Лабораторная работа №1

Освоение инструментальной среды для выполнения лабораторных работ

Структура процессора i8086 для программиста и обзор системы команд

Для программиста при программировании на языке ассемблера микропроцессор i8086 имеет в своём составе 14 шестнадцатиразрядных регистров:

- регистры общего назначения (РОН) – AX, BX, CX, DX, SI, DI ;
- сегментные регистры – CS, DS, ES, SS;
- специальные регистры – IP,SP, BP, FLAGS.

Регистры общего назначения

Регистры общего назначения (16 разрядные): AX(AH, AL), BX(BH, BL), CX(CH, CL), DX(DH, DL) делятся программно на пары однобайтных регистров и используются для хранения данных (8 или 16 битных);

SI, DI – шестнадцатиразрядные регистры для хранения данных.

AX (16 бит)	**AH (8 бит)**	**AL (8 бит)**
BX (16 бит)	**BH (8 бит)**	**BL (8 бит)**
CX (16 бит)	**CH (8 бит)**	**CL (8 бит)**
DX (16 бит)	**DH(8 бит)**	**DL (8 бит)**
SI (16 бит)		
DI (16 бит)		

Сегментные регистры

Регистры CS, DS, ES, SS – хранят адреса сегментов в памяти (кодового, данных, дополнительных данных, стека) и не могут использоваться для хранения данных.

CS (16 бит)	Начало сегмента кода (программы) в ОП
DS (16 бит)	Начало сегмента данных программы в ОП
ES (16 бит)	Начало дополнительного сегмента в ОП
SS (16 бит)	Начало сегмента стека программы в ОП

Специальные регистры

SP, BP – указатель и база стека, соответственно, обеспечивают доступ к данным в стеке, *могут использоваться для хранения данных*, но делать это не рекомендуется, так как при этом возможно нарушение адресации в стеке, особенно при использовании SP.

IP – регистр инструкций (счетчик команд) – хранит адрес следующей исполняемой команды (относительно смещения).

FLAGS – регистр флагов содержит набор битовых флагов, определяющий результат выполнения предыдущей команды.

SP (16 бит)	Указатель начала стека в ОП
BP (16 бит)	Указатель начала базы в ОП
IP (16 бит)	Указатель (счетчик) команд ОП
FLAGS (16 бит)	Регистр флагов

Флаги

OF

SF

ZF

CF

Регистр флагов процессора		
Флаг	Название	Назначение
O	Переполнение	Переполнение при выполнении арифметических операций
D	Направление	Направление пересылки данных при выполнении строковых команд
I	Прерывание	Разрешает/Запрещает внешние прерывания
T	Пошаговый режим	Останов после выполнения каждой команды(используется отладчиками)
S	Знак	Знак результата выполненной команды(0 – плюс, 1 – минус)
Z	Ноль	Значение результата выполненной команды(0 – ненулевой, 1 – нулевой)
A	Внешний перенос	Используется для специальных арифметических операций
P	Контроль чётности	Число единиц в операнде(0 – нечётное, 1 – нечётное)
C	Перенос	Содержит перенос из старшего бита при выполнении арифметических операциях

Оперативная память

Память, с которой взаимодействует процессор при выполнении программы, называется Оперативным Запоминающим Устройством(**ОЗУ**) или Random Access Memory(**RAM**). Также используется аббревиатура – ОП.

Память состоит из набора однобайтных ячеек, обращение к которым происходит по их номерам(физическим адресам). Адресация начинается с 0000

Исполняемая программа (загруженный exe-файл) в ОП состоит из трех последовательно расположенных сегментов (частей). Начало каждого сегмента определяется значением регистров DS (данные), CS (код программы), SS (стек программы).

Значение этих регистров определяется при линковке программы (Tlink).

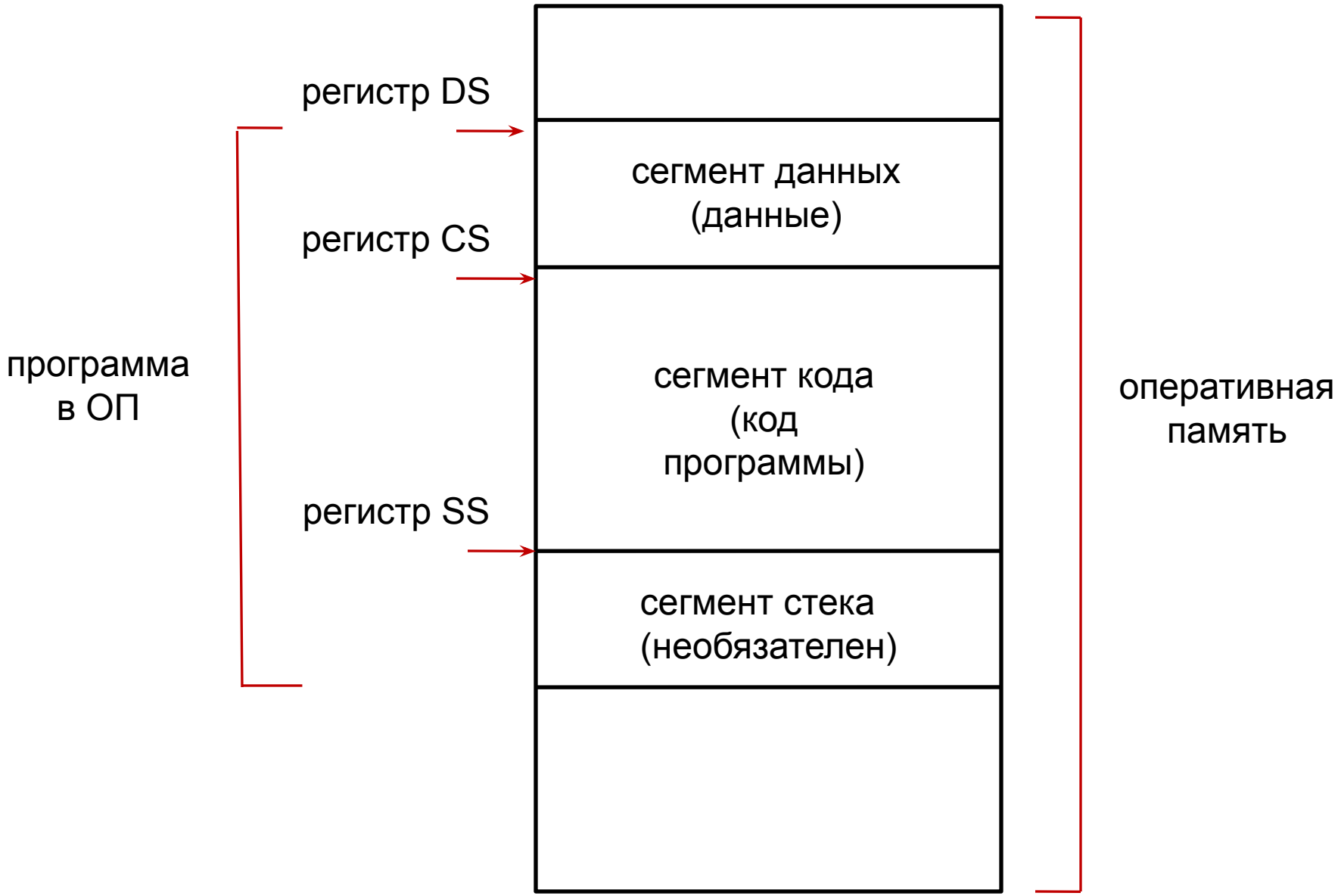
Используемый инстументарий

Для получения exe-файла и его отладки будут нужны:

- текстовый редактор – Notepad, Notepad++ и др. -> file.asm
- компилятор языка ассемблера – Tasm -> file.obj
- линковщик – Tlink -> file.exe
- отладчик - Td

Tasm, Tlink, Td – это 16-ти разрядные приложения и для их работы в Windows 7, 8, 10 потребуется приложение "Dosbox". Внутри этого приложения будет использоваться файловый менеджер Norton Commander (NC)

Структура данных и кода в оперативной памяти

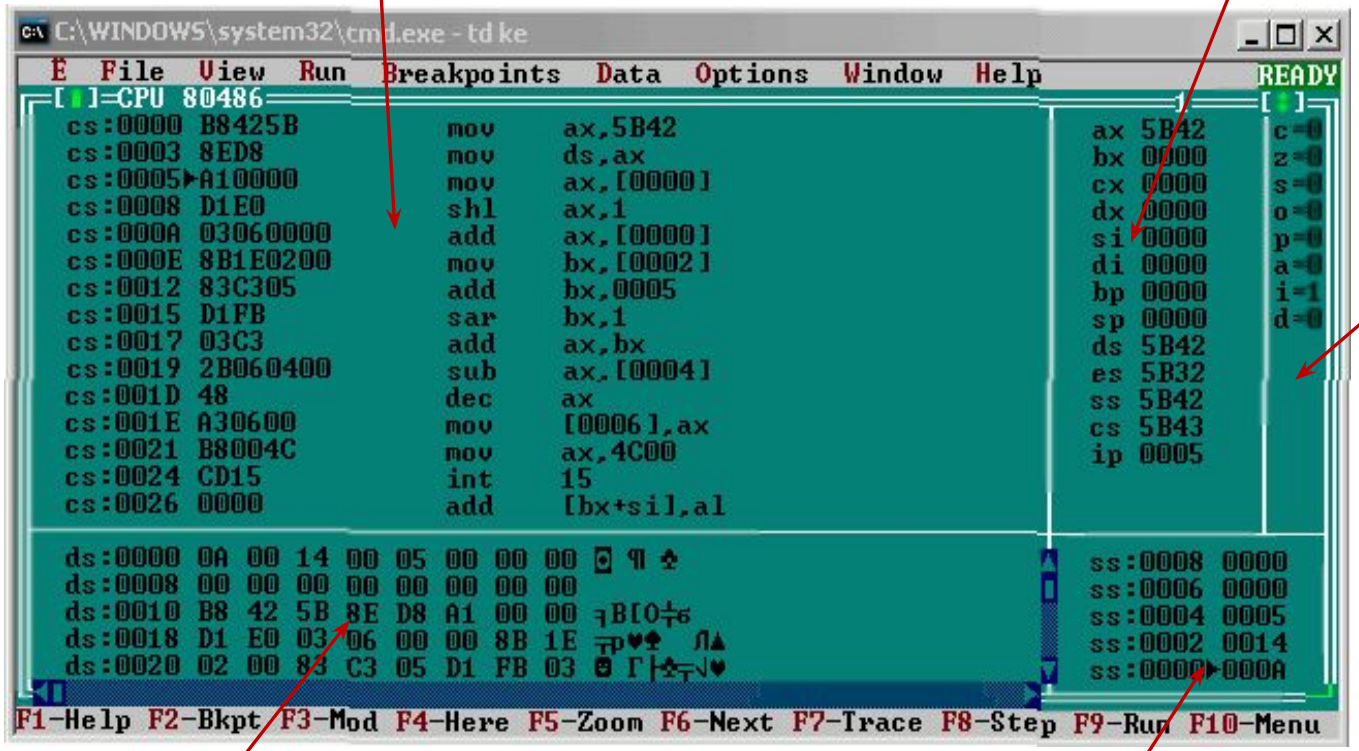


Turbodebugger (отладчик)

окно процессора
(код программы)

окно регистров процессора

окно флагов
процессора



окно ОП
(данные)

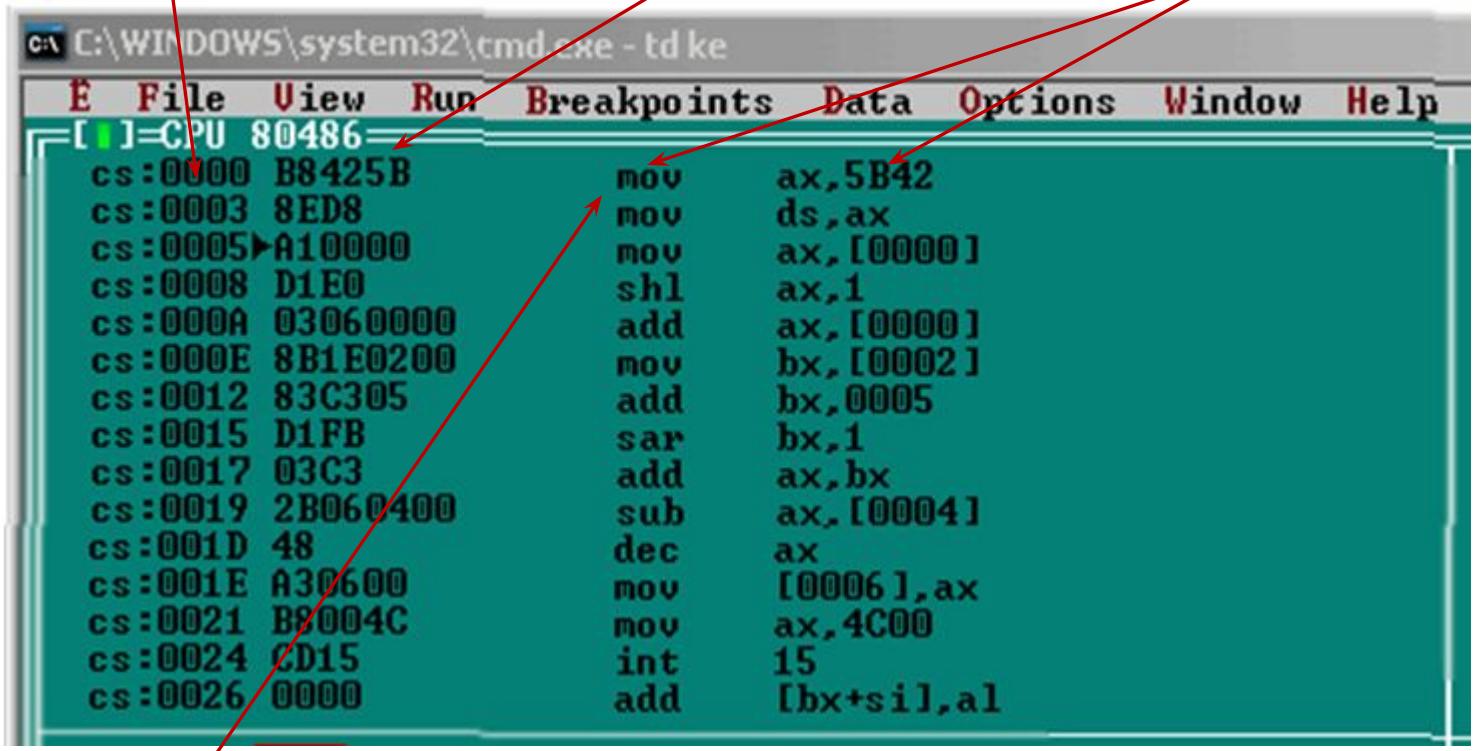
окно стека
(стек)

Окно процессора

столбец адресов команд

столбец кодов команд

два столбца мнемоники команд



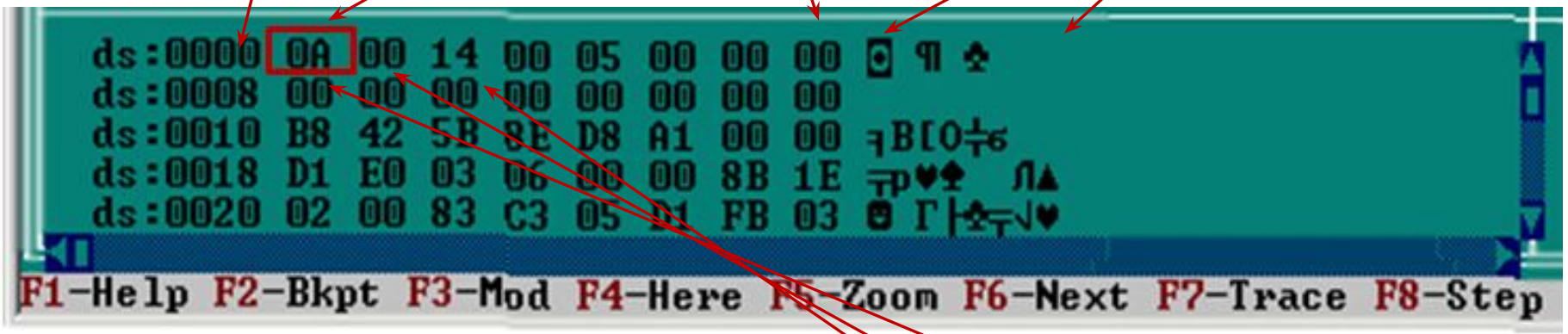
команда mov ax,5B42 находится в ОП по адресам 0000 – 0002 (занимает три байта) и имеет код - B8425B

Окно ОП (ОЗУ)

столбец адресов
байт ОП

значение байт
по этим адресам

символьное отображение
байтов

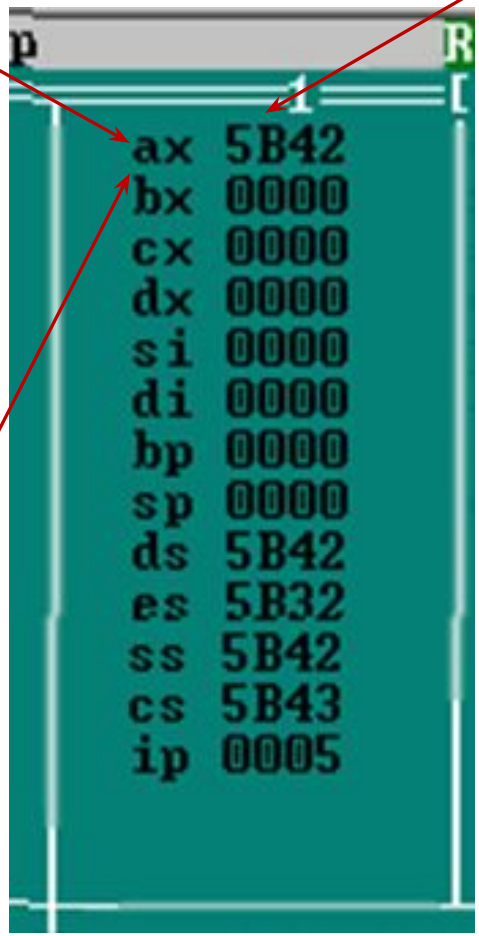


значение ds=5B42
по адресу ОЗУ = 5B42+0000=5B42 значение байта=0Ah
по адресу ОЗУ = 5B42+0001=5B42 значение байта=00h
по адресу ОЗУ = 5B42+0002=5B42 значение байта=14h

Окно регистров

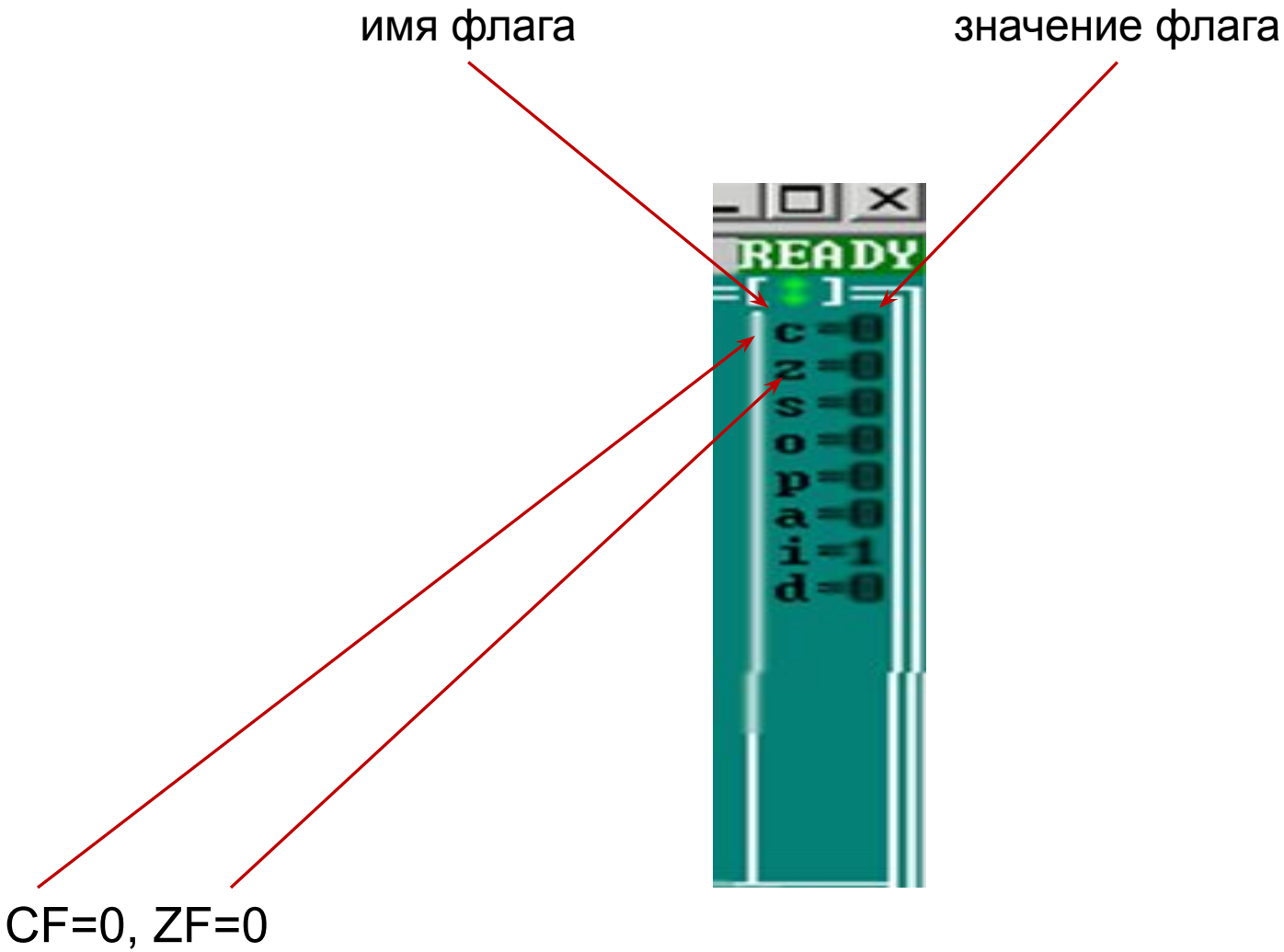
столбец имен регистров

столбец значений регистров

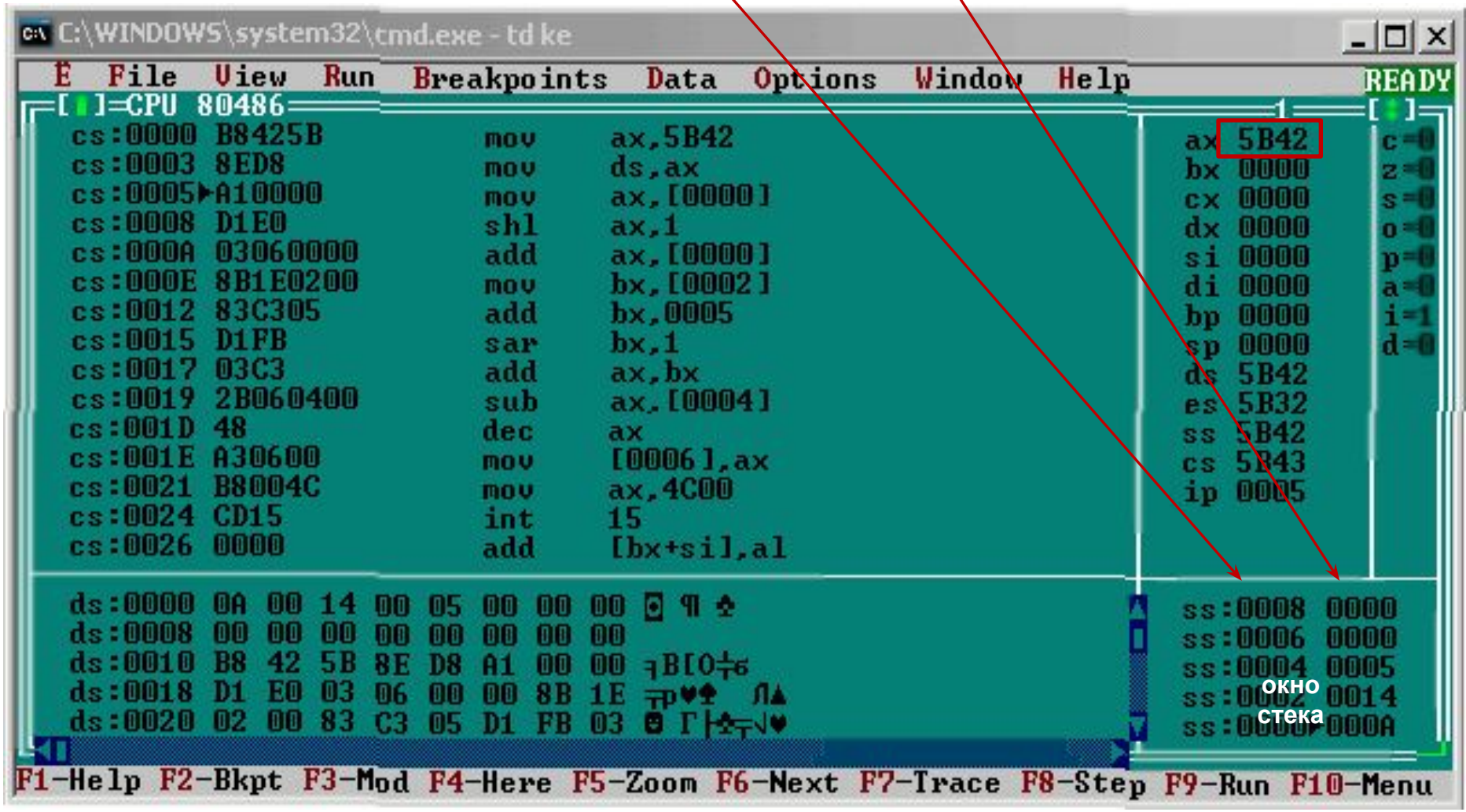


регистр AX=5B42h=0101101110000010b

Окно флагов



окно стека: адрес байта, значение байта



Задание на лабораторную работу и порядок её выполнения смотри в файле:

Лабораторная работа №1 часть 2 Задание.docx