**Лекция 11.Шпион, клавиатурный шпион…**

**СЕГОДНЯ СНОВА ЛИСТОЧКИ!!!!!!!**

**На прошлой Лекции была записана ФРАЗА:**

**… при нажатии и отпускании клавиши на клавиатуре в буфер клавиатуры попадает Scan-code этой клавиши. Обманул?**

**Вопросы:**

**1. Что такое буфер клавиатуры?**

**2. действительно ли при нажатии клавиши на клавиатуре в этот буфер попадает Scan-code этой клавиши? Или же я Вас обманул?**

**Прежде чем отвечать на эти вопросы, прочитайте то, что написано НИЖЕ и взято из следующего источника (а потом отвечайте):**

**Аппаратное обеспечение IBM PC**

*© Александр Фролов, Григорий Фролов  
Том 2, книга 1, М.: Диалог-МИФИ, 1992.*

|  |  |  |
| --- | --- | --- |
| [[Назад]](https://frolov-lib.ru/books/bsp/v02/ch1.htm) | [[Содеожание]](https://frolov-lib.ru/books/bsp/v02/index.html) | [[Дальше]](https://frolov-lib.ru/books/bsp/v02/ch3.htm) |

**2.3. Аппаратное прерывание клавиатуры**

Клавиатура подключена к линии прерывания IRQ1. Этой линии соответствует прерывание INT 09h. ВСЁ ПОНЯТНО?

**Вопрос 3: Озаботьтесь ответом на вопросы:**

**3.1. Что такое IRQ1**

**3.2. От каких английских слов получатся буквы IRQ**

**3.3. Сколько таких IRQ имеется в 64-разрядных ЭВМ (надо посмотреть параметры системы Вашего компьютера)…**

**Ответы записать на листочках.**

Клавиатурное прерывание обслуживается модулями BIOS. Драйверы клавиатуры и резидентные программы могут организовывать дополнительную обработку прерывания INT 09h.

Как работает стандартный обработчик клавиатурного прерывания, входящий в состав BIOS?

Этот обработчик выполняет следующие действия:

* читает из порта 60h скан-код нажатой клавиши;
* ***записывает вычисленное по скан-коду значение ASCII-кода нажатой клавиши в специальный буфер клавиатуры, расположенный в области данных BIOS;***
* устанавливает в 1 бит 7 порта 61h, разрешая дальнейшую работу клавиатуры;
* возвращает этот бит в исходное состояние;
* записывает в порт 20h значение 20h для правильного завершения обработки аппаратного прерывания.

***Обработчик прерывания INT 09h не просто записывает значение ASCII-кода в буфер клавиатуры.*** Дополнительно отслеживаются нажатия таких комбинаций клавиш, как Ctrl-Alt-Del, обрабатываются специальные клавиши PrtSc и SysReq. ***При вычислении кода ASCII нажатой клавиши учитывается состояние клавиш Shift и CapsLock.***

***Буфер клавиатуры имеет длину 32 байта и расположен по адресу 0000h:041Eh.***

Клавиатурный буфер организован циклически. Это означает, что при его переполнении самые старые значения будут потеряны. Две ячейки памяти, находящиеся в области данных BIOS с адресами 0000h:041Ah и 0000h:041Ch содержат, соответственно, маркеры начала и конец буфера. Если значения этих маркеров равны друг другу, буфер пуст.

Вопрос 4:

4.1. Что такое «маркер».

4.2. Какова длина ячеек памяти.

Помимо управления содержимым буфера клавиатуры, обработчик прерывания INT 09h отслеживает нажатия на так называемые переключающие клавиши - NumLock, ScrollLock, CapsLock, Ins. Состояние этих клавиш записывается в область данных BIOS в два байта с адресами 0000h:0417h и 0000h:0418h.

Формат байта 0000h:0417h:

Биты Значение

0 Нажата правая клавиша Shift.

1 Нажата левая клавиша Shift.

2 Нажата комбинация клавиш Ctrl-Shift с любой стороны.

3 Нажата комбинация клавиш Alt-Shift с любой стороны.

4 Состояние клавиши ScrollLock.

5 Состояние клавиши NumLock.

6 Состояние клавиши CapsLock.

7 Состояние клавиши Insert.

Формат байта 0000h:0418h:

Биты Значение

0 Нажата левая клавиша Shift вместе с клавишей Ctrl.

1 Нажата левая клавиша Shift вместе с клавишей Alt.

2 Нажата клавиша SysReq.

3 Состояние клавиши Pause.

4 Нажата клавиша ScrollLock.

5 Нажата клавиша NumLock.

6 Нажата клавиша CapsLock.

7 Нажата клавиша Insert.

В таблице приведены эти комбинации и действия, выполняемые обработчиком прерывания при их обнаружении:

Комбинация клавиш Выполняемые действия

Ctrl-Alt-Del Сброс и перезагрузка системы.

Ctrl-NumLock, Перевод машины в состояние ожидания Pause до нажатия любой клавиши.

Shift-PrtSc Распечатка на принтере содержимого видеопамяти.

Ctrl-Break Выполнение прерывания INT 1Bh, завершающего работу программы.

Вопрос 5: В байте 0000h:0417h находится число 15. Что это значит?

Многие типы клавиатур имеют отдельную альтернативную цифровую панель, напоминающую клавиатуру калькулятора. Если одновременно с нажатием на клавишу Alt набрать число на этой панели (не большее, чем 255 и не равное 0), то это число будет помещено в буфер клавиатуры, как будто бы оно было введено нажатием на одну клавишу. Это число будет также записано в слове по адресу 0000h:0419h в области данных BIOS.

При переполнении внутреннего буфера клавиатуры или буфера, расположенного в области данных BIOS, программа-обработчик прерывания INT 09h генерирует звуковой сигнал.

Ну что? Можете ответить теперь НА ВОПРОСЫ, поставленные в начале Лекции? Если НЕТ, ТО СНОВА ПЕРЕЧИТЫВАЕМ (ТОЛЬКО С ЧУВСТВОМ, С ТОЛКОМ С РАССТАНОВКОЙ!!!!!!!!!!!!!!!!!!!!!!!!!!!!!). А ещё лучше – порисовать!!!!!

Клавиатурное прерывание обслуживается модулями BIOS. Драйверы клавиатуры и резидентные программы могут организовывать дополнительную обработку прерывания INT 09h.

Как работает стандартный обработчик клавиатурного прерывания, входящий в состав BIOS?

Этот обработчик выполняет следующие действия:

* читает из порта 60h скан-код нажатой клавиши;
* ***записывает вычисленное по скан-коду значение ASCII-кода нажатой клавиши в специальный буфер клавиатуры, расположенный в области данных BIOS;***
* устанавливает в 1 бит 7 порта 61h, разрешая дальнейшую работу клавиатуры;
* возвращает этот бит в исходное состояние;
* записывает в порт 20h значение 20h для правильного завершения обработки аппаратного прерывания.

***Обработчик прерывания INT 09h не просто записывает значение ASCII-кода в буфер клавиатуры.*** Дополнительно отслеживаются нажатия таких комбинаций клавиш, как Ctrl-Alt-Del, обрабатываются специальные клавиши PrtSc и SysReq. При вычислении кода ASCII нажатой клавиши учитывается состояние клавиш Shift и CapsLock.

***Буфер клавиатуры имеет длину 32 байта и расположен по адресу 0000h:041Eh.***

Клавиатурный буфер организован циклически. Это означает, что при его переполнении самые старые значения будут потеряны. Две ячейки памяти, находящиеся в области данных BIOS с адресами 0000h:041Ah и 0000h:041Ch содержат, соответственно, маркеры на начало и конец буфера. Если значения этих маркеров равны друг другу, буфер пуст.

Помимо управления содержимым буфера клавиатуры, обработчик прерывания INT 09h отслеживает нажатия на так называемые переключающие клавиши - NumLock, ScrollLock, CapsLock, Ins. Состояние этих клавиш записывается в область данных BIOS в два байта с адресами 0000h:0417h и 0000h:0418h.

Формат байта 0000h:0417h:

Биты Значение

0 Нажата правая клавиша Shift.

1 Нажата левая клавиша Shift.

2 Нажата комбинация клавиш Ctrl-Shift с любой стороны.

3 Нажата комбинация клавиш Alt-Shift с любой стороны.

4 Состояние клавиши ScrollLock.

5 Состояние клавиши NumLock.

6 Состояние клавиши CapsLock.

7 Состояние клавиши Insert.

Формат байта 0000h:0418h:

Биты Значение

0 Нажата левая клавиша Shift вместе с клавишей Ctrl.

1 Нажата левая клавиша Shift вместе с клавишей Alt.

2 Нажата клавиша SysReq.

3 Состояние клавиши Pause.

4 Нажата клавиша ScrollLock.

5 Нажата клавиша NumLock.

6 Нажата клавиша CapsLock.

7 Нажата клавиша Insert.

В таблице приведены эти комбинации и действия, выполняемые обработчиком прерывания при их обнаружении:

Комбинация клавиш Выполняемые действия

Ctrl-Alt-Del Сброс и перезагрузка системы.

Ctrl-NumLock, Перевод машины в состояние ожидания Pause до нажатия любой клавиши.

Shift-PrtSc Распечатка на принтере содержимого видеопамяти.

Ctrl-Break Выполнение прерывания INT 1Bh, завершающего работу программы.

Многие типы клавиатур имеют отдельную альтернативную цифровую панель, напоминающую клавиатуру калькулятора. Если одновременно с нажатием на клавишу Alt набрать число на этой панели (не большее, чем 255 и не равное 0), то это число будет помещено в буфер клавиатуры, как будто бы оно было введено нажатием на одну клавишу. Это число будет также записано в слове по адресу 0000h:0419h в области данных BIOS.

При переполнении внутреннего буфера клавиатуры или буфера, расположенного в области данных BIOS, программа-обработчик прерывания INT 09h генерирует звуковой сигнал.

***Ну что? Можете ответить теперь НА ВОПРОСЫ, поставленные в начале Лекции? Если НЕТ, ТО ПИШЕМ ПРАВИЛЬНЫЕ ОТВЕТЫ (правильные ли они?):***

Вопрос 1:

**Что такое буфер клавиатуры?**

***Буфер клавиатуры – Область в ОП, имеющая длину 32 байта и расположенная по адресу 0000h:041Eh***

Вопрос 2:

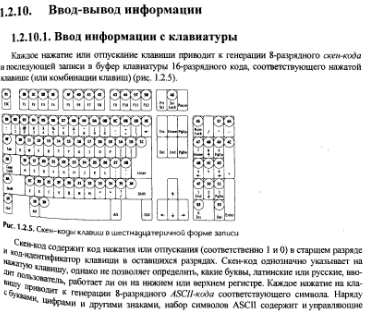
**Действительно ли при нажатии клавиши на клавиатуре в этот буфер попадает Scan-code этой клавиши? Или же я Вас обманул? Или Вас обманул кто-то ещё?**

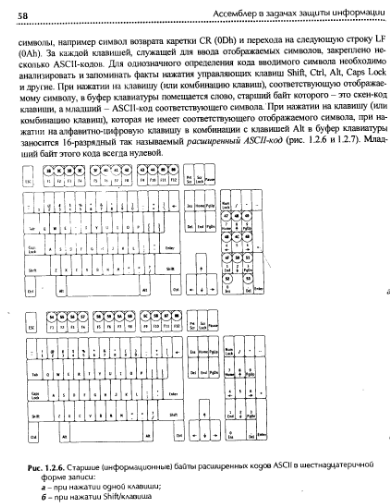
**Ответ 2: Вы нас обманули, так как:**

***Обработчик прерывания 09h выполняет следующие действия:***

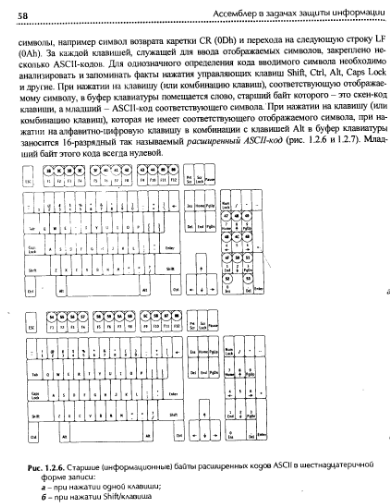
* ***читает из порта 60h скан-код нажатой клавиши;***
* ***записывает вычисленное по скан-коду значение ASCII-кода нажатой клавиши в специальный буфер клавиатуры, расположенный в области данных BIOS;***

**Продолжаем читать и пытаемся правильно ПЕРЕответить на вопросы 1,2,3,4,5, ничего не исправляя на своих листочках, продолжая писать-рисовать на них (чтобы был виден процесс познания – «от конкретного к абстрактному и от абстрактного к конкретному».** Познание начинается с исследования конкретного, т. е. с анализа восприятия внешнего мира посредством органов чувств, человеческого опыта. В этом процессе происходит мысленное отделение одних свойств и связей от других свойств и связей. При этом явления расчленяются, теряют свою целостность, внутреннюю связь сторон. Абстракция дает возможность рассматривать главные, существенные признаки явления и устанавливать, таким образом, закономерности их развития. Однако познание только тогда истинно, когда оно характеризует явления действительности в целостном единстве их сторон. Такое знание может быть получено в результате движения мысли от односторонних, абстрактных определений, к более глубоким, объясняющим многообразие конкретных явлений. Конкретное потому является конкретным, что оно есть синтез многих определений, единство многообразного. Этот процесс движения мысли называют процессом восхождения от абстрактного к конкретному. **В книжке про ассемблер записано следующее:**





***Выделяем главное ДЛЯ ПРАВИЛЬНОГО ОТВЕТА:***



**Понятно, что если Вы дочитали до этого места, то Вам должно быть ПОНЯТНО, что ВСЁ НЕПОНЯТНО (ВСЕ ВРУТ), что во всём этом «чёрт ногу сломит», а «дьявол скрывается в мелочах», и что остаётся только ДУРКовать, и, используя ещё два компаса – «здравый смысл» и «результаты функционирования компа», попытаться дать ответы, ЗАПИСАВ ИХ НА ТОТ ЖЕ ЛИСТОК, на следующие вопросы: Вопрос 6. БУДЬТЕ ВНИМАТЕЛЬНЫ!! Вопросы с подвохом.**

**6.1. На клавиатуре пользователь нажимает комбинацию клавиш Shift + A (A латинское большое), а затем отпускает эти клавиши. НАРИСОВАТЬ!!!!!!! в 16 с.с. что получается в буфере клавиатуры в результате указанного нажимания. НАРИСОВАТЬ то, что находится в байтах по адресам:** 0000h:0417h, 0000h:0418h, 0000h:041Ah и 0000h:041Ch.

**6.2. Буфер клавиатуры состоит из 32 байтов. Какое количестве нажатий на клавиатуре может быть сохранено в этом буфере без издания звукового сигнала?**

**6.3. Нарисовать содержимое буфера клавиатуры, маркеров начала и конца, если набран текст «Мама Ьшдф Ramu»,** а также состояние областей данных BIOS с адресами 0000h:0417h и 0000h:0418h.

**Р.S.Понятно, что ответы на все перечисленные вопросы требуют использования отладчика, доступа к буферу клавиатуры и областям памяти BIOS, поэтому отвечаем на эти вопросы В ТЕЧЕНИЕ ДВУХ ЗАНЯТИЙ. 13 группа СНАЧАЛА на лабораторном занятии (с 16-00 до 17 – 20) ЧИТАЕТ ЛЕКЦИЮ и ОТВЕЧАЕТ на вопросы вплоть ДО КОНЦА занятия под названием Лекция (с 17-30 до 18-50), не забывая при этом о первой части Лабораторной работы №3. А 12 группа ЧИТАЕТ ЛЕКЦИЮ на Лекции с 17-30 до 18-50 И ОТВЕЧАЕТ НА ВОПРОСЫ вплоть до конца занятия с 19-00 до 20-20, не забывая при этом о первой части Лабораторной работы №3. То есть результаты 13 группа сдаёт к 18-50, а 12 группа – к 20-20.**