Министерство науки и высшего образования РФ

Севастопольский государственный университет

Кафедра информационных систем

ОТЧЕТ

по лабораторной работе №6

Исследование безопасности программного обеспечения

информационных систем в среде отладчика OllyDbg

по дисциплине «Технические средства информационных систем»

Выполнил:

Студент группы ИС/б 17-2-о

Черняев Н.Г.

Проверил:

Чернега В.С.

г. Севастополь 2019

1.Цель работы

Углубление знаний архитектуры 32-разрядных процессоров и системы команд языка ассемблера. Исследование методов защиты программного обеспечения информационных систем и ее нейтрализации, приобретение практических навыков исследования и отладки программ с помощью пакета OllyDbg.

2.постановка задачи

* Повторить теоретический материал, касающийся архитектуры 32-разрядных микропроцессоров, программно доступных регистров и системы команд языка ассемблера (выполняется при домашней подготовке).
* Исследовать способы парольной защиты в программе CRAСKME1.EXE. Для этого выполнить последовательность действий, описных в п. 2 методических указаний. Изменить программу таким образом, чтобы принимался любой вводимый пароль, независимо от того, верный он или неверный.
* С помощью отладчика OllyDbg исследовать способы парольной защиты программ CRAСKME2.EXE, CRAСKME3.EXE и CRAСKME4.EXE, которые расположены в папке лабораторных работ. Определить на каких языках написаны программы. Изменить программы таким образом, чтобы принимался любой вводимый пароль, независимо от того, верный он или неверный.
* С помощью отладчика OllyDbg исследовать способ защиты программы CRAСKME5.EXE. Определите на каком языке написана программа. В данной программе ключ генерируется по введенному в первом поле имени.
* Разработать рекомендации по усилению защиты вскрытия пароля.

3. Ход работы

Первым делом запустим программу OllDgb, а также в ней наше приложение, которое мы попытаемся дизассемблировать, чтобы узнать пароль.

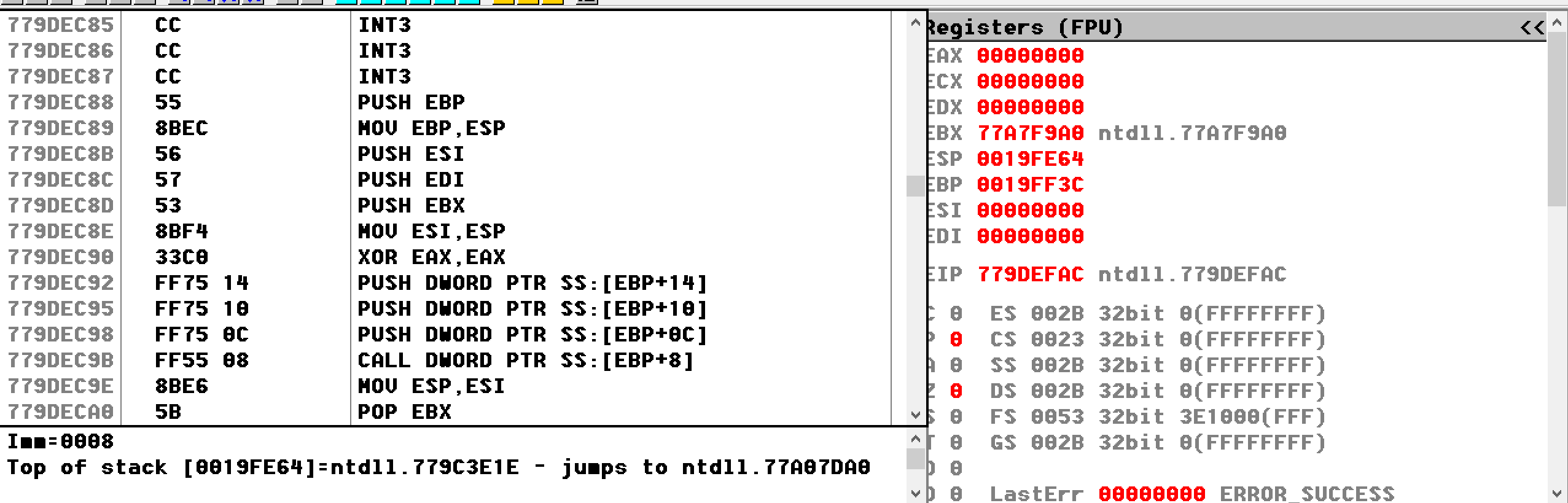


Рисунок 3.1 – Программа открытая в OllDBG

Далее необходимо найти функцию, которая выдает окно с запросом ввода ключа. Для этого выполняем программу пошагово нажимая клавишу F8 до тех пор, пока не появится окошко с запросом ввода

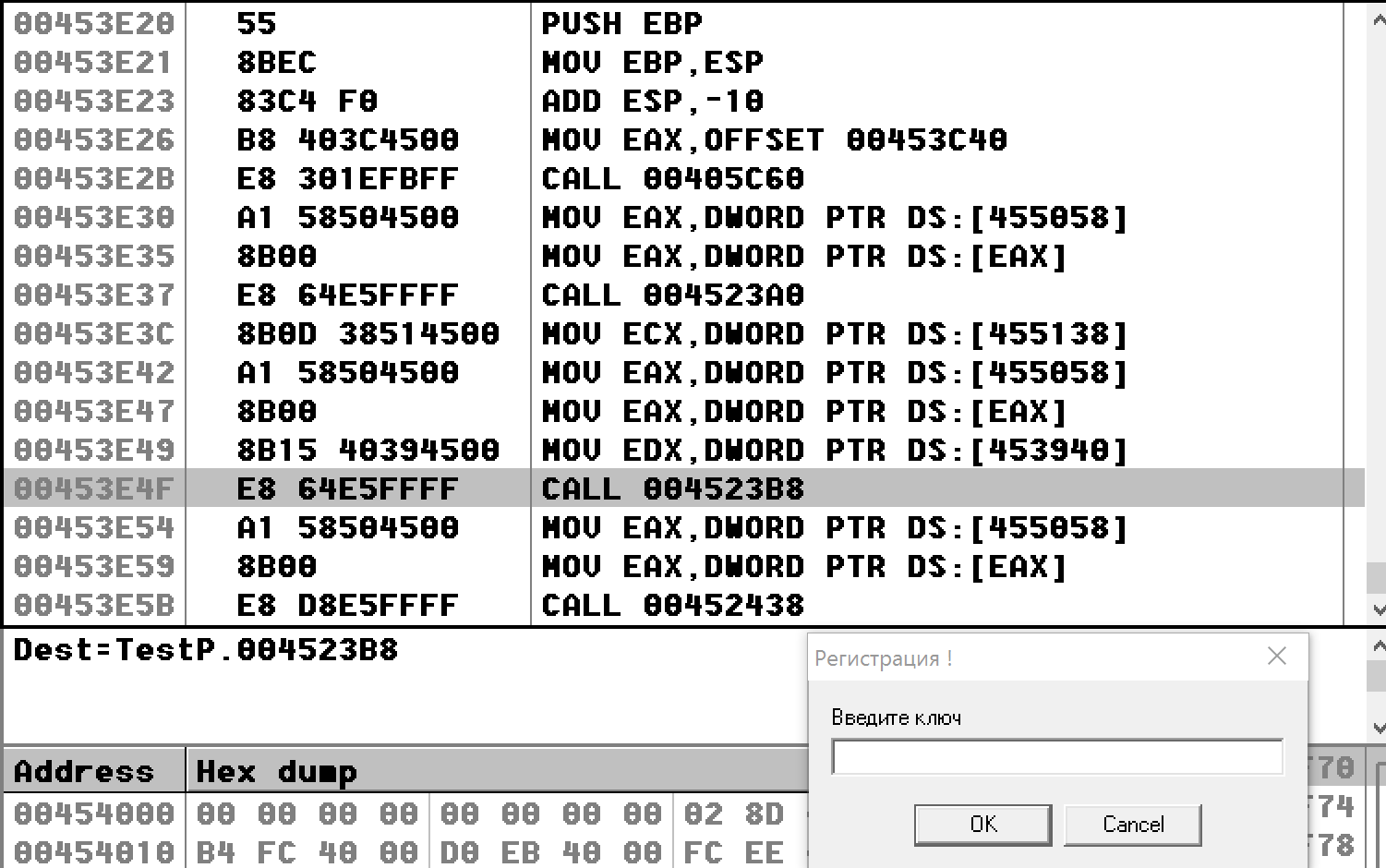


Рисунок 3.2 – Выполнение пошаговой отладки, чтобы найти вызов функции, которая отображает окошко с запросом на ввод пароля.

После нахождения вызова функции окошка нам необходимо найти функцию, которая выводить окно, для этого надо зайти в эту функцию. Для этого была поставлена точка остановы (Breakpoint), и запустить программу.

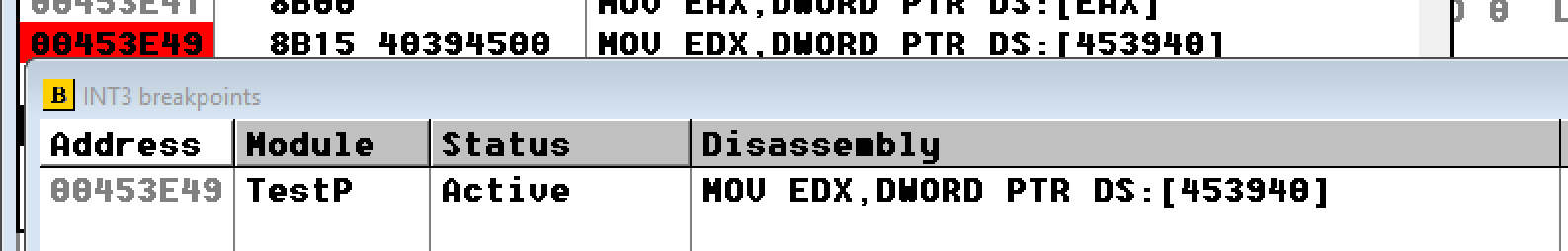


Рисунок 3.3 – Точка останова.

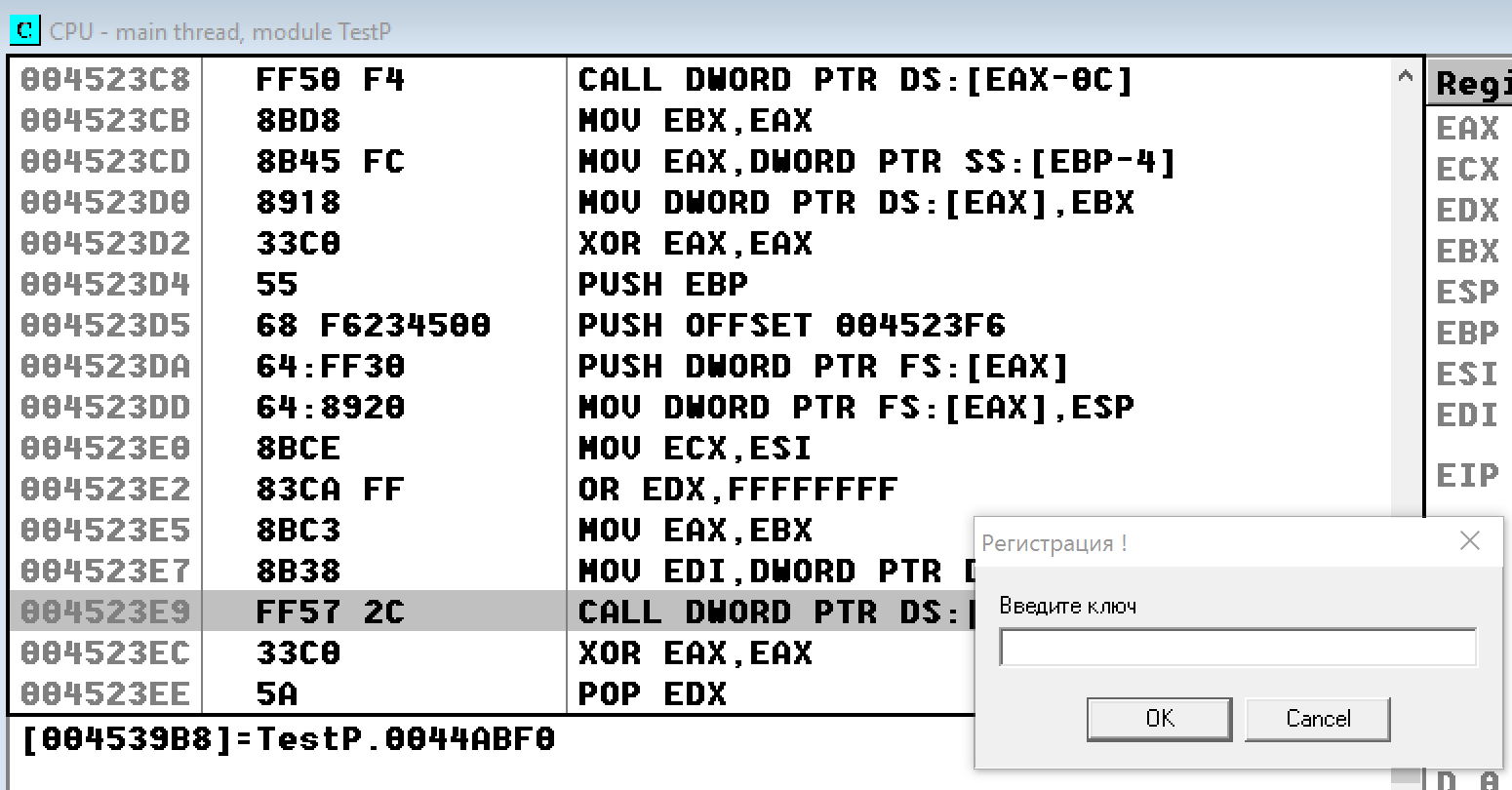


Рисунок 3.4 – Вызов отрисовки окна

Далее установим точки остановы до момента полной отрисовки окна

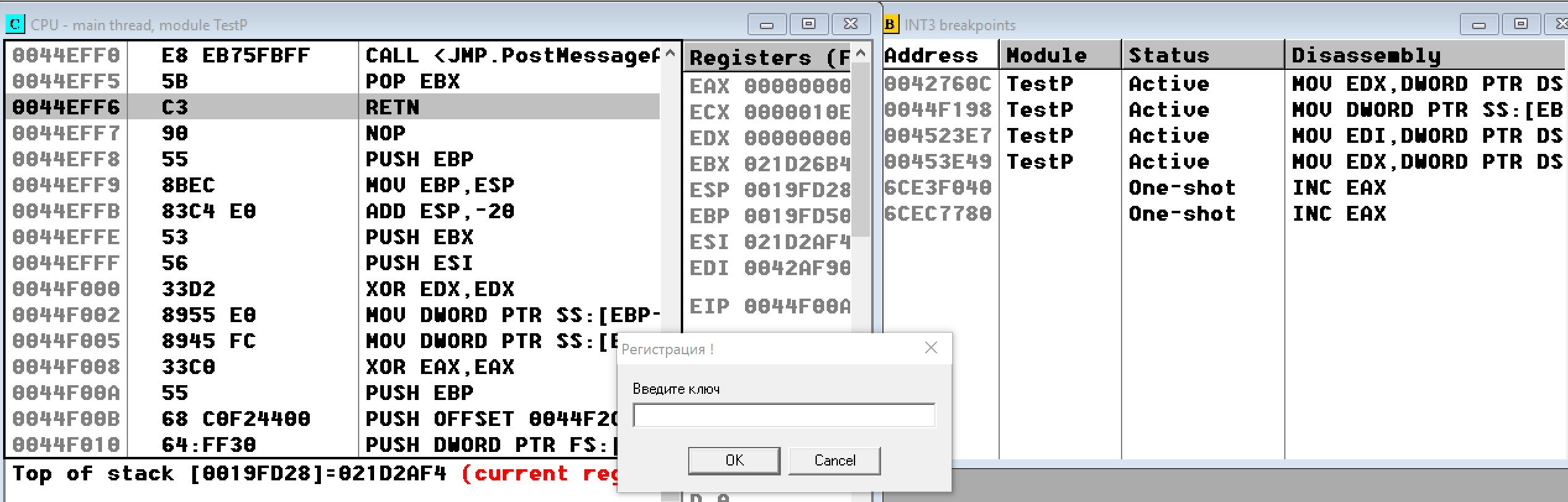


Рисунок 3.5 – Точки остановы

Далее необходимо ввести любой пароль, чтобы появилась ошибка, и поставить точку остановы на данную функцию

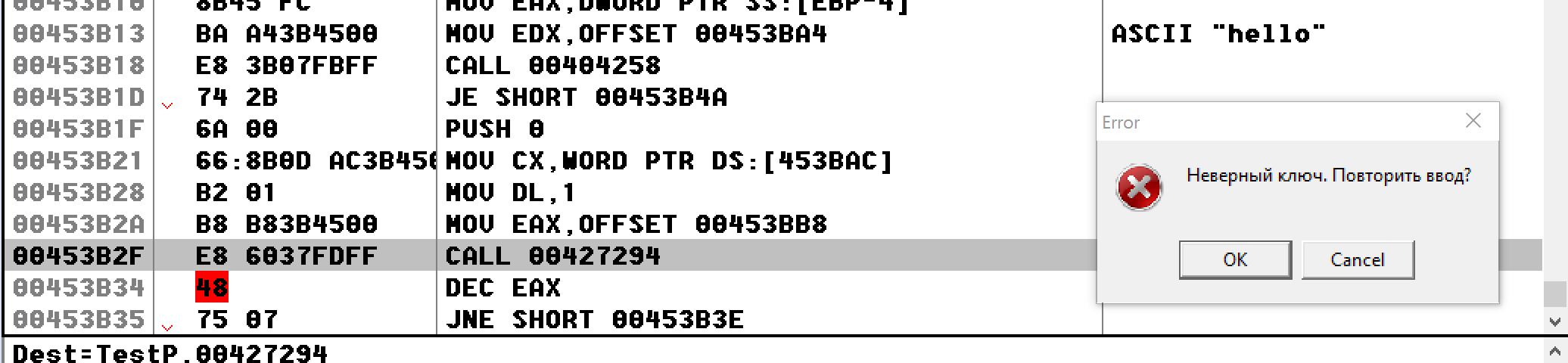


Рисунок 3.6 – Найденная функция для оповещения об ошибке ввода.

Так же можно заметить пароль “hello”, который является ключом для входа в программу. Обычно пароль не хранится просто так в памяти, поэтому сделаем так, чтобы принимался любой пароль.

Для этого необходимо ввести неправильный пароль и найти то место, где сравнивается введенный пароль и неправильный в окне регистров

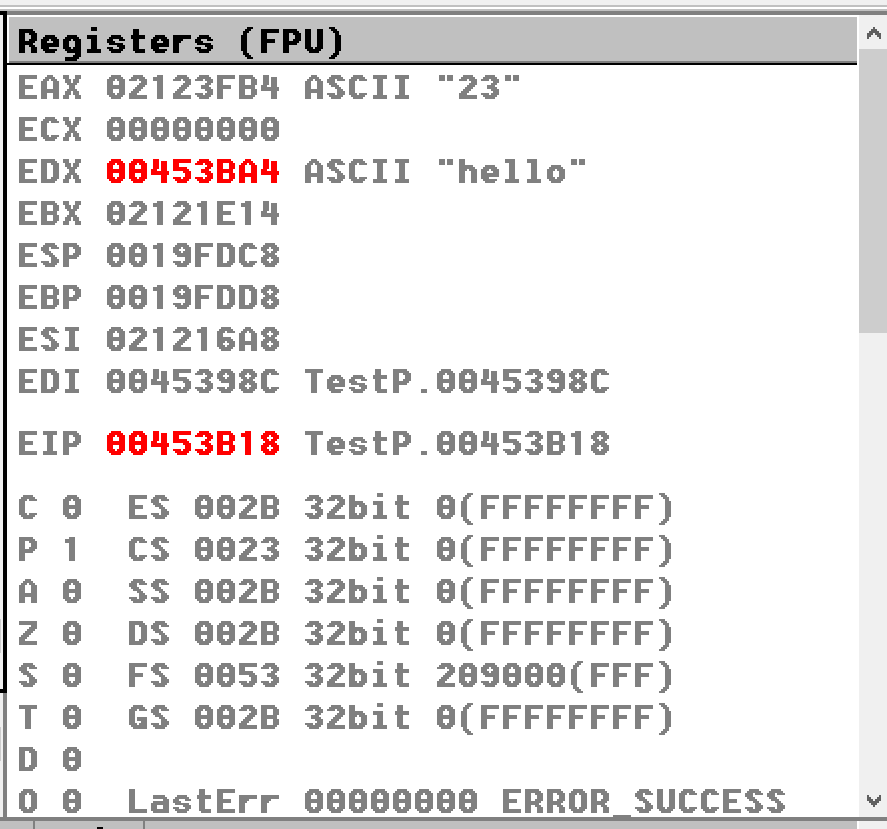


Рисунок 3.7 – Сравнение введенного пароля с правильным.

Далее необходимо найти фрагмент кода, в котором идет проверка и поменять, чтобы программа вне зависимости от введённого пароля открывалась.

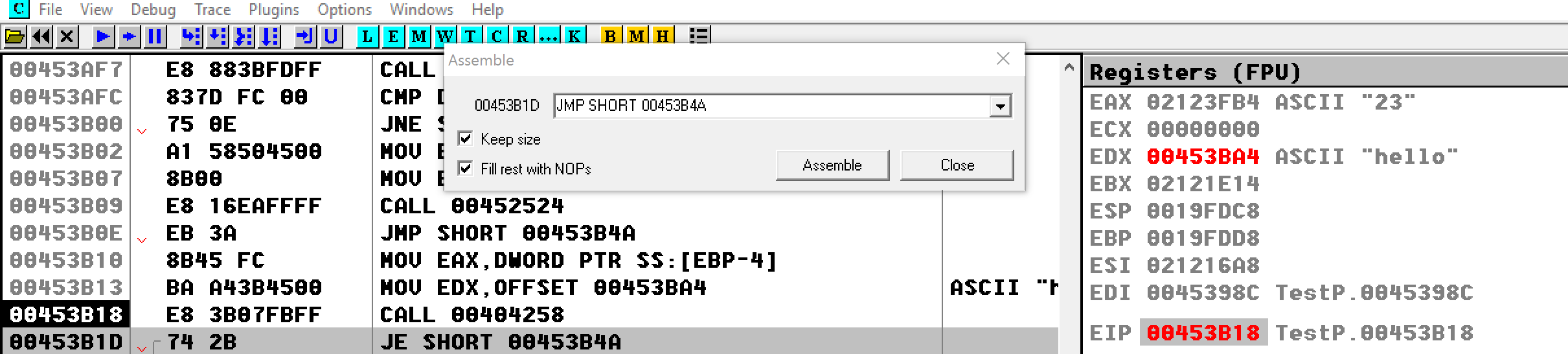


Рисунок 3.8 – Изменение, чтобы программа открывалась вне зависимости от ввода пароля

Далее протестируем программу и увидим, что она открывается вне зависимости от введенного пароля.

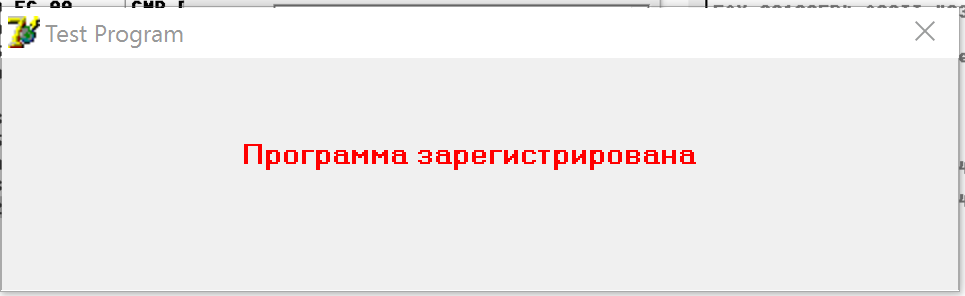


Рисунок 3.9 – Открытие программы при любом вводе.

4.Вывод

В ходе лабораторной работы были углублены знаний архитектуры 32-разрядных процессоров и системы команд языка ассемблера. Были исследованы методов защиты программного обеспечения информационных систем и ее нейтрализации, приобретение практических навыков исследования и отладки программ с помощью пакета OllyDbg.