

18.12.2023

## Курс:

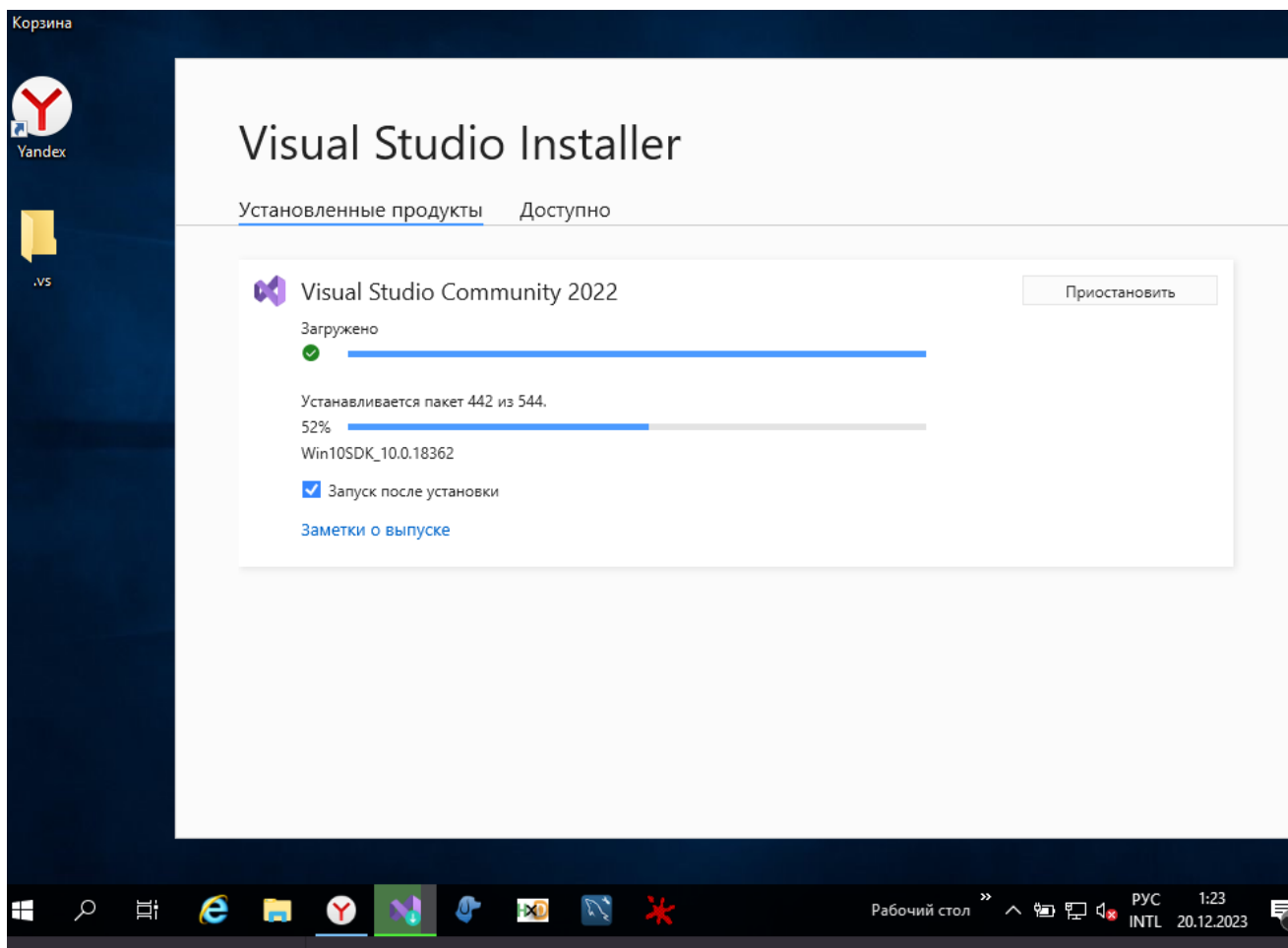
## Практическая работа к уроку № Lesson\_2

--

Знакомство с Ассемблером

Загружаем:

- virtualbox
- Win2019serv core2
- Visual Studio Community 2022  
<https://visualstudio.microsoft.com/ru/>  
<https://marketplace.visualstudio.com/>
  - JIT-debugger, SDK Windows 10, MSVC v143 32/64, C++ Basic ...
  - MASM  
<https://metanit.com/assembler/tutorial/1.4.php>
- ...
- OllyDBG 110  
<https://www.ollydbg.de/odbg110.zip>
- PPEE (puppy)  
<https://www.mzrst.com/>
- HxD  
<https://mh-nexus.de/en/hxd/>



ml.exe

```
C:\Program Files\Microsoft Visual  
Studio\2022\Community\VC\Tools\MSVC\14.35.32215\bin\Hostx86\x86
```

## Задание:

Разработать программу на языке Ассемблер, которая при старте должна запускать калькулятор Windows.

prog-home.exe

<https://learn.microsoft.com/ru-ru/windows/win32/api/winbase/nf-winbase-winexec>

```
les2.asm
```

```
.386  
.model flat, stdcall  
  
ExitProcess PROTO, ExitCodo:DWORD  
WinExec PROTO, lpCmdLine:DWORD, uCmdShow:DWORD  
  
_data segment
```

```

        lpCmdLine db 'calc', 0
_data ends

_text segment
start:

        push 1      ; значение SW_SHOWNORMAL
        push offset lpCmdLine    ; указатель на имя приложения
        call WinExec

        push 0
        call ExitProcess

_text ends
end start

```

## Компиляция

```

C:\Users\Администратор\Documents\GB>ml /c /coff les2.asm
Microsoft (R) Macro Assembler Version 14.35.32217.1
Copyright (C) Microsoft Corporation. All rights reserved.

Assembling: les2.asm

C:\Users\Администратор\Documents\GB>dir
Том в устройстве C не имеет метки.
Серийный номер тома: 0C0D-34C4

Содержимое папки C:\Users\Администратор\Documents\GB

20.12.2023  01:41    <DIR>          .
20.12.2023  01:41    <DIR>          ..
20.12.2023  01:30    <DIR>          .vs
19.12.2023  23:40             316 les2.asm
20.12.2023  01:41             692 les2.obj
                2 файлов             1 008 байт
                3 папок      6 370 045 952 байт свободно

```

```
C:\Users\Администратор\Documents\GB>link /SUBSYSTEM:WINDOWS les2.obj kernel32.lib
Microsoft (R) Incremental Linker Version 14.35.32217.1
Copyright (C) Microsoft Corporation. All rights reserved.

C:\Users\Администратор\Documents\GB>dir
Том в устройстве C не имеет метки.
Серийный номер тома: 0C0D-34C4

Содержимое папки C:\Users\Администратор\Documents\GB

20.12.2023  01:47    <DIR>        .
20.12.2023  01:47    <DIR>        ..
20.12.2023  01:30    <DIR>        .vs
19.12.2023  23:40                316 les2.asm
20.12.2023  01:47                3 072 les2.exe
20.12.2023  01:41                692 les2.obj
                3 файлов                4 080 байт
                3 папок   5 357 740 032 байт свободно
```

Заменяем название файла (скопируем) на *prog-home.exe* и запустим .exe

```
Администратор: x86 Native Tools Command Prompt for VS 2022

3 папок   5 357 740 032 байт свободно

C:\Users\Администратор\Documents\GB>cp les2.exe prog-home.exe
"cp" не является внутренней или внешней
командой, исполняемой программой или пакетным файлом.

C:\Users\Администратор\Documents\GB>copy les2.exe prog-home.exe
Скопировано файлов:          1.

C:\Users\Администратор\Documents\GB>dir
Том в устройстве C не имеет метки.
Серийный номер тома: 0C0D-34C4

Содержимое папки C:\Users\Администратор\Documents\GB

20.12.2023  01:54    <DIR>        .
20.12.2023  01:54    <DIR>        ..
20.12.2023  01:30    <DIR>        .vs
19.12.2023  23:40                316 les2.asm
20.12.2023  01:47                3 072 les2.exe
20.12.2023  01:41                692 les2.obj
20.12.2023  01:47                3 072 prog-home.exe
                4 файлов                7 152 байт
                3 папок   5 465 567 232 байт свободно

C:\Users\Администратор\Documents\GB>prog-home.exe
```

OllyDbg - prog-home.exe - [CPU - thread 00001A0C, module ntdll]

File View Debug Plugins Options Window Help

Registers (FPU)

EAX	7758E230	ntdll.7758E230
ECX	00000000	
EDX	00000000	
EBX	00000000	
ESP	017DF75C	
EBP	017DF918	
ESI	015E5558	
EDI	015E3268	
EIP	775B216C	ntdll.775B216C
C 0	ES 002B 32bit 0 (FFFFFFFF)	
P 1	CS 0023 32bit 0 (FFFFFFFF)	
A 0	SS 002B 32bit 0 (FFFFFFFF)	
Z 0	DS 002B 32bit 0 (FFFFFFFF)	
S 0	FS 0053 32bit 1077000 (FFF)	
T 0	GS 002B 32bit 0 (FFFFFFFF)	
D 0		
O 0	LastErr ERROR_SUCCESS (00000000)	
EFL	00000206	(NO, NB, NE, A, NS, PE, GE, G)
ST0	empty 0.0	
ST1	empty 0.0	
ST2	empty 0.0	
ST3	empty 0.0	
ST4	empty 0.0	
ST5	empty 0.0	
ST6	empty 0.0	
ST7	empty 0.0	

FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0  
FCW 027F Prec NEAR, S3 Mask 1 1 1 1 1 1

Address	Hex dump	ASCII
004B3000	63 61 6C 63 00 00 00 00	calc...
004B3008	00 00 00 00 00 00 00 00	
004B3010	00 00 00 00 00 00 00 00	
004B3018	00 00 00 00 00 00 00 00	
004B3020	00 00 00 00 00 00 00 00	
004B3028	00 00 00 00 00 00 00 00	
004B3030	00 00 00 00 00 00 00 00	
004B3038	00 00 00 00 00 00 00 00	
004B3040	00 00 00 00 00 00 00 00	
004B3048	00 00 00 00 00 00 00 00	
004B3050	00 00 00 00 00 00 00 00	
004B3058	00 00 00 00 00 00 00 00	
004B3060	00 00 00 00 00 00 00 00	
004B3068	00 00 00 00 00 00 00 00	
004B3070	00 00 00 00 00 00 00 00	
004B3078	00 00 00 00 00 00 00 00	
004B3080	00 00 00 00 00 00 00 00	
004B3088	00 00 00 00 00 00 00 00	
004B3090	00 00 00 00 00 00 00 00	
004B3098	00 00 00 00 00 00 00 00	
004B30A0	00 00 00 00 00 00 00 00	
004B30B0	00 00 00 00 00 00 00 00	

Process terminated, exit code 0

017DF75C 7758E406 RETURN to ntdll.  
017DF760 00000004  
017DF764 015E5558  
017DF768 00000010  
017DF76C 017DF7F0  
017DF770 017DF8BC  
017DF774 5948BF4E  
017DF778 7758E230 ntdll.7758E230  
017DF77C 7758E230 ntdll.7758E230  
017DF780 015E3268  
017DF784 775B216C ntdll.RtlUserThre  
017DF788 00000023  
017DF78C 00000020  
017DF790 00000004  
017DF794 00000000  
017DF798 00000004  
017DF79C 00000000  
017DF7A0 00000000  
017DF7A4 00000000  
017DF7A8 00000000  
017DF7AC 00000000  
017DF7B0 00001F30  
017DF7B4 0000FFFF

\*Выполнил: AndreiM