МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное автономное бюджетное образовательное учреждение высшего

образования

«Севастопольский государственный университет»

Кафедра Информационных систем

Куркчи Ариф Эрнестович

Институт информационных технологий и управления в технических системах

Курс 3 группа ИС(б) – 31о

09.03.02 Информационные системы (уровень бакалавриата)

ОТЧЁТ

о лабораторном практикуме №4

по дисциплине «Инструментальные средства информационных систем»

на тему: «Исследование способов анализа и отладки приложений Win32

в среде отладчика OllyDbg»

Отметка о зачёте \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(дата)

Руководитель практикума

\_доцент\_ \_\_\_\_\_\_\_\_\_\_\_ Карлусов В.Ю.

Севастополь

2016

1. Цель работы

Исследование архитектуры 32-разрядных процессоров и возможностей отладчики при разработке приложений Win32 в OllyDbg, приобретение практических навыков по анализу и отладке программ на языке ассемблера.

2. Постановка задачи

1. Создать приложение типа Win32 с графическим интерфейсом, вычисляющее сумму и разность двух чисел: первое число – номер в группе, второе – число, противоположное номеру первой буквы фамилии в алфавите (отрицательное число в дополнительном коде). Противоположным к некоторому *х* называется число, равное *х* по абсолютной величине, но обратное по знаку (выполняется при домашней подготовке).

2. Загрузить созданное приложение в отладчик OllyDbg и в режиме пошагового выполнения исследовать его работу.

3. В рамках открытого в отладчике OllyDbg приложения произвести следующие операции:

* изменить значения регистров EAX и EBX таким образом, чтобы произошли изменения состояний флагов O, P, Z, S, C;
* поместить значение в стек с помощью инструкции PUSH;
* извлечь значение из стека с помощью инструкции POP;
* изменить значение регистра ESP;
* изменить значение регистра EIP;
* найти инструкцию PUSH 0 и занопать ее.

4. В рамках этого же приложения изучить принцип работы инструкции MOV c 8-ми, 16-ти и 32-х разрядными регистрами и математических инструкций: INC, DEC, ADD, SUB, MUL, IMUL, DIV, NEG (путем выполнения данных инструкций в отладчике OllyDbg). Проанализировать в каких регистра и флагах происходят изменения.

3. Ход работы

Создадим приложения Win32 с использованием Windows Forms (рисунок 3.1)

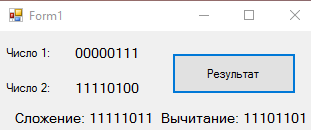


Рисунок 3.1 – Созданное приложение

Запустим отладчик OllyDbg и откроем в нем разработанное приложение.

Изменим значения регистров EAX и EBX таким образом, чтобы произошли изменения состояний флагов O, P, Z, S, C.

Флаг О: Поместим в EAX значение FFFFFFFF и выполним команду ADD EAX,1. Значение флага О изменится (рисунок 3.2)

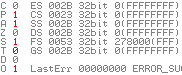
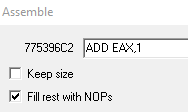
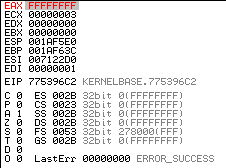


Рисунок 3.1 – Изменение флага О

Флаг P: Сейчас в EAX содержится значение 00000000. Трижды выполним команду ADD EAX,1 и значение флага изменится.

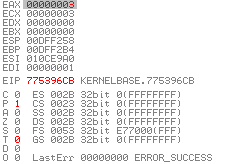


Рисунок 3.2 – Изменение флага Р

Флаг Z: Занесем в EAX значение FFFFFFFF и выполним команду ADD EAX,1. Содержимое станет равно 00000000 и состояние флага Z изменится.

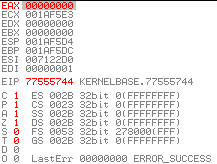


Рисунок 3.3 – Изменение флага Z

Флаг S: изменим значение EAX на FFFFFFF8, что равно ‒8 в десятичной форме. Выполним команду ADD EAX,1 и значение флага S изменится.

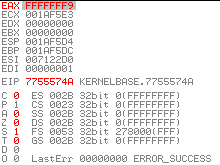


Рисунок 3.4 – Изменение флага S

Флаг С: поместим в EAX значение FFFFFFFF и прибавим 1, флаг переноса станет равен 1.

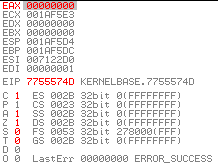


Рисунок 3.5 – Изменение флага С

Для помещения значения в стек выполним команду PUSH 0.

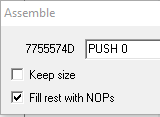


Рисунок 3.6 – Выполнение команды

Состояние стека изменится и в самый его верх будет помещено значение 0 (рисунок 3.7).



Рисунок 3.7 – Состояние стека

Поместим значение из стека в EAX (рисунок 3.8).



Рисунок 3.8 – Состояние стека

Выполним команду POP EAX. Результат работы команды представлен на рисунке 3.9.



Рисунок 3.9 – Значение, помещенное из стека

Для помещения значения в регистр ESP выполним команду POP EAX (рисунок 3.10).



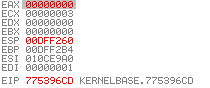


Рисунок 3.10 – Изменение значения регистра ESP

Для изменения значения регистра EIP снова выполним команду POP EAX (рисунок 3.11).

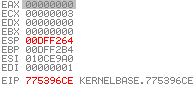


Рисунок 3.11 – Изменение значения регистра EIP

Вывод

В ходе работы была исследована архитектура 32-разрядных процессоров и возможностей отладчики при разработке приложений Win32 в OllyDbg, приобретены практические навыки по анализу и отладке программ на языке ассемблера.