Белорусский Государственный Университет Информатики и Радиоэлектроники

Кафедра ЭВМ

Отчет по лабораторной работе № 7

# Тема: «Защищенный и реальный режим процессора. Переход из одного режима в другой и обработка прерываний»

Выполнил студент гр.950502: Проверил:

Киреев Ю.В. Одинец Д.Н.

Минск 2021

# Задание

Написать программу, которая выполняет следующие действия:

* 1. Переход из реального режима в защищенный.
  2. Перехватывает аппаратное прерывание от клавиатуры и заданное аппаратное прерывание, в обработчике которого выполняет определенные действия. Номер аппаратного прерывания задается по вариантам (***два варианта)***.

1. Прерывание от таймера.
2. Прерывание от часов реального времени.
   1. По наступлению определенного события выполняет обратный переход из защищенного режима в реальный и завершает свою работу.

Для прерываний от таймера и часов реального времени обработчик прерывания должен отслеживать количество вызовов прерывания и отсчитывать секунды, выводя их на экран. Количество секунд после которых выполняется обратный переход в реальный режим и выход из программы (то самое определенное событие) считывается с клавиатуры перед переходом в защищенный режим.

Для прерывания от клавиатуры необходимо считывать скан-коды клавиш и выводить их на экран. По нажатию определенной клавиши (любой на выбор студента) осуществляется обратный переход в реальный режим и выход из программы.

При выполнении данной лабораторной работы должны быть соблюдены следующие условия:

1. После завершения работы программы компьютер должен продолжать корректно функционировать. Зависания, перезагрузки и другие аналогичные

«события» недопустимы.

1. Переход в защищенный режим процессора должен быть выполнен по алгоритму, используемому в процессорах начиная с 386. Переход в защищенный режим с использованием алгоритма для 286 процессора недопустим.

# Разработка алгоритма

* 1. Структура программы

Программа состоит из нескольких процедур: BUFFER\_CLEAR – процедура очистки буфера

BUFFER\_OUTPUT – процедура вывода буфера через видеопамять CLR\_SCR – процедура очистки экрана

KEYBOARD\_HANDLER – обработчик прерывания от клавиатуры TIMER\_HANDLER – обработчик прерывания системного таймера DUMMY\_IRQ\_MASTER/SLAVE – заглушка для обработчиков прерываний ведущего/ведомого контроллера

EXC\_HANDLER – обработчик исключений BYTE\_TO\_HEX – перевод числа в шестнадцатеричный вид DIGIT\_TO\_DEC – перевод цифры в десятичный вид WORD\_TO\_DEC – перевод числа в десятичный вид

INPUT – ввод количества секунд

* 1. Описание переменных

GDT – глобальная таблица дескрипторов;

CODE\_RM\_DESC – селектор сегмента кода реального режима; DATA\_DESC – селектор сегмента данных реального/защищенного режима; STACK\_DESC – сегмент стека реального/защищенного режима; TEXT\_DESC – селектор видеопамяти компьютера;

CODE\_PM\_DESC – селектор кода защищенного режима; CODE\_IDT – селектор таблицы IDT;

TIME – время, которое компьютер будет находится в защищенном режиме COUNT – количество вызовов прерывания системного таймера KEY\_SCAN\_CODE – последняя введенная клавиша

SECOND – текущая секунда времени

* 1. Описание алгоритма программы

При запуске пользователь вводит число секунд, которые программа будет находиться в защищенном режиме. Затем после нажатия любой клавиши программа начинает переходить в защищенный режим.

Для этого:

* + 1. Подготавливаются часы RTC – формат представления данных в двоичном виде
    2. Разрешается линия A20
    3. Сохраняются маски прерываний
    4. Запрещаются маскируемые и немаскируемые прерывания
    5. Таблица GDT заполняется дескрипторами
    6. Заполняется таблица IDT
    7. 0 бит регистра cr0 ставится в 1
    8. Перезагружается регистр cs.
    9. Перезагружаются другие сегментные регистры
    10. В стек заносятся регистр cs и точка возврата в реальный режим 11.В стек заносятся точка входа в защищенный режим и дескриктор

сегмента кода защищенного режима

12.Переинициализируется контроллеры прерываний на шлюзы 20 – 2F 13.Разрешаются маскируемые и немаскируемые прерывания 14.Программа переходит в сегмент 32-битного кода

1. Вызываются процедуры очистки экрана и вывода сообщения
2. Запускается бесконечный цикл, в котором обработчики прерываний клавиатуры и таймера производят необходимые действия
3. По команде выхода программа возвращается в сегмент кода реального режима
4. По возвращению вновь запрещаются все прерывания
5. Контроллеры прерываний переинициализируются на старые вектора 20.Устанавливаются новые лимиты сегментов данных, кода и стека 21.Перезагружается регистр cs
6. Включается реальный режим
7. Восстанавливаются сегментные регистры
8. Восстанавливаются маски контроллера прерываний 25.Запрещается линия A20

26.Программа выводит сообщение о успешном возврате

# Текст программы

.386P

.MODEL LARGE

;Структуры данных

S\_DESC struc ;Структура сегментного дескриптора

LIMIT dw 0 ;Лимит сегмента (15:00)

BASE\_L dw 0 ;Адрес базы, младшая часть (15:0)

BASE\_M db 0 ;Адрес базы, средняя часть (23:16)

ACCESS db 0 ;Байт доступа

ATTRIBS db 0 ;Лимит сегмента (19:16) и атрибуты

BASE\_H db 0 ;Адрес базы, старшая часть S\_DESC ends

I\_DESC struc ;Структура дескриптора таблицы прерываний

OFFS\_L dw 0 ;Адрес обработчика (0:15)

SEL dw 0 ;Селектор кода, содержащего код обработчика

PARAM\_CNT db 0 ;Параметры

ACCESS db 0 ;Уровень доступа

OFFS\_H dw 0 ;Адрес обработчика (31:16) I\_DESC ends

R\_IDTR struc ;Структура IDTR

LIMIT dw 0

IDT\_L dw 0 ;Смещение биты (0-15)

IDT\_H dw 0 ;Смещение биты (31-16) R\_IDTR ends

;Флаги уровней доступа сегментов

ACS\_PRESENT EQU 10000000B ;PXXXXXXX - бит присутствия, сегмент присутствует в оперативной памяти ACS\_CSEG EQU 00011000B ;XXXXIXXX - тип сегмента, для данных = 0, для кода 1

ACS\_DSEG EQU 00010000B ;XXXSXXXX - бит сегмента, данный объект сегмент(системные объекты могут быть не сегменты) ACS\_READ EQU 00000010B ;XXXXXXRX - бит чтения, возможность чтения из другого сегмента

ACS\_WRITE EQU 00000010B ;XXXXXXWX - бит записи, для сегмента данных разершает запись ACS\_CODE = ACS\_PRESENT or ACS\_CSEG ;AR сегмента кода

ACS\_DATA = ACS\_PRESENT or ACS\_DSEG or ACS\_WRITE;AR сегмента данных ACS\_STACK= ACS\_PRESENT or ACS\_DSEG or ACS\_WRITE;AR сегмента стека ACS\_INT\_GATE EQU 00001110B

ACS\_TRAP\_GATE EQU 00001111B ;XXXXSICR - сегмент, подчиненный сегмент кода, доступен для чтения ACS\_IDT EQU ACS\_DATA ;AR таблицы IDT

ACS\_INT EQU ACS\_PRESENT or ACS\_INT\_GATE ACS\_TRAP EQU ACS\_PRESENT or ACS\_TRAP\_GATE

ACS\_DPL\_3 EQU 01100000B ;X<DPL,DPL>XXXXX - привелегии доступа, доступ может получить любой код

;Сегмент кода реального режима CODE\_RM segment para use16 CODE\_RM\_BEGIN = $

assume cs:CODE\_RM,DS:DATA,ES:DATA ;Инициализация регистров для ассемблирования START:

mov ax,DATA ;Инициализиция сегментных регистров mov ds,ax

mov es,ax

lea dx,MSG\_ENTER mov ah,9h

int 21h

call INPUT ;Ввод времени

mov ds:[TIME], al lea dx,MSG\_HELLO mov ah,9h

int 21h mov ah,7h

int 21h ;Ожидание подтверждения

PREPARE\_RTC: ;Подготовка часов RTC

mov al,0Bh

out 70h,al ;Выбрать регистр состояния 0Bh

in al,71h ;Получить значение регистра 0Bh

or al,00000100b ;Установить бит DM в 1 - формат представления время в двоичном виде

out 71h,al ;Записать измененное значение

ENABLE\_A20: ;Открыть линию A20

in al,92h

or al,2 ;Установить бит 1 в 1

out 92h,al

;Или так для старых компьютеров

;mov al, 0D1h

;out 64h, al

;mov al, 0DFh

;out 60h, al

SAVE\_MASK: ;Сохранить маски прерываний in al,21h

mov INT\_MASK\_M,al in al,0A1h

mov INT\_MASK\_S,al

DISABLE\_INTERRUPTS: ;Запрет маскируемых и немаскируемых прерываний

cli ;Запрет маскирумых прерываний

in al,70h

or al,10000000b ;Установить 7 бит в 1 для запрета немаскируемых прерываний out 70h,al

nop

LOAD\_GDT: ;Заполнить глобальную таблицу дескрипторов mov ax,DATA

mov dl,ah xor dh,dh shl ax,4 shr dx,4 mov si,ax mov di,dx

WRITE\_GDT: ;Заполнить дескриптор GDT lea bx,GDT\_GDT

mov ax,si mov dx,di

add ax,offset GDT adc dx,0

mov [bx][S\_DESC.BASE\_L],ax mov [bx][S\_DESC.BASE\_M],dl mov [bx][S\_DESC.BASE\_H],dh

WRITE\_CODE\_RM: ;Заполнить дескриптор сегмента кода реального режима lea bx,GDT\_CODE\_RM

mov ax,cs xor dh,dh mov dl,ah shl ax,4 shr dx,4

mov [bx][S\_DESC.BASE\_L],ax mov [bx][S\_DESC.BASE\_M],dl mov [bx][S\_DESC.BASE\_H],dh

WRITE\_DATA: ;Записать дескриптор сегмента данных lea bx,GDT\_DATA

mov ax,si mov dx,di

mov [bx][S\_DESC.BASE\_L],ax mov [bx][S\_DESC.BASE\_M],dl mov [bx][S\_DESC.BASE\_H],dh

WRITE\_STACK: ;Записать дескриптор сегмента стека lea bx, GDT\_STACK

mov ax,ss xor dh,dh mov dl,ah shl ax,4 shr dx,4

mov [bx][S\_DESC.BASE\_L],ax mov [bx][S\_DESC.BASE\_M],dl mov [bx][S\_DESC.BASE\_H],dh

WRITE\_CODE\_PM: ;Записать дескриптор кода защищенного режима lea bx,GDT\_CODE\_PM

mov ax,CODE\_PM xor dh,dh

mov dl,ah shl ax,4 shr dx,4

mov [bx][S\_DESC.BASE\_L],ax mov [bx][S\_DESC.BASE\_M],dl mov [bx][S\_DESC.BASE\_H],dh or [bx][S\_DESC.ATTRIBS],40h

WRITE\_IDT: ;Записать дескриптор IDT

lea bx,GDT\_IDT mov ax,si

mov dx,di

add ax,OFFSET IDT adc dx,0

mov [bx][S\_DESC.BASE\_L],ax mov [bx][S\_DESC.BASE\_M],dl mov [bx][S\_DESC.BASE\_H],dh mov IDTR.IDT\_L,ax

mov IDTR.IDT\_H,dx

FILL\_IDT: ;Заполнить таблицу дескрипторов шлюзов прерываний

irpc N, 0123456789ABCDEF ;Заполнить шлюзы 00-0F исключениями lea eax, EXC\_0&N

mov IDT\_0&N.OFFS\_L,ax shr eax, 16

mov IDT\_0&N.OFFS\_H,ax endm

irpc N, 0123456789ABCDEF ;Заполнить шлюзы 10-1F исключениями lea eax, EXC\_1&N

mov IDT\_1&N.OFFS\_L,ax shr eax, 16

mov IDT\_1&N.OFFS\_H,ax endm

lea eax, TIMER\_HANDLER ;Поместить обработчик прерывания таймера на 20 шлюз mov IDT\_TIMER.OFFS\_L,ax

shr eax, 16

mov IDT\_TIMER.OFFS\_H,ax

lea eax, KEYBOARD\_HANDLER ;Поместить обработчик прерывания клавиатуры на 21 шлюз mov IDT\_KEYBOARD.OFFS\_L,ax

shr eax, 16

mov IDT\_KEYBOARD.OFFS\_H,ax

irpc N, 234567 ;Заполнить вектора 22-27 заглушками lea eax,DUMMY\_IRQ\_MASTER

mov IDT\_2&N.OFFS\_L, AX shr eax,16

mov IDT\_2&N.OFFS\_H, AX endm

irpc N, 89ABCDEF ;Заполнить вектора 28-2F заглушками lea eax,DUMMY\_IRQ\_SLAVE

mov IDT\_2&N.OFFS\_L,ax shr eax,16

mov IDT\_2&N.OFFS\_H,ax endm

lgdt fword ptr GDT\_GDT ;Загрузить регистр GDTR

lidt fword ptr IDTR ;Загрузить регистр IDTR

mov eax,cr0 ;Получить управляющий регистр cr0

or al,00000001b ;Установить бит PE в 1

mov cr0,eax ;Записать измененный cr0 и тем самым включить защищенный режим

OVERLOAD\_CS: ;Перезагрузить сегмент кода на его дескриптор db 0EAH

dw $+4

dw CODE\_RM\_DESC

OVERLOAD\_SEGMENT\_REGISTERS: ;Переинициализировать остальные сегментные регистры на дескрипторы mov ax,DATA\_DESC

mov ds,ax mov es,ax

mov ax,STACK\_DESC mov ss,ax

xor ax,ax

mov fs,ax ;Обнулить регистр fs

mov gs,ax ;Обнулить регистр gs

lldt ax ;Обнулить регистр LDTR - не использовать таблицы локальных дескрипторов

PREPARE\_TO\_RETURN:

push cs ;Сегмент кода

push offset BACK\_TO\_RM ;Смещение точки возврата

lea edi,ENTER\_PM ;Получить точку входа в защищенный режим

mov eax,CODE\_PM\_DESC ;Получить дескриптор кода защищенного режима

push eax ;Занести их в стек

push edi

REINITIALIAZE\_CONTROLLER\_FOR\_PM: ;Переинициализировать контроллер прерываний на вектора 20h, 28h mov al,00010001b ;ICW1 - переинициализация контроллера прерываний

out 20h,al ;Переинициализируем ведущий контроллер

out 0A0h,al ;Переинициализируем ведомый контроллер

mov al,20h ;ICW2 - номер базового вектора прерываний

out 21h,al ;ведущего контроллера

mov al,28h ;ICW2 - номер базового вектора прерываний

out 0A1h,al ;ведомого контроллера

mov al,04h ;ICW3 - ведущий контроллер подключен к 3 линии out 21h,al

mov al,02h ;ICW3 - ведомый контроллер подключен к 3 линии out 0A1h,al

mov al,11h ;ICW4 - режим специальной полной вложенности для ведущего контроллера out 21h,al

mov al,01h ;ICW4 - режим обычной полной вложенности для ведомого контроллера out 0A1h,al

mov al, 0 ;Размаскировать прерывания

out 21h,al ;Ведущего контроллера

out 0A1h,al ;Ведомого контроллера

ENABLE\_INTERRUPTS\_0: ;Разрешить маскируемые и немаскируемые прерывания in al,70h

|  |  |  |
| --- | --- | --- |
| and | al,01111111b | ;Установить 7 бит в 0 для запрета немаскируемых прерываний |
| out | 70h,al |  |
| nop |  |  |
| sti |  | ;Разрешить маскируемые прерывания |

GO\_TO\_CODE\_PM: ;Переход к сегменту кода защищенного режима db 66h

retf

BACK\_TO\_RM: ;Точка возврата в реальный режим

cli ;Запрет маскируемых прерываний

in al,70h ;И не маскируемых прерываний

or AL,10000000b ;Установить 7 бит в 1 для запрета немаскируемых прерываний out 70h,AL

nop

REINITIALISE\_CONTROLLER: ;Переиницализация контроллера прерываний

mov al,00010001b ;ICW1 - переинициализация контроллера прерываний

out 20h,al ;Переинициализируем ведущий контроллер

out 0A0h,al ;Переинициализируем ведомый контроллер

mov al,8h ;ICW2 - номер базового вектора прерываний

out 21h,al ;ведущего контроллера

mov al,70h ;ICW2 - номер базового вектора прерываний

out 0A1h,al ;ведомого контроллера

mov al,04h ;ICW3 - ведущий контроллер подключен к 3 линии out 21h,al

mov al,02h ;ICW3 - ведомый контроллер подключен к 3 линии out 0A1h,al

mov al,11h ;ICW4 - режим специальной полной вложенности для ведущего контроллера out 21h,al

mov al,01h ;ICW4 - режим обычной полной вложенности для ведомого контроллера out 0A1h,al

PREPARE\_SEGMENTS: ;Подготовка сегментных регистров для возврата в реальный режим mov GDT\_CODE\_RM.LIMIT,0FFFFh ;Установка лимита сегмента кода в 64KB

mov GDT\_DATA.LIMIT,0FFFFh ;Установка лимита сегмента данных в 64KB

mov GDT\_STACK.LIMIT,0FFFFh ;Установка лимита сегмента стека в 64KB

db 0EAH ;Перезагрузить регистр cs

dw $+4

dw CODE\_RM\_DESC ;На сегмент кода реального режима

mov ax,DATA\_DESC ;Загрузим сегментные регистры дескриптором сегмента данных mov ds,ax

mov es,ax mov fs,ax mov gs,ax

mov ax,STACK\_DESC

mov ss,ax ;Загрузим регистр стека дескриптором стека

ENABLE\_REAL\_MODE: ;Включим реальный режим mov eax,cr0

and al,11111110b ;Обнулим 0 бит регистра cr0 mov cr0,eax

db 0EAH dw $+4

dw CODE\_RM ;Перезагрузим регистр кода mov ax,STACK\_A

mov ss,ax mov ax,DATA mov ds,ax mov es,ax xor ax,ax mov fs,ax mov gs,ax

mov IDTR.LIMIT, 3FFH

mov dword ptr IDTR+2, 0 lidt fword ptr IDTR

REPEAIR\_MASK: ;Восстановить маски прерываний mov al,INT\_MASK\_M

out 21h,al ;Ведущего контроллера

mov al,INT\_MASK\_S

out 0A1h,al ;Ведомого контроллера

ENABLE\_INTERRUPTS: ;Разрешить маскируемые и немаскируемые прерывания in al,70h

and al,01111111b ;Установить 7 бит в 0 для разрешения немаскируемых прерываний out 70h,al

nop

sti ;Разрешить маскируемые прерывания

DISABLE\_A20: ;Закрыть вентиль A20

in al,92h

and al,11111101b ;Обнулить 1 бит - запретить линию A20 out 92h, al

EXIT: ;Выход из программы

mov ax,3h

int 10H ;Очистить видео-режим

lea dx,MSG\_EXIT mov ah,9h

int 21h ;Вывести сообщение

mov ax,4C00h

int 21H ;Выход в dos

INPUT proc near ;Процедура ввода время-нахождения в защищенном режиме mov ah,0ah

xor di,di

mov dx,offset ds:[INPUT\_TIME] int 21h

mov dl,0ah mov ah,02 int 21h

mov si,offset INPUT\_TIME+2 cmp byte ptr [si],"-"

jnz ii1 mov di,1 inc si

II1:

xor ax,ax mov bx,10

II2:

mov cl,[si] cmp cl,0dh jz ii3

cmp cl,'0' jl er

cmp cl,'9' ja er

sub cl,'0' mul bx add ax,cx

inc si jmp ii2

ER:

mov dx, offset MSG\_ERROR mov ah,09

int 21h int 20h

II3:

ret

INPUT endp

SIZE\_CODE\_RM = ($ - CODE\_RM\_BEGIN) ;Лимит сегмента кода CODE\_RM ends

;Сегмент кода реального режима CODE\_PM segment para use32 CODE\_PM\_BEGIN = $

assume cs:CODE\_PM,ds:DATA,es:DATA ;Указание сегментов для компиляции

ENTER\_PM: ;Точка входа в защищенный режим

call CLRSCR ;Процедура очистки экрана

xor edi,edi ;В edi смещение на экране

lea esi,MSG\_HELLO\_PM ;В esi адрес буфера

call BUFFER\_OUTPUT ;Вывести строку-приветствие в защищенном режиме

add edi,160 ;Перевести курсор на следующую строку lea esi,MSG\_KEYBOARD

call BUFFER\_OUTPUT ;Вывести поле для вывода скан-кода клавиатуры mov edi,320

lea esi,MSG\_TIME

call BUFFER\_OUTPUT ;Вывести поле для вывода время mov edi,480

lea esi,MSG\_COUNT call BUFFER\_OUTPUT mov DS:[COUNT],0

WAITING\_ESC: ;Ожидание нажатия кнопки выхода из защищенного режима

jmp WAITING\_ESC ;Если был нажат не ESC

EXIT\_PM: ;Точка выхода из 32-битного сегмента кода

db 66H

retf ;Переход в 16-битный сегмент кода

EXIT\_FROM\_INTERRUPT: ;Точка выхода для выхода напрямую из обработчика прерываний popad

pop es pop ds

pop eax ;Снять со стека старый EIP

pop eax ;CS

pop eax ;И EFLAGS

sti ;Обязательно, без этого обработка аппаратных прерываний отключена db 66H

retf ;Переход в 16-битный сегмент кода

WORD\_TO\_DEC proc near ;Процедура перевода слова в строку pushad

movzx eax,ax xor cx,cx mov bx,10

LOOP1: ;Цикл по извлечению цифры

xor dx,dx div bx add dl,'0' push dx inc cx test ax,ax

jnz LOOP1

LOOP2: ;Цикл по заполнению буфера

pop dx mov [di],dl inc di

loop LOOP2 popad

ret

WORD\_TO\_DEC endp

DIGIT\_TO\_HEX proc near ;Процедура перевода цифры в шеснадцатеричный вид add al,'0'

cmp al,'9'

jle DTH\_END add al,7

DTH\_END:

ret DIGIT\_TO\_HEX endp

BYTE\_TO\_HEX proc near ;Процедура перевода числа в шеснадцатеричный вид push ax

mov ah,al shr al,4

call DIGIT\_TO\_HEX mov [di],al

inc di mov al,ah

and al,0Fh

call DIGIT\_TO\_HEX mov [di],al

inc di pop ax ret

BYTE\_TO\_HEX endp M = 0

IRPC N, 0123456789ABCDEF

EXC\_0&N label word ;Обработчики исключений cli

jmp EXC\_HANDLER

endm

M = 010H

IRPC N, 0123456789ABCDEF ;Обработчики исключений EXC\_1&N label word

cli

jmp EXC\_HANDLER

endm

EXC\_HANDLER proc near ;Процедура вывода обработки исключений

call CLRSCR ;Очистка экрана

lea esi, MSG\_EXC mov edi, 40\*2

call BUFFER\_OUTPUT ;Вывод предупреждения

pop eax ;Снять со стека старый EIP

pop eax ;CS

pop eax ;И EFLAGS

sti ;Обязательно, без этого обработка аппаратных прерываний отключена db 66H

retf ;Переход в 16-битный сегмент кода

EXC\_HANDLER ENDP

DUMMY\_IRQ\_MASTER proc near ;Заглушка для аппаратных прерываний ведущего контроллера push eax

mov al,20h out 20h,al pop eax iretd

DUMMY\_IRQ\_MASTER endp

DUMMY\_IRQ\_SLAVE proc near ;Заглушка для аппаратных прерываний ведомого контроллера push eax

mov al,20h out 20h,al out 0A0h,al pop eax iretd

DUMMY\_IRQ\_SLAVE endp

TIMER\_HANDLER proc near ;Обработчик прерываний системного таймера push ds

push es

pushad ;Занести в стек расширенные регистры общего назначения

mov ax,DATA\_DESC ;Переинициализировать сегментные регистры mov ds,ax

inc ds:[COUNT] ;Увеличить значение счетчика lea edi,ds:[BUFFER\_COUNT]

mov ax,ds:[COUNT]

call WORD\_TO\_DEC ;Преобразовать счётчик в строку mov edi,538

lea esi,BUFFER\_COUNT

call BUFFER\_OUTPUT ;Вывести значение счетчика

SHOW\_TIMER:

mov al,0h ;Выбрать регистр секунд cmos

out 70h,al

in al,71h ;Прочитать значение секунд

cmp al,ds:[SECOND] ;Если секунда та же самая

je SKIP\_SECOND ;То пропустить вывод

mov ds:[SECOND],al ;Иначе записать значение новой секунды

mov al,ds:[TIME] ;Получить значение оставшегося время

cmp ds:[TIME],0 ;Если время подошло к концу

je DISABLE\_PM ;То на выход из защищенного режима

xor ah,ah

lea edi,ds:[BUFFER\_TIME]

call WORD\_TO\_DEC ;Преобразовать его в строку

mov edi,422

lea esi,BUFFER\_TIME

call BUFFER\_OUTPUT ;Вывести значение оставшегося время

dec ds:[TIME] ;Уменьшить значение оставшегося времени lea esi,BUFFER\_TIME

call BUFFER\_CLEAR ;Очистка буфера

jmp SKIP\_SECOND ;На выход из обработки время

DISABLE\_PM: ;Выход из защищенного режима

mov al,20h out 20h,al

db 0eah ;Дальний jmp

dd OFFSET EXIT\_FROM\_INTERRUPT ;На метку

dw CODE\_PM\_DESC ;В сегменте

SKIP\_SECOND: ;Секунда та же, не надо производить никаких действий mov al,20h

out 20h,al ;Отпарвка сигнала контроллеру прерываний

popad pop es pop ds iretd

TIMER\_HANDLER endp

KEYBOARD\_HANDLER proc near ;Обработчик прерывания клавиатуры push ds

push es

pushad ;Сохранить расширенные регистры общего назначения

in al,60h ;Считать скан код последней нажатой клавиши ;

cmp al,1 ;Если был нажат 'ESC'

je KEYBOARD\_EXIT ;Тогда на выход из защищенного режима

mov ds:[KEY\_SCAN\_CODE],al ;Записать его в память lea edi,ds:[BUFFER\_SCAN\_CODE]

mov al,ds:[KEY\_SCAN\_CODE] xor ah,ah

call BYTE\_TO\_HEX ;Преобразовать скан-код в строку

mov edi,200

lea esi,BUFFER\_SCAN\_CODE

call BUFFER\_OUTPUT ;Вывести строку со скан-кодом jmp KEYBOARD\_RETURN

KEYBOARD\_EXIT:

mov al,20h out 20h,al db 0eah

dd OFFSET EXIT\_FROM\_INTERRUPT dw CODE\_PM\_DESC

KEYBOARD\_RETURN:

mov al,20h

out 20h,al ;Отпарвка сигнала контроллеру прерываний

popad ;Восстановить значения регистров

pop es pop ds

iretd ;Выход из прерывания

KEYBOARD\_HANDLER endp

CLRSCR proc near ;Процедура очистки консоли push es

pushad

mov ax,TEXT\_DESC ;Поместить в ax дескриптор текста

mov es,ax xor edi,edi

mov ecx,80\*25 ;Количество символов в окне

mov ax,700h rep stosw popad

pop es ret

CLRSCR endp

BUFFER\_CLEAR proc near ;Процедура очистки буфера mov al,' '

mov [esi+0],al mov [esi+1],al mov [esi+2],al mov [esi+3],al mov [esi+4],al mov [esi+5],al mov [esi+6],al mov [esi+7],al ret

BUFFER\_CLEAR endp

BUFFER\_OUTPUT proc near ;Процедура вывода текстового буфера, оканчивающегося 0 push es

PUSHAD

mov ax,TEXT\_DESC ;Поместить в es селектор текста mov es,ax

OUTPUT\_LOOP: ;Цикл по выводу буфера

lodsb or al,al

jz OUTPUT\_EXIT ;Если дошло до 0, то конец выхода stosb

inc edi

jmp OUTPUT\_LOOP

OUTPUT\_EXIT: ;Выход из процедуры вывода

popad pop es ret

BUFFER\_OUTPUT ENDP

SIZE\_CODE\_PM = ($ - CODE\_PM\_BEGIN) CODE\_PM ENDS

;Сегмент данных реального/защищенного режима

DATA segment para use16 ;Сегмент данных реального/защищенного режима DATA\_BEGIN = $

;GDT - глобальная таблица дескрипторов GDT\_BEGIN = $

GDT label word ;Метка начала GDT (GDT: не работает) GDT\_0 S\_DESC <0,0,0,0,0,0>

GDT\_GDT S\_DESC <GDT\_SIZE-1,,,ACS\_DATA,0,> GDT\_CODE\_RM S\_DESC <SIZE\_CODE\_RM-1,,,ACS\_CODE,0,> GDT\_DATA S\_DESC <SIZE\_DATA-1,,,ACS\_DATA+ACS\_DPL\_3,0,> GDT\_STACK S\_DESC <1000h-1,,,ACS\_DATA,0,>

GDT\_TEXT S\_DESC <2000h-1,8000h,0Bh,ACS\_DATA+ACS\_DPL\_3,0,0> GDT\_CODE\_PM S\_DESC <SIZE\_CODE\_PM-1,,,ACS\_CODE+ACS\_READ,0,> GDT\_IDT S\_DESC <SIZE\_IDT-1,,,ACS\_IDT,0,>

GDT\_SIZE = ($ - GDT\_BEGIN) ;Размер GDT

;Селлекторы сегментов

CODE\_RM\_DESC = (GDT\_CODE\_RM - GDT\_0) DATA\_DESC = (GDT\_DATA - GDT\_0) STACK\_DESC = (GDT\_STACK - GDT\_0) TEXT\_DESC = (GDT\_TEXT - GDT\_0) CODE\_PM\_DESC = (GDT\_CODE\_PM - GDT\_0) IDT\_DESC = (GDT\_IDT - GDT\_0)

;IDT - таблица дескрипторов прерываний

IDTR R\_IDTR <SIZE\_IDT,0,0> ;Формат регистра ITDR

IDT label word ;Метка начала IDT

IDT\_BEGIN = $

IRPC N, 0123456789ABCDEF

IDT\_0&N I\_DESC <0, CODE\_PM\_DESC,0,ACS\_TRAP,0> ; 00...0F ENDM

IRPC N, 0123456789ABCDEF

IDT\_1&N I\_DESC <0, CODE\_PM\_DESC, 0, ACS\_TRAP, 0> ; 10...1F ENDM

IDT\_TIMER I\_DESC <0,CODE\_PM\_DESC,0,ACS\_INT,0> ;IRQ 0 - прерывание системного таймера IDT\_KEYBOARD I\_DESC <0,CODE\_PM\_DESC,0,ACS\_INT,0> ;IRQ 1 - прерывание клавиатуры

IRPC N, 23456789ABCDEF

IDT\_2&N I\_DESC <0, CODE\_PM\_DESC, 0, ACS\_INT, 0> ; 22...2F ENDM

SIZE\_IDT = ($ - IDT\_BEGIN)

MSG\_HELLO db "press any key to go to the protected mode",13,10,"$" MSG\_HELLO\_PM db "wellcome in protected mode",0

MSG\_EXIT db "wellcome back to real mode",13,10,"$"

MSG\_KEYBOARD db "keyboard scan code: | press 'ESC' to come back to the real mode",0 MSG\_TIME db " | go back to RM in XXXXXXX seconds",0

MSG\_COUNT db "quantity of interrupt calls:",0 MSG\_EXC db "exception: XX",0

MSG\_ENTER db "enter time in protected mode: $" MSG\_ERROR db "incorrect error$"

HEX\_TAB db "0123456789ABCDEF" ;Таблица номеров исключений

ESP32 dd 1 dup(?) ;Указатель на вершину стека

INT\_MASK\_M db 1 dup(?) ;Значение регистра масок ведущего контроллера

INT\_MASK\_S db 1 dup(?) ;Значение регистра масок ведомого контроллера

KEY\_SCAN\_CODE db 1 dup(?) ;Ска-код последней нажатой клавиши

SECOND db 1 dup(?) ;Текущее значение секунд

TIME db 1 dup(10) ;Время нахождения в зазищенном режиме

COUNT dw 1 dup(0) ;Количество вызовов прерывания (диапазон от 0 до 65535)

BUFFER\_COUNT db 8 dup(' ') ;Буфер для вывода количества вызовов прерываинй db 1 dup(0)

BUFFER\_SCAN\_CODE db 8 dup(' ') ;Буфер для вывода скан-кода клавиатуры db 1 dup(0)

BUFFER\_TIME db 8 dup(' ') ;Буфер для вывода оставшегося время в защищенном режиме db 1 dup(0)

INPUT\_TIME db 6,7 dup(?) ;Буфер для ввода время

SIZE\_DATA = ($ - DATA\_BEGIN) ;Размер сегмента данных DATA ends

;Сегмент стека реального/защищенного режима STACK\_A segment para stack

db 1000h dup(?) STACK\_A ends end START

# Тестирование работы программы в DosBox-0.74 компилировалось в TASMе





