**Вопросы к экзамену по дисциплине «Операционные системы и системное программирование. Часть 2»**

1. Модель программного интерфейса операционной системы Windows. Нотация программного интерфейса. Понятие объекта ядра и описателя объекта ядра операционной системы Windows. Модель архитектуры ОС Windows.

2. Понятие пользовательского режима и режима ядра операционной системы Windows. Модель виртуальной памяти процесса в пользовательском режиме и в режиме ядра операционной системы Windows. Архитектура приложения в пользовательском режиме работы и в режиме ядра ОС Windows. Основные модули ОС Windows.

3. Системный реестр операционной системы Windows. Структура и главные разделы. Точки автозапуска программ. Средства редактирования реестра Windows. Функции работы с реестром из приложения.

4. Понятие окна в ОС Windows. Основные элементы окна. Понятие родительского и дочернего окна. Структура программы с событийным управлением. Минимальная программа для ОС Windows с окном на экране. Создание и отображение окна.

5. Структура программы с событийным управлением. Структура события – оконного сообщения Windows. Очередь сообщений. Цикл приема и обработки сообщений. Процедура обработки сообщений. Процедуры посылки сообщений. Синхронные и асинхронные сообщения.

6. Ввод данных с манипулятора «мышь». Обработка сообщений мыши. Ввод данных с клавиатуры. Понятие фокуса ввода. Обработка сообщений от клавиатуры.

7. Вывод информации в окно. Механизм перерисовки окна. Понятие области обновления окна. Операции с областью обновления окна.

8. Принципы построения графической подсистемы ОС Windows. Понятие контекста устройства. Вывод графической информации на физическое устройство. Управление цветом. Палитры цветов. Графические инструменты. Рисование геометрических фигур.

9. Растровые изображения. Виды растровых изображений. Значки и курсоры. Способ вывода растровых изображений с эффектом прозрачного фона. Аппаратно-зависимые и аппаратно-независимые растровые изображения. Операции с растровыми изображениями. Вывод растровых изображений.

10. Библиотека работы с двумерной графикой Direct2D. Инициализация библиотеки. Фабрика графических объектов библиотеки Direct2D. Вывод графики средствами библиотеки Direct2D.

11. Вывод текста в ОС Windows. Понятие шрифта. Характеристики шрифта. Понятия физического и логического шрифта. Операции с физическими шрифтами. Операции с логическими шрифтами. Параметры ширины и высоты логического шрифта.

12. Системы координат. Трансформации. Матрица трансформаций. Виды трансформаций и их представление в матрице трансформаций. Преобразования в страничной системе координат. Режимы масштабирования.

13. Понятие ресурсов программ Windows. Виды ресурсов. Операции с ресурсами.

14. Понятие динамически-загружаемой библиотеки. Создание DLL-библиотеки. Использование DLL-библиотеки в программе методом статического импорта процедур. Соглашения о вызовах процедур DLL-библиотеки. Точка входа-выхода DLL-библиотеки. Использование DLL-библиотеки в программе методом динамический импорта процедур.

Создание в DLL-библиотеке разделяемых между приложениями глобальных данных. Разделы импорта и экспорта DLL-библиотеки. Переадресация вызовов процедур DLL-библиотек к другим DLL-библиотекам. Исключение конфликта версий DLL.

17. Понятие объекта ядра ОС Windows. Виды объектов ядра. Атрибуты защиты объекта ядра. Дескриптор защиты объекта ядра. Создание и удаление объектов ядра.

18. Проецирование файлов в память. Отличие в механизме проецирования файлов в память в ОС Windows и UNIX/Linux. Действия по проецированию файла в память.

19. Современные многопроцессорные архитектуры SMP и NUMA. Многоуровневое кэширование памяти в современных процессорах. Проблема перестановки операций чтения и записи в архитектурах с ослабленной моделью памяти. Способы решения проблемы перестановки операций чтения и записи.

20. Средства распараллеливания вычислений в ОС Windows. Понятия процесса и потока. Достоинства и недостатки процессов и потоков. Создание и завершение процесса. Запуск процессов по цепочке. Создание и завершение потока. Приостановка и возобновление потока. Контекст потока.

22. Понятие пула потоков. Архитектура пула потоков. Операции с потоками при работе с пулом потоков.

23. Распределение процессорного времени между потоками ОС Windows. Механизм приоритетов. Класс приоритета процесса. Относительный уровень приоритета потока. Базовый и динамический приоритеты потока. Операции с приоритетами.

24. Механизмы синхронизации потоков одного и разных процессов в ОС Windows. Обзор и сравнительная характеристика механизмов синхронизации.

25. Синхронизация потоков в пределах одного процесса ОС Windows. Критическая секция. Операции с критической секцией. Атомарные операции. Ожидаемое условие (монитор Хора). Операции с ожидаемым условием. Пример использования ожидаемого условия для синхронизации потоков.

27. Синхронизация потоков разных процессов с помощью объектов ядра. Понятие свободного и занятого состояния объекта ядра. Процедуры ожидания освобождения объекта ядра. Перевод объекта ядра в свободное состояние. Объекты синхронизации: блокировки, семафоры, события. Ожидаемые таймеры. Оконные таймеры.

29. Структура системного программного интерфейса ОС Windows (Native API). Nt-функции и Zw-функции в пользовательском режиме и режиме ядра ОС Windows.

30. Системный вызов ОС Windows. Алгоритм системного вызова. Особенность системного вызова из режима ядра.

31. Отладка драйверов ОС Windows. Средства отладки драйверов. Посмертный анализ. Живая отладка.

32. Структуры данных общего назначения в режиме ядра ОС Windows. Представление строк стандарта Unicode. Представление двусвязных списков.

33. Механизм прерываний ОС Windows. Аппаратные и программные прерывания. Понятие прерывания, исключения и системного вызова. Таблица векторов прерываний (IDT).

34. Аппаратные прерывания. Программируемый контроллер прерываний. Механизм вызова прерываний. Обработка аппаратных прерываний. Понятие приоритета прерываний (IRQL). Понятие процедуры обработки прерываний (ISR).

35. Понятие приоритета прерываний (IRQL). Приоритеты прерываний для процессора x86 или x64. Процедура обработки прерываний (ISR). Схема обработки аппаратных прерываний.

36. Программные прерывания. Понятие отложенной процедуры (DPC). Назначение отложенных процедур. Механизм обслуживания отложенных процедур. Операции с отложенными процедурами.

37. Понятие асинхронной процедуры (APC). Назначение асинхронных процедур. Типы асинхронных процедур. Операции с асинхронными процедурами. Асинхронные процедуры режима ядра: специальная и нормальная APC-процедуры. Асинхронные процедуры пользовательского режима.

39. Понятие элемента работы (Work Item). Назначение элементов работы. Операции с элементами работы. Очереди элементов работы. Обслуживание элементов работы.

40. Управление памятью в ОС Windows. Менеджер памяти. Виртуальная память процесса. Управление памятью в пользовательском режиме. Страничная виртуальная память. Куча (свалка, heap). Проецирование файлов в память.

41. Управление памятью в пользовательском режиме ОС Windows. Оптимизация работы кучи с помощью списков предыстории (Look-aside Lists) и низко-фрагментированной кучи (Low Fragmentation Heap).

42. Структура виртуальной памяти в ОС Windows. Виды страниц. Состояния страниц. Структура виртуального адреса. Трансляция виртуального адреса в физический. Кэширование виртуальных адресов.

43. Управление памятью в режиме ядра ОС Windows. Пулы памяти. Выделение и освобождение памяти в пулах памяти. Структура описателя пула памяти. Доступ к описателям пулов памяти на однопроцессорной и многопроцессорной системах.

44. Пулы памяти ОС Windows. Пул подкачиваемой памяти, пул неподкачиваемой памяти, пул сессии, особый пул. Тегирование пулов. Структура данных пула. Выделение и освобождение памяти в пулах памяти. Организация списков свободных блоков в пуле памяти. Заголовок блока пула памяти.

45. Управление памятью в режиме ядра ОС Windows. Оптимизация использования оперативной памяти с помощью списков предыстории – Look-aside Lists.

46. Представление объекта ядра в памяти. Менеджер объектов.

47. Фиксация данных в физической памяти ОС Windows. Таблица описания памяти (MDL) и ее использование.

48. Понятие драйвера ОС Windows. Виды драйверов. Типы драйверов в режиме ядра. Точки входа в драйвер.

49. Объект, описывающий драйвер. Объект, описывающий устройство. Объект, описывающий файл. Структура и взаимосвязь объектов.

50. Понятие пакета ввода-вывода (IRP). Структура пакета ввода-вывода. Схема обработки пакета ввода-вывода при открытии файла. Схема обработки пакета ввода-вывода при выполнении чтения-записи файла.

52. Перехват API-вызовов ОС Windows в пользовательском режиме. Внедрение DLL с помощью реестра. Внедрение DLL с помощью ловушек. Внедрение DLL с помощью дистанционного потока. Замена адреса в таблице импорта. Перехват в точке входа в процедуру с помощью подмены начальных инструкций (Microsoft Detours).

54. Перехват API-вызовов ОС Windows в режиме ядра. Таблица системных функций KeServiceDescriptorTable. Таблица системных функций KeServiceDescriptorTableShadow. Понятие UI-потока. Защита от перехвата (Kernel Patch Protection) в 64-разрядной ОС Windows.

55. Перехват API-вызовов менеджера объектов ОС Windows в режиме ядра.

56. Перехват API-вызовов создания и уничтожения процессов и потоков ОС Windows в режиме ядра.

57. Перехват операций с реестром в ОС Windows в режиме ядра.

58. Перехват операций с файлами в ОС Windows в режиме ядра. Мини-фильтры файловой системы.