1.1. Переключення процесора в захищений режим

Перед переключенням у захищений режим потрібно заборонити переривання, а також зберегти логічну адресу вершини стека реального режиму, наприклад, в сегменті даних:

Top_real_mode dd ?

Переключение задач осуществляется, если:

- текущая задача выполняет дальний JMP или CALL на шлюз задачи или прямо на TSS;
- текущая задача выполняет IRET, если флаг NT равен 1;
- происходит прерывание или исключение, в качестве обработчика которого в IDT записан шлюз задачи.

При переключении процессор выполняет следующие действия:

1. Для команд CALL и JMP проверяет привилегии (CPL текущей задачи и RPL селектора новой задачи не могут быть больше, чем DPL шлюза или TSS, на который передается управление).
2. Проверяется дескриптор TSS (его бит присутствия и лимит).
3. Проверяется, что новый TSS, старый TSS и все дескрипторы сегментов находятся в страницах, отмеченных как присутствующие.
4. Сохраняется состояние задачи.
5. Загружается регистр TR. Если на следующих шагах происходит исключение, его обработчику придется доделывать переключение задач, вместо того чтобы повторять ошибочную команду.
6. Тип новой задачи в дескрипторе изменяется на занятый и устанавливается флаг TS в CR0.
7. Загружается состояние задачи из нового TSS: LDTR, CR3, EFLAGS, EIP, регистры общего назначения и сегментные регистры.

Если переключение задачи вызывается командами JUMP, CALL, прерыванием или

исключением, селектор TSS предыдущей задачи записывается в поле связи новой задачи и устанавливается флаг NT. Если флаг NT установлен, команда IRET выполняет обратное переключение задач.

При любом запуске задачи ее тип изменяется в дескрипторе на занятый. Попытка вызвать такую задачу приводит к #GP, сделать задачу снова свободной можно, только завершив ее командой IRET или переключившись на другую задачу командой JMP.