**Лабораторное занятие №5.**

**ВНИМАТЕЛЬНО ЧИТАЙТЕ ПОСТАНОВКУ ЗАДАЧИ!!!!**

1. НЕОБХОДИМО исполнить следующее:
   1. В рамках оболочки DOSBOX разместить в папке с «ПАПОЙ» (в папке, где находятся все необходимые файлы для получения программы по мытью папы вместо рамы) ПРОГРАММУ-ОТЛАДЧИК td.exe.
   2. Используя информацию с сайта правообладателя td.exe (в крайнем случае – из помойки) НАУЧИТЬСЯ осуществлять ОТЛАДКУ – пошаговое исполнение различных программ. Разобраться, где и как ОТОБРАЖАЮТСЯ ДАННЫЕ, касающиеся содержимого РЕГИСТРОВ, содержимого stack segment, code segment, data segment, extended segment.
   3. Загрузить для пошагового выполнения исполнимый модуль про маму и папу. После загрузки выписать (нарисовать) на отдельном подписанном листочке следующие данные в шестнадцатеричном виде (а в скобках в 10 системе счисления):
2. Содержимое регистров CS, DS, SS, ES, IP.
3. Адрес точки входа.
4. Представление самой короткой и самой длинной КОМАНД в шестнадцатеричной системе счисления, указать в десятичной системе счисления ДЛИНУ КАЖДОЙ ИЗ ЭТИХ КОМАНД (самой длинной и самой короткой), записать OFFSET (СМЕЩЕНИЕ) в шестнадцатеричной системе счисления каждой из этих команд.
5. После чего отобразить на экране СОДЕРЖИМОЕ СЕГМЕНТА ДАННЫХ (это там, где располагается последовательность символов «MAMA MILA RAMU»), используя значение, содержащееся в регистре DS. На листочке выписать шестнадцатеричное представление каждого из символов данной последовательности.
6. Исполнить пошагово две команды программы, записав на листочке содержимое регистров DS и AX в шестнадцатеричной системе счисления.
7. После выполнения команд:

**mov ah,10**

**lea dx,OblVvoda**

**int 21h**

**mov OblVvoda+12,’П’**

**mov OblVvoda+14,’П’**

**mov ah,9**

**lea DX,OblVvoda+2**

**mov OblVvoda+16,’$’**

**нарисовать на листочках в шестнадцатеричном виде содержимое регистров ax, ah, dx, IP, а также содержимое области памяти OblVvoda.**

1. **Сдать листочки в течении либо в конце занятия 1.10.2024 года. НЕ СПИСЫВАТЬ.**

1. ***Если кто-то готов, можно приступать к выполнению ЛАБОРАТОРНОЙ РАБОТЫ №2.***

**Лабораторная работа №2. Часть 1.**

**1.1. Используя оболочку DosBox, книгу про ассемблер, набрать исходный текст ВИРУСА DHog68, транслировать, линковать, получить com-файл в папке про ПАПУ.**

**1.2. Скопировать всё содержимое папки про ПАПУ в папку HOG.**

**1.3. Сделать папку HOG активной, используя исполнимый модуль td.exe ПОШАГОВО ВЫПОЛНИТЬ программу DHog68.**

**1.4. Проверить, действительно ли происходит заражение всех файлов папки. Для этого с помощью ОТЛАДЧИКА td.exe ПОШАГОВО ВЫПОЛНИТЬ программу, получаемую в результате загрузки в отладчик файла Mrak.asm (файл, в котором до выполнения шага 1.3. находился исходный текст решения задачи про папу).**

**1.5. Проверить, каким образом НА ПОЯВЛЕНИЕ ЭТОГО ФАЙЛА.com реагирует Ваша антивирусная защита (если пока её нет – установить любой бесплатный антивирусник).**

**1.6. Используя защиту, протестировать файлы, находящиеся только в папках DHOG и в папке про папу.**

**1.7. Весь процесс ЗАДОКУМЕНТИРОВАТЬ и прислать, как всегда, отчёт о проделанной работе в виде известных Вам трёх файлов до 23-59 14.10.2024 года!**