[Q]: Повиснет ли OS/2, если отключить прерывания по CLI и зациклиться?

[A]: Alex Iliynsky (2:5020/23)

В 286-х и выше процессорах, с появлением качественной защиты и режима Vm86(386+) появилось также понятие IOPL - Input Output Privilege Level - “переменная” системы, которая определяет, какому уровню привелегий (0-3) разрешено работать с командами ввода вывода и такими как cli/sti. То есть для того, чтобы обращаться в порты или запрещать перывание, задача должна иметь уровень привелегий ⇐ IOPL, иначе в момент выполнения, она фолтанется.

Задачи написанные для защищенного режима, обычно не используют cli/sti,

за исключением драверов, чего не скажешь о Vm86 (DOSовские чаще всего) - поскольку в real mode это ни к чему не критично. Задачи Vm86 всегда бегают в третьем кольце защиты - PL==3. Если IOPL==3, то при выполнении в Vm86 задаче CLI, аппаратные прерывания не будут генерится до тех пор, пока в этой задаче не пройдет STI. Если использовать IOPL!=3, то можно отслеживать выполнение CLI/STI по фолтам, которые они будут вызывать, но это приведет к падению скорости выполнения задач Vm86 за счет постоянного перехода в защищенный режим и обратно при каждом фолте.

При IOPL==3, и VM86 задаче, вызвавшей cli и к примеру зависнувшей, ничто не может вывести процессор из этого состояния, кроме NMI, которые не маскируются по CLI.

На этом принципе сделаны fail-safe (watchdog) NMI timer на EISA/MCA. Таймер

программируется на определенный интервал, после которого происходит NMI, который дает шанс операционной системе решить, что делать - останавливать больную задачу, или игнорировать ее(висеть дальше). Именно поэтому, OS/2, которая использует IOPL==3 не виснет на двухстрочной задаче на EISA и MCA шинах. Возможно, есть реалиации подобных FS NMI timers на обычной ISA, но я про это не слышал.

Intel, для убирания этого “бага” своих процессоров, добавил туда специальную фичу - VME - Virtual Mode Extension, информация по которой есть секрет фирмы Intel и выдается ею под подписку о неразглашении. Примерная суть ее следущая - появились два флажка VIP и VIF - Virtual Interrupt Pending и Virtual Interrupt Flag. Судя по названию - первое говорит о том, что VM86 задача хочет интеррапт, а второй - это виртуалтзованый аналог IF - Interrupt Flag, который и ставится/снимается cli/sti. Благодаря ему, получается виртуализовывать IF внутри VM86 задачи, и он не аффектит на общий IF, и как следствие машина не виснет на cli/jmp. VIP, вероятнее всего предназначен для увеличения скорости обработки прерываний для VM86 задач - при возникновении прерывания, (как я понимаю в момент выполнения VM86 задачи), оно не обрабатывается через protected mode interrupt handler, а выпоняется непосредственно в VM86 задаче. Как операционка разбирается со всем безобразием, мне не ведомо.

Выводы - OS/2 не виснет при выполнении cli/Jmp $ в следующих условиях:

1. компутер использует EISA(EISA/PCI)/MCA шину. Про PCI ничего не могу сказать

в каких-либо доступных доках ничего не видел.

1. Стоит процессор, поддерживающий VME - чаще всего,это тот

процессор от Intel(на других процессорах сей возможности не замечено),

```
который отвечает на CPUID.
```

From:
https://www.osfree.org/doku/ - **osFree wiki**

Permanent link:
https://www.osfree.org/doku/doku.php?id=ru:os2faq:os2gen:os2gen.076

Last update: **2014/06/20 05:08**