

**ОТЧЕТ О ВЫПОЛНЕНИИ**

**практической работы № 3**

**по предмету МДК 3.2**

**Управление проектами**

Выполнил: ст. гр. 2ИСП11-31ВБ Синицын О. Е.

Специальность: 09.02.07

Информационные системы и программирование

Проверил: преподаватель Голиков Д. А.

Москва 2023

**Тема:** Отладка и дизассемблтоование программ.

**Цель работы:** Практическое знакомство с методикой отладки и

дизассемблирования программ на языке ассемблера с помощью отладчика OllyDbg.

**Ход работы:**

**Задание 1**

Выбираем программу для выполнения задания.

**Задание 2**

Открываем программу OllyDbg

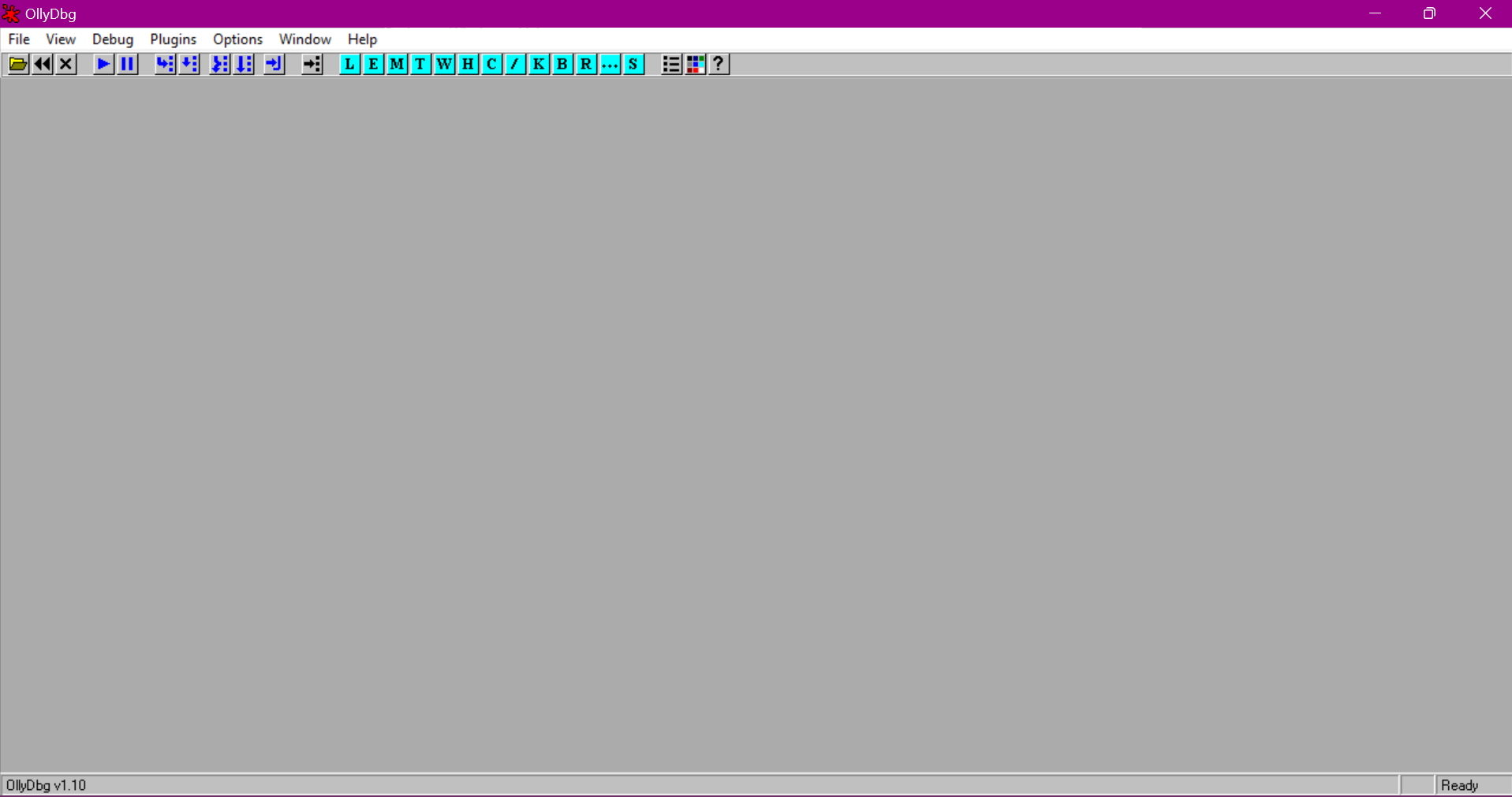


Рис.1

Выберем файл для открытия

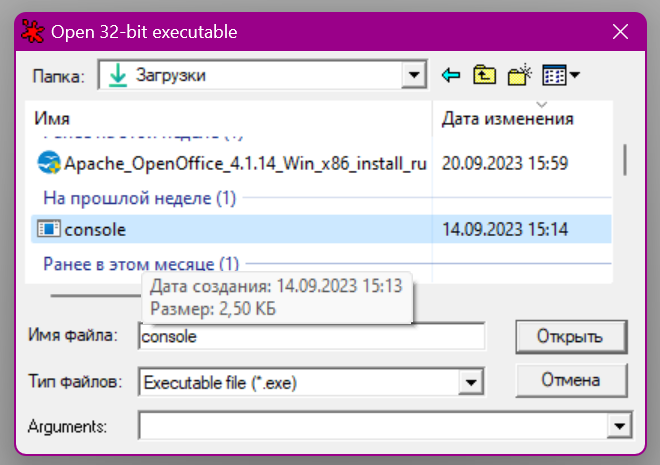


Рис.2

**Задание 3**

Смотрим на содержимое отлаженного файла

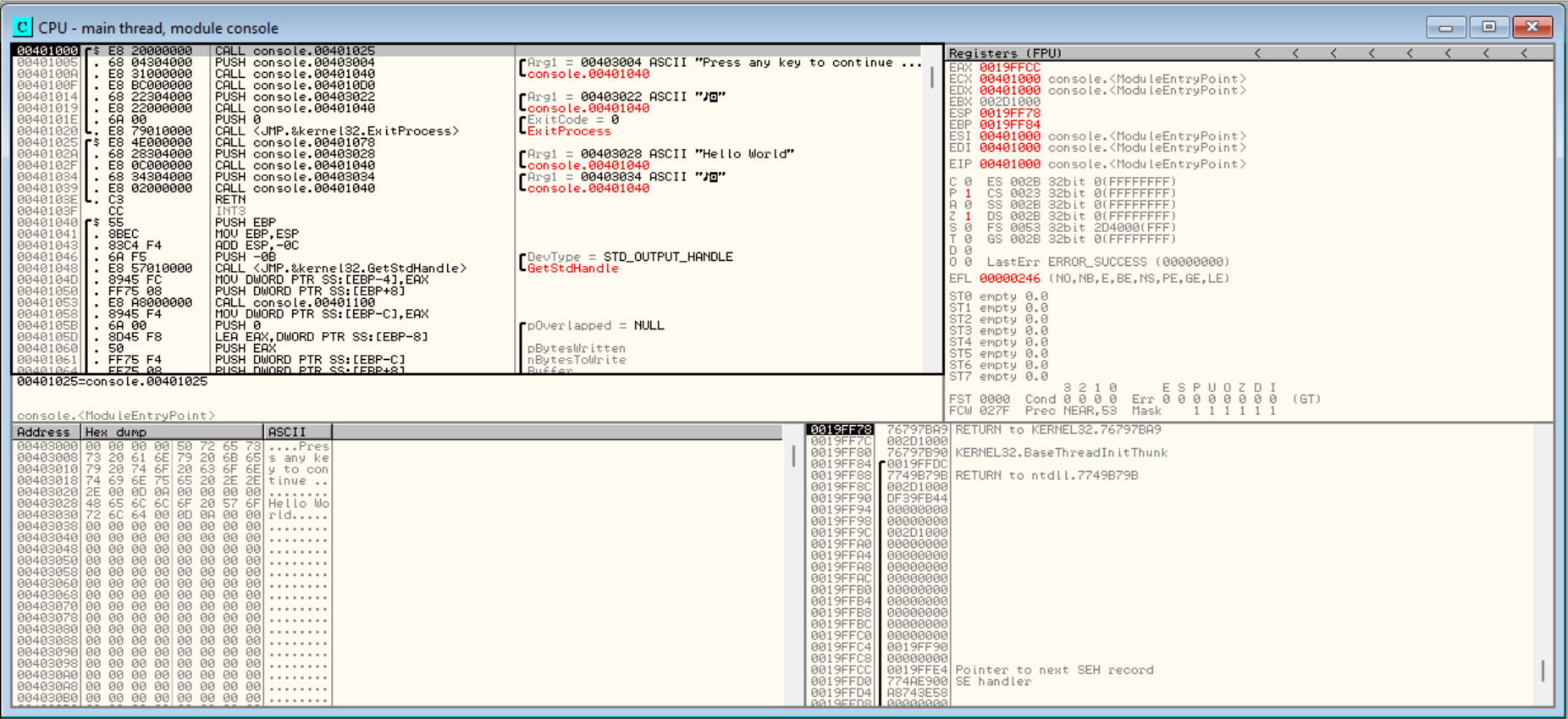


Рис.3

Открываем окно редактирование ассемблера

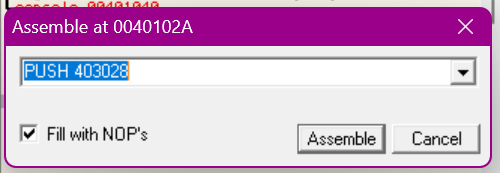


Рис.4

Открываем выбор из контекстного меню

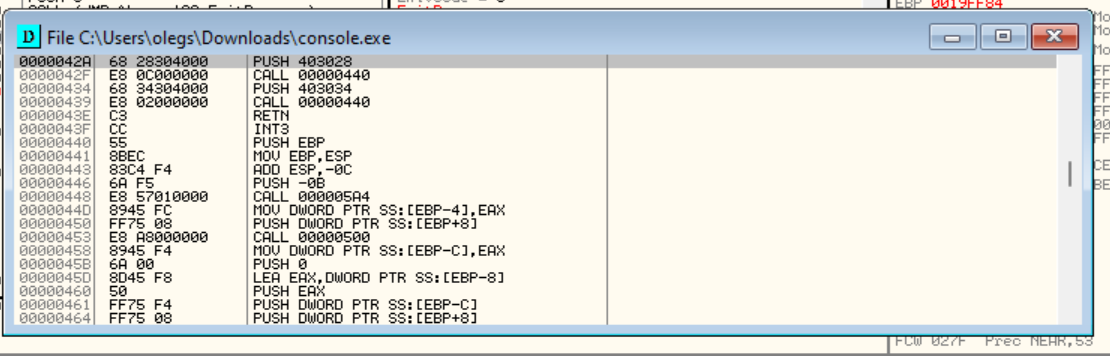


Рис.5

Hex

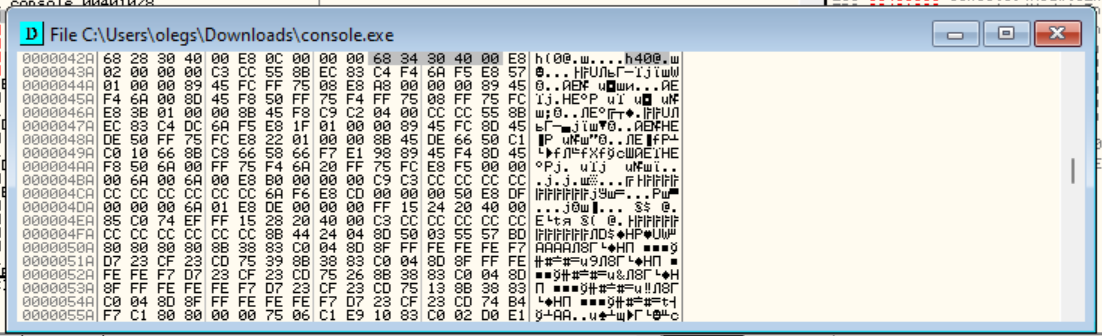


Рис.6

Disassembly

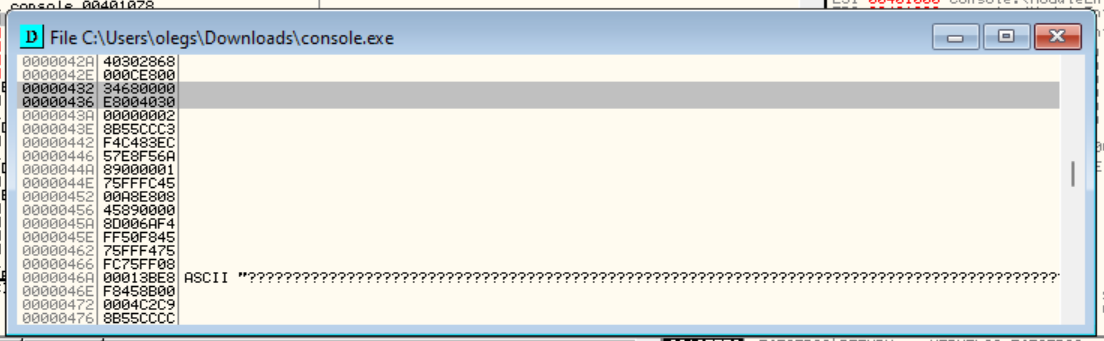


Рис.7

**Задание 4**

Открываем строку для ввода комментария

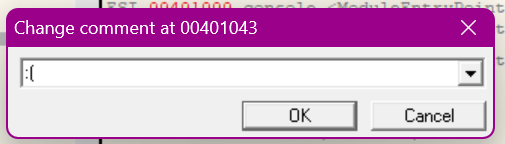


Рис.8

Добавляем 4 комментария

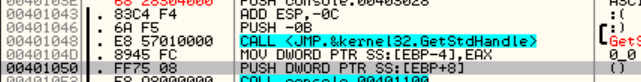


Рис.9

**Задание 5**

Сохраняем текущую версию

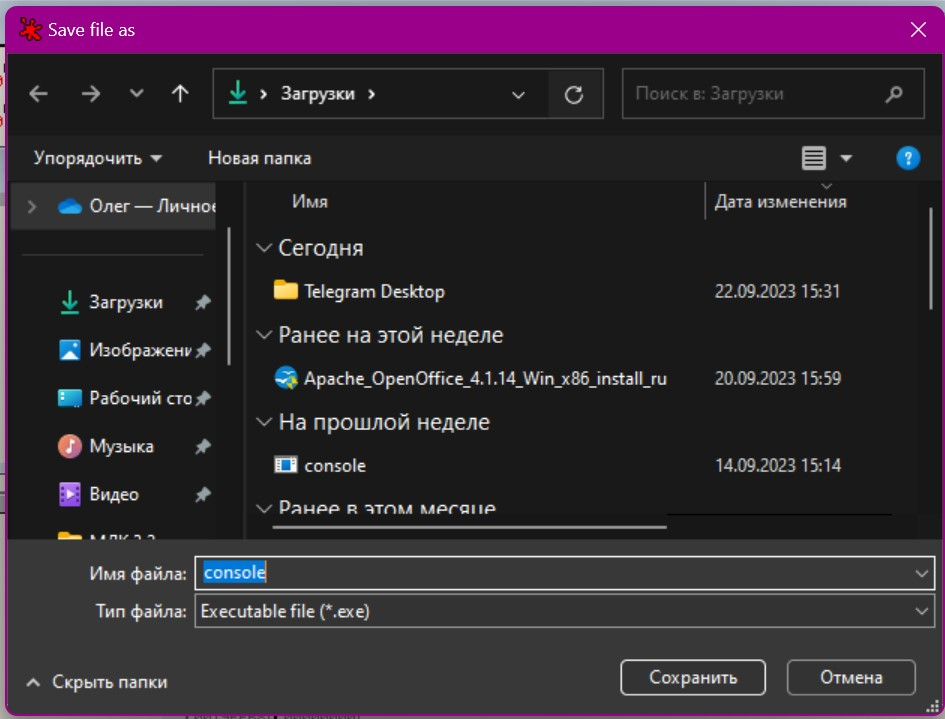


Рис.10

**Задание 6**

Меняем значения регисторв и сохраняем

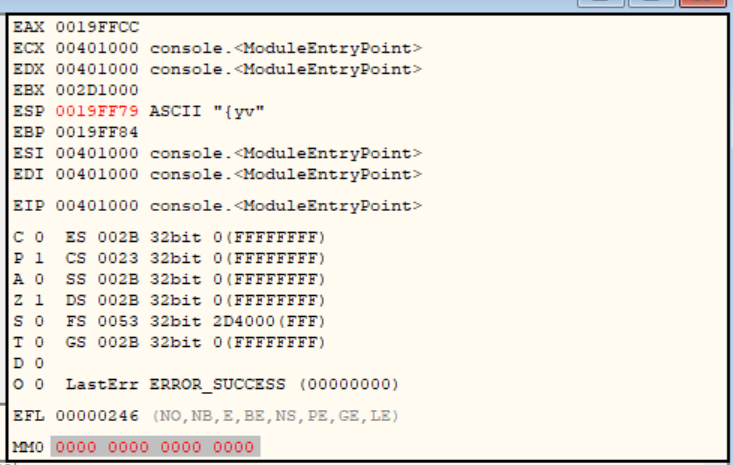


Рис.11

**Задание 7**

Выполняем программу в пошаговом режиме

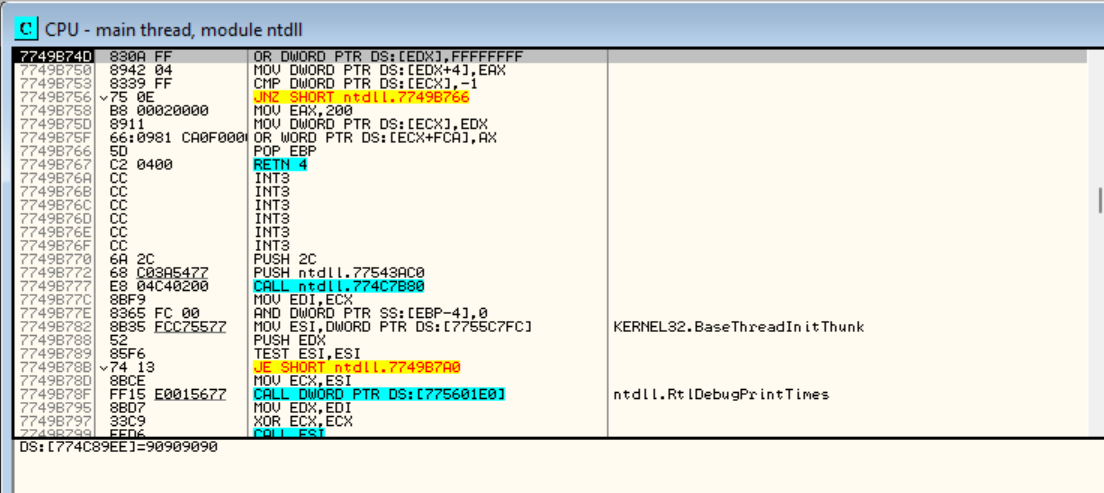


Рис.12

**Задание 8**

Добавляем 3 точки остановки(красные) и 2 точки остановки с условием(фиолетовые)



Рис.13

**Задание 9**

Сохраняем файл

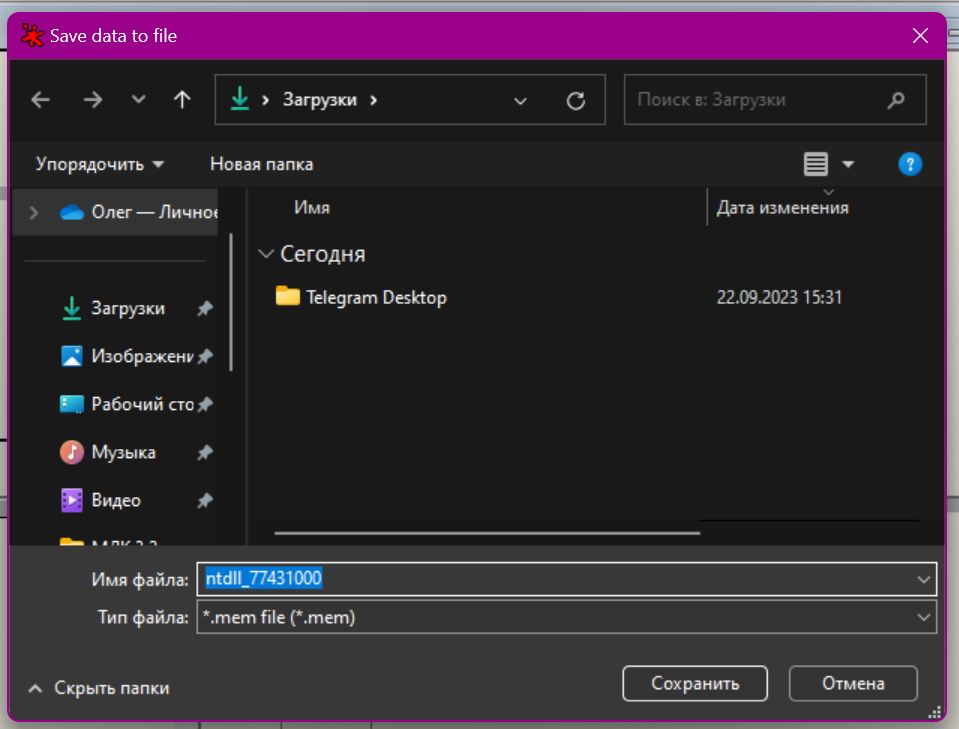


Рис.14

**Задание 10**

Открываем список модулей

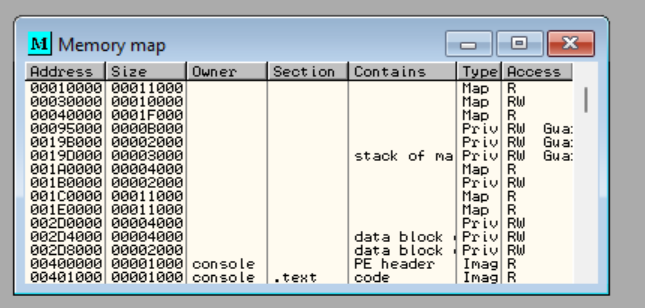


Рис.15

**Задание 11**

Выполняем трассировку программы

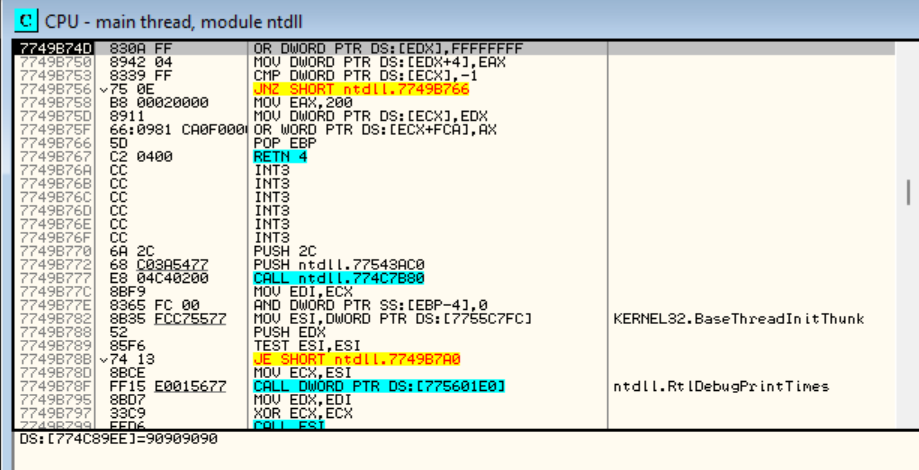


Рис.16



Рис.17

**Вывод:** Я ознакомился с методикой отладки и дизассемблирования программ на языке ассемблера с помощью отладчика OllyDbg.

**Ответы на контрольные вопросы:**

**1. Назначение программы OllyDbg. Версии программы.**

Выполнить программу пошагово, пошаговая отладка, прямая трассировка, профилирование, внесение исправлений; Версии: 1.10, 2.01

**2. Области применения программы**

Дизассемблирование, анализ выполнения программы и разветвление, встроенный ассемблер

**3. Средства отладки программ в OllyDbg**

Можете выполнять программу пошагово (команду за командой), со входом в подпрограммы или выполнять их за один шаг

**4. Пошаговая отладка.**

Устанавливает контрольную точку на каждой выбранной команде и удаляет ее, когда команда достигнута

**5. Прямая трассировка**

Выполняет программу пошагово и записывает еѐ выполнение в большой круговой буфер

**6. Горячие клавиши OllyDbg**

F7: выполняет одну строку кода (если находимся на CALL, то переходим внутрь вызванного участка кода).

F8: выполняет одну команду (строку кода) (если находимся на CALL, то просто выполняет вызов без перехода внутрь и переходит на следующую за CALL строку).  Выполняя одну команду за другой, мы можем в трех остальных окнах следить за тем, как меняется содержимое регистров, секции данных и секции стека.

F2: устанавливает обычную точку останова на отмеченной строке. Чтобы убрать эту точку останова, надо ещё раз нажать F2.

F9: запускает программу, которая будет выполняться до тех пор, пока не встретит точку останова, не произойдет исключение или же не прекратит работу по каким-либо причинам. Когда программа запущена, в нижнем правом углу OllyDbg отображается слово RUNNING. Чтобы временно прекратить выполнение программы, нужно нажать F12 или DEBUG-> PAUSE

**7. Просмотр значений переменных**

При нажатии комбинации Ctrl + B появляется окно поиска. Строка для поиска может вводиться в виде последовательности символов, байтов, символов в кодировке Unicode. Для поиска команд используется комбинация Ctrl + F. Командой меню можно вызвать окно наблюдения. В появившемся окне можно добавить наблюдение, т.е. определить выражение, за которым отладчик будет наблюдать (выводить значение этого выражения). Значения которых отслеживаются при каждом выполнении команды процессора.