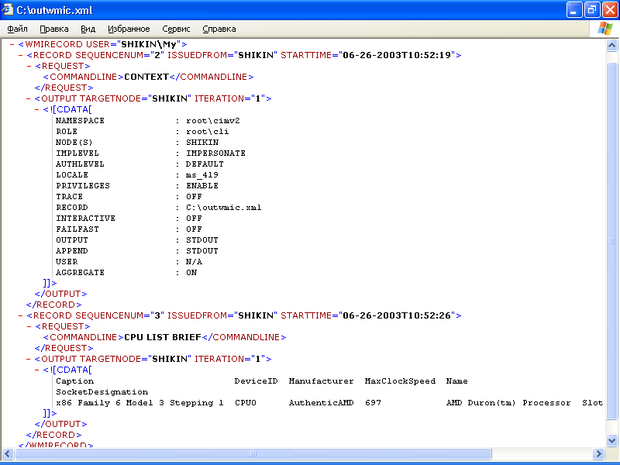


**Параметр /RECORD**

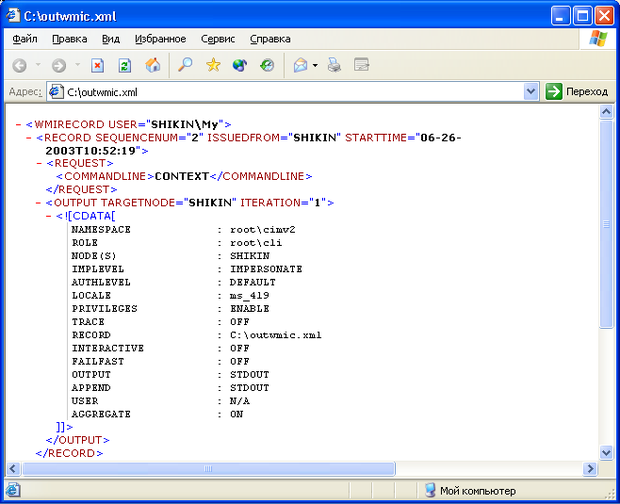
С помощью параметра /RECORD можно сохранять во внешнем XML-файле историю запускаемых в текущей сессии WMIC команд и результаты их выполнения. Для включения режима записи команд нужно указать в качестве значения параметра /RECORD имя выходного XML-файла, например:

/RECORD: C:\Users\Skooo\Desktop\outwmic.xml





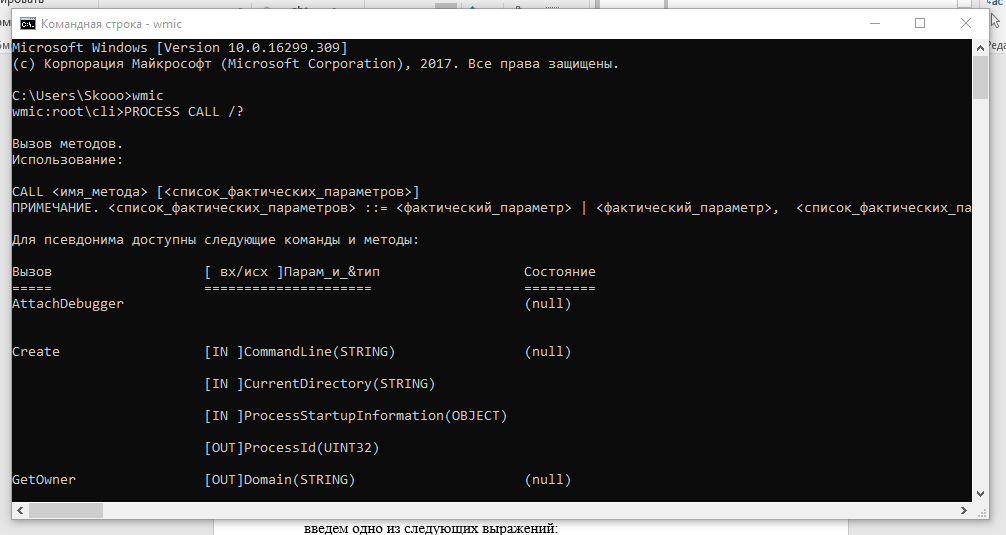
**Рис. 14.2.** Содержимое выходного XML-файла при включенном режиме записи команд



**Оператор CALL**

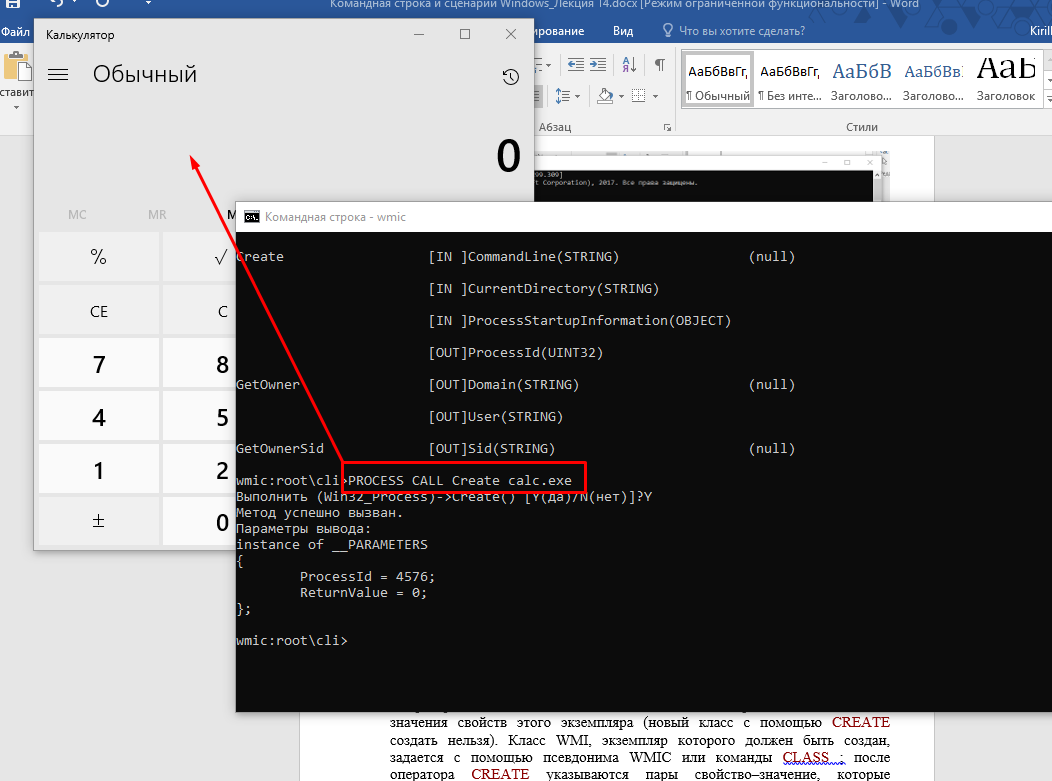
PROCESS CALL /?

CLASS Win32\_Process CALL /?



необходимо выполнить следующую команду:

PROCESS CALL Create calc.exe



Для того чтобы закрыть запущенный калькулятор, нужно вызвать метод Terminate:

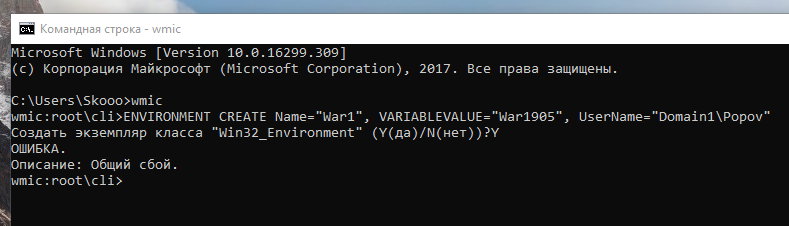
PROCESS WHERE Name="calc.exe" CALL Terminate

* калькулятор закрывается

**Оператор CREATE**

Например, для создания переменной War1 со значением War1905 для пользователя Popov из домена Domain1, нужно выполнить следующую команду:

ENVIRONMENT CREATE Name="War1", VARIABLEVALUE="War1905", UserName="Domain1\Popov"



**Оператор GET**

Оператор GET позволяет получить значения определенных свойств экземпляров классов WMI, которые могут задаваться с помощью псевдонимов WMIC или команды PATH.

Если же, используя команду CLASS, применить оператор GET к классу WMI, то мы получим описание этого класса. Например, после выполнения команды /OUTPUT:C:\1.htm CLASS Win32\_Process GET в файле 1.htm сформируется описание класса Win32\_Process.

Для того чтобы вывести на экран несколько свойств экземпляров класса, нужно указать имена этих свойств, разделенные запятыми, после оператора GET. Например: PROCESS GET Name, Handle.

Если ввести оператор GET без указания списка свойств, то будут выведены все свойства псевдонима.

Как уже отмечалось выше, одной из особенностей архитектуры WMIC является то, что XML-формат выходных данных может быть довольно легко изменен с помощью соответствующих таблиц стилей XSL. В операторе GET для этой цели служит параметр /FORMAT, в качестве значения которого указывается либо стандартное или определенное пользователем ключевое слово, задающее формат выходной информации, либо имя XSL-файла, с помощью которого будет происходить обработка выходных XML-данных. Стандартным ключевым словам (значениям параметра /FORMAT ) соответствуют XSL-файлы, которые расположены в каталоге %SystemRoot%\System32\Wbem; данное соответствие устанавливается в файле xsl-mapping.xml, который находится в том же каталоге (листинг 14.1).

<XSLMAPPINGS>

<XSLFORMAT KEYWORD="TABLE">WmiCliTableFormat.xsl</XSLFORMAT>

<XSLFORMAT KEYWORD="VALUE">WmiCliValueFormat.xsl</XSLFORMAT>

<XSLFORMAT KEYWORD="MOF">WmiCliMofFormat.xsl</XSLFORMAT>

<XSLFORMAT KEYWORD="LIST">WmiCliValueFormat.xsl</XSLFORMAT>

<XSLFORMAT KEYWORD="TVLIST">TextValueList.xsl</XSLFORMAT>

</XSLMAPPINGS>

Листинг 14.1. Стандартный файл xsl-mapping.xml

