

Языки программирования (Asm)

Занятие №4. Команды битовых сдвигов.

МИРЭА - РТУ, БК №252

Москва 2020

Команды сдвигов в NASM

Из языков программирования высокого уровня нам известны два оператора, которые реализуют битовые сдвиги. В языках C/C++ это операторы `>>`, `<<`.

```
1 block <<= 11; // Логический сдвиг на 11 разрядов влево
```

Далее мы рассмотрим следующие команды, которые реализуют операции сдвигов в процессорах архитектуры x86:

- 1 ROL, ROR
- 2 RCL, RCR
- 3 SAL, SAR
- 4 SHL, SHR
- 5 SHLD, SHRD

Синтаксис команд битовых сдвигов

Команды ROL, ROR, RCL, RCR, SAL, SAR, SHL, SHR имеют два параметра:

Команда приемник, число сдвигов

Приемник может задаваться как регистром, так и областью памяти

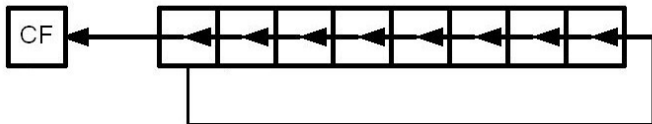
```
1 rol eax, 5 ; Сдвиг внутри регистра EAX на 5 бит
2 mov [var1], dword 0xF000F00F
3 rol dword [var1], 1 ; Сдвиг внутри переменной на 1 бит
```

При работе с областью памяти необходимо указывать, к скольким байтам мы хотим обратиться. В данном случае приставка **DWORD** означает, что мы работаем с четырьмя байтами, хранящимися по адресу **var1**.

```
1 rol word [var2], 3 ; Обращение к 2 байтам
2 rol byte [var3], 3 ; Обращение к 1 байту
```

Циклические сдвиги

ROL

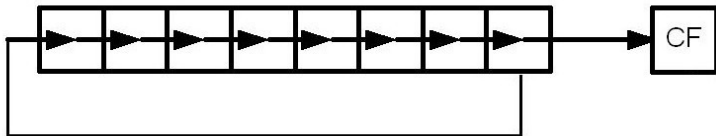


1 `rol eax, 5` ; Циклический сдвиг на 5 бит влево

Команда ROL циклически сдвигает все биты первого операнда влево на N разрядов, при этом старшие N бит первого операнда становятся на место младших N бит. Одновременно последний выдвигаемый бит становится значением флага переноса CF. Число сдвигаемых разрядов задается вторым операндом.

Циклические сдвиги

ROR

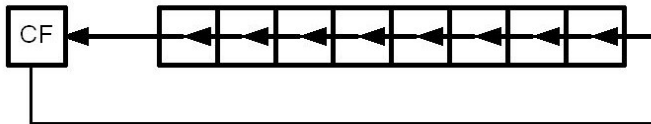


```
1 ror eax, 3 ; Циклический сдвиг на 3 бита вправо
```

Команда ROR циклически сдвигает все биты операнда вправо на N разрядов, при этом младшие N бит операнда становятся на место старших N бит. Одновременно последний выдвигаемый бит становится значением флага переноса CF. Число сдвигаемых разрядов задается вторым операндом.

Циклические сдвиги

RCL



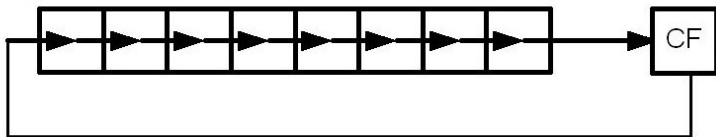
Команда RCL сдвигает все биты операнда влево на N разрядов, при этом старший бит становится значением флага переноса CF.

Одновременно старое значение флага переноса CF задвигается в операнд справа и становится значением младшего бита операнда.

```
1 rcl eax, 1
```

Циклические сдвиги

RCR



Команда RCR сдвигает все биты операнда вправо на N разрядов, при этом младший бит становится значением флага переноса CF.

Одновременно старое значение флага переноса CF задвигается в операнд слева и становится значением старшего бита операнда.

```
1 rcr ebx, 1
```

Левый сдвиг со знаком

Команда SAL сдвигает биты операнда влево на N разрядов, значение последнего вытолкнутого бита попадает во флаг переноса, а освободившиеся биты заполняются нулями. Данная команда выполняет то же действие, что и команда логического сдвига влево (SHL).

```
1 mov ax, -2116
2 sal ax, 4
3 mov [bytes], ax
4
5 mov ecx, 16
6
7 for_print: ; Начало цикла для вывода на экран
8     push ecx
9     rol word[bytes], 1
10    jnc print_zero
11
12    print_one:
```


Правый сдвиг со знаком

Команда SAR сдвигает биты операнда вправо на N разрядов, значение последнего вытолкнутого бита сохраняется во флаге переноса, а освободившиеся биты заполняются значением старшего бита (отвечающего за знак).

```
1 mov ecx, 10
2 mov eax, 298
3 m1:
4     sar eax, 1
5     push eax
6     loop m1
```

Логические сдвиги

Команды SHL и SHR сдвигают биты операнда соответственно влево или вправо на N разрядов и изменяют состояние флага переноса (CF). Как и во всех подобных командах, в CF сохраняется значение последнего вытолкнутого бита. Данные сдвиги ничем не отличаются от битовых сдвигов в языке программирования C или C++.

```
1 mov eax, 0xFA04
2 shl eax, 7
```

Логический сдвиг на 7 разрядов влево

```
1 mov eax, 0xFA04
2 shr eax, 4
```

Логический сдвиг на 4 разряда вправо

SHLD. Левый сдвиг двойной точности

SHLD приёмник, источник, количество сдвигов

Операнды приёмник и источник могут быть только регистрами общего назначения (РОН).

Команда сдвигает операнд приёмник влево на число битов, указанных операндом количество сдвигов. Операнд источник обеспечивает биты, которые задвигаются в приёмник справа (начиная с бита 0 приёмника). Операнд количество сдвигов — целое число без знака, которое может быть непосредственным 8-разрядным значением или содержимым регистра CL.

Флаг CF заполняется последним битом, сдвинутым из операнда приёмник. Флаг OF устанавливается в 1 для одноразрядного сдвига, если изменился знаковый разряд приёмника, иначе он равен нулю. Если операнд количество сдвигов равен нулю, то флаги не изменяются.

```
1 shld eax, ebx, 1
```

SHRD. Правый сдвиг двойной точности

SHRD приёмник, источник, количество сдвигов

Операнды приемник и источник могут быть только регистрами общего назначения (РОН).

Команда сдвигает операнд приемник вправо на число битов, указанных операндом количество сдвигов. Операнд источник обеспечивает биты, которые задвигаются в приемник слева (начиная со старшего бита приемника). Операнд количество сдвигов — целое число без знака, которое может быть непосредственным 8-разрядным значением или содержимым регистра CL.

Флаг CF заполняется последним битом, сдвинутым из операнда приемник. Флаг OF устанавливается в 1 для одноразрядного сдвига, если изменился знаковый разряд приемника, иначе он равен нулю. Если операнд количество сдвигов равен нулю, то флаги не изменяются.

```
1 shrd eax, ebx, 1
```