

Регістри стану та управління

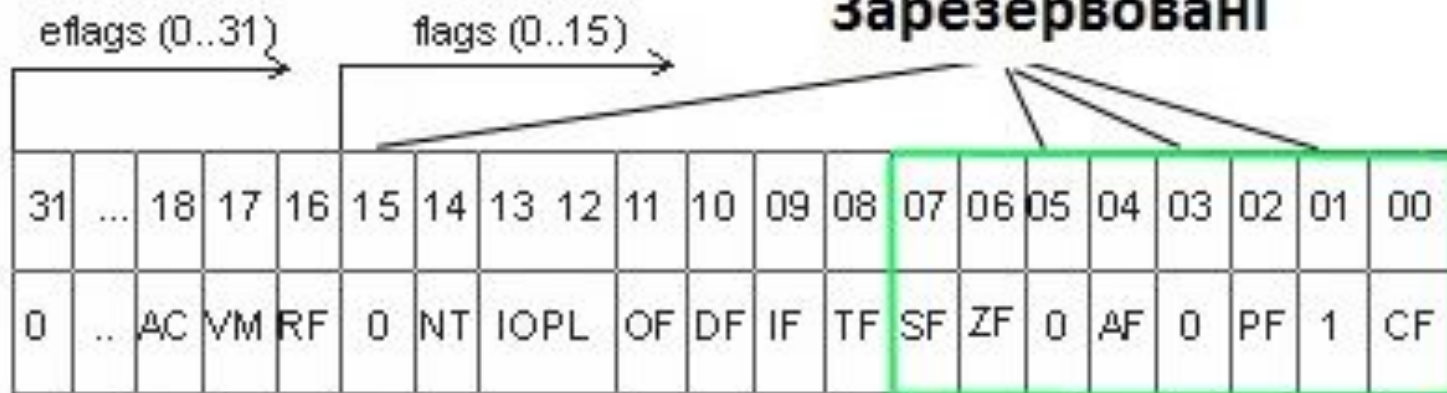
В мікропроцесор включені декілька реєстрів, які постійно містять інформацію про стан, як самого мікропроцесора, так і програми, команди якої в даний момент завантажені на конвеєр.

До цих реєстрів відносяться:

Регістр прапорців **eflags/flags**;

Регістр покажчика команди **eip/ip**.

Зарезервовані



```

CPU 80486
#lab1#main: PUSH DS
             cs:0000 1E          push    ds
#lab1#27: xor ax,ax
             cs:0001 33C0       xor     ax,ax
#lab1#28: mov bx,dfg
             cs:0003 8B1E1200   mov    bx,[0012]
#lab1#29: mov cx,50
             cs:0007 B93200   mov    cx,0032
#lab1#31: MOV AX,DSEG
             cs:000A B8A95B   mov    ax,5BA9
#lab1#32: MOV DS,AX
             cs:000D 8ED8     mov    ds,ax
#lab1#33: MOV AX,0; тхЕэεС№ёёИфрщчяЕюЎхфееЈ
             cs:000F B80000   mov    ax,0000
#lab1#34: CALL MY_PROC; т↓чютяЕюЎхфееЈ

ds:0000 CD 20 FF 9F 00 9A F0 FE = Я ЬЕИ
ds:0008 1D F0 E0 01 30 22 AA 01 +Ер00"к0
ds:0010 30 22 89 02 8B 1C FD 0D 0"Иел-хЈ
ds:0018 01 01 01 00 02 FF FF FF 000 0
ds:0020 FF FF FF FF FF FF FF FF

ax 0000 c=0
bx 0000 z=0
cx 0000 s=0
dx 0000 o=0
si 0000 p=0
di 0000 a=0
bp 0000 i=1
sp 0140 d=0
ds 5B85
es 5B85
ss 5B95
cs 5BAB
ip 0000

ss:0148 0002
ss:0146 3245
ss:0144 6791
ss:0142 0809
ss:0140 0501
    
```

Мнемоніка прапорця	Прапорець	№ біту в eflags	Вміст і призначення
CF	Прапорець перенесення (Carry Flag); Переповнення	0	1 — вказує на переповнення старшого біту при арифметичних командах. Більшим являється 7, 15, 31-ий біт в залежності від розмірності операнду.
ZF	Прапорець нуля (Zero Flag)	6	1 — результат нульовий; 0 — результат не нульовий
SF	Прапорець знаку (Sign Flag)	7	Відображає стан старшого біту результату (біти 7, 15, 31 для 8, 16, 32-розрядних операндів відповідно): 1 — старший біт результату дорівнює 1; 0 — старший біт результату дорівнює 0
OF	Прапорець переповнення (Overflow Flag)	11	1 — в результаті операції відбувається перенесення (займа) в(із) більшого знакового біта результату (біти 7, 15 чи 31 для 8, 16 чи 32-розрядних операнд відповідно);
PF	Прапорець парності (Parity Flag)	2	1 — 8 менших розрядів (тільки для 8 менших розрядів) результату містять парну кількість одиниць.
AF	Прапорець корекції (Adjust Flag)	4	1- якщо арифметична операція здійснює перенесення чи займа в(із) 3-го біта результату, інакше – скидається. Цей прапорець використовується для двійково-кодованої десяткової (BCD - Binary-Coded Decimal) арифметики.
IF	Прапорець дозволу переривань (Interrupt enable Flag)	9	1 – то у відповідь на IRQ процесор генерує переривання; 0 – процесор не відповідає на них(але не ігнорує).
DF	Прапорець напрямку (Direction Flag)	10	0 – рядкові команди опрацьовують рядки даних, переходячи від менших адрес до більших (CLD); 1 – у зворотному напрямку (STD).

Мнемоніка прапорця	Прапорець	№ біту в eflags	вміст і призначення
CF	Прапорець перенесення (Carry Flag); переповнення	0	1 — вказує на переповнення старшого біта при арифметичних командах. Старшим являється 7, 15, 31-ий біт в залежності від розмірності операнда ДЛЯ БЕЗЗНАКОВОЇ АРИФМЕТИКИ.
AF	Прапорець корекції (Adjust Flag)	4	1- якщо арифметична операція виконує перенесення чи займає в/із 3-ій біт результату, інакше – скидається. Цей прапорець використовується для двійково-кодованої десяткової (BCD - Binary-Coded Decimal) арифметики. для BCD-арифметики
OF	Прапорець переповнення (Overflow Flag)	11	1 — в результаті операції відбувається перенесення в(із) старшого, знакового результату (біти 7, 15 чи 31 для операндів відповідної розрядності) для знакової арифметики

SF	Прапорець знаку	7	Відображає стан старшого біта результату (біти 7, 15, 31 для операнд відповідної розрядності) 1 — старший біт результату дорівнює 1; 0 — старший біт результату дорівнює 0
TF	Прапорець пастки	8	1 – процесор використовує по-командне налаштування поточної програми; 0 - програма виконується звичним чином
IOPL	Рівень привілеїв введення/виведення (Input/Output Privilege Level)	12, 13	Використовується в безпечному режимі роботи мікропроцесора для контролю доступу до команд введення/виведення в залежності від привілейованості задачі
NT	Прапорець вкладеної задачі (Nested Task flag)	14	1 – поточна задача являється викликаною із попередньої; 0 – поточна задача НЕ являється викликаною з попередньої.
RF	Прапорець відновлення (Resume Flag)	16	Керує відповіддю процесора на виключення налагодження.
VM	Прапорець віртуального режиму 8086 (Virtual-8086 Mode flag)	17	1 – процесор переходить в режим віртуального 8086; 0 – повертається в безпечному режимі .
AC	Прапорець перевірки вирівнювань (Alignment Check flag)	18	1- змушує процесор перевіряти вирівнювання при доступі до пам'яті і у випадку не вирівняного доступу генерувати виключення.
VIF	Прапорець віртуальних переривань (Virtual Interrupt)	19	Це віртуальний образ прапорця IF, використовується спільно з прапорцем VIP при увімкненому розширенні режиму віртуального 8086.

VIP	Прапорець очікування віртуального переривання (Virtual Interrupt Pending flag)	20	Встановлюється, коли виникає переривання. Процесором лише зчитується і використовується разом з прапорцем VIF; змінюється лише програмно.
ID	Прапорець ідентифікації (IDentification flag)	21	Якщо програма змогла встановити і скинути цей прапорець, то значить, що процесор може виконати команду CPUID.

Взаємодія команд з прапорцями EFLAGS

в таблиці наведено вплив команд на прапорці в регістрі прапорців EFLAGS, при цьому використовуються наступні позначення:

- T** : прапорець перевіряється.
- M** : прапорець змінює своє значення
- 0** : прапорець скидається
- 1** : прапорець встановлюється
- : значення прапорця не визначене
- R** : значення прапорця відновлюється в попереднє
- Порожнє місце** : прапорець не змінюється

Опис	Команда	OF	SF	ZF	AF	PF	CF	TF	IF	DF	NT	RF
Додавання двох операндів	ADD	M	M	M	M	M	M					
Операція логічного множення	AND	0	M	M	-	M	0					
Передача управління близькій процедурі	CALL											
Порівняння двох операндів	CMP	M	M	M	M	M	M					
Виконання операції ділення двох беззнакових значень	DIV	-	-	-	-	-	-					
Операція ділення значень зі знаком	IDIV	-	-	-	-	-	-					
Операція множення цілих значень зі знаком	IMUL	M	-	-	-	-	M					
Збільшення значення операнда в пам'яті чи реєстрі на 1	INC	M	M	M	M	M						
Завантаження елемента із послідовності в реєстр-акумулятор	LODS									T		
Операція множення двох цілих чисел без врахування знаку	MUL	M	-	-	-	-	M					
Зміна знаку	NEG	M	M	M	M	M	M					
Інвертування всіх бітів операнда	NOT											
Операція логічного «АБО»	OR	0	M	M	-	M	0					

Опис	Команда	OF	SF	ZF	AF	PF	CF	TF	IF	DF	NT	RF
Виведення із пам'яті послідовності байт, слів, подвійних слів	OUTS									T		
Одержання слова чи подвійного слова із стеку	POP											
Одержання із стеку регістрів загального значення	POPA											
Одержання із стеку слова і відновлення його в регістрі прапорців flags	POPF	R	R	R	R	R	R	R	R	R	R	
Розміщення вмісту операнда в стек	PUSH											
Розміщення в стек регістрів загального значення	PUSHA											
Розміщення у вершині стеку (ss:sp) вмісту регістру прапорців flags	PUSHF											
Операція циклічного зміщення операнда ліворуч через прапорець перенесення cf	RCL на 1 бит	M					T M					
Операція циклічного перенесення операнда праворуч через прапорець перенесення cf	RCR на 1 бит	M					T M					
Операція циклічного зміщення операнда ліворуч	ROL на 1 бит	M					M					
Арифметичне зміщення операнда ліворуч	SAL на 1 бит	M	M	M	-	M	M					
Операція логічного виключаючого «АБО»	XOR	0	M	M	-	M	0					

Реалізація переривань

Зчитування символів і запис до пам'яті триває кілька мікросекунд. Якщо ЦП буде лише приймати ці символи, то більшість часу він буде простоювати. Тому, після завершення обробки символу, ЦП переходить до виконання іншої програми. Кожен раз, після натиснення кнопки, пристрій подає запит на переривання, ЦП перериває виконання програми і переходить до виконання процедури опрацювання для переривань клавіатури.

Кожна така процедура являється певною програмою, яка записана в пам'яті.

Для того, щоб до неї підійти – потрібно знати її початкову адресу. Ця початкова адреса і записана в так званому векторів переривань. Кожне з можливих 256 переривань має свій номер в таблиці векторів переривань в пам'яті. Вектор переривань складається із двох слів:

CS:IP

Записані в початкових адресах від 0 до 03FFH (1024 байти).