



ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно
&& видно?



Напишите в чат, если есть проблемы!

Ставьте если все хорошо

Защищенный режим

Перехват прерываний в RM

Сегментная организация памяти



Три режима работы:

- Реальный
- Защищённый
- Виртуальный

Увеличенный размер регистров:

- 32-ые регистры
- 4GB памяти

Наиболее важное:

- ✓ Аппаратная многозадачность
- ✓ Одновременное выполнение нескольких программ
- ✓ Изоляция программ друг от друга
- ✓ Использование виртуальной памяти
- ✓ Разграничение доступа – 4 уровня привилегий

Специальные регистры:

- Cr0
- Cr3
- GDTR
- LDTR
- IDTR

Организация памяти

- Сегментная
- Страничная

Разные виды адресов:

- Логический (виртуальный)
- Линейный
- Физический

Связанные понятия

- Дескрипторы
- Селекторы

Из реального режима в защищённый



Global Descriptor Table

System Table Registers

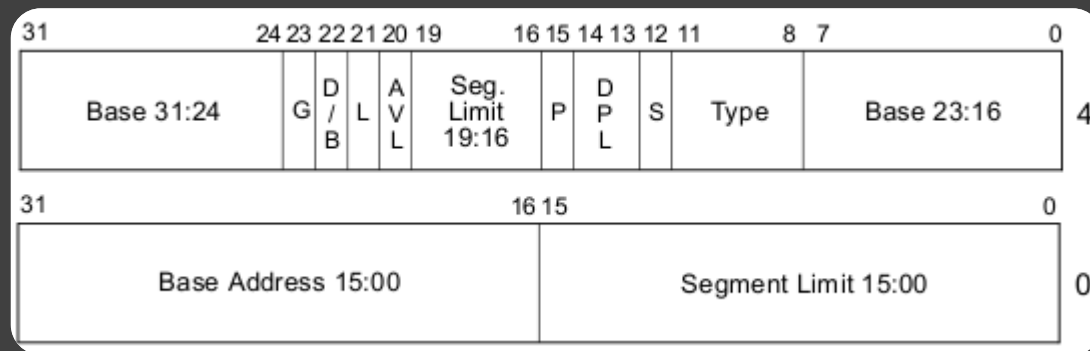
	47(79)	16 15	0
GDTR	32(64)-bit Linear Base Address		16-Bit Table Limit
IDTR	32(64)-bit Linear Base Address		16-Bit Table Limit

System Segment Registers

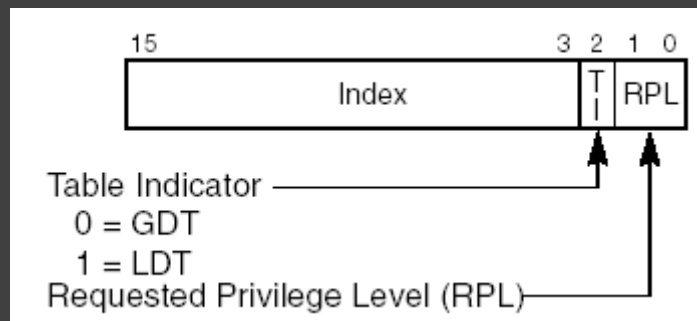
Segment Descriptor Registers (Automatically Loaded)

	15	0	Attributes		
Task Register	Seg. Sel.	32(64)-bit Linear Base Address	Segment Limit		
LDTR	Seg. Sel.	32(64)-bit Linear Base Address	Segment Limit		

Дескриптор – описатель всех сегментов



Индекс дескриптора в GDT



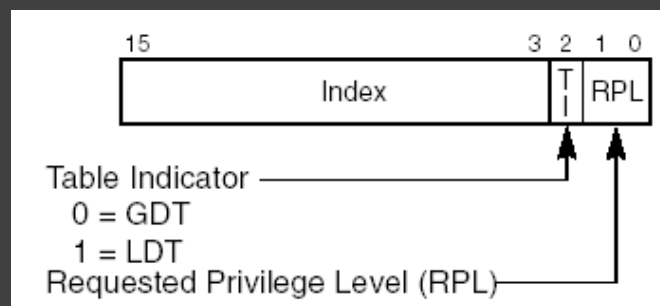
TI = 0 → GDT

RPL = 0 → режим ядра

TI = 1 → LDT

RPL = 3 → режим пользователя

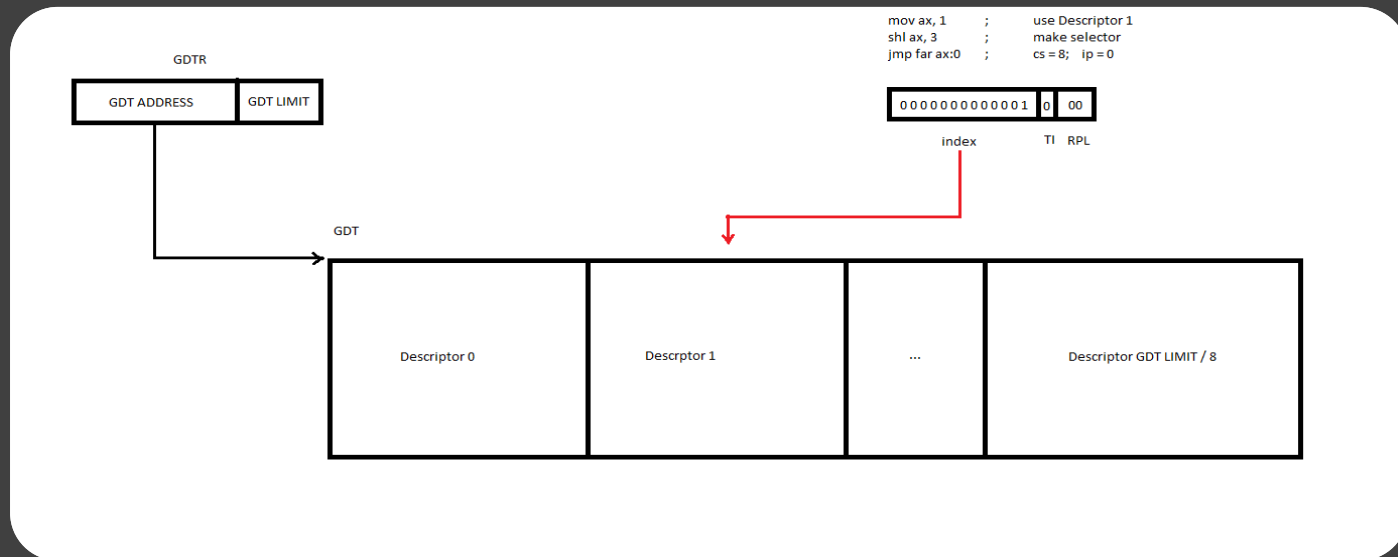
Индекс дескриптора в GDT



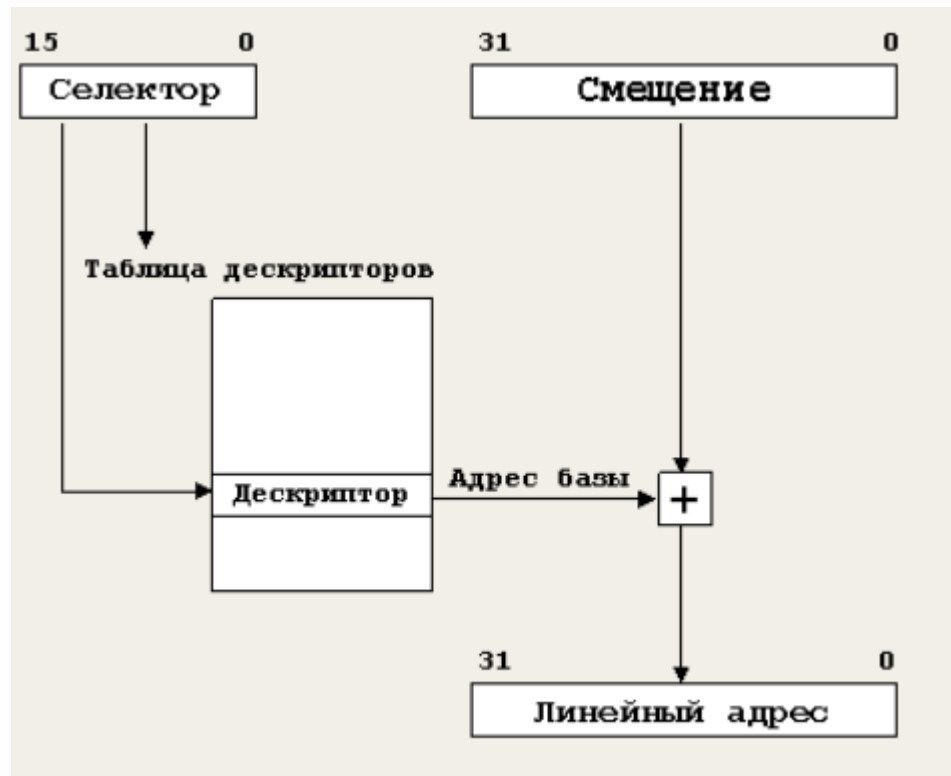
Селектор кода в ядре: 0x08 = 00000000000001 00 0

Селектор данных в ядре: 0x10 = 00000000000010 00 0

Селектор состоит из индекса сегмента в GDT, TI и RPL



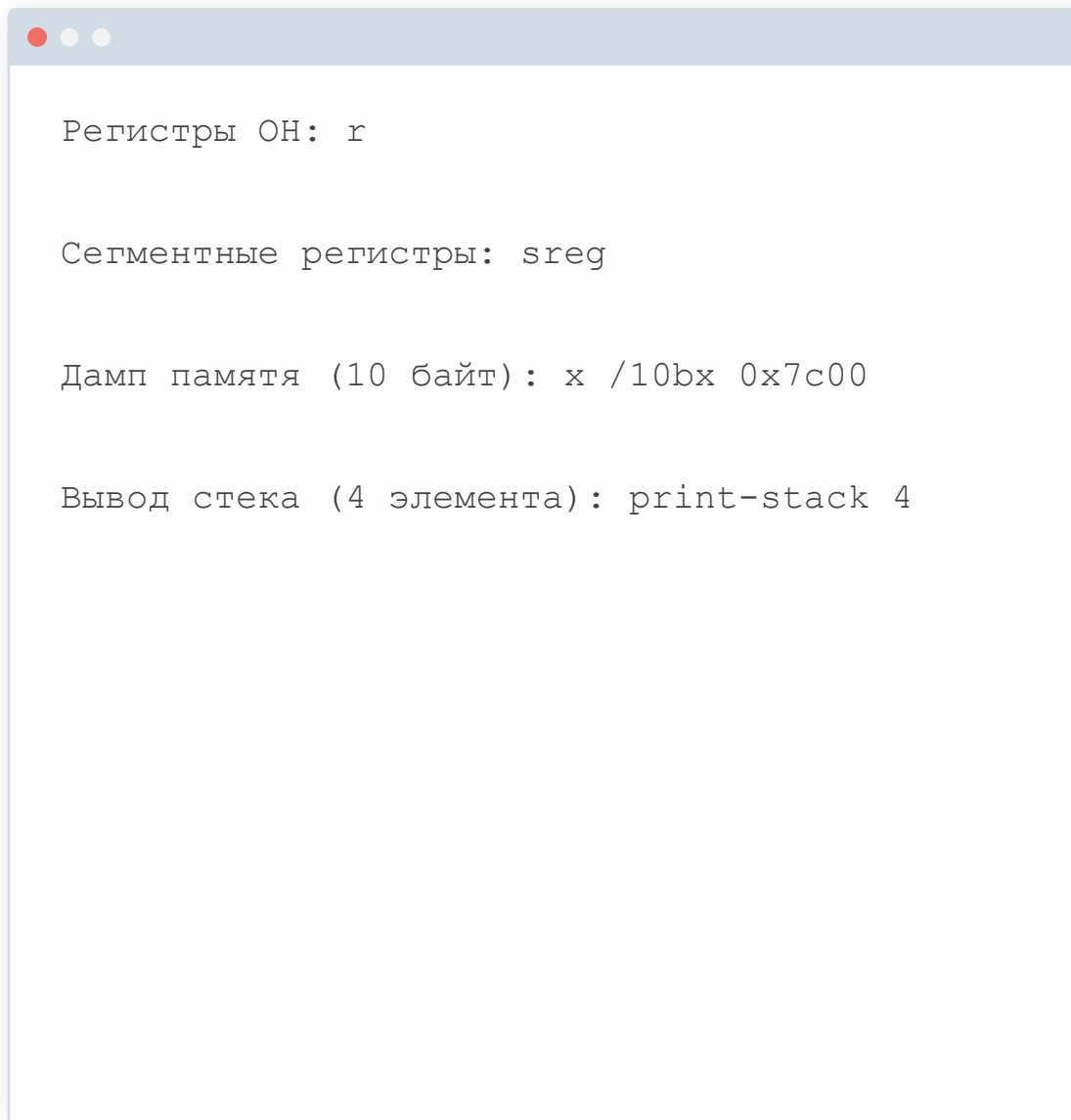
Преобразование логического адреса в линейный



Линейный адрес == физическому!

Настраиваем Bochs

```
# configuration file generated by Bochs
plugin_ctrl: unmapped=1, biosdev=1, speaker=1, extfpuirq=1, parallel=1, serial=1, gameport=1, iodebug=1
config_interface: win32config
display_library: win32
memory: host=32, guest=32
romimage: file="D:\Program Files (x86)\Bochs-2.6.8\BIOS-bochs-latest"
vgaromimage: file="D:\Program Files (x86)\Bochs-2.6.8\VGABIOS-lgpl-latest"
boot: floppy
floppy_bootsig_check: disabled=0
floppya: type=1_44, 1_44="D:\Languages\fasm\programs\segmodel.bin", status=inserted, write_protected=0
floppyb: type=1_44, 1_44="D:\Languages\fasm\programs\floppy2.bin", status=inserted, write_protected=0
ata0: enabled=1, ioaddr1=0x1f0, ioaddr2=0x3f0, irq=14
ata0-master: type=none
ata0-slave: type=none
ata1: enabled=1, ioaddr1=0x170, ioaddr2=0x370, irq=15
ata1-master: type=none
ata1-slave: type=none
ata2: enabled=0
ata3: enabled=0
pci: enabled=1, chipset=i440fx
vga: extension=vbe, update_freq=5, realtime=1
cpu: count=1, ips=4000000, model=bx_generic, reset_on_triple_fault=1, cpuid_limit_winnt=0, ignore_bad_msrs=1, mwait_is_nop=0
cpuid: level=0, stepping=3, model=3, family=6, vendor_string="GenuineIntel", brand_string="Intel(R) Pentium(R) 4 CPU"
cpuid: mmx=1, apic=xapic, simd=sse2, sse4a=0, misaligned_sse=0, sep=1, movbe=0, adx=0
cpuid: aes=0, sha=0, xsave=0, xsaveopt=0, x86_64=1, 1g_pages=0, pcid=0, fsgsbase=0
cpuid: smep=0, smap=0, mwait=1, vmx=1
print_timestamps: enabled=0
debugger_log: -
magic_break: enabled=1
port_e9_hack: enabled=0
private_colormap: enabled=0
clock: sync=none, time0=local, rtc_sync=0
# no cmosimage
# no loader
log: -
logprefix: %t%e%d
debug: action=ignore
info: action=report
error: action=report
panic: action=ask
keyboard: type=mf, serial_delay=250, paste_delay=100000, user_shortcut=none
mouse: type=ps2, enabled=0, toggle=ctrl+mbutton
sound: waveoutdrv=win, waveout=none, waveindrv=win, wavein=none, midioutdrv=win, midiout=none
speaker: enabled=1, mode=sound
parport1: enabled=1, file=none
parport2: enabled=0
com1: enabled=1, mode=null
com2: enabled=0
com3: enabled=0
com4: enabled=0
```



```
Регистры OH: r

Сегментные регистры: sreg

Дамп памяти (10 байт): x /10bx 0x7c00

Вывод стека (4 элемента): print-stack 4
```

консольные команды
дебагера bochs

консольные команды дебагера bochs

Если параметр `magic_break` включен:

```
magic_break: enabled=1
```

То, можно в любое место кода вставить команду

```
xchg bx, bx
```

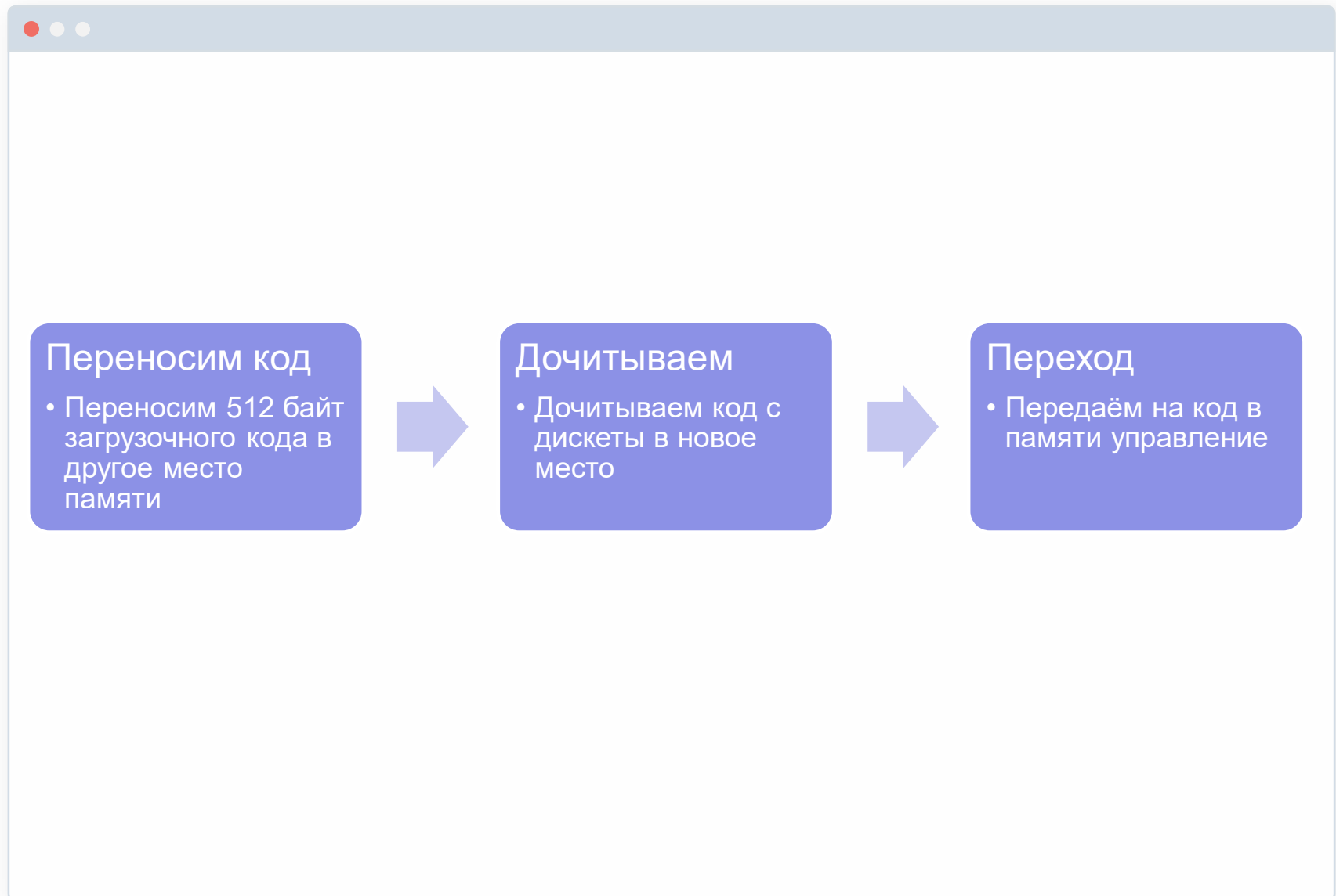
Тогда, `bochsdbg` брякнется на этой команде

```
;clrscr
mov ax,3
int 10h
mov ax, 0xb800
mov es, ax
lea si, str
xor di, di
mov ah, 7 ;абтибут
L:
  lodsb
  stosw ;!пишем вместе с атрибутом
  test al, al
  jnz L
str db 'hello', 0
INT 19h
```

Таблица атрибутов

Атрибут состоит из x:y: x - цвет фона, y - цвет символа

Код	Цвет	Код	Цвет
0h	Черный	8h	Серый
1h	Синий	9h	Голубой
2h	Зеленый	0Ah	Салатовый
3h	Бирюзовый	0Bh	Светло-бирюзовый
4h	Красный	0Ch	Розовый
5h	Фиолетовый	0Dh	Светло-фиолетовый
6h	Коричневый	0Eh	Желтый
7h	Белый	0Fh	Ярко-белый



Первые 512 байт

- 16-разрядный код
- Копируют данные дискеты в новое место
- Переводят процессор в PM



Вторые 512 кода

- 32 разрядный код
- Тестовое использование селекторов

```
mov ax, 3
int 10h
    cld
    xor ax, ax

    mov ds, ax
    mov si, CURRENT_OFFSET

    mov di, ax
    mov ax, NEW_SEG
    mov es, ax

    mov cx, 0x200
    mov bx, cx
    rep movsb

    mov ah, 2
    mov al, 1
    mov dx, 0
    mov cx, 2
    int 13h

    push NEW_SEG
    push NEW_OFFSET-CURRENT_OFFSET
    retf
```

NEW_OFFSET:

```
NEW_OFFSET:
    in al, 0x92
    or al, 2
    out 0x92, al

    cli
    mov al, 0x8F
    out 0x70, al
    in al, 0x71

xchg bx, bx
    mov eax, NEW_SEG
    shl eax, 4                ;physical address = segmeng*0x10 + offset
    add eax, GDT-CURRENT_OFFSET
    mov [(GDTR-CURRENT_OFFSET) + 2], eax    ;physical address of GDT table

    lgdt fword [GDTR-CURRENT_OFFSET]
    mov eax, cr0
    or al, 1
    mov cr0, eax

xchg bx, bx
    jmp fword 8: pm_Main-CURRENT_OFFSET
```

```
use32
pm_Main:
    mov ax, 0x10
    mov ds, ax
    mov fs, ax
    mov ss, ax
    mov esp, -1
    mov ax, 18h
    mov gs, ax

    mov esi, Hello-CURRENT_OFFSET
    call print
    hlt
    jmp $

print:
    pushad
    mov ah, 7
    xor ebx, ebx
    xchg ebx, ebx

puts:
    mov al, byte [cs:esi+ebx]
    mov [gs:(ebx*2)], ax
    inc ebx
    test al, al
    jnz puts
    popad
    hlt
    ret

Hello db 'pm_Main', 0
```

ДЗ

Переключить
процессор в
защищённый режим

Вопросы???





Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!

