# Лабораторные работы №1

## Цель работы

Приобретение практических навыков диагностики работы программного обеспечения (собственного и стороннего).

## Задание

*Часть 1.* Написать собственную программу, которая демонстрирует работу с различными системными вызовами (8-15) операционной системы. Произвести диагностику работы написанной программы с помощью утилит ОС, изучив основные принципы применения используемых утилит.

*Часть2.* Выбрать стороннее программное обеспечение. Произвести диагностику ПО. Выявить ключевые особенности работы. Выявить предполагаемые ключевые системные вызовы, которые используются в стороннем программном обеспечении.

Отчет должен включать описания:

* выбранных системных вызовов
* используемых утилит диагностики
* принципов работы стороннего ПО (на основании обнаруженных системных вызовов)

## Список возможных стороннего программного обеспечения

1. Notepad
2. Notepad++
3. Powershell
4. Cmd
5. Paint
6. Shutdown
7. Fsutil
8. Cscript
9. И др.

## Средства диагностики

Для ОС Windows

* Windbg
  + <http://windbg.info/doc/1-common-cmds.html>
* Sysinternals Suite
  + Handle.exe
  + Procmon.exe
  + Procexp.exe