Материалы XIX Республиканской научной конференции студентов и аспирантов «Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях», Гомель, 21–23 марта 2016г.

И. Г. Пинчук, М. И. Жадан
(ГГУ им. Ф. Скорины, Гомель)

РАЗРАБОТКА МОНИТОРА АКТИВНОСТИ WINDOWS ПО ТЕХНОЛОГИИ WINDOWS BATCH SCRIPTING

Все программы и действия в операционной системе Windows выполняются в определенных процессах (стандарт ISO 9000:2000 определяет процесс как совокупность взаимосвязанных и взаимодействующих действий, преобразующих входящие данные в исходящие). Процесс Windows по своей сути является контейнером, в котором хранится код команд из исполняемого файла. Он представляет собой объект процесса ядра и Windows использует этот объект процесса и связанные с ним структуры данных для хранения и сопровождения информации об исполняемом коде приложения. Также, процессом называют выполняющуюся программу и её элементы: адресное пространство, глобальные переменные, регистры, стек, открытые файлы и т.д.

У пользователя может возникнуть необходимость отслеживать какие процессы запущены в системе, запускаются и завершаются в ней, а также от чьего имени был запущен процесс и в какое время.

Из всего многообразия средств язык пакетных команд Windows был выбран в силу возможности запуска скрипта на данном языке на любом компьютере, под управлением операционной системы Windows. Код программы организован в пакетный файл. Интерфейс программы представлен в виде консоли коммандной оболочки Windows.

В ходе работы изучены следующие вопросы:

– процессы в операционной системе Windows;

– язык командной строки Windows;

– интерпретатор командной оболочки Windows cmd.exe;

– пакетные файлы.

Спроектировано и реализовано приложение для операционной системы Windows. Данное приложение подходит для различных версий операционной системы. Программа совершает поиск запущенных процессов, выводит информацию о них в консоль и сохраняет данные в файл журнала, создаваемый при каждом запуске программы.

Разработанное приложение позволяет отслеживать активность процессов, что даёт возможность отследить работу того или иного приложения, обнаружить и устранить вредоносную программу (ви-

рус), выявить скрытые программы и сервисы, которые работают в фоновом режиме и не видны пользователю. Это поможет упорядочить и обезопасить работу системы, а также повысить её производительность и скорость.