**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИИ**  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ**  
**ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»**  
**(БГТУ им. В.Г.Шухова)**

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

Лабораторная работа №2

Дисциплина «Архит. ВС»

Тема «Структура команд процессора»

Выполнил: ст. группы ПВ-31  
Ковалев Павел Александрович

Проверил: Осипов Олег Васильевич

**Белгород 2020**

**Цель работы:** изучить структуру команд процессора, научиться составлять машинный код простейших команд.

**Задания для выполнения к работе**

1. Ознакомиться с теоретическим материалом главы 2 учебника *В.И. Юро- ва «Assembler» “Программно-аппаратная архитектура IA-32 процессоров Intel”*.
2. В соответствии с вариантом задания определить по символьному описанию команд их машинный код (для 5 команд), а также по машинному коду команд определить их символьное описание (для 2 машинных кодов).

**Выполнение работы**

**AND AL, 'n'**

Команда применяет логическое И к содержимому регистра AL и символу ‘n’ = 01101110.

КОП – 24 - 00100100.

SIB не задействован.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Преф. | КОП |  |  |  | | | SIB | | | Смещ. | Непоср. Операнд |
|  |  | D | W | Mod | Reg/КОП | r/m | Scale | Index | base |  |  |
|  | 001001 | 0 | 0 |  |  |  |  |  |  |  | 01101110 |

В результате получим 24 6E

**MOV [EBX+200], AL**

КОП – 88, d = 0, w = 0. Mod = 10, поскольку размер смещения – 1 байт. Поскольку d = 0, то первый операнд – 001 = EBX, второй – 000 = AL. Так же укажем смещение в обратном порядке.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Преф. | КОП |  |  |  | | | SIB | | | Смещ. | Непоср.Операнд |
|  |  | D | W | Mod | Reg/КОП | r/m | Scale | Index | base |  |  |
|  | 100010 | 0 | 0 | 10 | 000 | 011 |  |  |  | 1100 1000 0000 0000 00000 0000 0000 0000 |  |

В результате получим 8883 С800 0000

**ADD BX, 1110101010101b**

Команда складывает содержимое регистра ВХ с 0001 1101 0101 0101 b = 1D55h.

Операнды имеют размер 16 бит, следовательно префикс – 66h, и w = 1. КОП – 81.

Mod – 11, т. к. операндов в памяти нет. Reg – 000.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Преф. | КОП |  |  |  | | | SIB | | | Смещ. | Непоср. Операнд |
|  |  | D | W | Mod | Reg/КОП | r/m | Scale | Index | base |  |  |
| 01100110 | 100000 | 0 | 1 | 11 | 000 | 011 |  |  |  |  | 0101 0101 0001 1101 |

В результате получим 66:81С3 551D

**CMP DI, BX**

Сравнивает содержимое DI и BX.

Поскольку операция проводится над регистрами размером 16 байт, то префикс будет 66h, и w = 1.

КОП – 00111011, d = 1, w = 1. Поскольку d = 1, то первый операнд в reg, второй в r/m.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Преф. | КОП |  |  |  | | | SIB | | | Смещ. | Непоср. Операнд |
|  |  | D | W | Mod | Reg/КОП | r/m | Scale | Index | base |  |  |
| 01100110 | 001110 | 1 | 1 | 00 | 111 | 011 |  |  |  |  |  |

**TEST [ECX\*2+EDI+761], 4567**

Команда выполняет логическое сравнение над содержимым реестра bx и 4567 = 11D7h, устанавливая флаги SF, ZF, и PF, при этом обнуляя OF и CF. КОП – F7h = 1111 0111, т.к. первый операнд -регистр, а второй – значение imm16.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Преф. | КОП |  |  |  | | | SIB | | | Смещ. | Непоср. Операнд |
|  |  | D | W | Mod | Reg/КОП | r/m | Scale | Index | base | 1001 1111 0000 0010 |  |
|  | 111101 | 1 | 1 | 10 | 000 | 001 | 01 | 001 | 111 | 0000 0000 0000 0000 | 1101 0111 0001 0001 0000 0000 0000 0000 |

**8807**

Первый байт - 10001000, КОП – 10001000b = 88h, что соответствует команде MOV.

Второй байт – 0000 0111.

Mod = 00, следовательно поле смещения отсутствует, при reg = 000 и w = 0 первым операндом будет регистр [EDI], вторым - AL. Поскольку размер регистра EDI больше размера регистра AL, приведем размер до байта.

MOV word ptr [EDI], AL. Не работает.

**8B55 1F**

Первый байт – 1000 1011, КОП = 100010, d = 1, w = 1.

Такой КОП соответствует команде MOV.

Второй байт – 0101 0101, mod = 01, reg = 010, r/m = 101.

Поскольку d = 1, то первый операнд при w = 1 будет EDX, второй – EBP.

MOD EDX, [EBP+1Fh]