**Введение в защищенный режим**

**Проблемы реального режима:**

* ОС и все программы используют общую память
  + Ошибка в одной из программ может нарушить согласованной данных в других программах и в самой ОС.
  + Количество одновременно запущенных программ ограничено размерами ОЗУ.
* Отсутствует аппаратная поддержка многозадачности.
  + Многозадачность можно эмулировать но для этого требуется, чтобы все программы «вели себя честно».

Многозадачность – способность ОС обеспечивать одновременное выполнение нескольких программ

**Виды многозадачности:**

* **Кооперативная** – при которой переключение задач переходит при вызове определенных функций ОС
* **Вытесняющая** – ОС сама решает, в какой момент выполнить переключение контекста
* Количество ядер процессора меньше количества программ.
  + Одновременно может выполняться только часть запущенных программ
  + Требуется переключаться между программами
* Какую информацию о программе нужно сохранять для такого переключения?
  + Регистры
  + Проследить, чтобы в памяти не поменялось

Контекст (потока) – информация, достаточная для возобновления выполнения программы:

* Значения регистров
* Состояние оперативной памяти

Эмуляция многозадачности

* ОС подписывается на прерывание от таймера
  + В обработчике ОС решает, нужно ли переключаться на другую задачу
  + Переключение:
    - Сохранить контекст прерванной задачи
    - Восстановить контекст какой-либо другой задачи.
* То же самое можно делать при вызове программой функций ОС.

Защищенный режим

* Введен в 80286, доработан в 80386
* Используется современными ОС
  + 64-битный режим IA32e является под режимом protected mode
* Реализует аппаратную поддержку для разграничения приложений:
  + Сегментация
  + Страничная адресация (подкачка)
* Вводится понятие колец защиты:
  + Ring 0 – самый привилегированный (для ОС)
  + Ring 3 – для прикладных программ
  + Ring 1 и Ring 2, как правил, не используются из соображений производительности. (Мб ток для драйверов, и то не юзаются)
* Сегментные регистры хранят не номера сегментов, а селекторы.
  + ОС строит в ОЗУ специальный **таблицы дескрипторов**, в которых для всех сегментов задаются:
    - Расположение в физической памяти
    - Размер
    - Уровень привилегий дескриптора (DPL);
    - Другие характеристики
  + Селектор состоит из нескольких частей:
    - Биты 0-1 задают **запрашиваемый** уровень привилегий (RPL)
    - Бит 2 выбирает таблицу дескрипторов, содержащую описание сегмента
    - Остальные биты (3-15) задают индекс в таблицы дескрипторов
  + Селектор в CS **текущий** уровень привилегий (CPL)
  + При выполнении команды:
    - Значения CPL, DPL, DPR проверяются на соответствие ряду правил
    - Если правила нарушаются:
      * Команда не выполняется
      * Генерируется исключение
* Сегменты могут выходить за границы физической памяти
* Адресное пространство – диапазон адресов, которые можно задать при обращение к памяти
  + В защищенном режиме становится **виртуальным.**
* Некоторые инструкции считаются привилегированными и могут выполняться только при **CPL = 0**
  + Т.е. могут выполнятся только ОС
  + При попытке выполнения с CPL > 0 – исключение
* ОС может разрешить выполнение некоторых таких инструкций на других уровнях.
* Прерывания теперь делятся на:
  + Прерывания:
    - Аппаратные события
    - Инструкции int
  + Исключения:
    - Ошибочные ситуации
* Механизм обработки одинаковый, полностью подчинен ОС.
* Вместо IVT используется IDT
  + IVT – массив адресов обработчиков, расположенный по адресу 0000:0000
  + IDT – массив дескрипторов:
    - Расположение в памяти выбирает ОС
    - Кроме адреса обработчика задается уровень привилегий дескриптора (DRL) и ряд других свойств
* ОС может включить **страничной адресации**:
  + Виртуальное адресное пространство разбивается на страницы:
    - Как правило, размером 4 КБ каждая.
  + Каждой странице в виртуальном адресном пространстве может быть поставлена в соответствие страница в физической памяти.
  + В защищенном режиме страницы имеют также следующие свойства:
    - Доступ на чтение (да/нет)
    - Доступ на запись (да/нет)
    - Доступ на выполнение (да/нет)
    - И др.

Программирование в Windows

* Windows настраивает все сегментные регистры на сегменты размером 4 ГБ.
  + Адресное пространство программы – 4 ГБ
    - Старшие 2 ГБ используются ОС.
    - Программе доступны для использования только младшие 2 ГБ.
    - Можно настроить «1 к 3» (large-address aware)
* Задача:
  + Написать “Hello World”