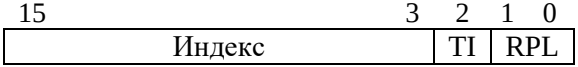
Разбор контрольной работы № 2

1	Защищенный режим процессоров x86
1. Описать формат селектора сегмента в МП Intel x86.	
2. Какие таблицы используются при сегментном преобразовании адреса в защищенном режиме МП Intel x86?	
3. Какие обращения к памяти осуществляются при выполнении команды LDS SI, [BX] в защищенном режиме МП Intel x86?	
4. Какие особые случаи (и при каких условиях) могут возникнуть при выполнении команды DIV word ptr [BX] в защищенном режиме МП Intel x86?	
5. Дано содержимое регистров (SP)=0100H, (SS)=0030H, (Flags)=0240H. Команда INT 8 имеет смещение 00A0H в сегменте с селектором 0020H. Определите содержимое SP, SS, IP, CS, IF и трех верхних слов стека после выполнения команды INT 8 в защищенном режиме МП Intel x86, если обработчик прерывания описан 16-битным шлюзом специального прерывания. Переключения уровня привилегий не происходит.	

Задание 3

Какие обращения к памяти осуществляются при выполнении команды LDS SI, [BX] в защищенном режиме МП Intel x86?

В случае успешного выполнения команды
1. Первое обращение к памяти по адресу
Addr1 = Базовый адрес сегмента DS (из теневого регистра для DS) + (BX);
BX <- Mem{Addr1}; Смещение
DS<- Mem{Addr1+2}; Селектор



2. Второе обращение к памяти по адресу
Addr2 = Базовый адрес GDT (из GDTR) + Индекс*8 (TI = 0);
Addr2 = Базовый адрес LDT (из теневого регистра для LDTR) + Индекс*8 (TI = 1)
Теневой регистр для DS <- Mem{Addr2}; 8 байт дескриптора

Задание 4.

Какие особые случаи и при каких условиях могут возникнуть при выполнении команды DIV word ptr [BX] в защищенном режиме МП Intel x86?

1. Особый случай общей защиты 13, если сегментный регистр DS загружен нулевым селектором.

2. Особый случай общей защиты 13, если смещение в сегменте данных (содержимое регистра BX+1) превышает максимальное смещение сегмента данных из теневого регистра для DS

(BX) + 1 > Предел;

3. Ошибка деления 0, если частное не помещается в отведенный формат 16 бит, если делитель равен 0.

Задание 5

Дано содержимое регистров (SP)=0100H, (SS)=0030H, (Flags)=0240H. Команда INT 8 имеет смещение 00A0H в сегменте с селектором 0020H. Определите содержимое SP, SS, IP, CS, IF и трех верхних слов стека после выполнения команды INT 8 в защищенном режиме МП Intel x86, если обработчик прерывания описан 16-битным шлюзом специального прерывания. Переключения уровня привилегий не происходит.

В случае успешного выполнения команды
IF не изменяется; шлюз специального прерывания
Mem{SS:SP-2} = M{SS:00FEh} <- Flags = 0240h;
Mem{SS:SP-4} = M{SS:00FCh}<- CS = 0020h;
Mem{SS:SP-6} = M{SS:00FAh}<- IP = 00A2h; длина команды INT 8 – 2 байта
SP<- (SP) -6 = 00FAh
SS не изменяется
IP<- M{базовый адрес IDT из IDTR + 8*8}; смещение точки входа в обработчик прерывания
CS<- M{базовый адрес IDT из IDTR + 8*8 + 2}; сегмент точки входа в обработчик прерывания

Задание 3-5 (устные комментарии)

Какие обращения к памяти осуществляются при выполнении команды;
Какие особые случаи и при каких условиях могут возникнуть;
Определить содержимое регистров и стека.

Варианты команд

```
MOV DS, AX
MOV SS, AX
LFS EDI, [EBP+4]
LDS SI, [BP+10]
BOUND SI, dword ptr [BX]
POP DS
INTO
INT n
FAR JMP dword ptr [BX]
FAR CALL dword ptr [bx]
```