1. Санкт-Петербургский Политехнический Университет Петра Великого
2. Институт кибербезопасности и защиты информации

**ЛАБОРАТОРНАЯ РАБОТА № 1 (дополнительная)**

**«ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ WINDOWS MANAGEMENT  
INSTRUMENTATION»**

1. по дисциплине «Безопасности современных информационных технологий»
2. Выполнил
3. студент группы
4. 4831001/00302 Ташкент В.В.

<*подпись*>

1. Проверил

ассистент Соловей Р.С.

<*подпись*>

1. Санкт-Петербург
2. 2022

**Оглавление**

[Цель работы 3](#_Toc122091923)

[Теоретические сведения 3](#_Toc122091924)

[Результаты работы 7](#_Toc122091925)

[Контрольные вопросы 9](#_Toc122091926)

[Вывод 10](#_Toc122091927)

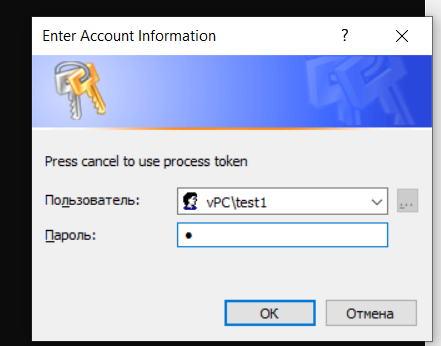
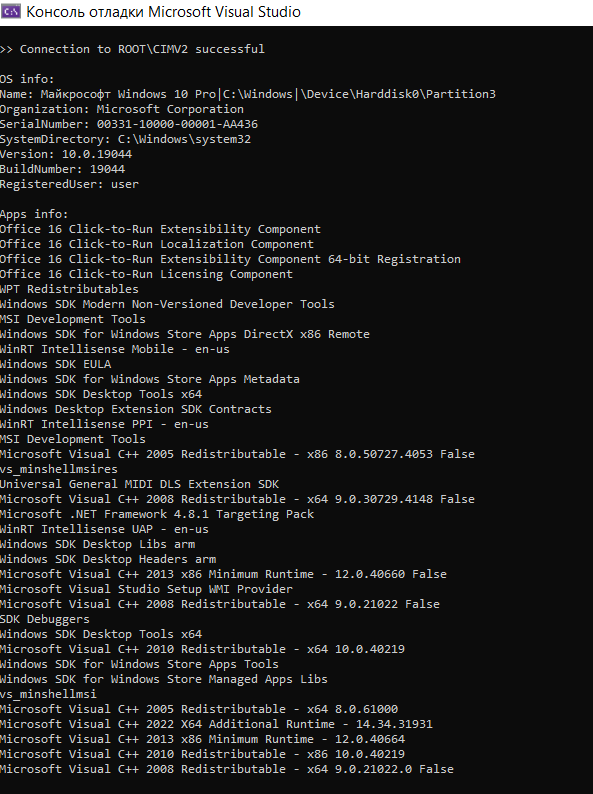
# **Цель работы**

Получить навыки работы с инструментарием управления Windows.

# **Теоретические сведения**

1. **Windows Management Instrumentation** (WMI) — это одна из базовых технологий для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением платформы Windows.
2. Технология WMI — это расширенная и адаптированная под Windows реализация стандарта WBEM, в основе которого лежит идея создания универсального интерфейса мониторинга и управления различными системами и компонентами распределенной информационной среды предприятия с использованием объектно-ориентированных идеологий и протоколов HTML и XML.
3. В основе структуры данных в WBEM лежит Common Information Model (CIM), реализующая объектно-ориентированный подход к представлению компонентов системы. CIM является расширяемой моделью, что позволяет программам, системам и драйверам добавлять в неё свои классы, объекты, методы и свойства.
4. WMI, основанный на CIM, также является открытой унифицированной системой интерфейсов доступа к любым параметрам операционной системы, устройствам и приложениям, которые функционируют в ней.
5. Важной особенностью WMI является то, что хранящиеся в нём объекты  
   соответствуют динамическим ресурсам, то есть параметры этих ресурсов постоянно меняются, поэтому параметры таких объектов не хранятся постоянно, а создаются по запросу потребителя данных.
6. Так как WMI построен по объектно-ориентированному принципу, то все данные операционной системы представлены в виде объектов и их свойств и методов.
7. Все классы группируются в пространства имен, которые иерархически упорядочены и логически связаны друг с другом по определенной технологии или области управления. В WMI имеется одно корневое пространство имен Root, которое в свою очередь имеет 4 подпространства: CIMv2, Default, Security и WMI.
8. Классы имеют свойства и методы и находятся в иерархической зависимости друг от друга, то есть классы-потомки могут наследовать или переопределять свойства классовродителей, а также добавлять свои свойства.
9. Свойства классов используются для однозначной идентификации экземпляра класса и для описания состояния используемого ресурса. Обычно все свойства классов доступны только для чтения, хотя некоторые из них можно модифицировать определенным методом. Методы классов позволяют выполнить действия над управляемым ресурсом.
10. Экземпляры классов могут генерировать события, к которым можно подписываться. При наступлении события WMI автоматически создает экземпляр того класса, которому соответствует это событие. Такой механизм удобно использовать для выполнения определенной команды при наступлении определенного события, то есть следить за состоянием объектов операционной системы.
11. Общая безопасность в WMI реализуется на уровне операционной системы, а  
    дополнительная политика безопасности основана на уровнях пространств имен и протокола DCOM. То есть если пользователь не имеет права делать какое-то действие через операционную систему, он не сможет это сделать и через WMI. Если же пользователю дано какое-то право в операционной системе, то это ещё не означает, что это право будет и в WMI, так как в WMI действуют дополнительные параметры безопасности на уровне пространств имен.
12. Каждый объект операционной системы имеет своё описание безопасности (SD) со своим списком доступа (ACL), в котором перечислены идентификаторы пользователей (SID) и их привилегии. Каждое пространство имен может иметь собственное SD со своим ACL, где пользователям могут быть назначены разрешения на чтение данных, выполнение методов, запись классов и данных и другие. Данные о дополнительных разрешениях хранятся в репозитории WMI. Отдельные классы из пространств имен не имеют собственных описаний безопасности, они наследуют их от своего пространства имен.
13. По умолчанию администратор компьютера имеет полные права на использование WMI, а остальные пользователи могут лишь вызывать методы, считывать данные и записывать в репозиторий экземпляры классов провайдеров WMI.
14. Для доступа к инфраструктуре WMI используется протокол DCOM, через который пользователь подключается к WMI. Чтобы определить, какие права будут у подключившегося пользователя, используются механизмы олицетворения и  
    аутентификации протокола DCOM.
15. Для обращения к объектам WMI используется специфический язык запросов WMI Query Language (WQL), который является одной из разновидностей SQL. Основное его отличие от ANSI SQL — это невозможность изменения данных, то есть с помощью WQL возможна лишь выборка данных с помощью команды SELECT. Помимо ограничений на работу с объектами, WQL не поддерживает такие операторы как DISTINCT, JOIN, ORDER, GROUP, математические функции. Конструкции IS и NOT IS применяются только в сочетании с константой NULL.
16. Запросы WQL обычно применяются в скриптах, но их также можно протестировать в программе Wbemtest и в консольной утилите Wmic (утилита wmic не требует написания ключевого слова SELECT и полей выборки)

# **Результаты работы**

1. В ходе лабораторной работы был реализован клиент-серверное приложение под ОС Windows 7-10.
2. Программа-клиент запрашивает по интерфейсу WMI информацию об удаленной системе, на которой работает программа-сервер.
3. Так ж были реализованы требования к работе, а именно:
4. - Все данные о системе должны получены с помощью обращения к WMI API;
5. - При установке соединения производится имперсонация клиента (через  
   WMI);
6. - Необходимо запросить минимум 10 параметров системы, из которых обязательными является информация об установленных приложениях, а также информация из центра безопасности Windows (Windows Security Center, WSC) об установленном антивирусе, файерволле, противошпионском ПО;
7. - Программа написана на C/C++.
8. 
9. *Рис.1 Подключение к удаленной системе*
10. ****
11. *Рис 2. Результат работы программы*

# **Контрольные вопросы**

1. **1) Что такое WMI и зачем данный инструмент нужен?**
2. Ответ: Windows Management Instrumentation – технология удаленного доступа между устройствами с ОС Windows.
3. **2) Какие основные возможности у WMI?**
4. Ответ: WMI может передавать, изменять и принимать данные с удаленных устройств при помощи простых пространств имен и классов. Делает он это по защищенным каналам с шифрованием.
5. **3) Опишите архитектуру и принципы работы WMI?**
6. Ответ: WMI основан на объектно-ориентированной модели CIM(Control Information Model). Все данные передаются по протоколу DCOM. Иерархия такова - сначала идет пространство имен, которых всего четыре. Эти пространства содержат в себе классы, которые описывают тот или иной аспект пространства имен. В свою очередь, классы содержат методы и имеют некоторые свойства. Для обращения ко всем этим объектам используется специальный язык WQL, который является одной из разновидностей SQL.

# **Вывод**

1. В данной лабораторной работе были получены навыки работы с инструментарием управления Windows. Он подходит для получения информации от удаленного устройства, изменения данных на удаленных устройствах, а также для администрирования сетей и распределения прав доступа.