18.12.2023

Курс:

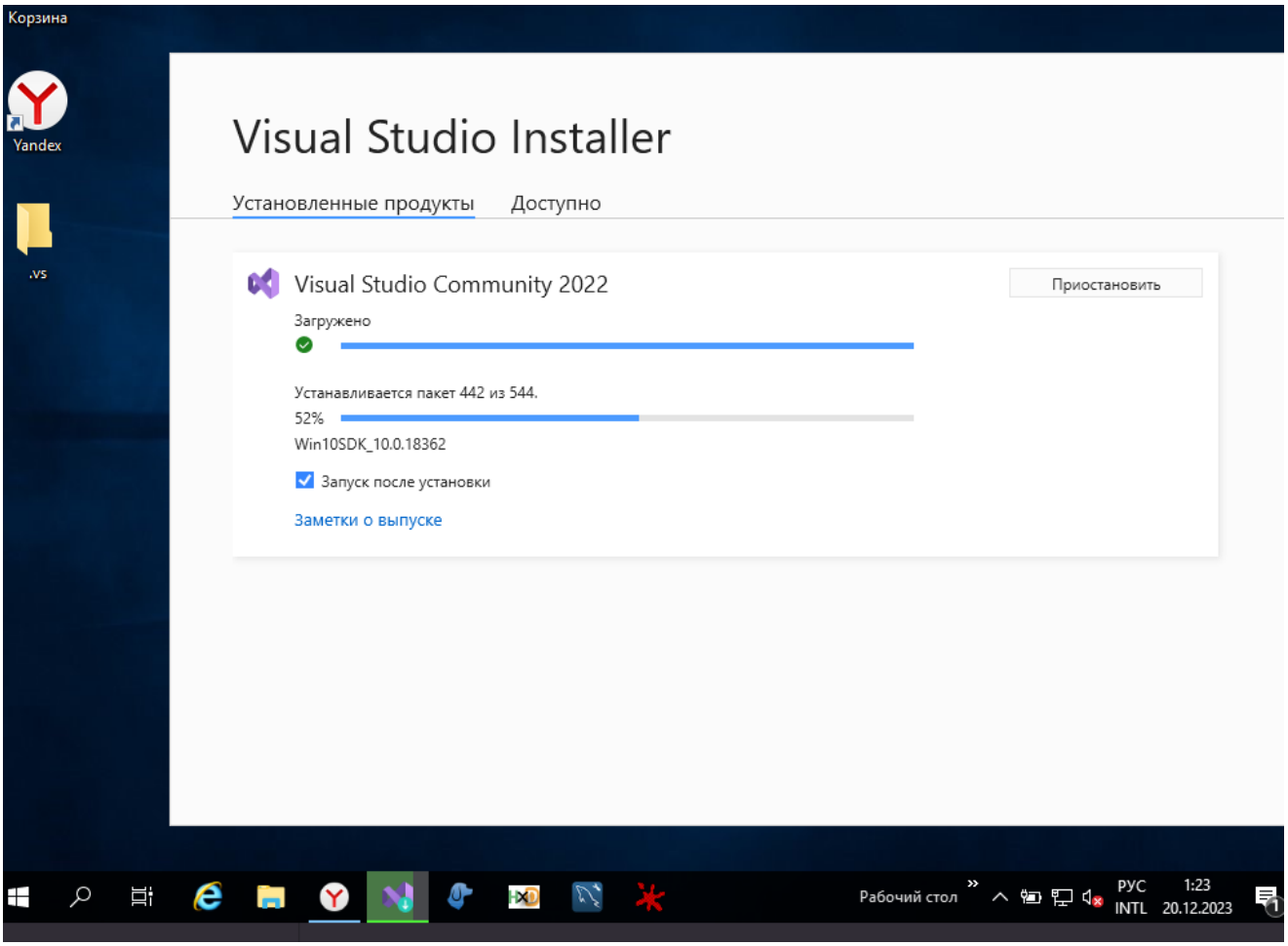
Практическая работа к уроку № Lesson_2

--

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:

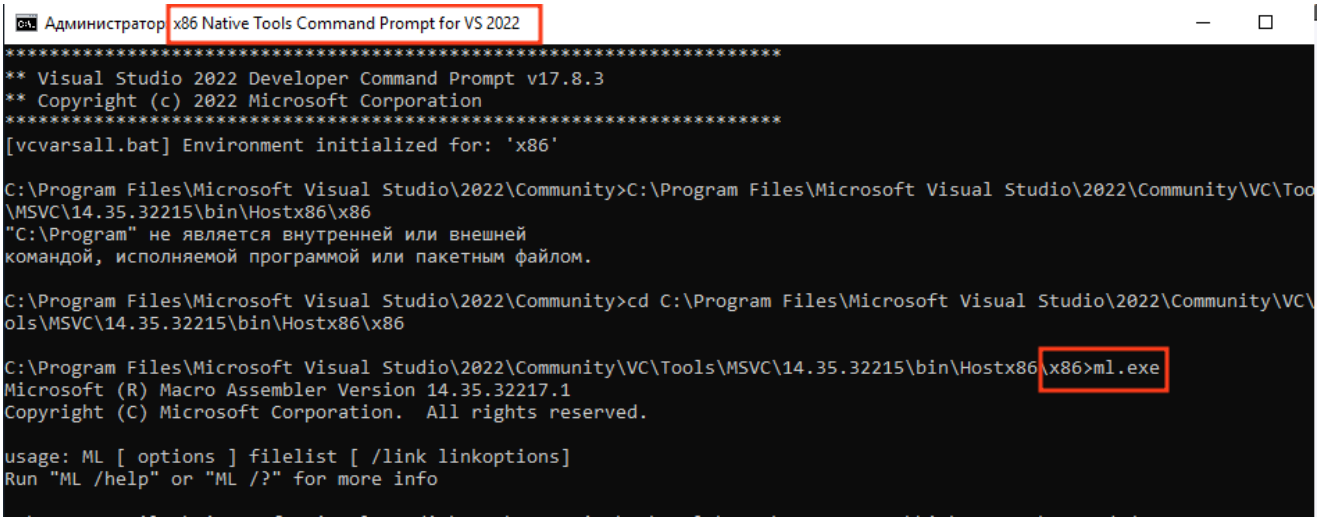
Разработать программу на языке Ассемблер, которая при старте должна запускать калькулятор Windows.
prog-home.exe

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
```



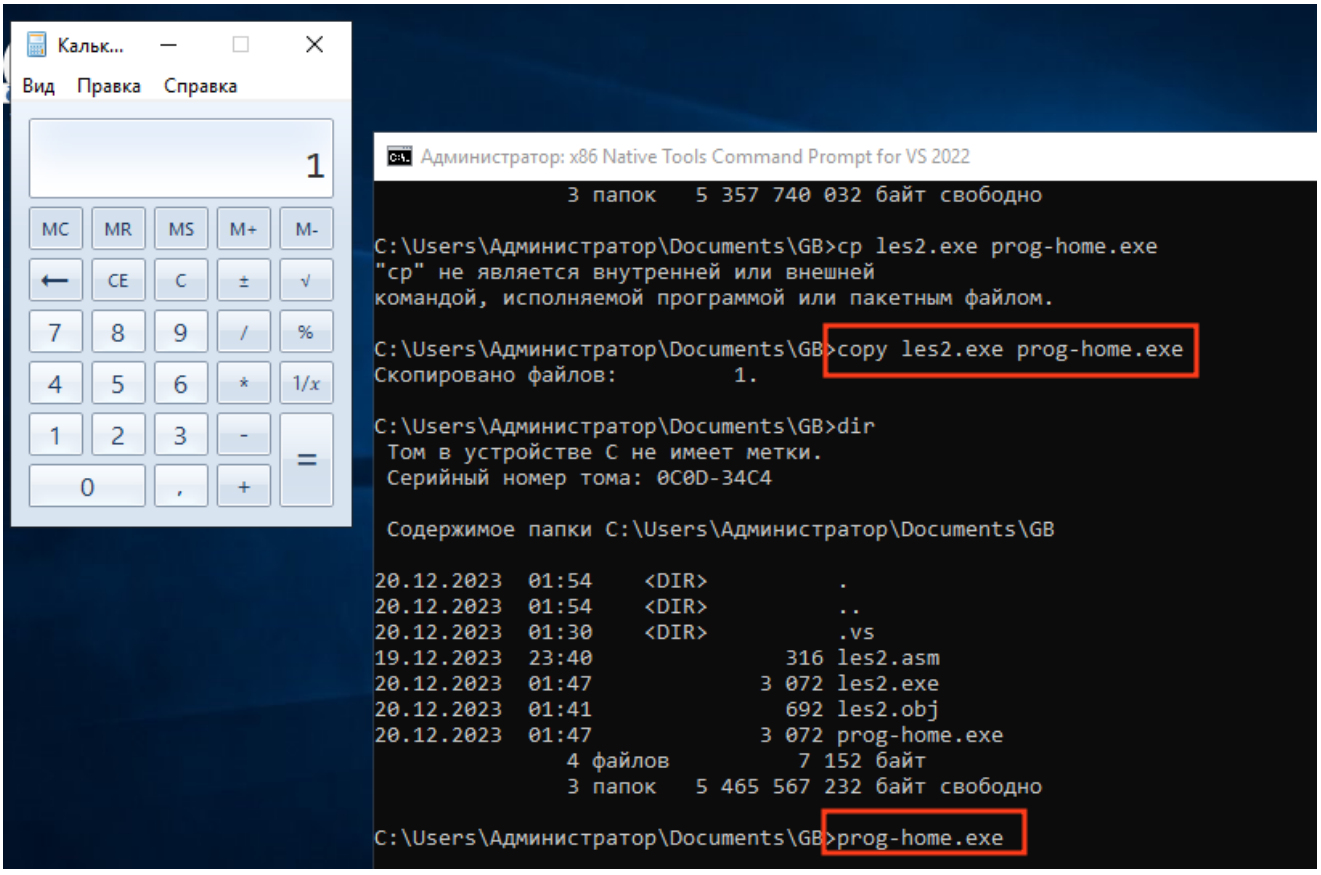
Компиляция

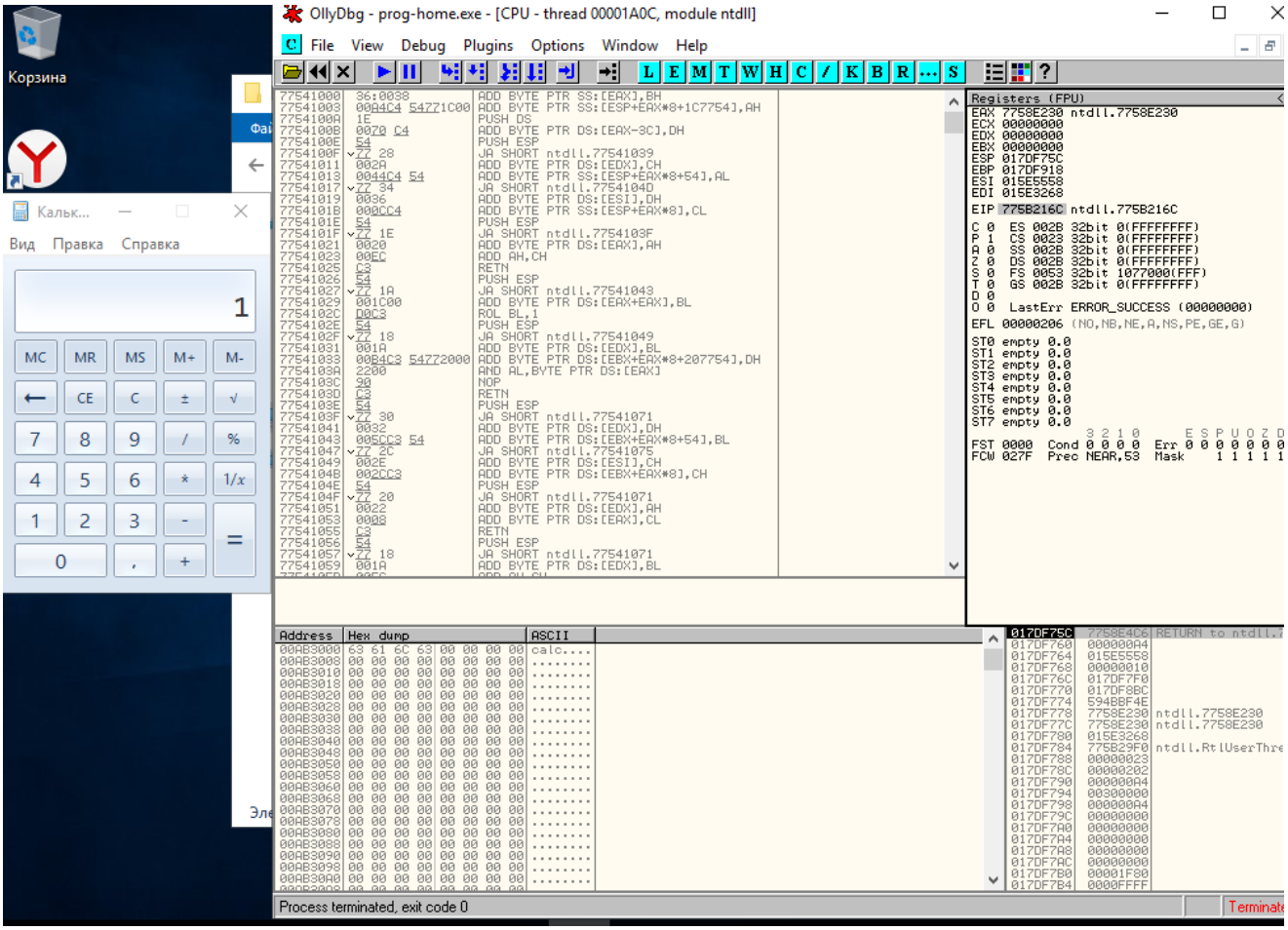
```
C:\Users\Администратор\Documents\GB>ml /c /coff les2.asm
Microsoft (R) Macro Assembler Version 14.35.32217.1
Copyright (C) Microsoft Corporation.  All rights reserved.

 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
```

Линовка

```
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
```

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





*Выполнил: AndreiM