**Лабораторная работа №1 «Знакомство со средой разработки»**

Программа на языке ассемблера (ЯА) имеет следующую структуру

.586; модель процессора

.model flat, stdcall; плоская модель памяти

; объявление внешних функций

extern ExitProcess@4:near; завершение процесса – выход из программы

; присоединение внешних библиотек

includelib c:\masm32\lib\user32.lib

includelib c:\masm32\lib\kernel32.lib

data segment; сегмент данных

*;описание переменных*

data ends

text segment; сегмент кода

start:

*;текст программы*

push 0; выход из программы, завершить процесс

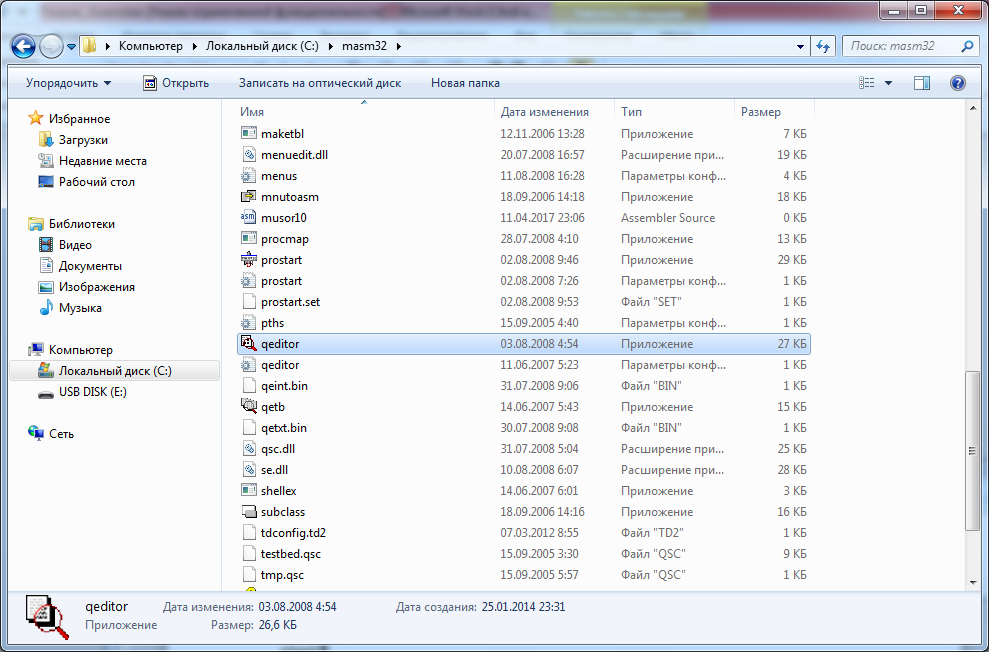
call ExitProcess@4

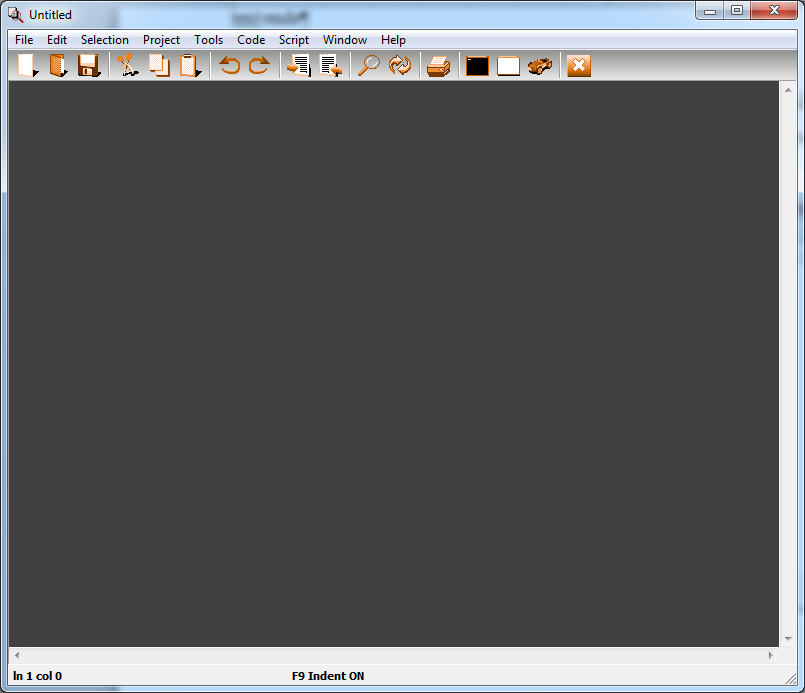
text ends

end start

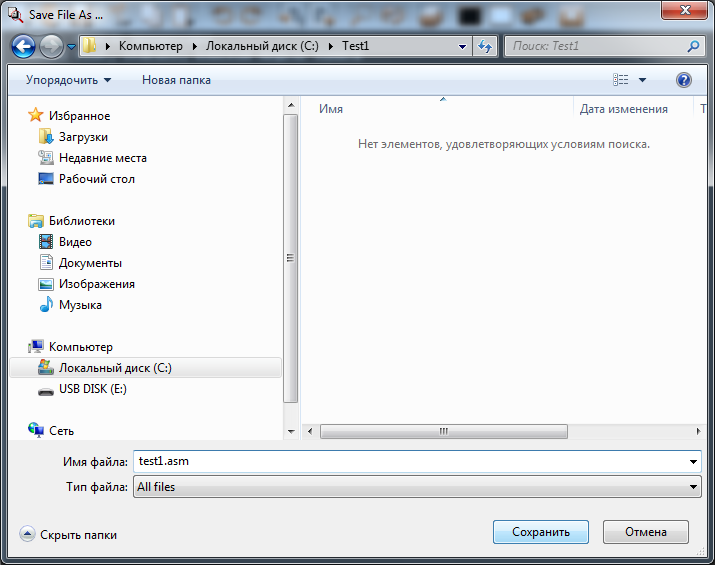
Создание программы на ЯА с использованием пакета MASM32

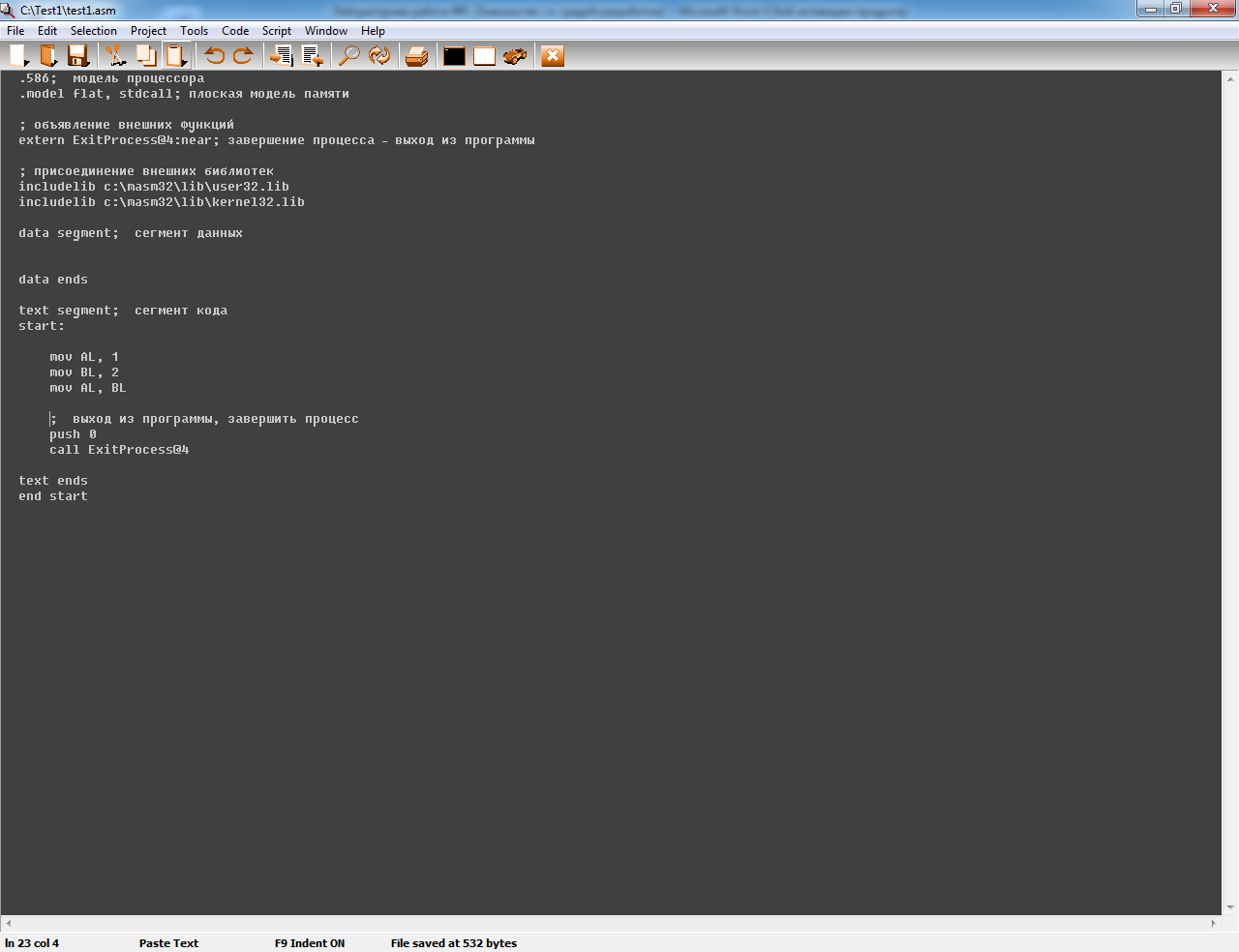
1. Ввод текста – с помощью текстового редактора qeditor или редактора «Блокнот». Текст не должен содержать символов форматирования.





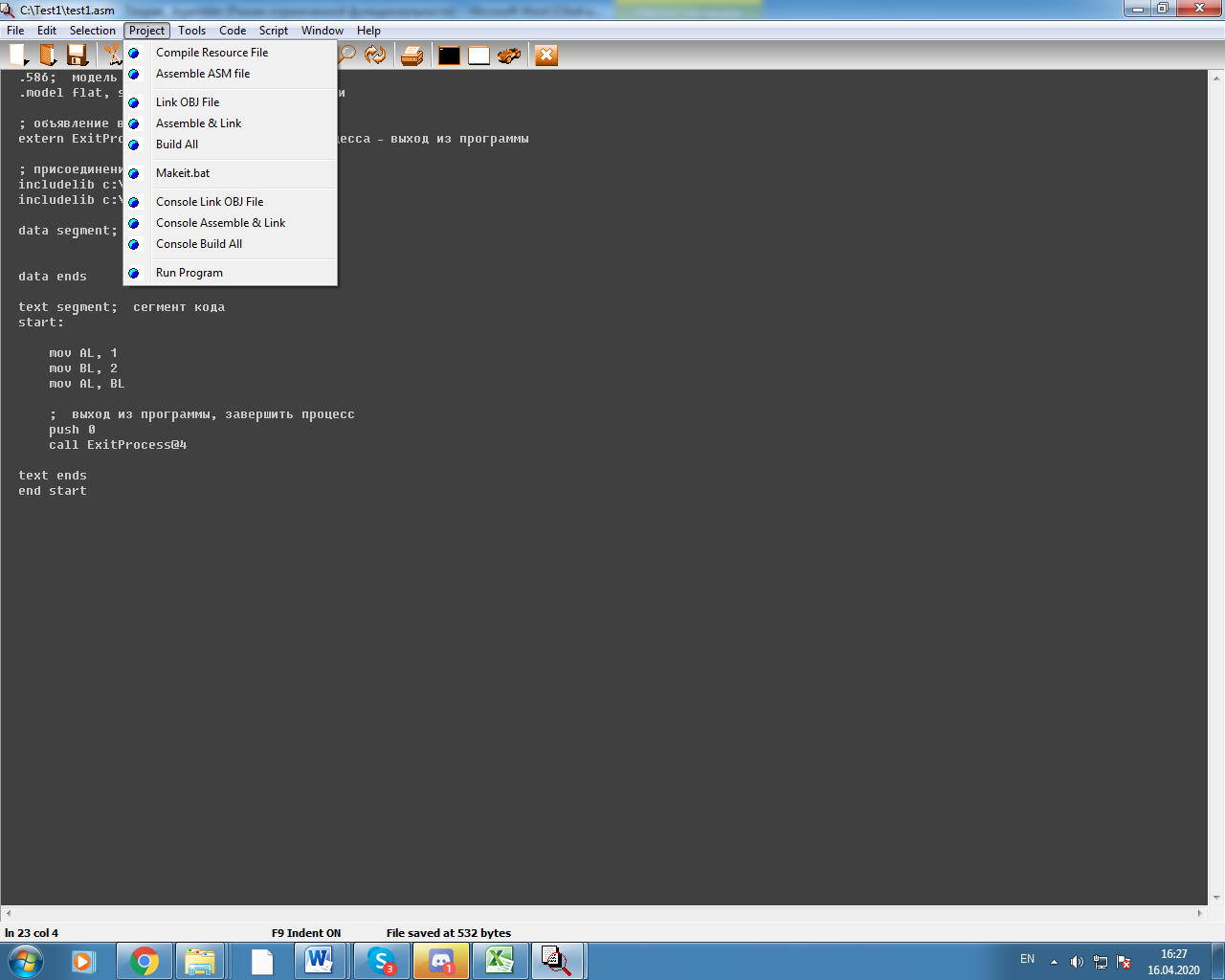
Файл текста программы должен иметь расширение **asm**.





2. Трансляция программы (ассемблирование)

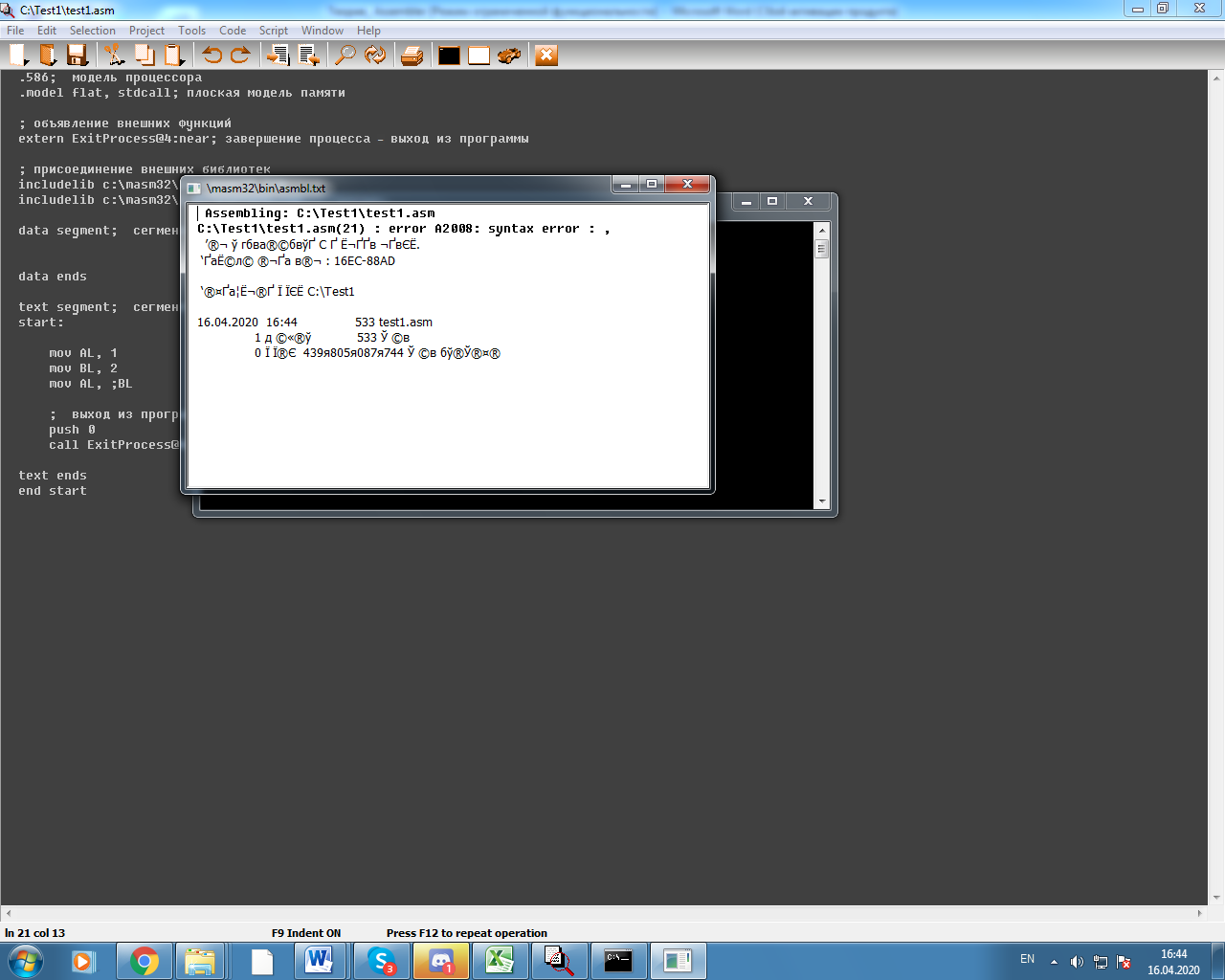
Project – Assemble ASM file



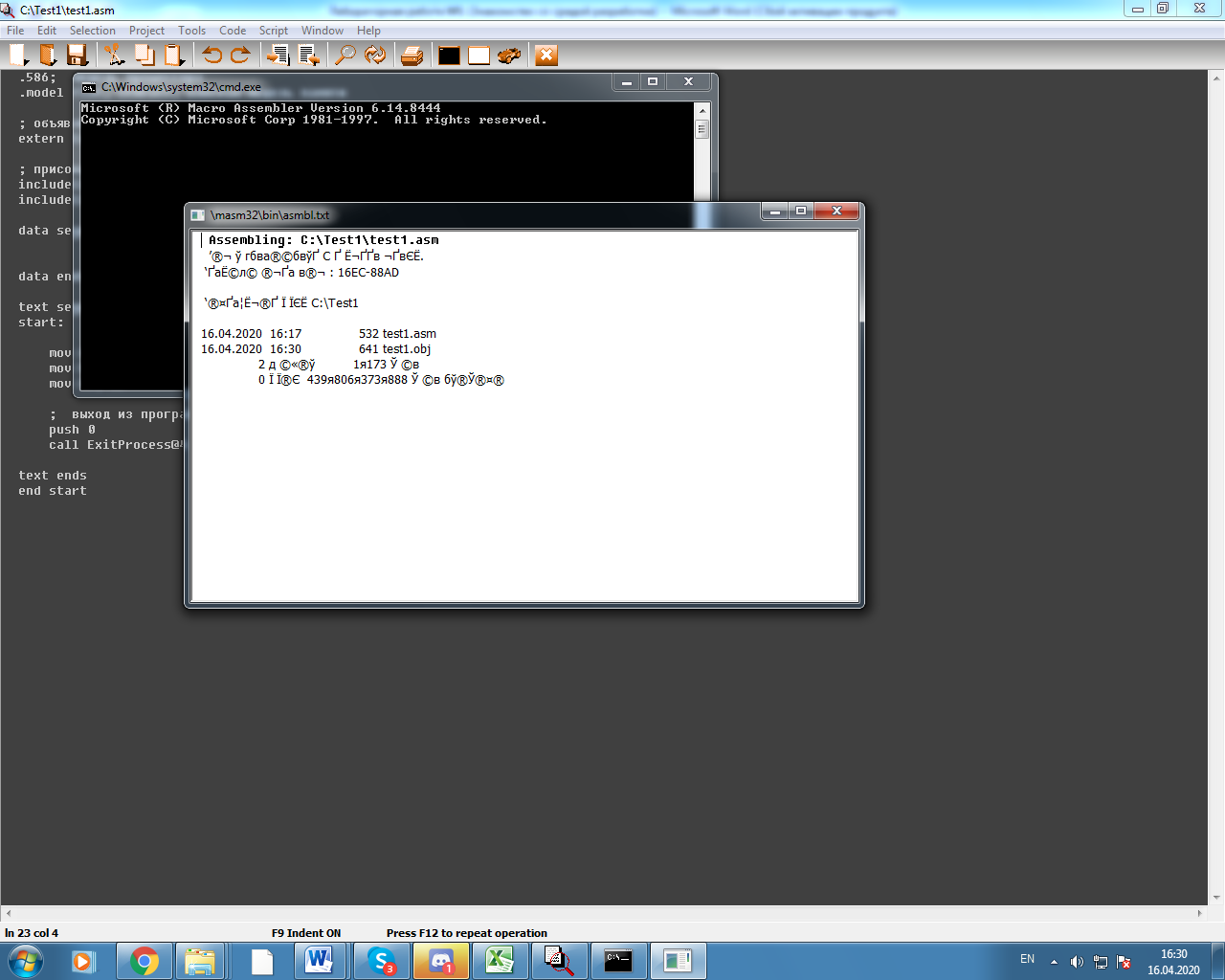
В результате создаётся файл с расширением obj – объектный модуль, который содержит представление исходной программы в машинных кодах и информацию необходимую для отладки и компоновки с другими модулями.

В результате трансляции на экран будет выдано сообщение об ошибках с указанием строки текста.

Трансляция с ошибками

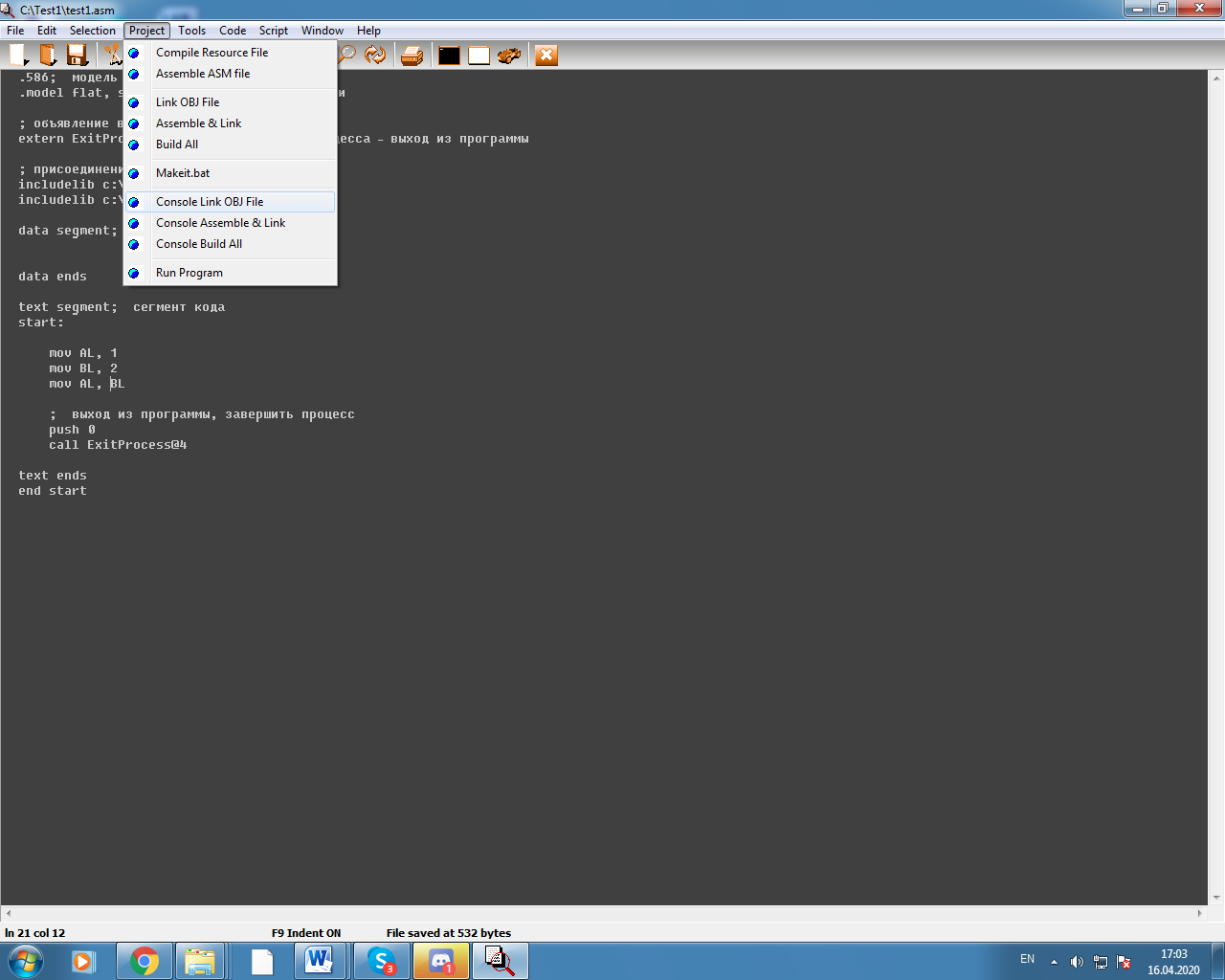


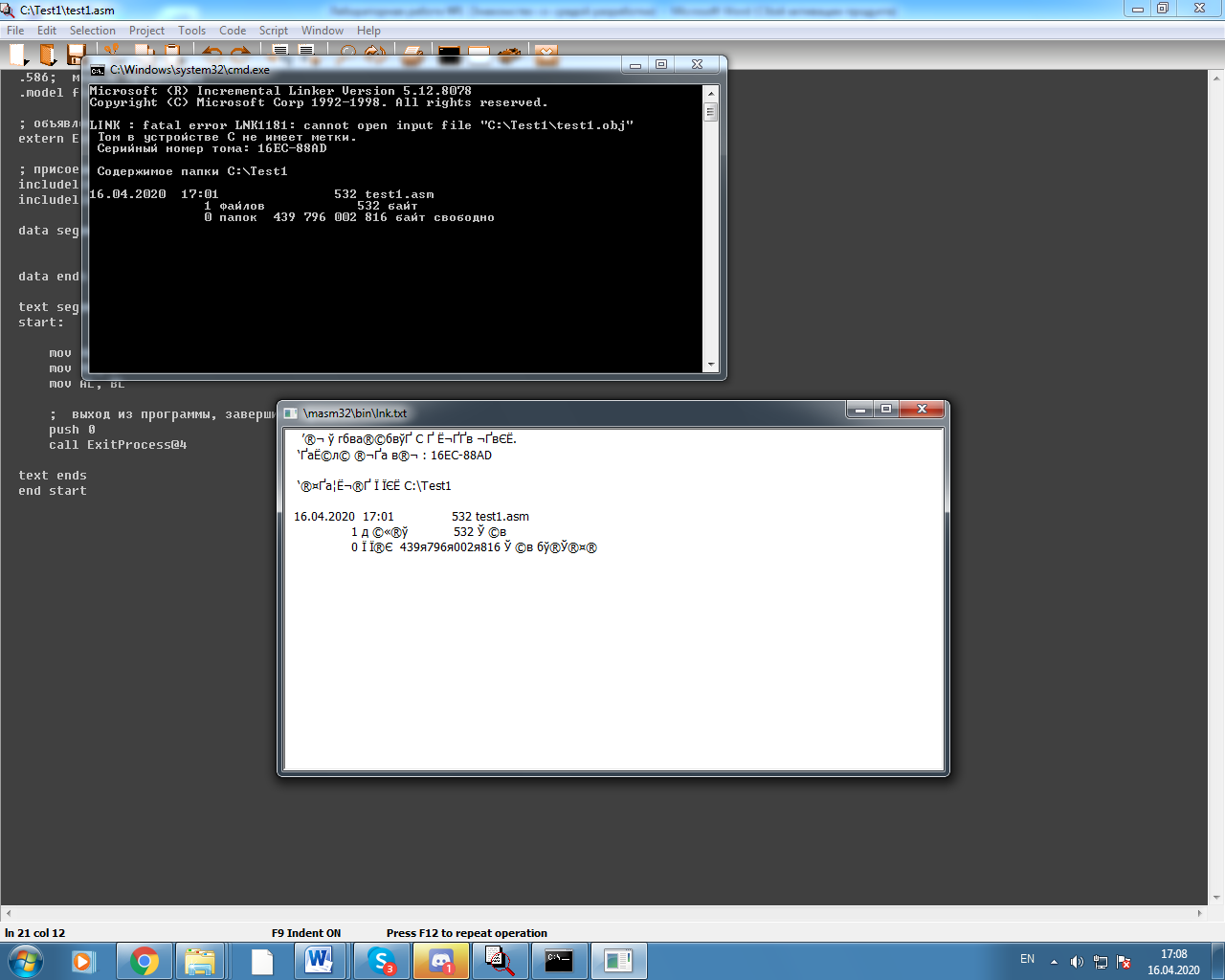
Трансляция без ошибок



3. Компоновка программы – создание исполняемого модуля, т.е. файла с расширением exe.

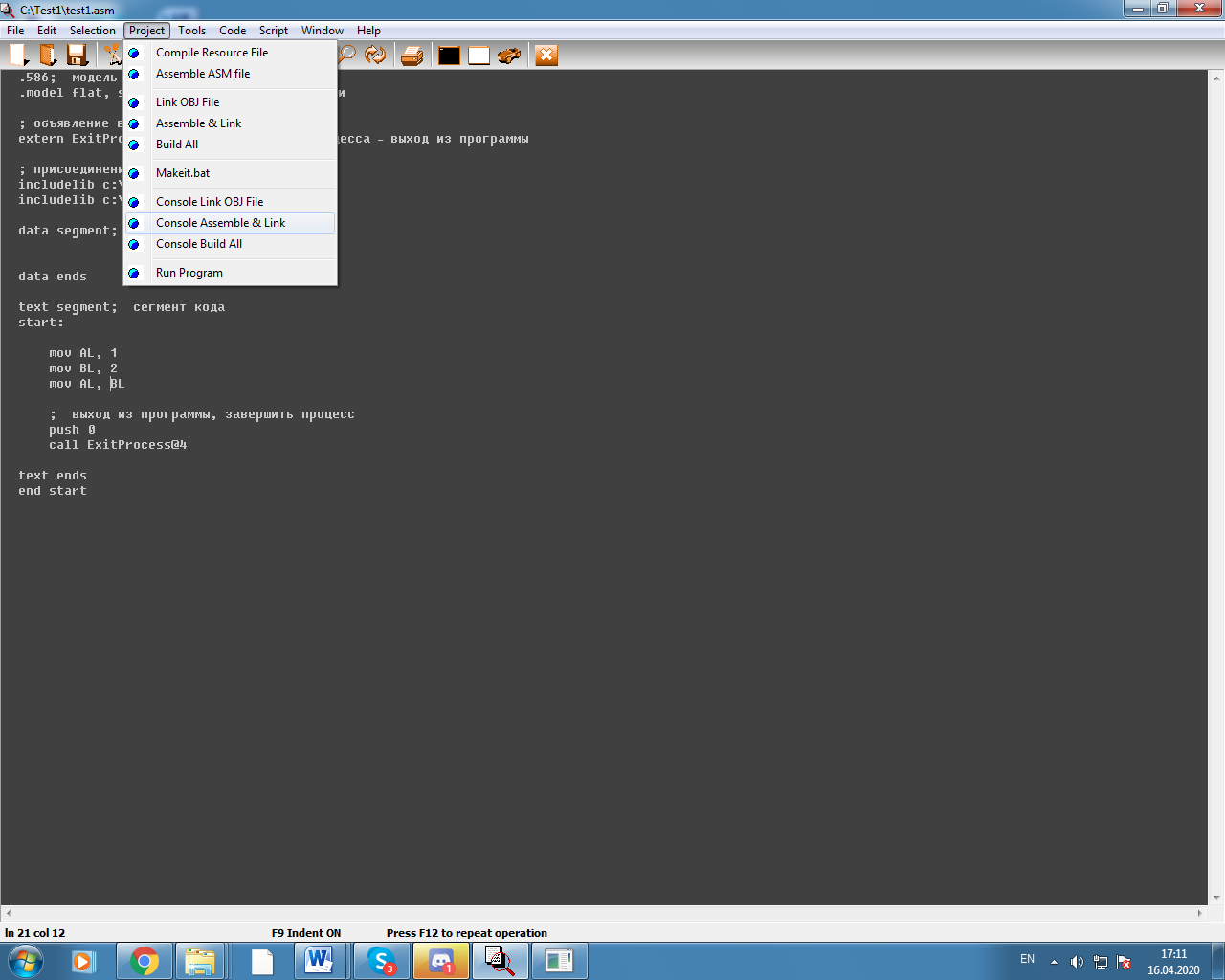
Project – Console Link OBJ File



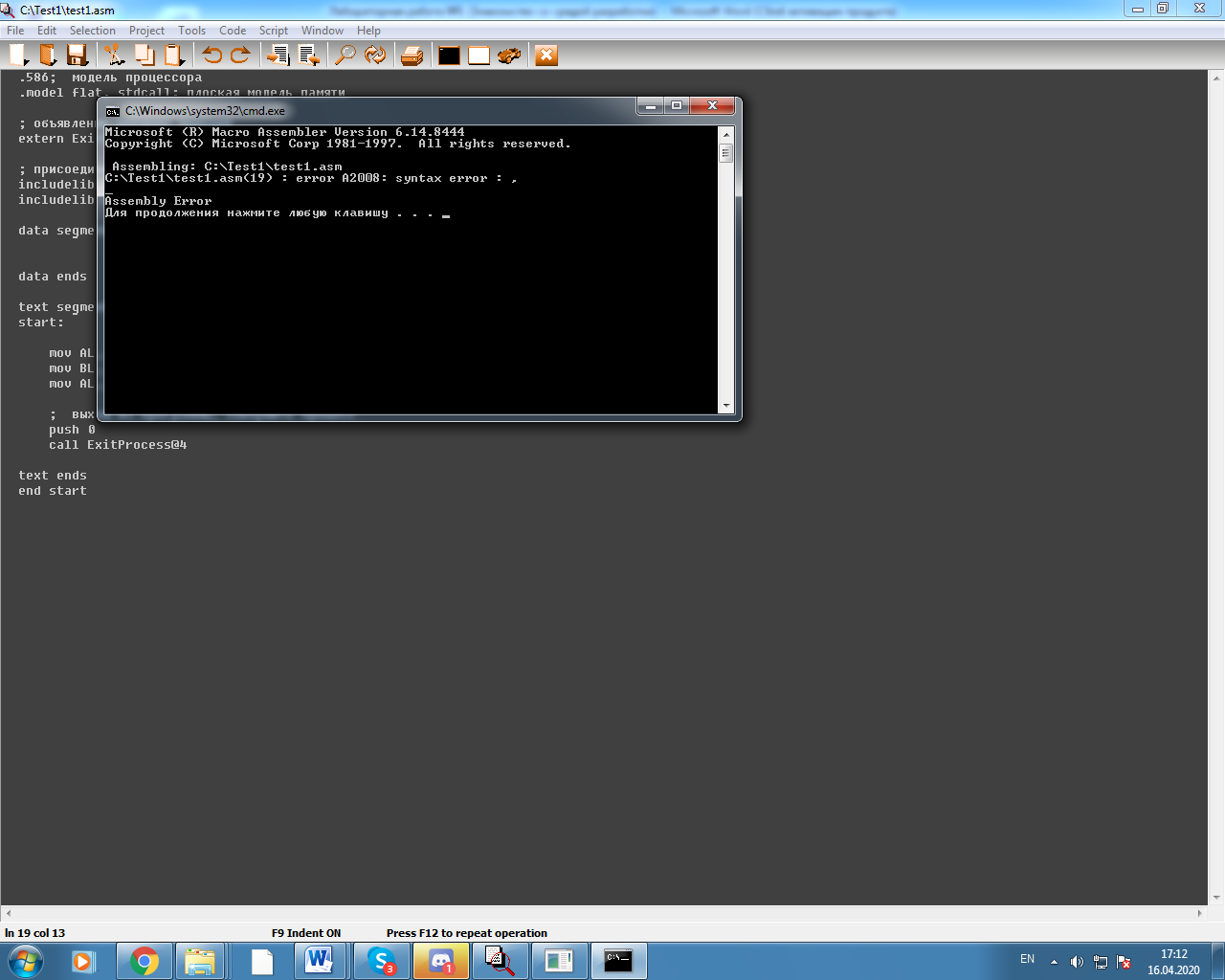


Трансляцию и компоновку можно запускать одной командой

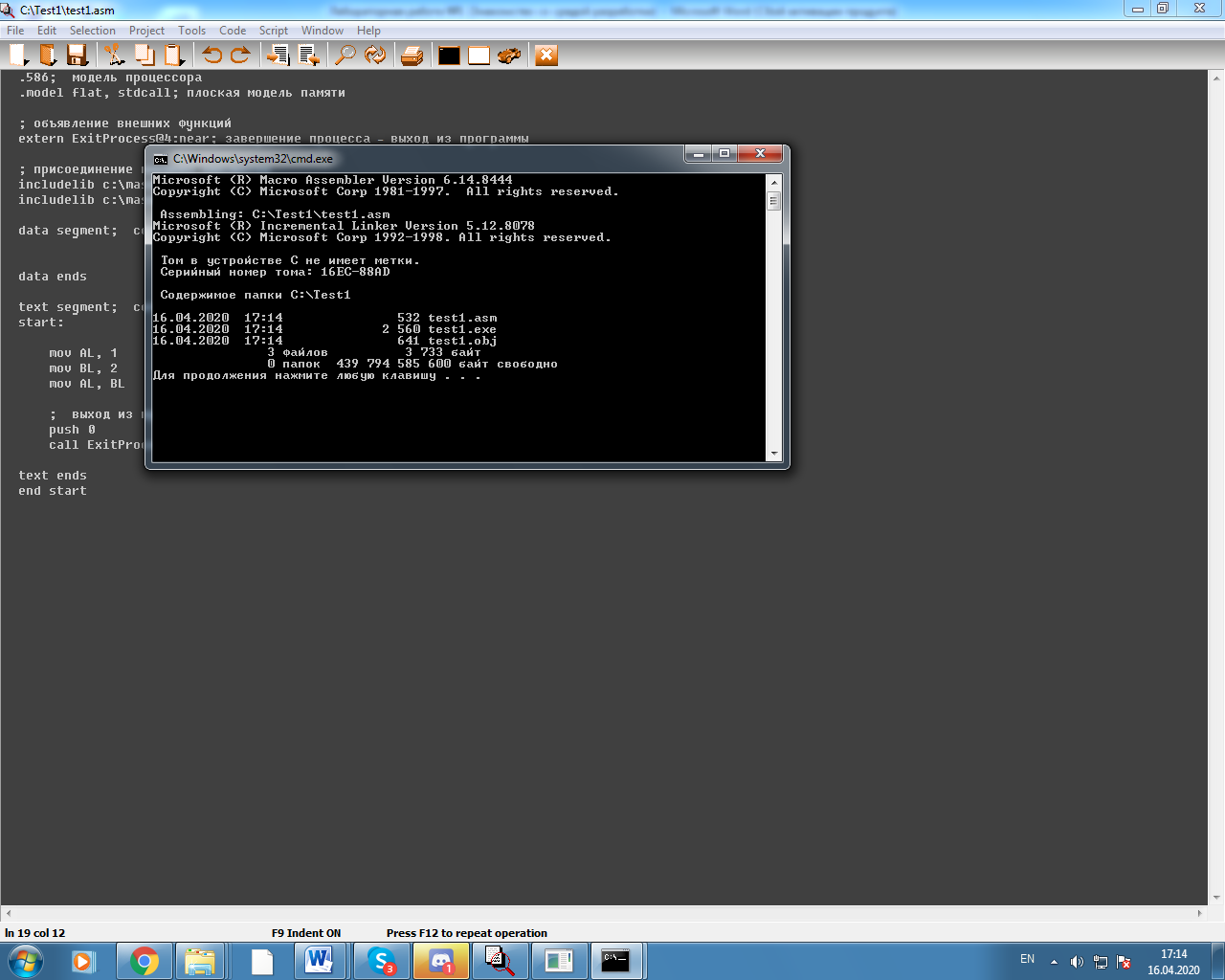
Project – Console assemble & Link



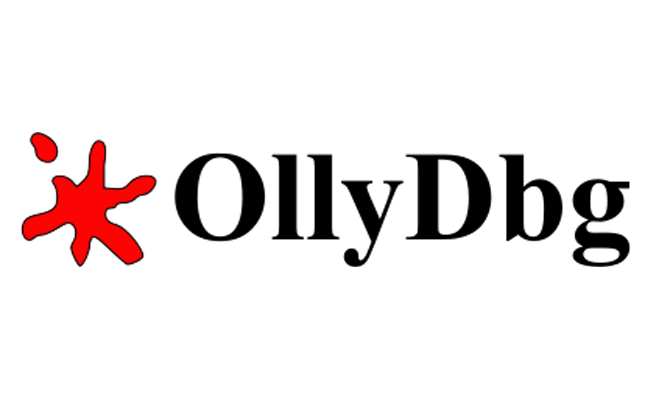
Трансляция с ошибками

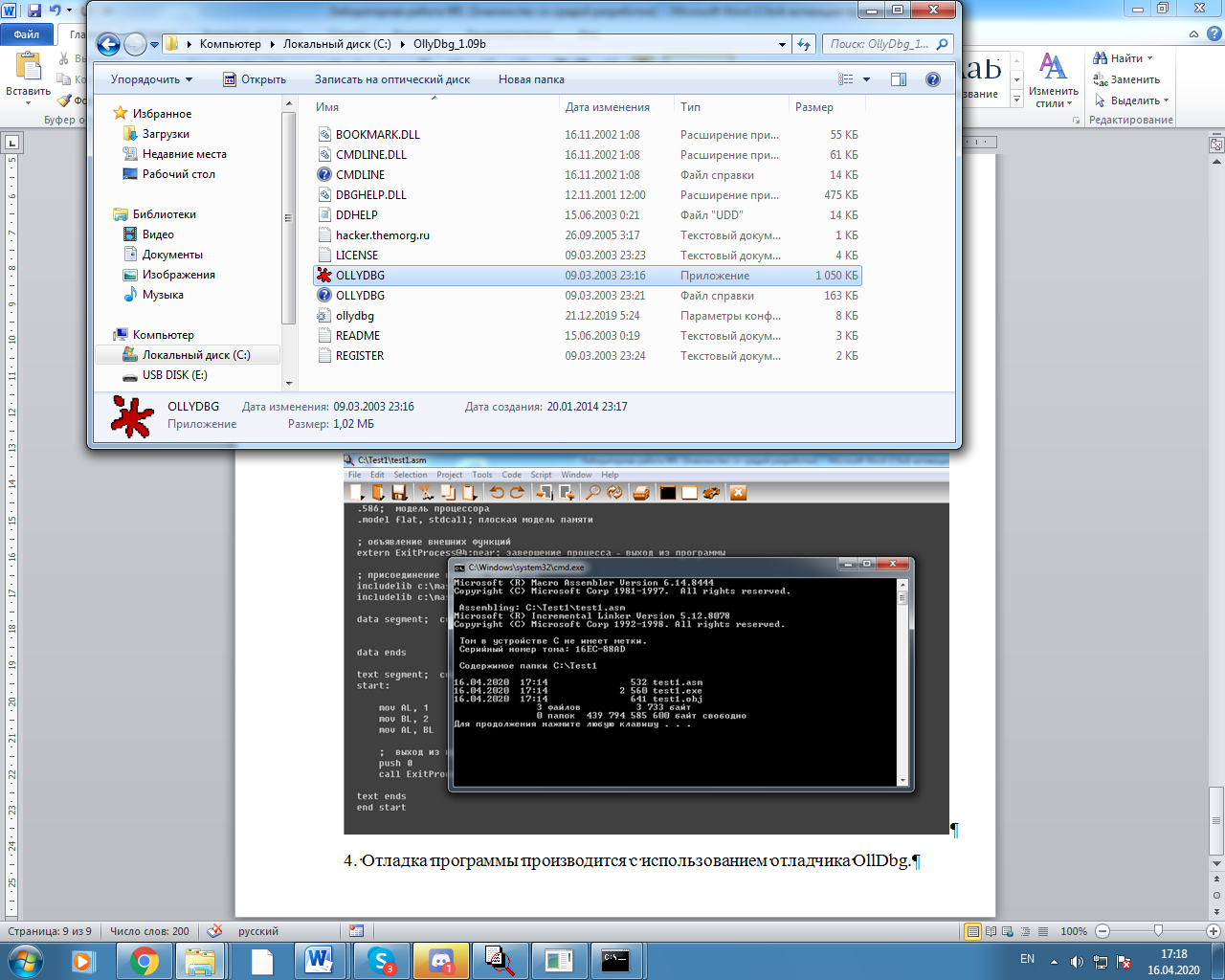


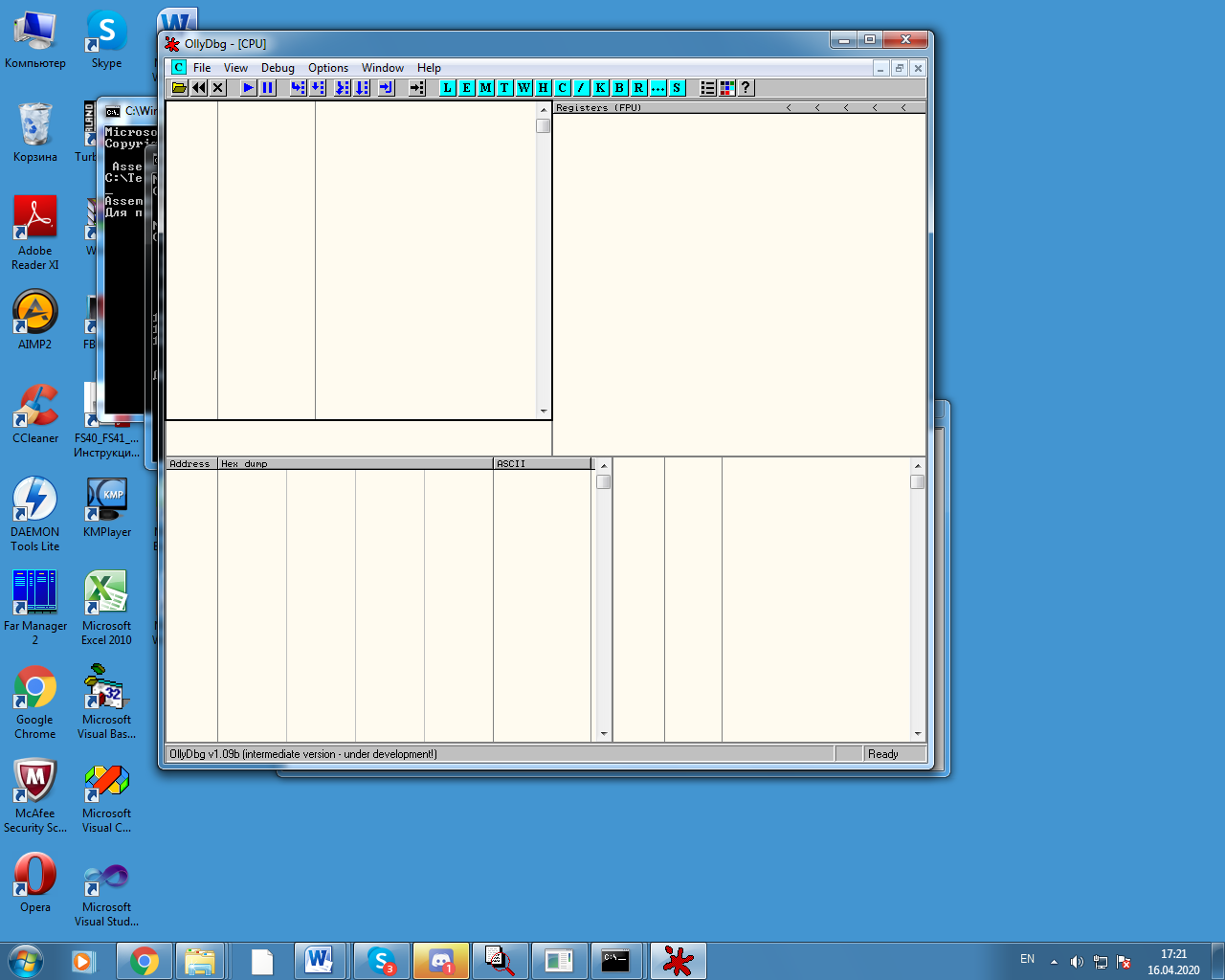
Трансляция без ошибок



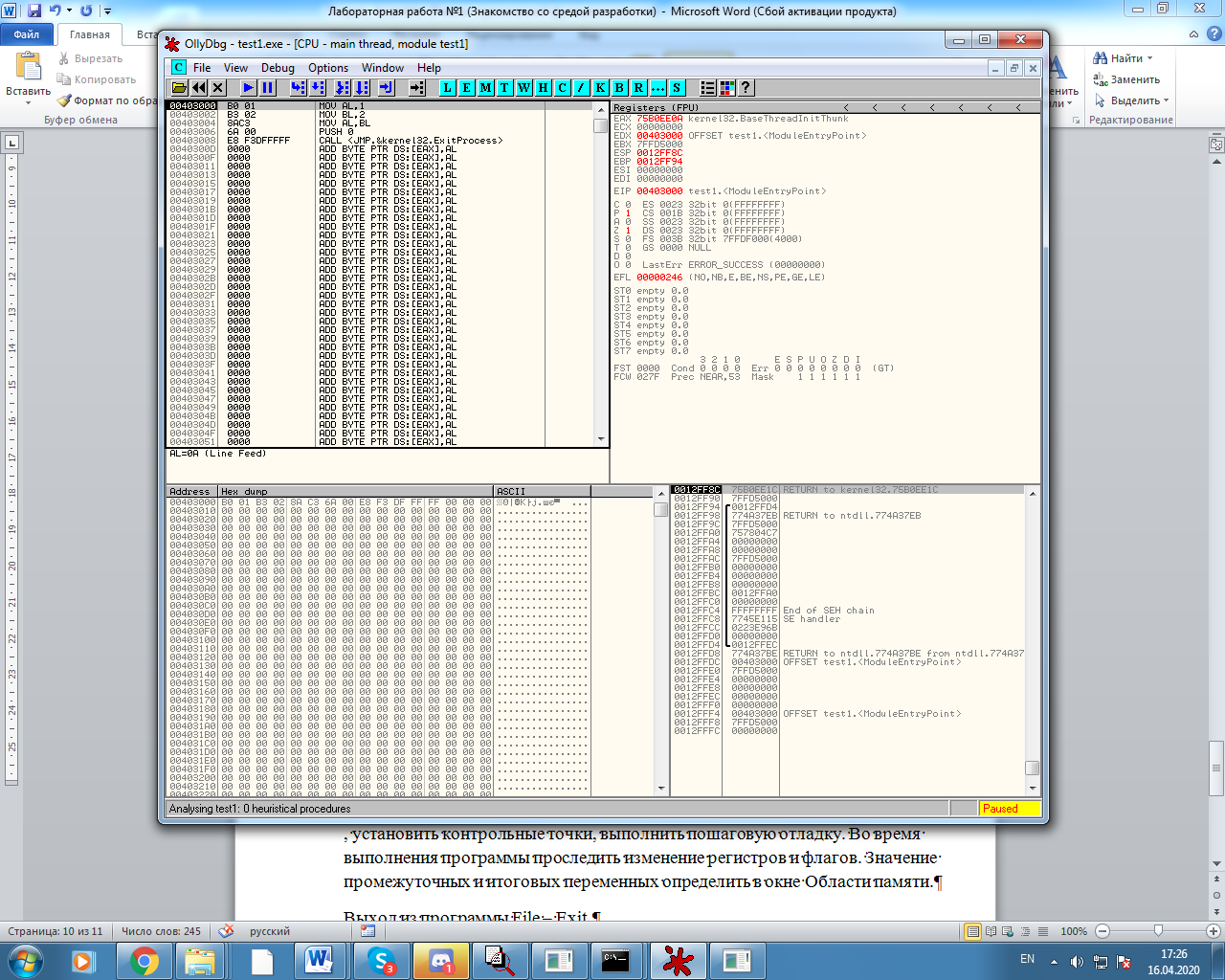
4. Отладка программы производится с использованием отладчика OllyDbg.

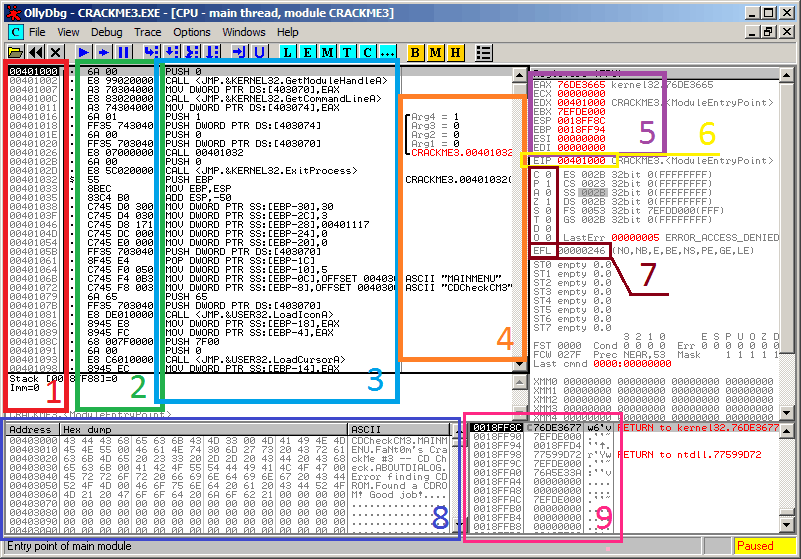






Для отладки программы следует с помощью команды File – Open загрузить исполняемый файл программы (exe-файл).





Рабочее окно отладчика OllyDbg:

1 - адреса,

2 - машинный код,

3 - дизассемблированный листинг (команды ассемблера),

4 - комментарии отладчика,

5 - регистры общего назначения,

6 - EIP регистр (показывает адрес следующей выполняемой команды),

7 - флаги и регистр флагов,

8 – сегмент данных (дамп памяти),

9 – стек.

**Главное окно (1 - 4)**

В этом окне происходит собственно сама отладка. Все инструкции приведены в дизассемблированном виде. Можно перемещать указательную строку при помощи курсора. При помощи указательной строки можно выбирать, какие скопировать данные (выделить Ctrl+C, зайти куда надо и Ctrl+V), какую изменить команду, куда поставить точку останова и т.д. Сбоку выделен адрес, который должен выполниться следующим. Между колонкой адресов и колонкой дизассемблированного листинга есть колонка с машинным кодом инструкции. Самая последняя колонка содержит в себе комментарии.

**Окно регистров (5-7)**

В окне регистров отображаются все 32-битные регистры, регистры флагов и различные другие регистры. Для того, чтобы изменить регистр, надо щёлкнуть по его значению 2 раза и ввести новое значение. Реверсировать регистр флага можно путём двойного щелчка по одному из них.

**Область памяти (8)**

В окне отображается участок оперативной памяти, в котором указаны номера ячеек памяти и содержимое ячеек. Все данные отображаются в 16–ричном виде.

**Панель стека (9)**

В панели стека можно изменить нужные байты в памяти, ставить точки останова, подсматривать правильные рег. коды и т.д.

Запустить программу на выполнение в отладчике можно в одном из режимов:

- режим выполнения по шагам – **F8 (F7)**;

- выполнение с установкой контрольных точек;

- режим безусловного выполнения – **F9** – используется для выполнения отлаженной программы.

**Горячие клавиши панели управления:**

первая кнопка – открыть файл (F3),

вторая кнопка – перезапустить файл (Ctrl+F2),

третья кнопка – закрыть файл (Alt+F2),

четвёртая кнопка – запустить программу (F9),

пятая кнопка – приостановить запуск (F12),

шестая кнопка – трассировать с заходом в подпрограммы (F7),

седьмая кнопка - трассировать без захода в подпрограммы (F8),

восьмая кнопка – запустить автоматическую трассировку заходя в подпрограммы (Ctrl+F11),

девятая кнопка - запустить автоматическую трассировку без захода в подпрограммы (Ctrl+F12),

десятая кнопка – выполнить программу до выхода из подпрограммы (Ctrl+F9),

одиннадцатая кнопка – перейти на адрес (Ctrl+G).

Задания

1. Сложить содержимое двух регистров длиной 1 байт.

2. Найти разность двух переменных длиной слово.

3. Найти произведение двух переменных длиной байт.

4. Переменную длиной двойное слово разделить на переменную длиной слово.