WYOS - Выпуск №15
Эксперименты в коде
commrade, Среда, 30 Июнь 2004, 23:45

Напиши свою ОС! #15

Привет вам, земляне!

Сегодня в рассылке особой какой-то темы, направления не будет, так как еще не готов окончательно материал. А выдавать, что то сырое мне не очень хочется. В этом номере я подведу итоги прошедшей недели, расскажу о ваших письмах по поводу рассылки, немножко расскажу о будущих темах.

Упражнение 1

Найдите и исправьте ошибки в текстах обеих программ.

Что касается этого упражнения, то здесь вы справились наполовину. То есть вариантов правильного кода
для загрузочного сектора было много, но наиболее правильнее у Dmitri Alexeenko
и Zensor.
<code style="color:green">
<pre>
org 7C00h

start:
mov ax,0b800h   ;0xb800 -- это адрес
;сегмента видеопамяти в текстовом режиме.
mov es,ax   ;копируем это значение
;в сегментный регистр es
xor di,di
mov ax,2041h
stosb
loop1: jmp loop1   ;команда jmp указывающая
;на саму себя
</pre>
</code>
Так же хочется сказать спасибо за присланные ответы и Zensor, и остальным кто
решился на подобный эксперимент.
Что же касаемо второй части первого упражнения, то здесь почему-то никто не решился попробовать свои силы.
Ну да это не страшно я все-таки добил приложение для записи кода в загрузочный сектор диска A.
Для начала создайте в BCB 5.0 новый проект. Переднюю панель приведите к виду как показано на рисунке.
<img src='files/images/articles/wyos/frontpanel.png' alt='frontpanel.jpg' width='514' height='354'>

Это что касается внешнего вида программы. А вот с кодом программы пришлось повозиться, здесь все
не так просто как казалось. Получившийся вариант кода показан ниже, от себя же я хочу сказать,
что по идее программа корректно должна работать как под Win98, так и под WinNT (правда под WinNT я ее
не тестировал.)

```
<code style="color:green">
<pre>
<i style="color:gray">//---------------------------------------------------------------------------</i>

#include &lt;vcl.h&gt;
#pragma hdrstop

#include "Unit1.h"
<i style="color:gray">//---------------------------------------------------------------------------</i>
#pragma package(smart_init)
#pragma resource "*.dfm"
TForm1 *Form1;
<i style="color:gray">//---------------------------------------------------------------------------</i>
__fastcall TForm1::TForm1(TComponent* Owner)
: TForm(Owner)
{

}
<i style="color:gray">//---------------------------------------------------------------------------</i>

void __fastcall TForm1::ReadClick(TObject *Sender)
{
int drive=0;<i style="color:gray">//drive=0 -диск A, drive=1 - диск B.</i>
int startinglogicalsector=0;<i style="color:gray">//сектор с которого начинаем </i>
int numberofsectors=1;<i style="color:gray">//кол-во секторов для чтения</i>


if(drive==-1 || startinglogicalsector==-1 || numberofsectors==-1)
{
MessageBox(Handle,"Ошибка при вводе параметров.",NULL,MB_OK|MB_ICONINFORMATION);
return;
}

if(!numberofsectors)
{
MessageBox(Handle,"Вы должны задать хотя бы один сектор для чтения.",
NULL,MB_OK|MB_ICONINFORMATION);
return;
}

PBYTE buff=(PBYTE)malloc(numberofsectors*512); <i style="color:gray">//для чтения секторов
```

</i>

```
#pragma pack(1)
struct
{
DWORD StartingSector;
WORD NumberOfSectors;
DWORD pBuffer;
} ControlBlock;
#pragma pack()

#pragma pack(1)
typedef struct _DIOC_REGISTERS
{
DWORD reg_EBX;
DWORD reg_EDX;
DWORD reg_ECX;
DWORD reg_EAX;
DWORD reg_EDI;
DWORD reg_ESI;
DWORD reg_Flags;
} DIOC_REGISTERS;
#pragma pack()

DIOC_REGISTERS reg;

OSVERSIONINFO vi;
vi.dwOSVersionInfoSize = sizeof vi; <i style="color:gray">// это обя</i>
GetVersionEx(&vi);
BOOL NT=(vi.dwPlatformId==VER_PLATFORM_WIN32_NT); <i style="color:gray">//проверка на
соответствие NT-</i>

HANDLE hFile;

if(!NT)
{
<i style="color:gray">//используем драйвер vwin32</i>
hFile=CreateFile("\\.\vwin32",0,0,NULL,0,FILE_FLAG_DELETE_ON_CLOSE,NULL);
if(hFile==INVALID_HANDLE_VALUE)
{
MessageBox(Handle,"Нет доступа к файлу vwin32.vxd.",NULL,MB_OK|MB_ICONSTOP);
return;
}
ControlBlock.StartingSector=startinglogicalsector;
ControlBlock.NumberOfSectors=numberofsectors;
ControlBlock.pBuffer=(DWORD)buff;
<i style="color:gray">// в SI помещаем: 0 - для чтения или 1 - для записи
// CX должно быть равно FFFFh для расширения 7305h прерывания int 21h
```

```
// DS:BX -> адрес структуры ControlBlock
// DL - номер диска (01h=A:, 02h=B: etc)</i>
reg.reg_ESI=0;
reg.reg_ECX=-1;
reg.reg_EBX=(DWORD)&ControlBlock;
reg.reg_EDX=drive+1;
reg.reg_EAX=0x7305;
DWORD cb;
<i style="color:gray">// 6 == VWIN32_DIOC_DOS_DRIVEINFO - вызываемая функция</i>
BOOL result=DeviceIoControl(hFile,6,&reg,sizeof reg,&reg,sizeof reg,&cb,0);
if(!result || (reg.reg_Flags & 0x0001))return; //произошла ошибка
}
else
{
<i style="color:gray">//WinNT</i>
DWORD bytesread;
char drive_name[] = "\\.\a:";
drive_name[4] += drive;
hFile=CreateFile(drive_name,GENERIC_READ,FILE_SHARE_READ|FILE_SHARE_WRITE,
NULL,OPEN_EXISTING,0,NULL);
if(hFile==INVALID_HANDLE_VALUE)
{
MessageBox(Handle,"Нет доступа к диску.",NULL,MB_OK|MB_ICONSTOP);
return;
}
SetFilePointer(hFile,512*startinglogicalsector,0,FILE_BEGIN);
if(!ReadFile(hFile,buff,numberofsectors*512,&bytesread,NULL))return;
}

CloseHandle(hFile);

Memo1->Clear();
AnsiString str="";
if(RadioGroup1->ItemIndex)
for(int i=0; i&lt;numberofsectors*512; ++i)
str=str+IntToHex(buff[i],2)+" ";
else
{
MessageBox( Handle,
"Вы выбрали TEXT режим вывода данных.nВсе символы с кодом ASCII 0 будут заменены на
пробелы.",
NULL,
MB_OK|MB_ICONINFORMATION);
<i style="color:gray">//для того что бы отобразить в Memo символы, следующие за символами
с кодом 0</i>
for(int i=0; i&lt;numberofsectors*512; ++i)
if(!buff[i])buff[i]=0x20;
str=(char*)buff+'';
```

```
}
Memo1->Lines->Add(str);

free(buff);

}
<i style="color:gray">//---------------------------------------------------------------------------</i>

void __fastcall TForm1::BrowseClick(TObject *Sender)
{
OpenDialog1->Execute();
Addres->Text=OpenDialog1->FileName;
}
<i style="color:gray">//---------------------------------------------------------------------------</i>
void __fastcall TForm1::WriteClick(TObject *Sender)
{
int drive=0;
int startinglogicalsector=0;
int numberofsectors=1;

int iFileHandle=FileOpen(OpenDialog1->FileName, fmOpenRead);
int iFileLength = FileSeek(iFileHandle,0,2);
FileSeek(iFileHandle,0,0);

Edit1->Text=iFileLength;

if(drive==-1 || startinglogicalsector==-1 || numberofsectors==-1)
{
MessageBox(Handle,"Ошибка привводе параметров.",NULL,MB_OK|MB_ICONINFORMATION);
return;
}

if(!numberofsectors)
{
MessageBox(Handle,"Вы должны задать хотя бы один сектор для чтения.",
NULL,MB_OK|MB_ICONINFORMATION);
return;
}

PBYTE buff=(PBYTE)malloc(numberofsectors*512); <i style="color:gray">//для записи в
загрузочный </i>
FileRead(iFileHandle, buff, iFileLength);
FileClose(iFileHandle);
buff[510]=0x55; <i style="color:gray">//обезательно, что бы в конце были </i>
buff[511]=0xaa;


#pragma pack(1)
```

struct
{
DWORD StartingSector;
WORD NumberOfSectors;
DWORD pBuffer;
} ControlBlock;
#pragma pack()

#pragma pack(1)
typedef struct _DIOC_REGISTERS
{
DWORD reg_EBX;
DWORD reg_EDX;
DWORD reg_ECX;
DWORD reg_EAX;
DWORD reg_EDI;
DWORD reg_ESI;
DWORD reg_Flags;
} DIOC_REGISTERS;
#pragma pack()

DIOC_REGISTERS reg;

OSVERSIONINFO vi;
vi.dwOSVersionInfoSize = sizeof vi;
GetVersionEx(&vi);
BOOL NT=(vi.dwPlatformId==VER_PLATFORM_WIN32_NT);
HANDLE hFile;

if(!NT)
{
//используем драйвер vwin32
hFile=CreateFile("\\.\vwin32",0,0,NULL,0,FILE_FLAG_DELETE_ON_CLOSE,NULL);
if(hFile==INVALID_HANDLE_VALUE)
{
MessageBox(Handle,"Нет доступа к файлу vwin32.vxd.",NULL,MB_OK|MB_ICONSTOP);
return;
}
ControlBlock.StartingSector=startinglogicalsector;
ControlBlock.NumberOfSectors=numberofsectors;
ControlBlock.pBuffer=(DWORD)buff;
// в SI помещаем: 0 - для чтения или 1 - для записи
// CX должно быть равно FFFFh для расширения 7305h прерывания int 21h
// DS:BX -> адрес структуры ControlBlock
// DL - номер диска (01h=A:, 02h=B: etc)
reg.reg_ESI=1;
reg.reg_ECX=-1;
reg.reg_EBX=(DWORD)&ControlBlock;

reg.reg_EDX=drive+1;
reg.reg_EAX=0x7305;
DWORD cb;
// 6 == VWIN32_DIOC_DOS_DRIVEINFO - вызываемая функция
BOOL result=DeviceIoControl(hFile,6,&reg,sizeof reg,&reg,sizeof reg,&cb,0);
if(!result || (reg.reg_Flags & 0x0001))return; //произошла
}
else
{
//WinNT
DWORD bytesread;
char drive_name[] = "\\.\a:";
drive_name[4] += drive;
hFile=CreateFile(drive_name,GENERIC_READ,FILE_SHARE_READ|FILE_SHARE_WRITE,
NULL,OPEN_EXISTING,0,NULL);
if(hFile==INVALID_HANDLE_VALUE)
{
MessageBox(Handle,"Нет доступа к диску.",NULL,MB_OK|MB_ICONSTOP);
return;
}
SetFilePointer(hFile,512*startinglogicalsector,0,FILE_BEGIN);
if(!WriteFile(hFile,buff,numberofsectors*512,&bytesread,NULL))return;
}

CloseHandle(hFile);
}
//---
</pre>
</code>
Если будут вопросы по поводу кода - пишите, будем разбираться.

Упражнение 2

Модифицируйте программу так, чтобы она выводила надписи на русском языке.
Честно говоря, здесь я, по-моему, перестарался. Как оказалось это не такая простая задача. Так что вопрос временно снимается с повестки дня, хотя, если будет желание, пишите - с радостью примем ваши варианты.

О будущем

В ближайших выпусках рассылки мы с вами рассмотрим вопросы запуска ОС, перехода в защищенный режим работы процессора.

Именно над этими вопросами я щас и потею. Ну вот и все на сегодня, наверное слишко коротко получилось, ну да ничего, на наш с вами век еще хватит и, кто знает, может быть среди вас, читающих эту рассылку, щас сидит и мотает на ус будущий Билл Гейтс (не к ночи будет сказано) или Питер Нортон. Дай вам Бог всем здоровья, удачи и счастья.

Ваш горячий товарищ commrade.