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 систем»

тема: «Использование средств инструментария для управления

Windows (WMI) в администрировании»

Выполнил: студент группы ВТ-41

Ковалёв И. Д.

Проверил:

Федотов Е. А.

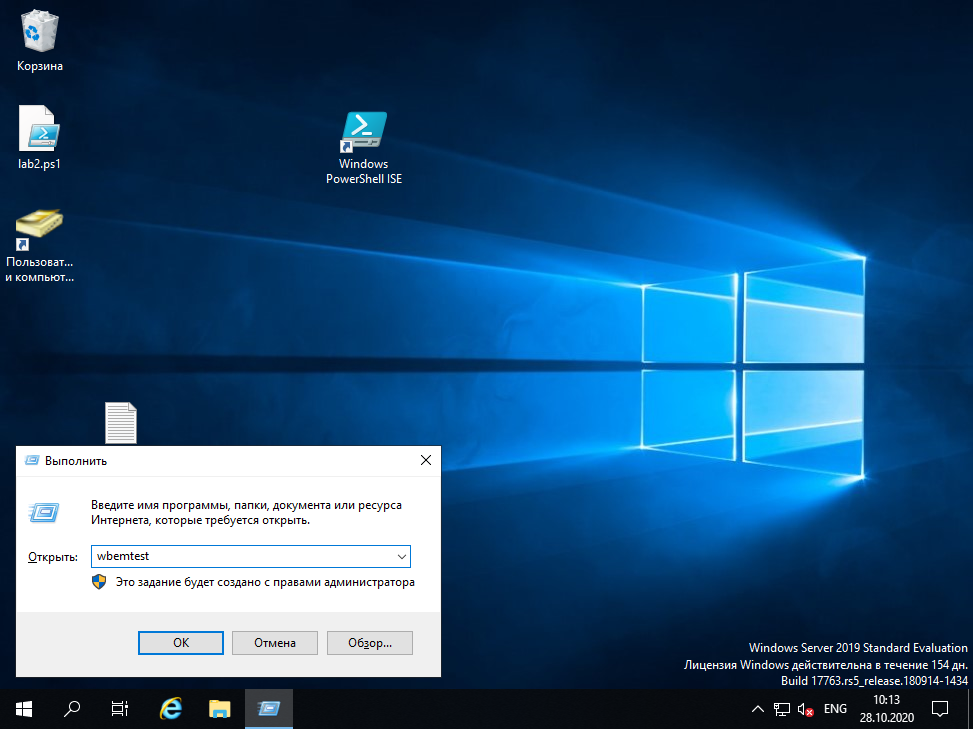
Белгород 2020

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

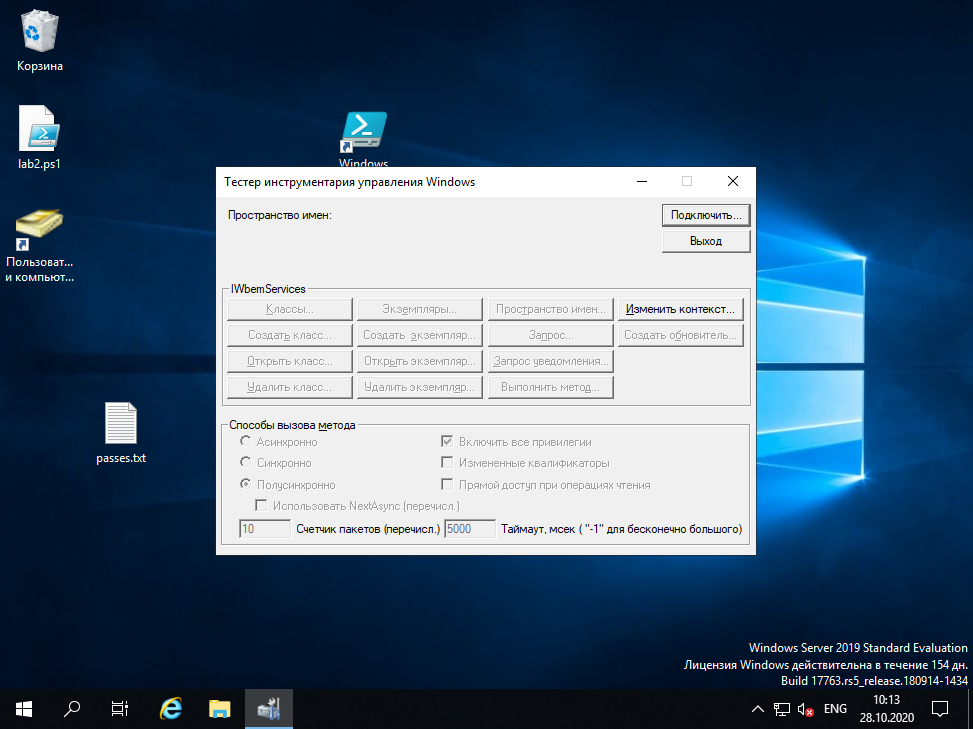
**Задания к работе:**

**1. Просмотр набора классов в репозитории WMI.**

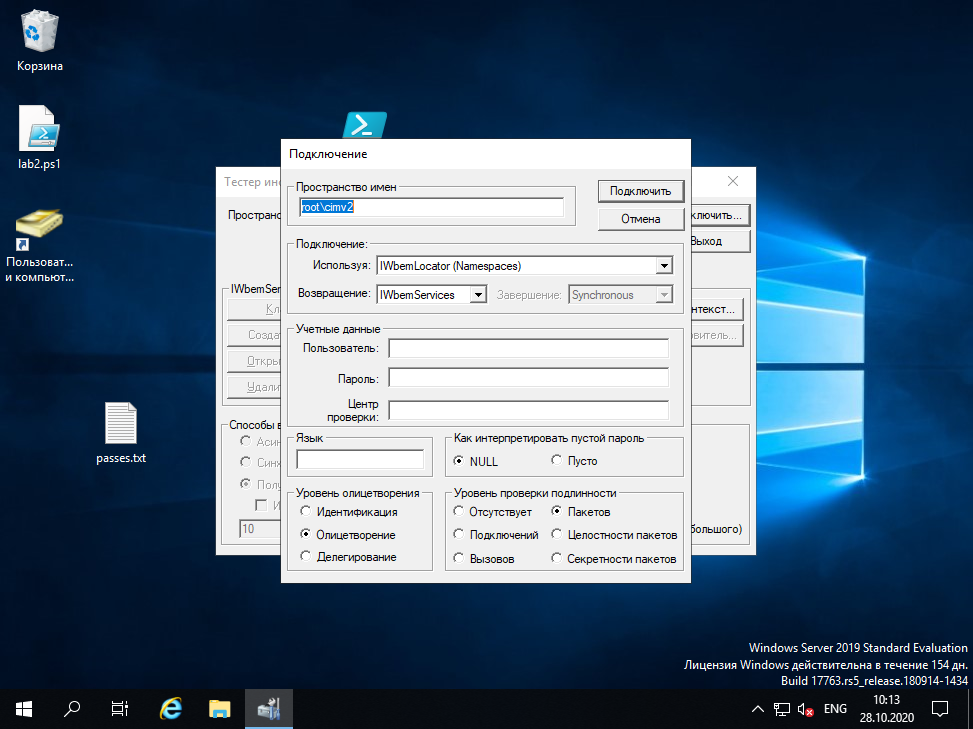
Щелкните Пуск\Выполнить, введите wbemtest.



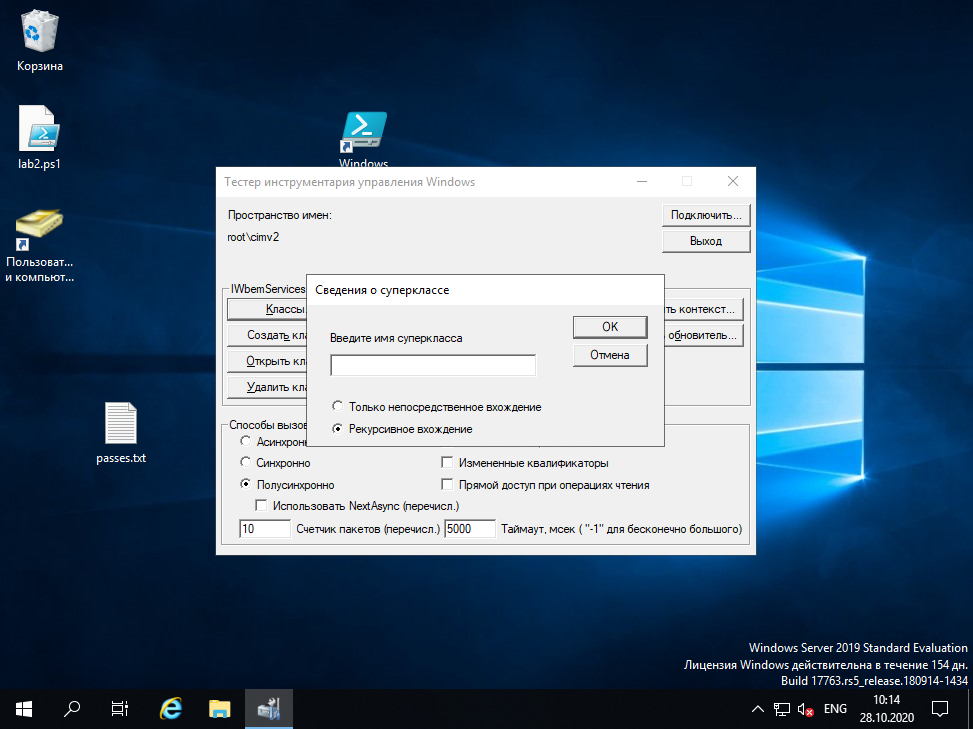
Установите флажок «Включить все привилегии». Нажмите Подключить.



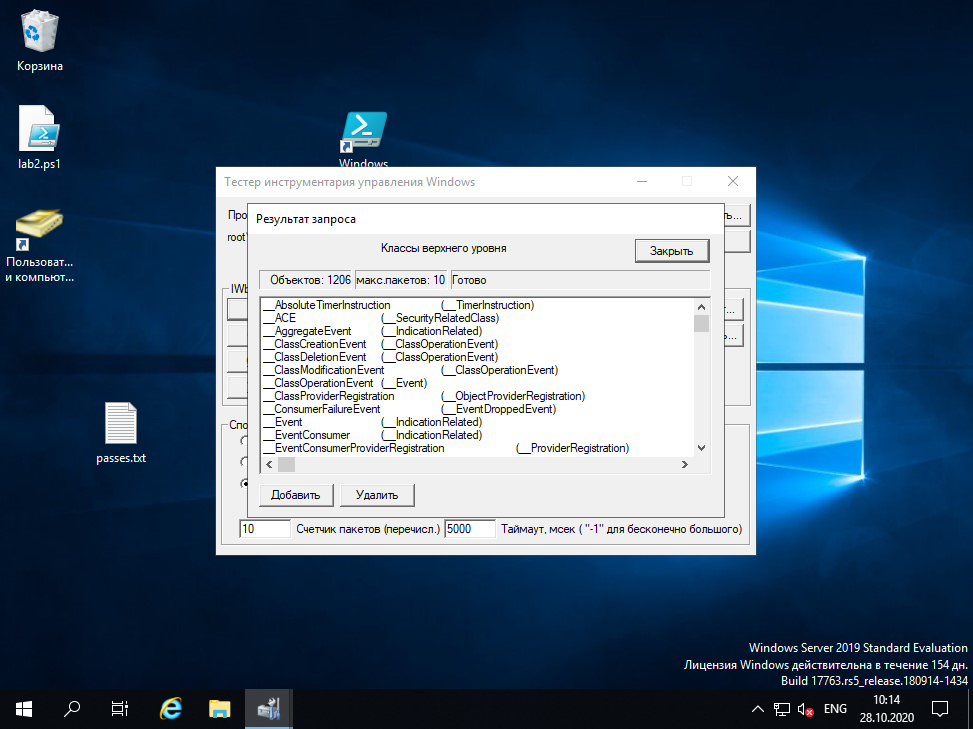
В окне подключения введите в поле Пространство имен \\Server01\root\cimv2 и нажмите Подключить.



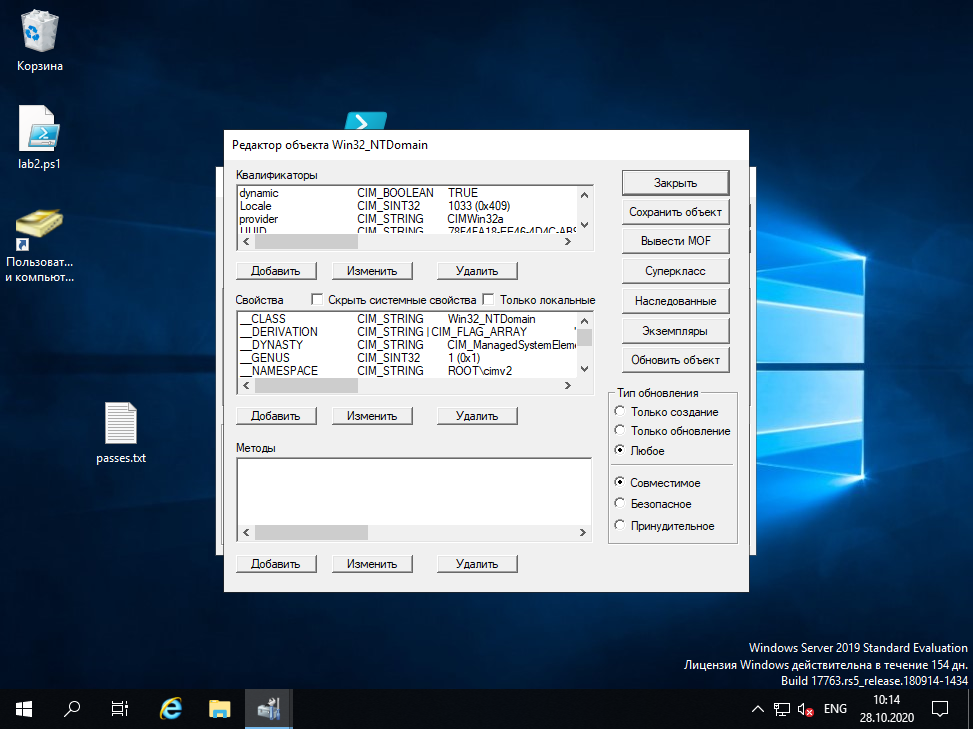
Затем нажмите кнопку «Классы...», выберите «Рекурсивно», не заполняйте поле суперкласса и нажмите «Ok».



В результате вы получите список классов, определенный в вашем репозитории WMI, в пространстве имен CIMv2.

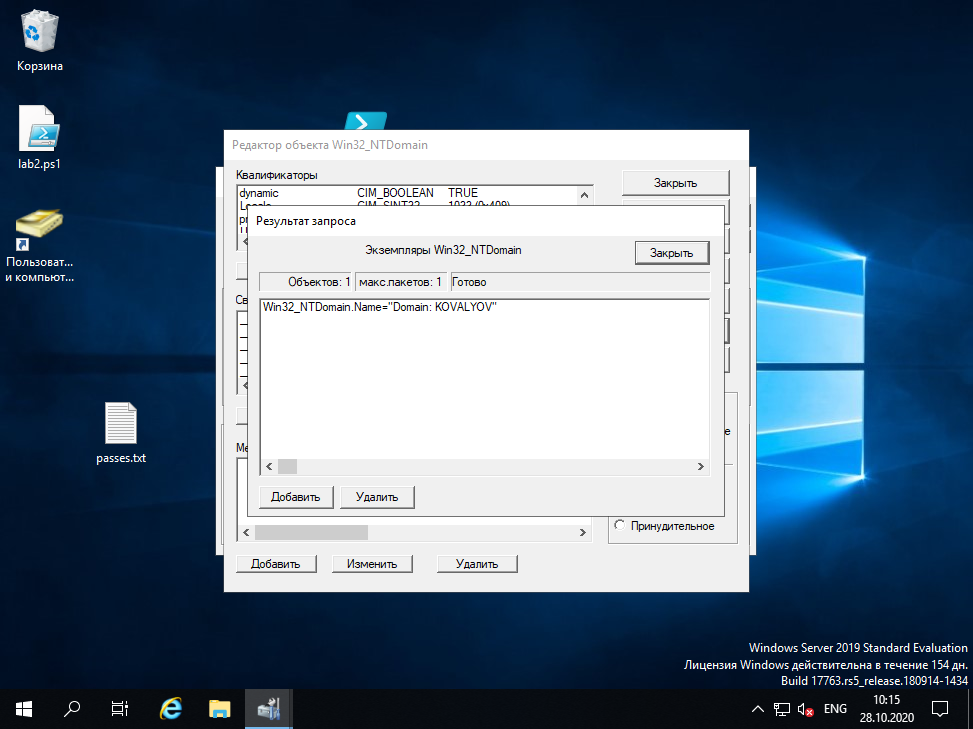


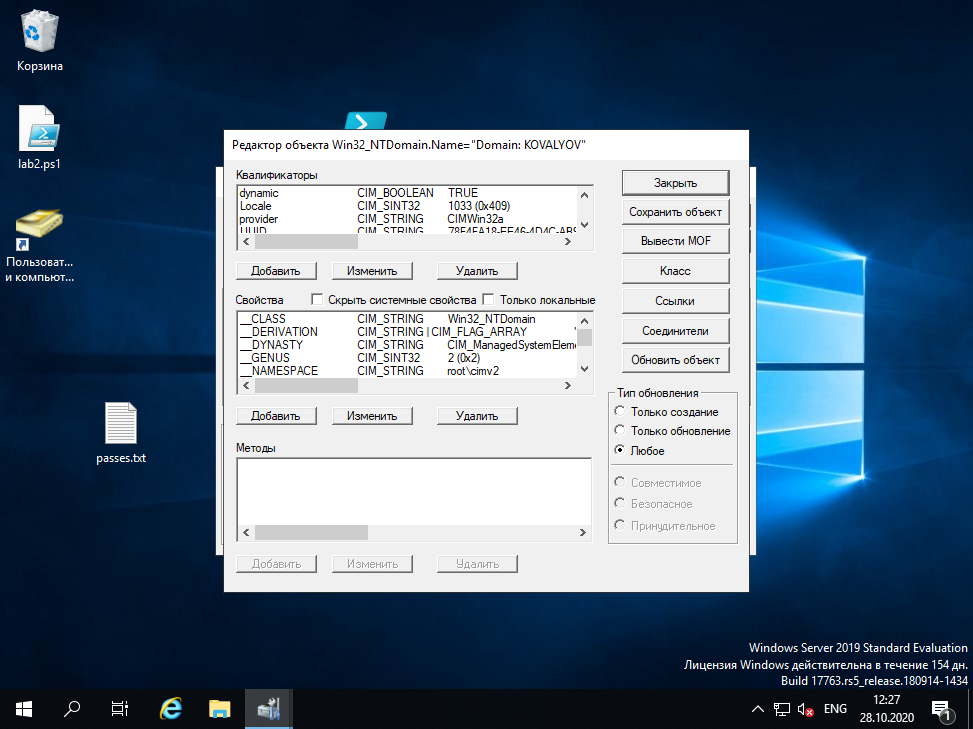
Найдите класс Win32\_NTDomain и щелкните на нем дважды левой кнопкой мыши.



В открывшемся окне редактора нажмите кнопку Экземпляры, чтобы увидеть список экземпляров. Найдите свой домен и зайдите в окно свойств для данного

экземпляра.



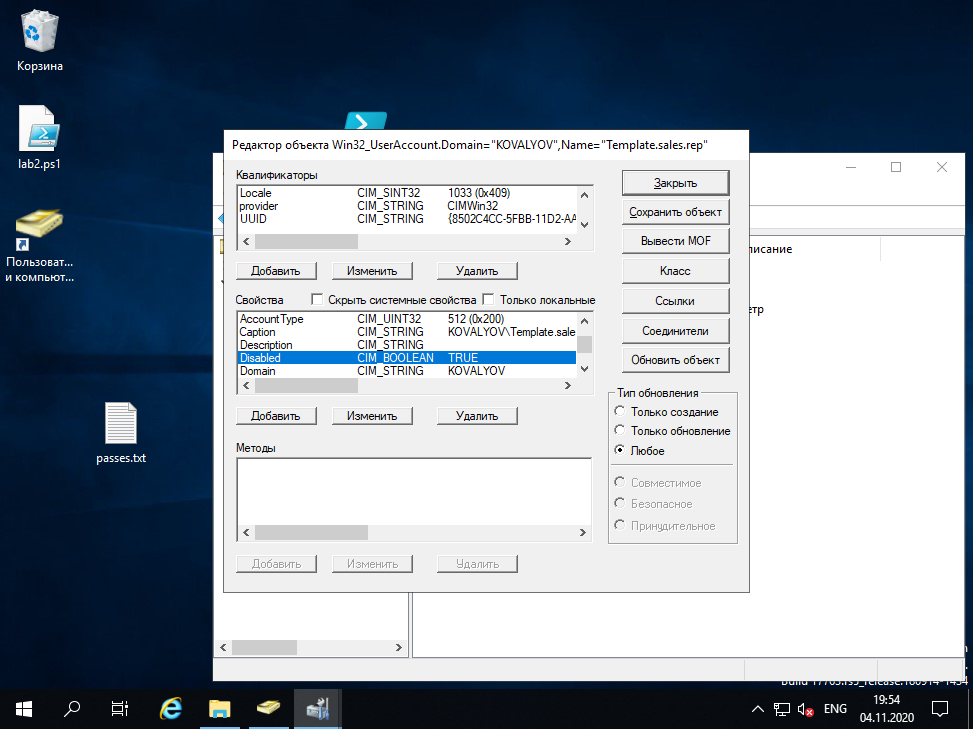


Нажмите кнопку Соединители. Используя утилиту wbemtest, получите список экземпляров групп домена.

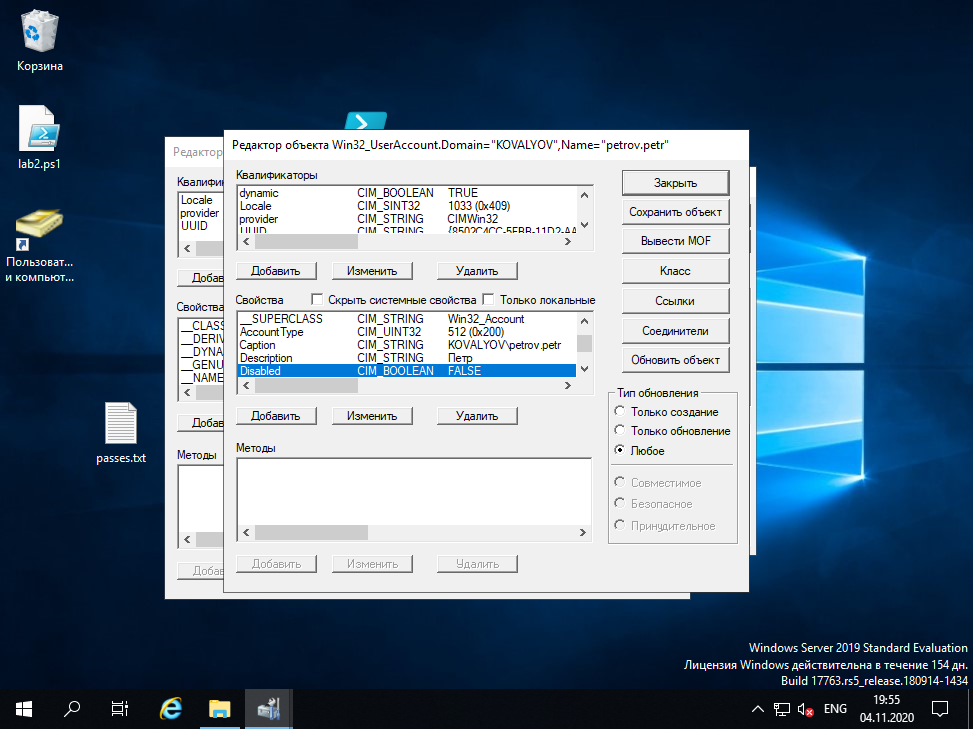


Найдите в экземплярах класса учетных записей пользователей Templatesalesrep и petr.petrov. Убедитесь, что свойство Disabled у первого установлено в True, а у второго – в False. Измените значение Disabled у petr.petrov.

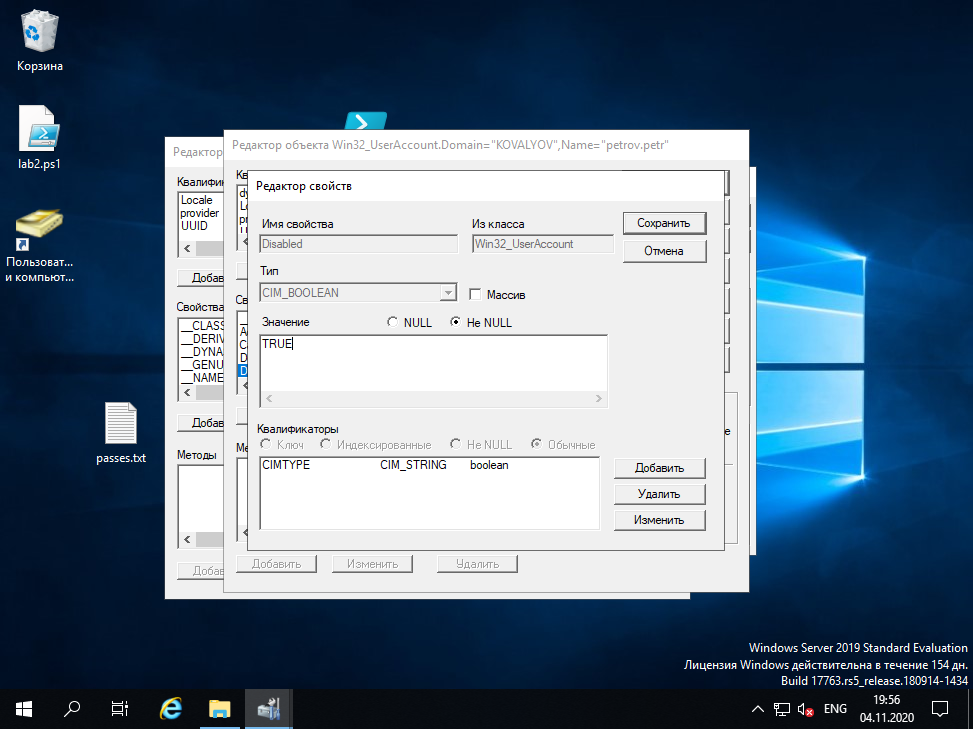
Template.sales.rep:



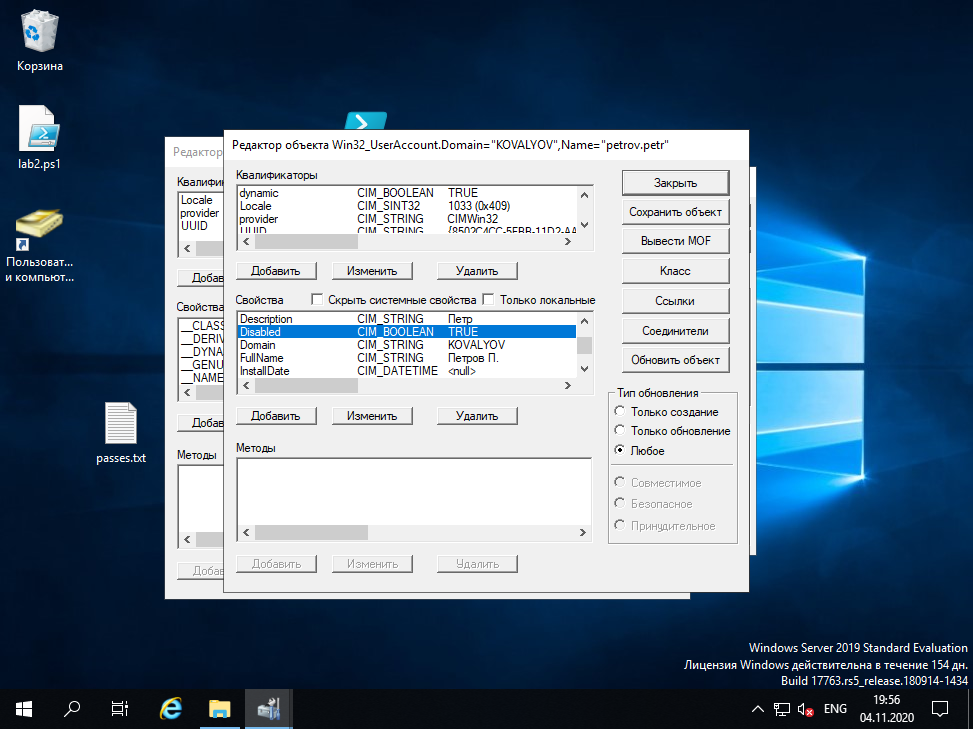
Petr.petrov:



Изменим данное значение:

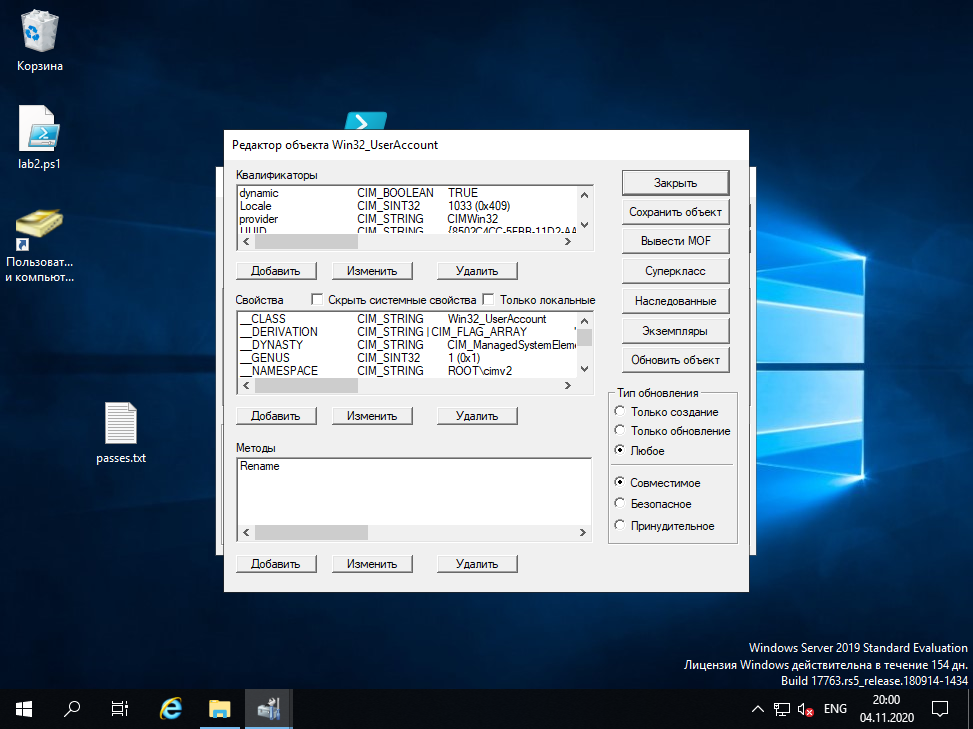


Проверим результат:



Изменение параметра Disabled прошло успешно.

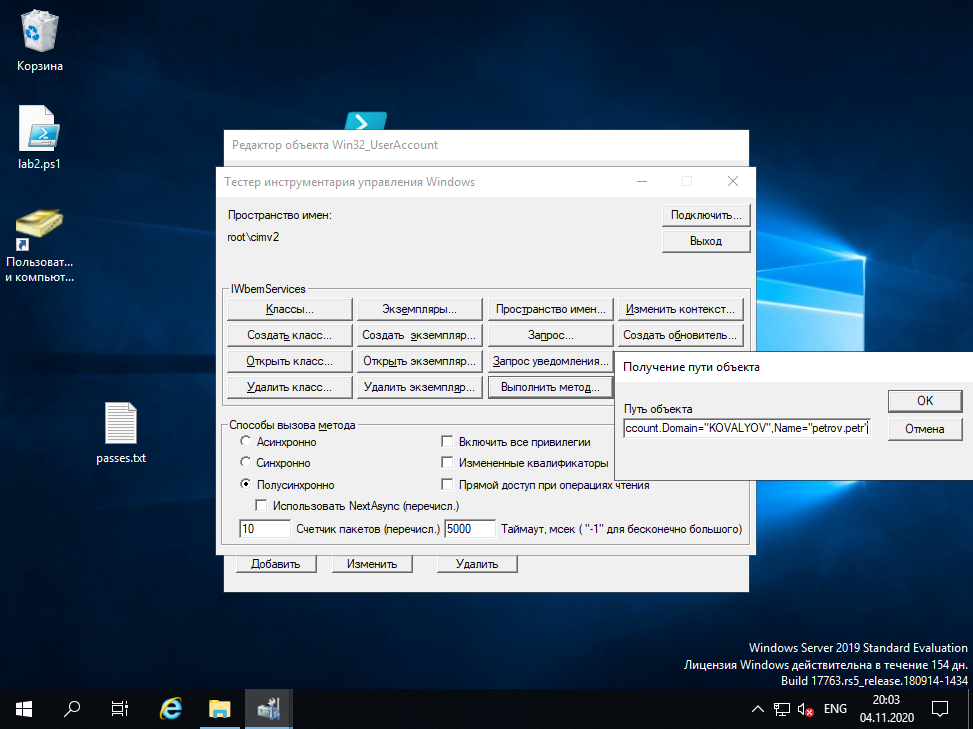
2. Найдите класс Win32\_UserAccount.



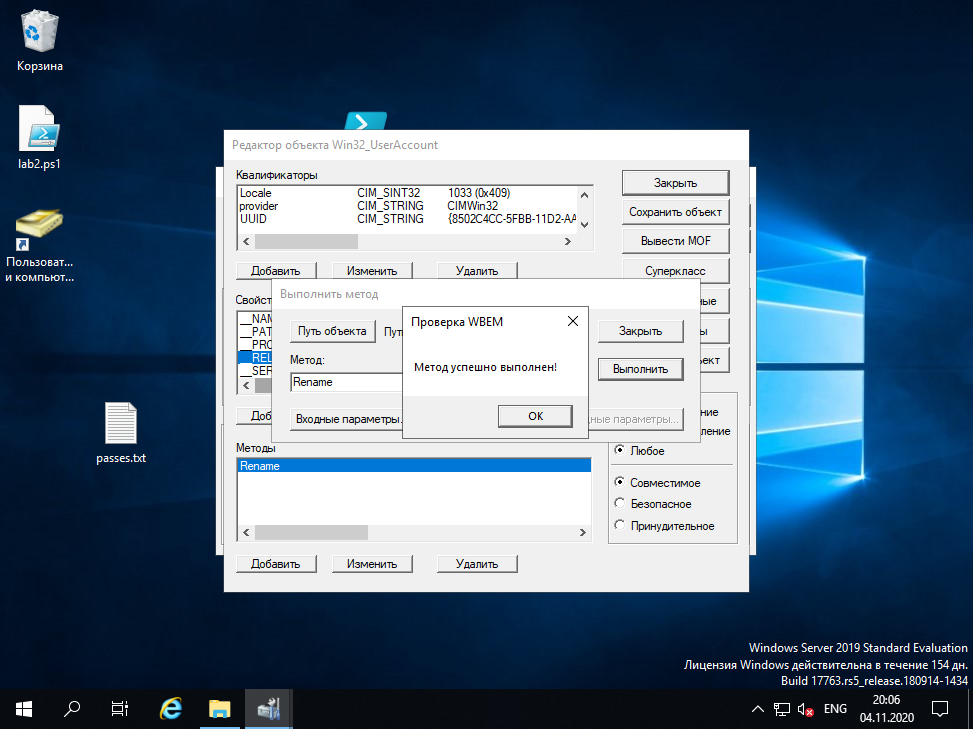
В окне методов этого класса значится метод Rename. Найдите экземпляр petr.petrov, скопируйте в буфер обмена значение его свойства \_RELPATH: Win32\_UserAccount.Domain="KOVALYOV",Name="petrov.petr".

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

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

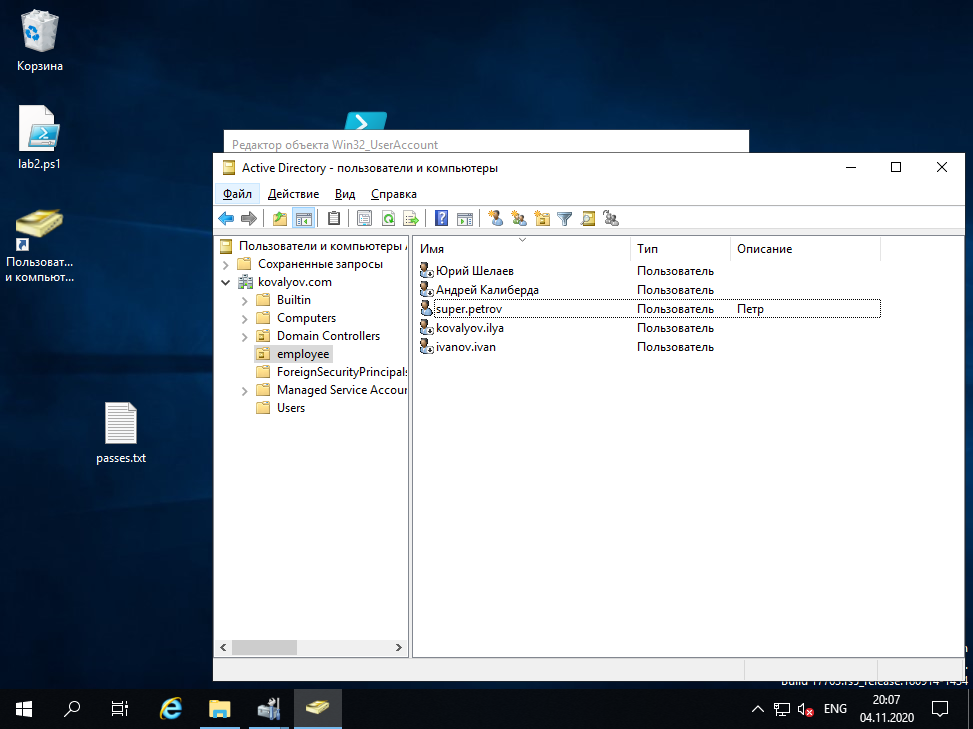


Вы получили доступ к методу Rename для этого экземпляра. Задайте входные параметры для метода (свойство Name) и выполните метод.



Убедитесь в Active Directory Users and Computers, что в свойствах

аккаунта изменилось имя. Измените его обратно на petr.petrov.



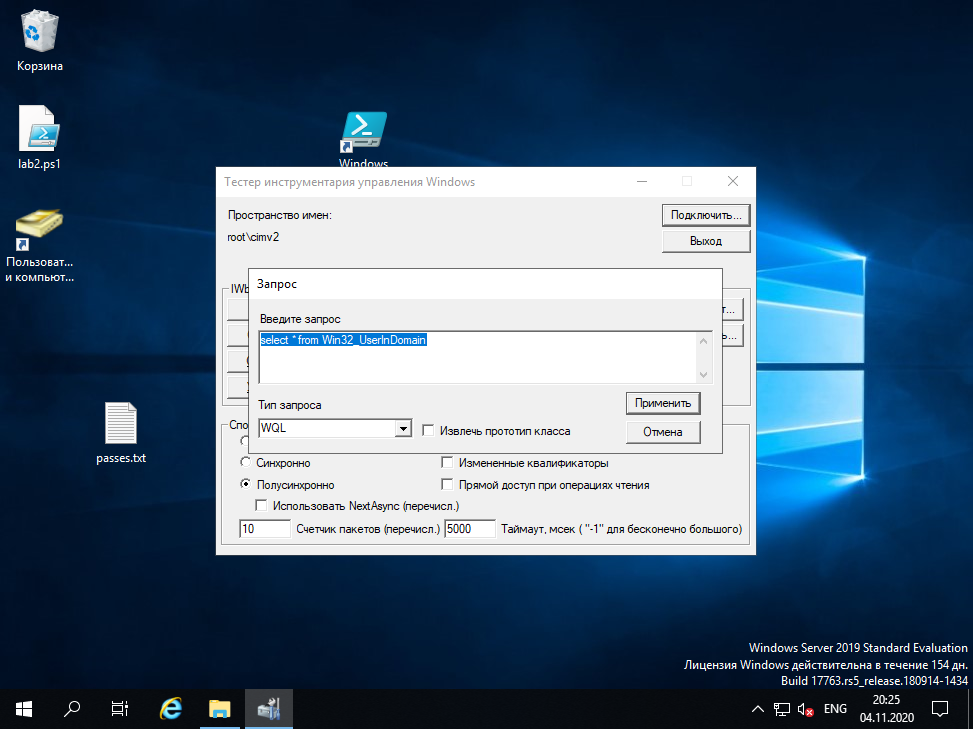
**3. Запросы WQL.**

Нажмите на кнопку Query в окне утилиты wbemtest.

Убедитесь, что в качестве типа запроса выбран WQL.

В поле ввода напишите запрос.

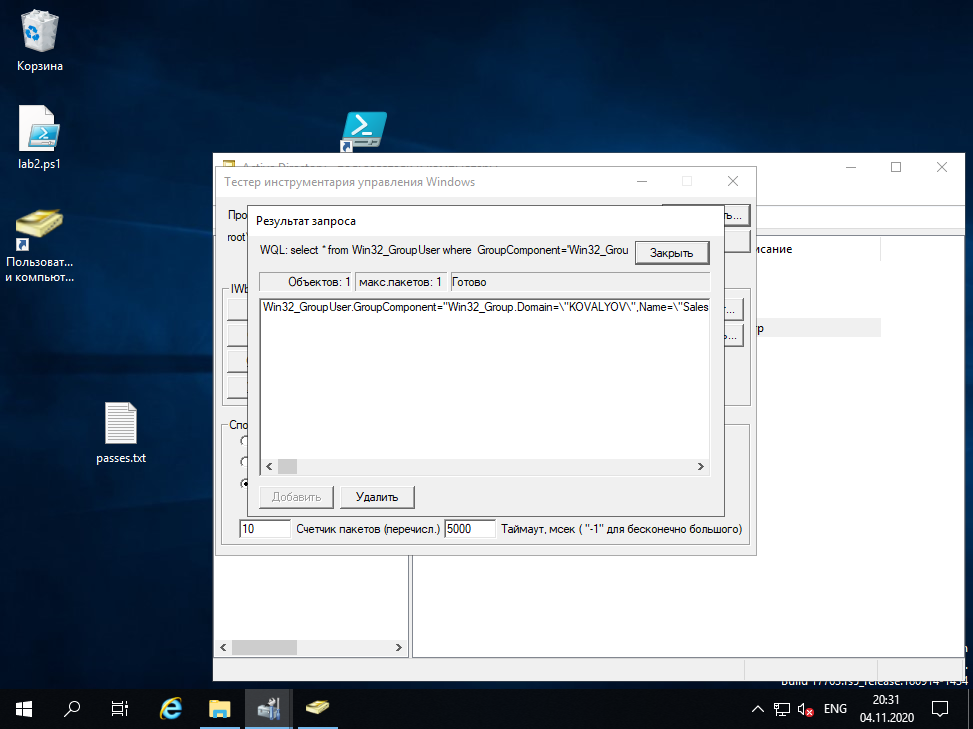
select \* from Win32\_UserInDomain



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

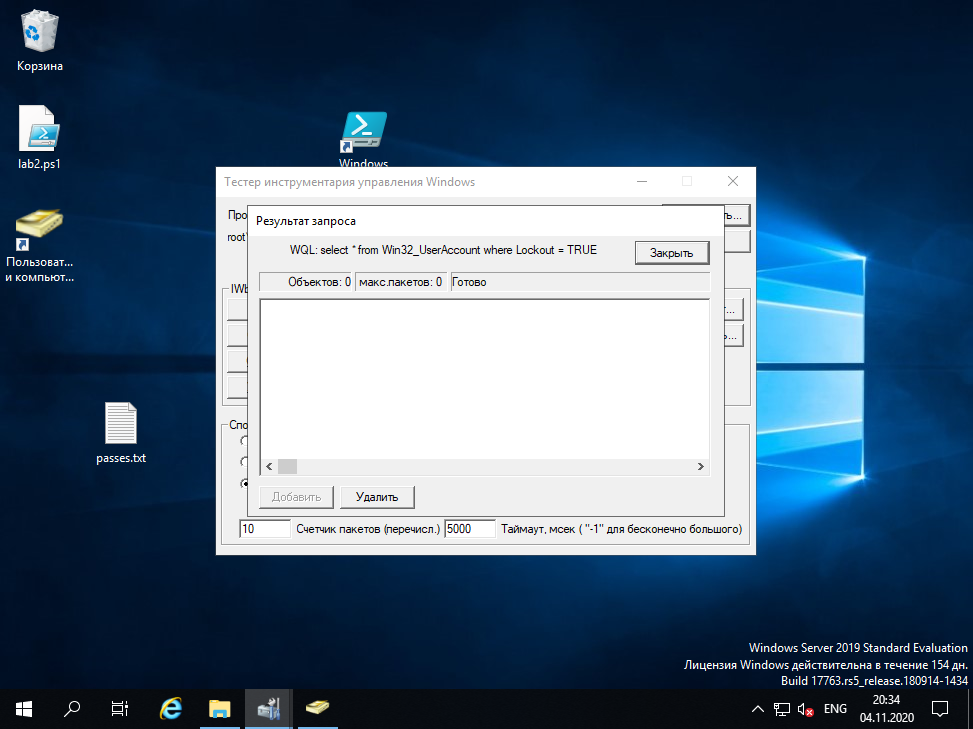
select \* from Win32\_GroupUser where

GroupComponent='Win32\_Group.Domain="KOVALYOV",Name="Sales Representative"'



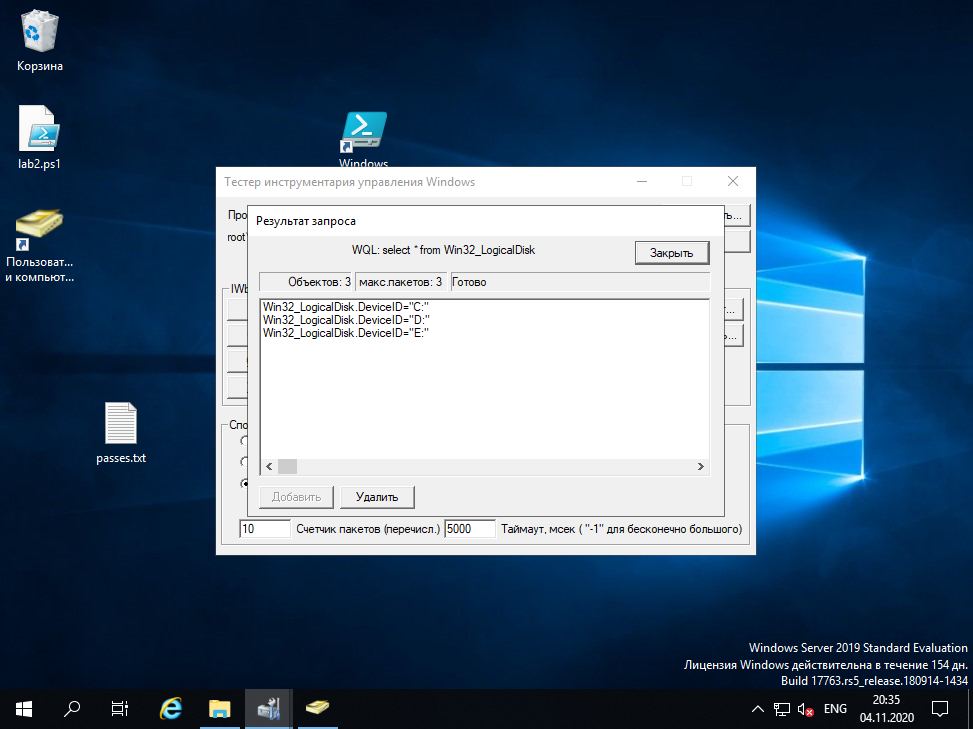
Составьте и выполните запрос, выводящий список заблокированных учетных записей пользователей.

select \* from Win32\_UserAccount where Lockout = TRUE



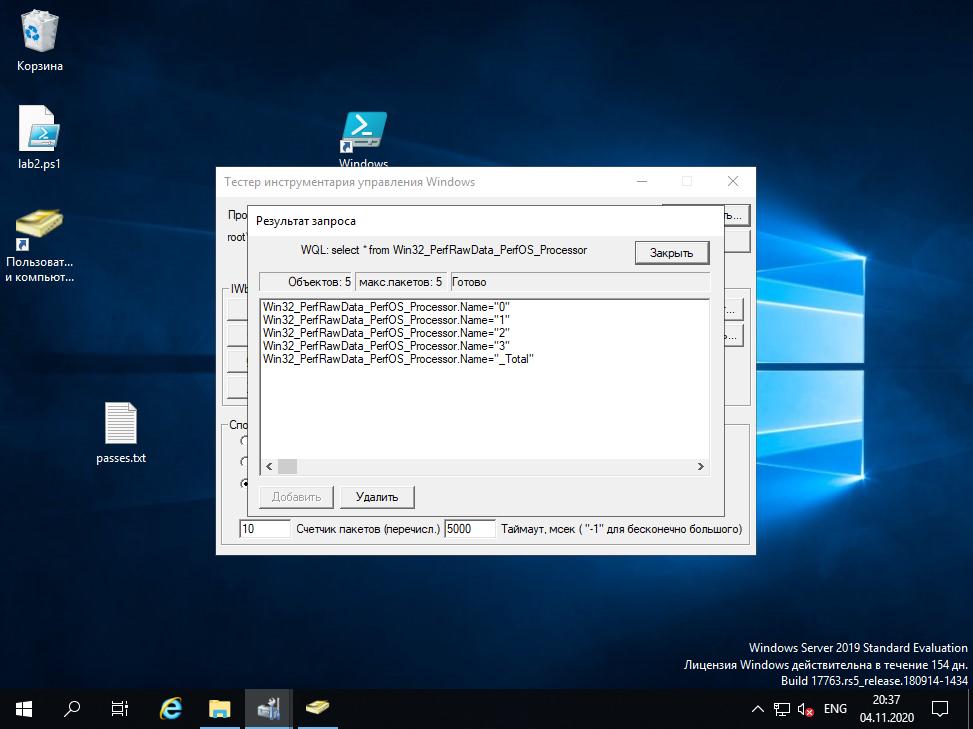
Составьте и выполните запросы, перечисляющие логические диски:

select \* from Win32\_LogicalDisk



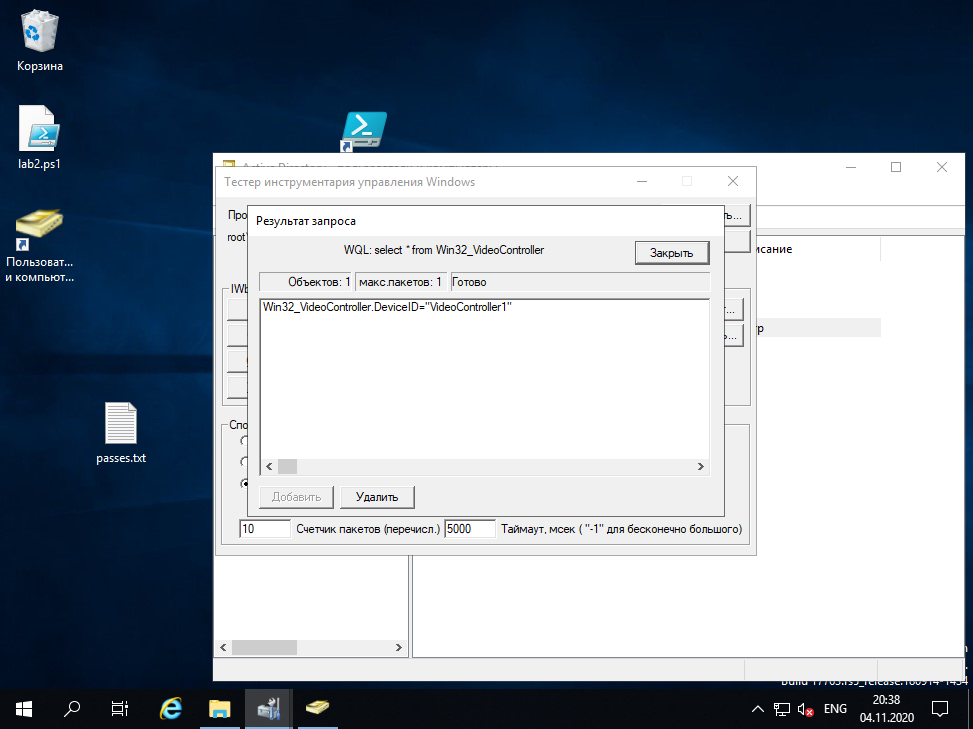
Процессоры:

select \* from Win32\_PerfRawData\_PerfOS\_Processor



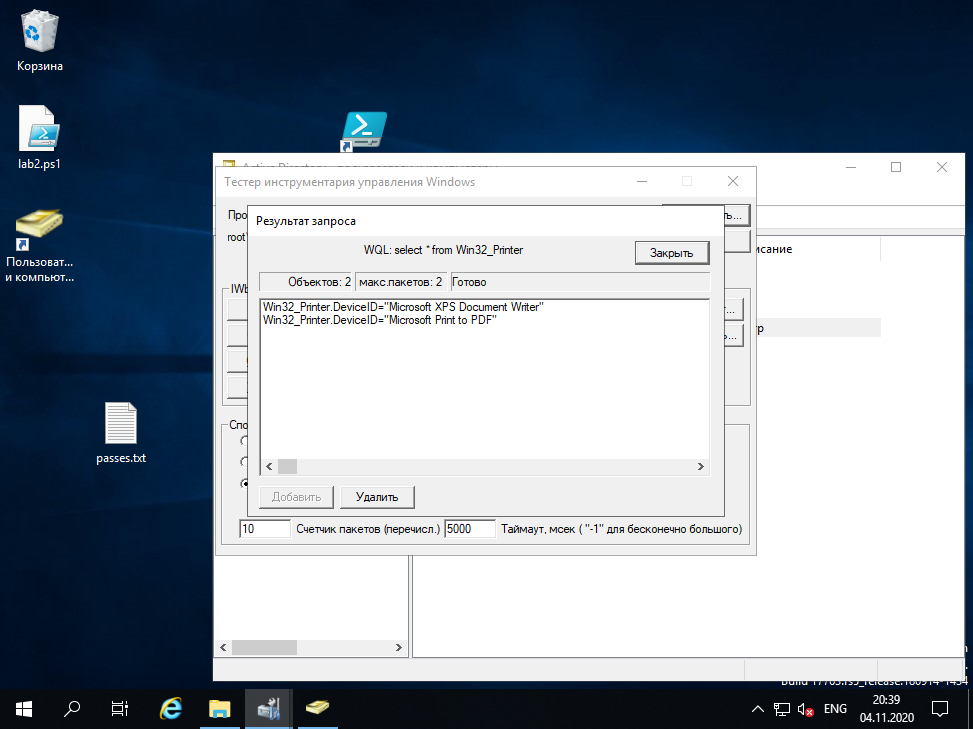
Видеокарты:

select \* from Win32\_VideoController



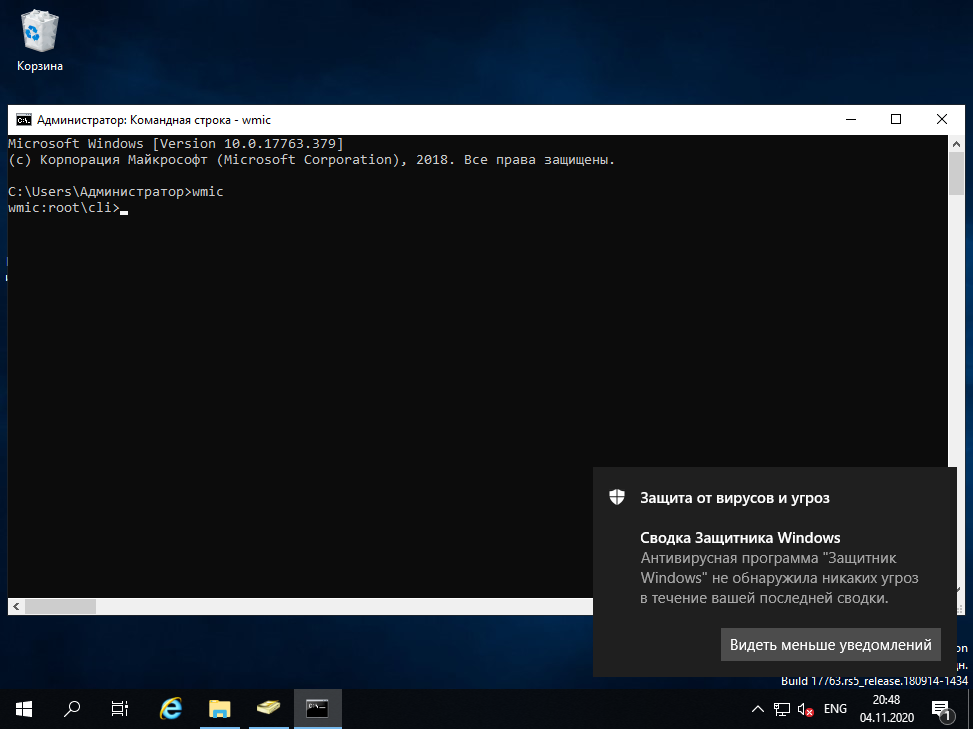
Принтеры:

select \* from Win32\_Printer

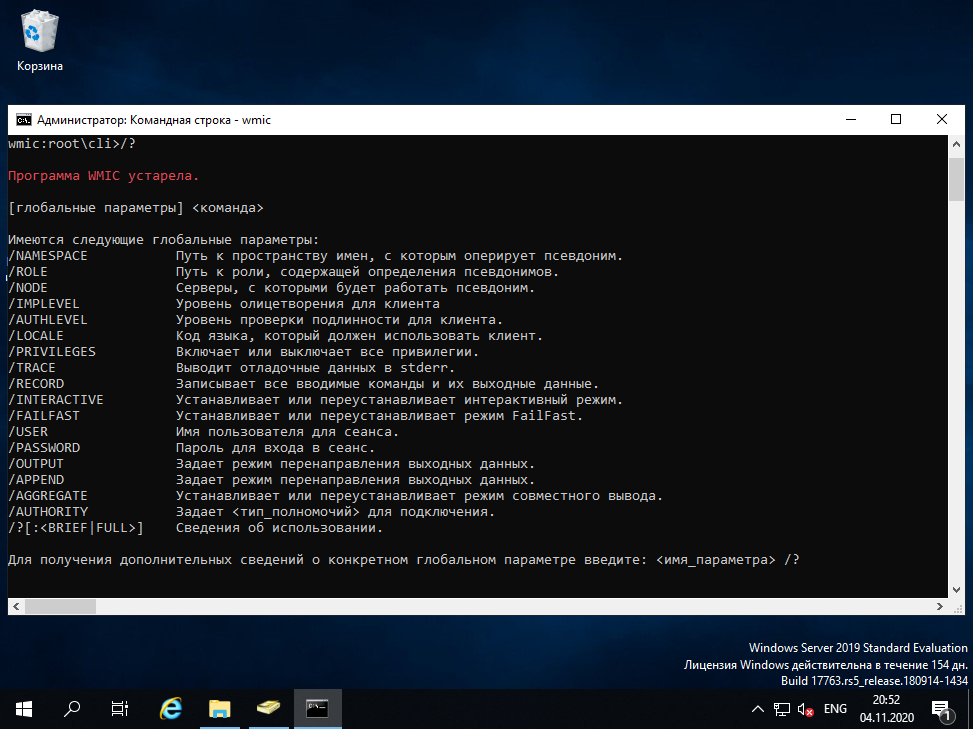


**4. Утилита Wmic.**

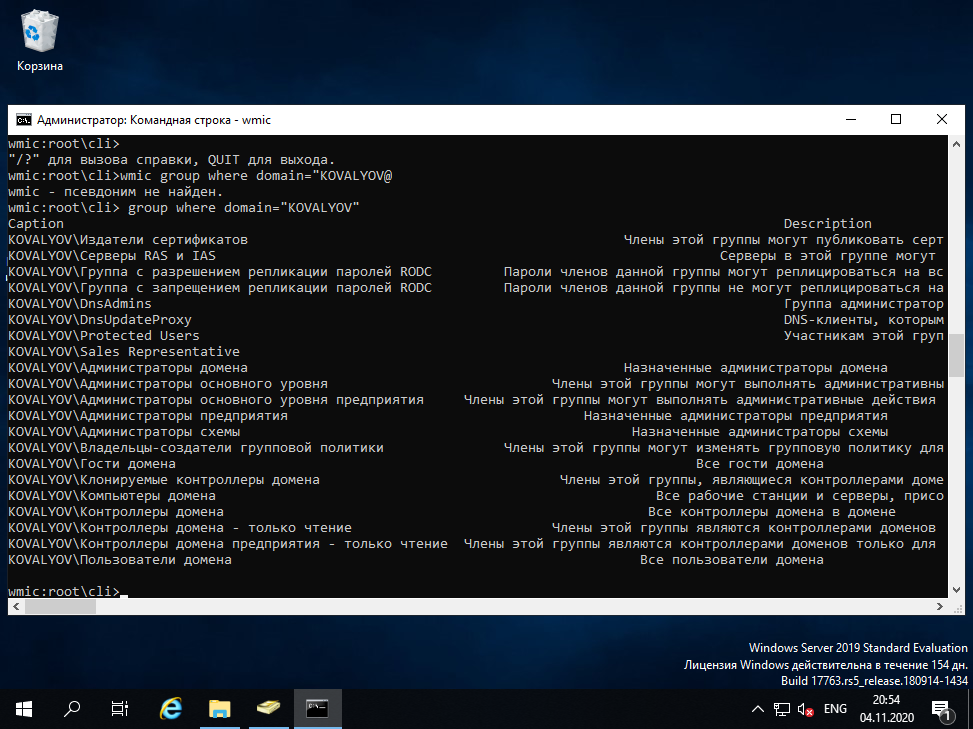
Запустите интерпретатор командной строки cmd.exe и в строке приглашения наберите WMIC. После этого появится приглашение консоли WMI.



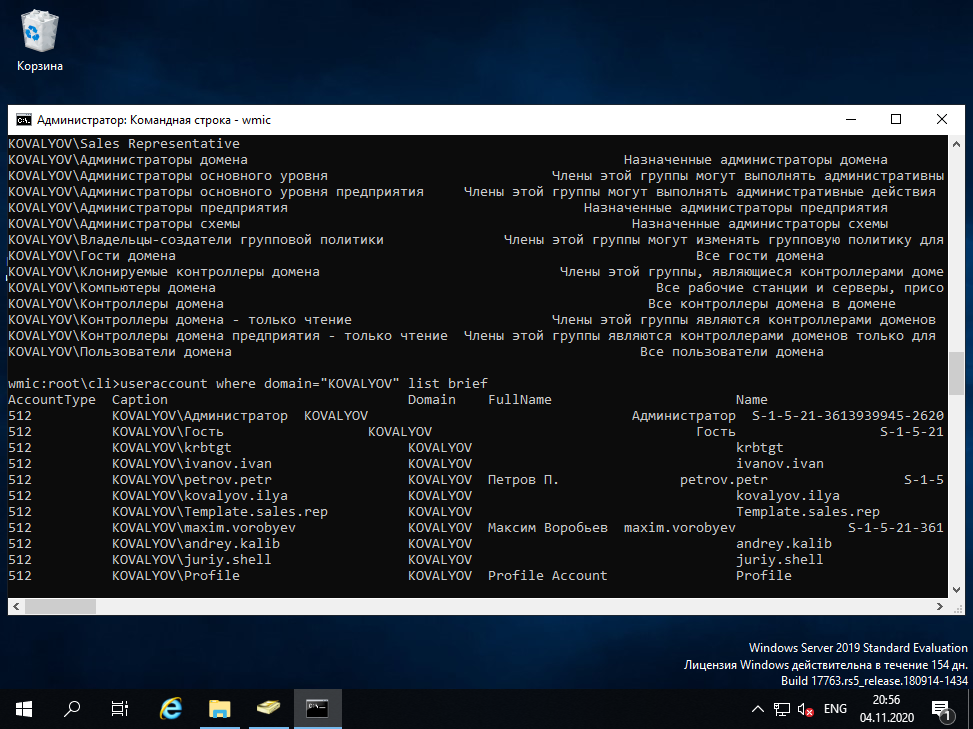
Просмотрите весь список команд и псевдонимов при помощи команды wmic /? (wmic:root\cli>/?).



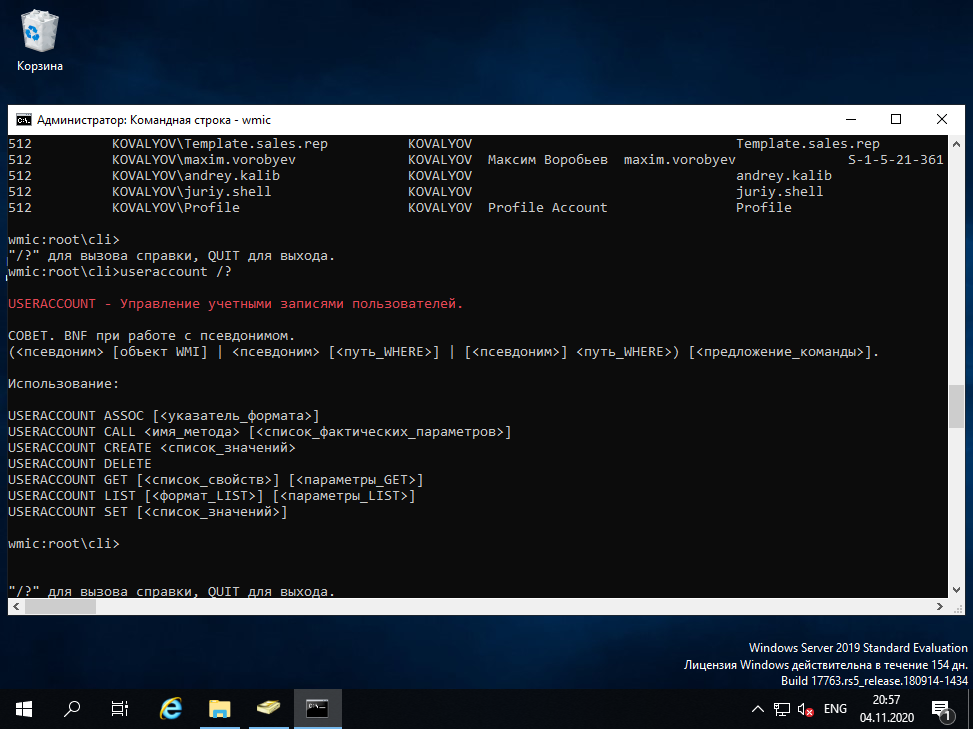
Используя команду wmic group where domain=”<Имя\_домена>”, получите список групп домена.

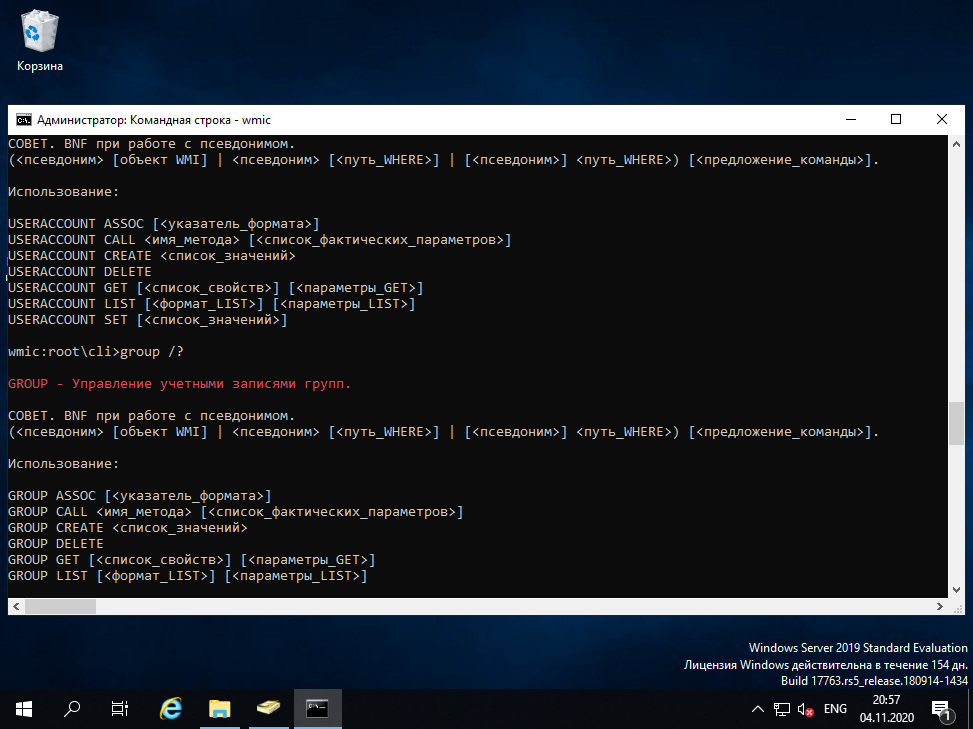


Выполните команду useraccount where domain=”KOVALYOV” list brief

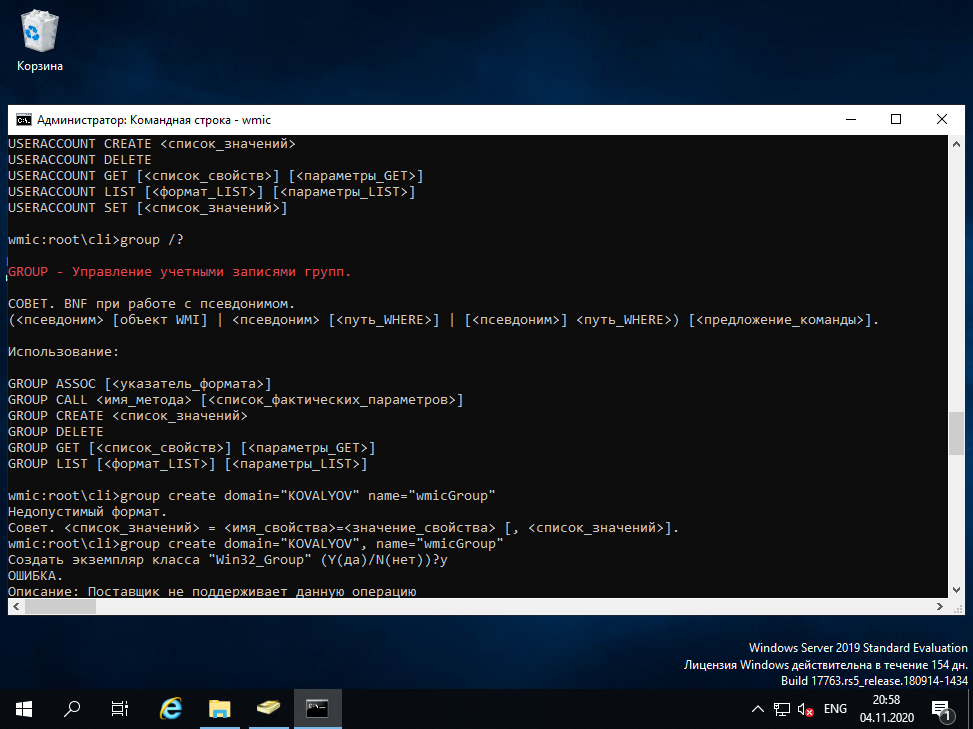
.

Просмотрите возможные команды для useraccount и group.





Создайте новую группу в своем домене.

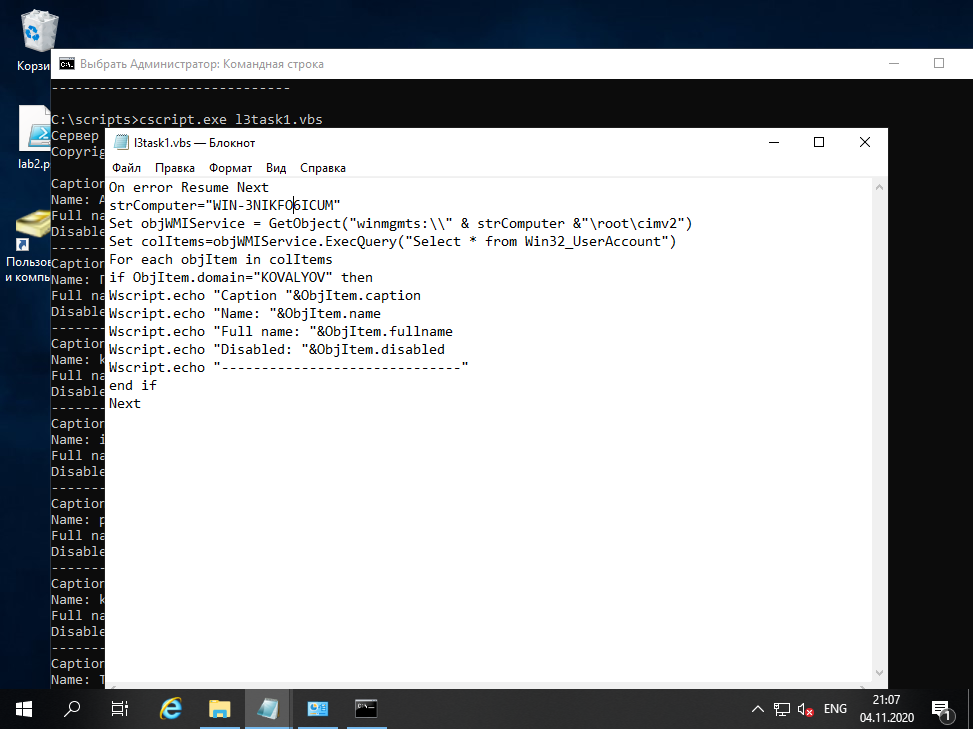


К сожалению, не смотря на все попытки, создать группу не удалось, поскольку wmic является устаревшей, о чем она информирует пользователя при запуске.

5. Сценарии с использованием WMI

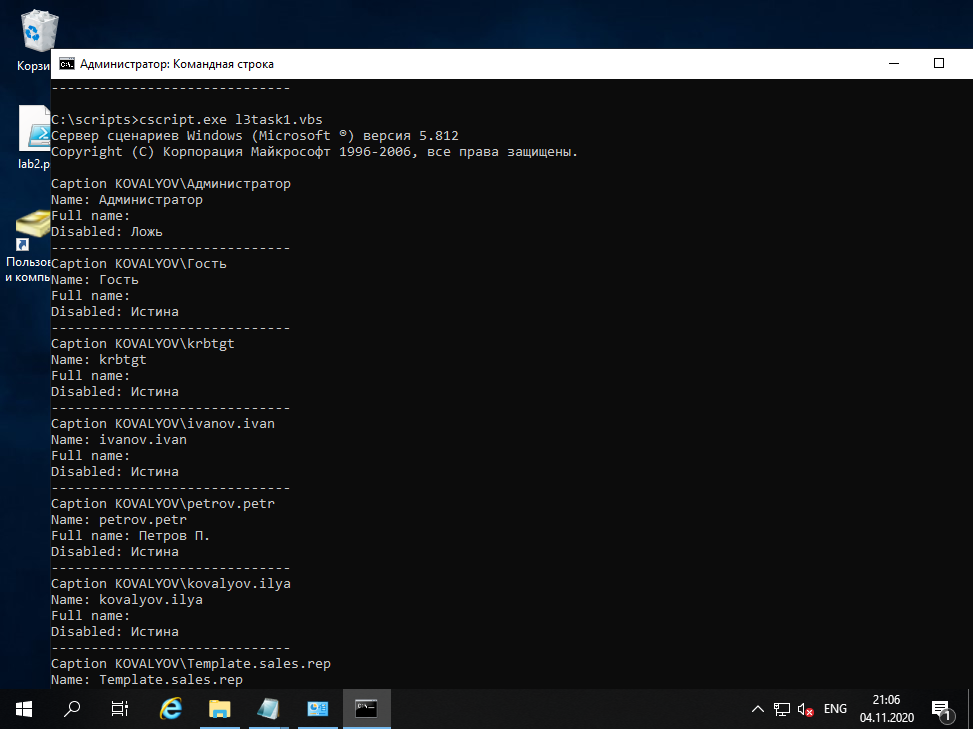
**5.1. Просмотр списка процессов при помощи сценария**

Необходимый сценарий:



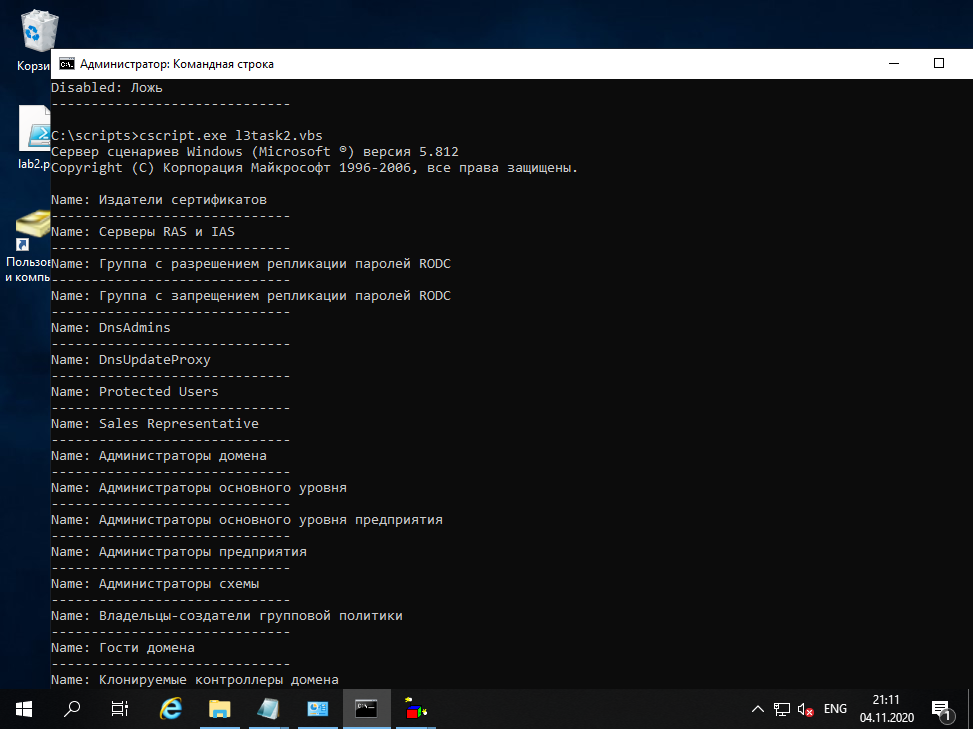
Сохраните файл, сменив расширение на \*.vbs.

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.



**5.2. Управление объектами с помощью сценариев WMI**

Выведите список групп, присутствующих в домене.



**Вывод:** в процессе выполнения лабораторной работы был изучен интерфейс Windows Management Instrumentation, получены навыки в получении доступа к ресурсам системы, создании новых пользователей через различные утилиты, предоставляемые «с коробки» с Windows Server 2019. Благодаря наличию графического интерфейса имеется возможность просматривать существующие классы, а также использовать различные методы и запросы WQL в удобоваримом формате.

Были изучены принципы формирования WQL-запросов, а также утилита Wmic, позволяющая исполнять сложные запросы к системе с использованием скриптов Visual Basic. К сожалению, на данный момент работает некорректно.

**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.

1. wmimgmt.msc – Позволяет управлять ММС для настройки WMI на локальном ПК.
2. winmgmt.exe – Позволяет управлять WMI локального компьютера
3. wbemtest.exe – Позволяет взаимодействовать со структурой WMI на локальном или удаленном ПК.
4. wmic.exe – Аналогично, но без графического интерфейса.
5. mofcomp.exe - компилятор MOF-файлов для расширения структуры WMI, управления библиотекой классов WMI и восстановления репозитория.

3. Общая структура WMI.

Архитектура WMI состоит из 3 частей:

Управляемые объекты/ресурсы (managed resources) — любые логические или физические компоненты информационной системы, доступ к которым может быть получен с помощью WMI. В качестве управляемых ресурсов могут выступать, например, файлы на жестком диске, запущенный экземпляр приложения, системное событие, предоставленный в общее пользование ресурс, сетевой пакет или установленный в компьютере процессор.

Ядро WMI (WMI infrastructure). Это связующее звено архитектуры WMI, отвечающее за связь управляющих программ с управляемыми объектами. Ядро WMI, в свою очередь, можно разделить на три части: менеджер объектов CIM (Common Information Model Object Manager, CIMOM), репозиторий (хранилище классов и объектов) CIM и провайдеры WMI. Кроме этого, для доступа к WMI с помощью сценариев необходима специальная библиотека поддержки сценариев WMI (WMI scripting library), которая располагается в файле wbemdisp.dll в каталоге %SystemRoot%\System32\Wbem.

Управляющие программы (management applications), которые являются потребителями сервисов WMI. В качестве потребителей могут выступать полновесные Win32-приложения, Web-приложения, сценарии WSH или другие инструменты администрирования, с помощью которых происходит доступ к управляемым объектам посредством WMI.

4. Опишите возможности программы WMIC.

Инструментарий WMI, основанный на CIM, является открытой унифицированной системой интерфейсов доступа к любым параметрам операционной системы, устройствам и приложениям, которые функционируют в ней, и используется для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением платформы Windows. для сбора информации о статусе локальных и удаленных компьютерных систем

5. Опишите возможности программы WBEMTEST.

Утилита командной строки WMIC позволяет использовать функциональные возможности Windows Management Instrumentation. WMIC реализует возможность просматривать структуру WMI как на локальной, так и на удаленной системе, выполнять методы классов, работать с экземплярами классов, выполнять WQL запросы к различным классам и объектам.

6. Использование WQL-запросов.

Запросы WQL (SQL for WMI) очень похожи на запросы SQL с тем отличием, что в WQL производится выборка не записей таблиц, а экземпляров классов.