Программа контрольной работы 2

Архитектура ОС Windows

1. Основные компоненты операционной системы. Основные файлы подсистемы Windows. Способы реализации функций библиотек подсистемы. Функции процесса подсистемы окружения (`Csrss.exe`), библиотек процесса подсистемы окружения, драйвера `Win32k.sys`, библиотеки поддержки системы (`Ntdll.dll`). Виды функций, компоненты и назначение исполнительной системы (`Ntoskrnl.exe`). Функции ядра и уровня HAL. Драйверы устройств: принцип работы, виды. Модель WDM, виды драйверов с точки зрения модели WDM. Каркас WDF. Системные процессы, их родительски-дочерние отношения. Системные потоки. Диспетчер сеансов (`smss.exe`): порядок запуска и выполняемые функции. Оконная станция, рабочий стол. Работа процесса инициализации (`Wininit.exe`). Функции диспетчера локальных сеансов (`Lsm.exe`). Функции и работа процесса входа в систему (`Winlogon.exe`).

2. Динамически связываемые библиотеки. Виды библиотек. Модульный подход к проектированию ПО. Преимущества динамических библиотек. Статическое связывание с библиотекой при помощи DEF-файла и языковых конструкций экспорта. Использование объявлений «`extern "C"`». Динамическое связывание при помощи Windows API. Точка входа библиотеки, сериализация её вызовов. Структуры данных загрузчика образа. Порядок поиска библиотек в безопасном режиме. Перенаправление библиотек. Основные поля базы данных модулей.

3. Запуск процесса. Секции модуля, разделяемые между процессами секции. Обзор формата PE. Заголовок NT. Заголовок файла, архитектура. Дополнительный заголовок, подсистема. Таблица каталога данных, индексы его основных элементов. Заголовок секции, флаги. Таблицы экспорта и импорта. Способ вызова функции при наличии/отсутствии

в её объявлении описания `__declspec (dllimport)`. Таблица перемещений, типы перемещения. Алгоритм работы функции `CreateProcess()`. Функции исполнительной системы при запуске процесса.

4. Службы. Виды и компоненты служб. Функции диспетчера служб (`Services.exe`). База данных диспетчера служб. Способы обновления информации о службах. Функции, реализующие службу. Функции установки/удаления служб. Функция `StartServiceCtrlDispatcher()`: алгоритм её работы и работы диспетчера служб при её запуске. Функции регистрации обработчиков управляющих сообщений. Функция установки состояния службы. Функции работы с журналом Windows. Правила реализации точки входа в службу и основной функции программы службы. Поведение функции `StartServiceCtrlDispatcher()` при запуске очередной службы. Правила реализации функции службы. Реализация управления/конфигурации службы.