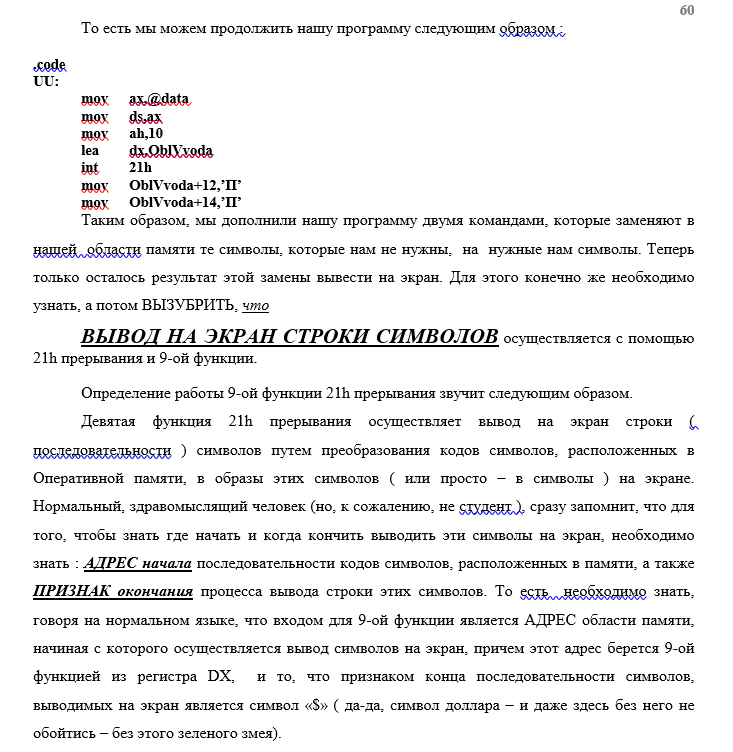
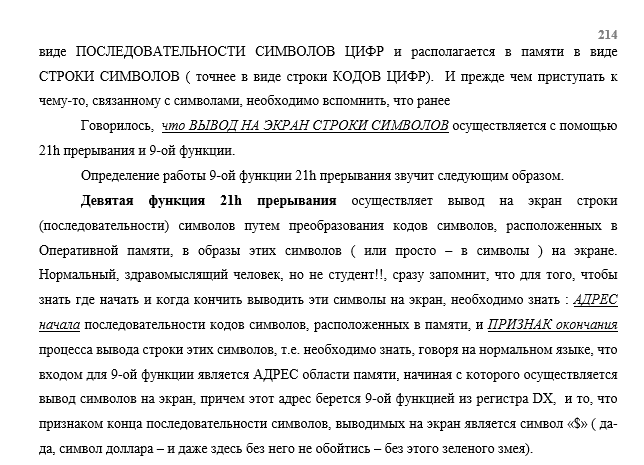
**Вопрос 1.1**

**Ответ:**

Лекция 4, стр. 60



Лекция 11, стр.



**Вопрос 1.2**

**Ответ:**

область памяти Text содержит следующие символы: 'Mama', перевод строки (ASCII 10), 'Mila', возврат каретки (ASCII 13), 'ramu', '10' (две цифры 1 и 0), возврат каретки (ASCII 13) и завершающий нулевой байт "$".

Поэтому будет выведено на экран следующее:

Mama

Mila

ramu10

**Вопрос 2**

**Ответ:** Если речь идет о макрокоманде PutStr, то макрорасширение, сформированное препроцессором, будет состоять из последовательности команд для вывода строки на экран. В данном случае, макрокоманда PutStr используется для вывода строк TitleStr, NormStr и CureStr. Препроцессор заменит вызовы PutStr на соответствующий исходный текст вывода строк.

**Вопрос 3**

**Ответ:** Если речь идет об утверждении, что «первый совпадающий по маске файл» определяется «текущим признаком сортировки» файлов в папке (по имени, по Дате изменения, по типу, по размеру), то оно не является корректным, так как сортировка файлов в папке не влияет на результат поиска первого совпадающего файла по маске. Когда выполняется операция поиска файлов по маске, операционная система просто возвращает первый файл, найденный в соответствии с заданной маской без учета сортировки.

**Вопрос 4**

**Ответ:** Если речь идет об адресе памяти FN\_Ofs, который определен следующим образом:

FN\_Ofs equ offset DTA+1eh, то:

Equ является директивой ассемблера, используемой для определения константы или макроса. В данном случае, FN\_Ofs определяется как символическая константа.

Адрес - это числовое значение, указывающее на позицию в памяти компьютера.

DTA+1Eh означает, что к адресу DTA добавляется смещение в размере 1Eh, чтобы получить новый адрес в памяти.

offset - оператор ассемблера, который возвращает смещение, которое яявляется адресом указанной метки или переменной относительно начала сегмента или блока исходного текста.

**Вопрос 5**

**Ответ:** Если речь идет о фрагменте исходного текста, представленного в лекции 8, то после выполнения команды MOV CX, -128 содержимое регистра CX будет представлено числом 0xFF80. Если же фрагмент исходного текста заменить, то будет произведена попытка скопировать байты, но операция не будет выполнена, так как CX отрицательно.

**Вопрос 6**

**Ответ:** Если речь идет об имени файла и Handle файла из фрагмента исходного текста антивируса, то ответ следующий:

; Вывод имени файла

mov ah, 9

mov dx, offset FName

int 21h

; Вывод Handle файла

mov ah, 9

mov dx, offset TitleStr

int 21h

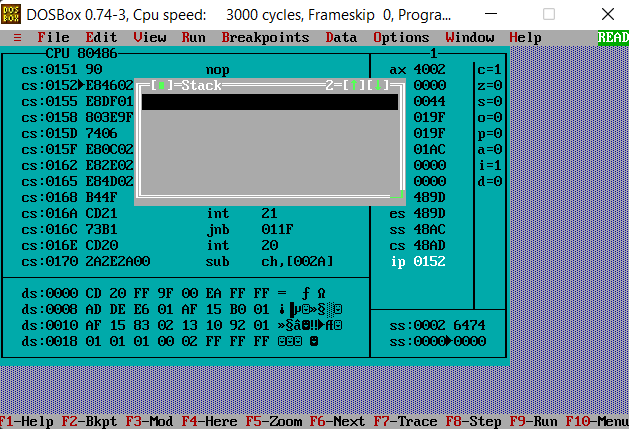
**Вопрос 7**

**Ответ:** Если речь идет об исходном тексте антивируса, то в данном фрагменте исходного текста команды NOP (No Operation) используются для создания задержки или паузы в программе. Они не выполняют никаких операций и являются пустыми инструкциями. Если их убрать, время выполнения можжет измениться.

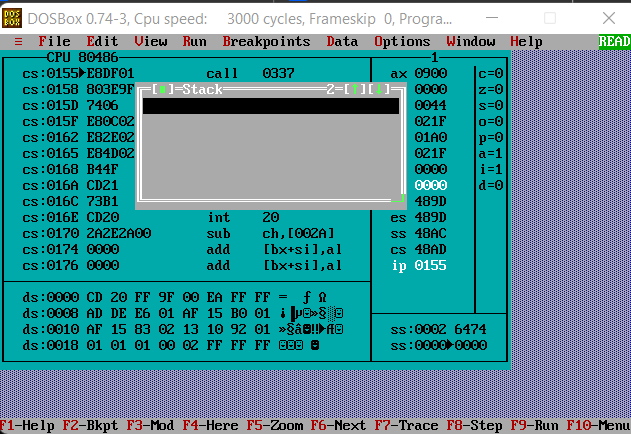
**Вопрос 8**

**Ответ:** Если речь идет об исходном тексте антивируса, то при вызове процедуры InfoAboutFile происходит передача управления этой процедуре, аргументы (если они есть) передаются через регистры или стек, а также происходит сохранение и восстановление контекста стека.

До вызова процедуры:



После выхода из процедуры:



Адрес точки возврата:

CS+0155

**Вопрос 9**

**Ответ:** Если речь идет об антивируснике, то УДАЛИТЬ значит удалить имя файла из реестра файлов

(реально же ТЕЛО исполнимого файла, который при загрузке в оперативную память и передаче ему

управления превращается в вирус, ФИЗИЧЕСКИ ПРОДОЛЖАЕТ ЛЕЖАТЬ НА ВИНЧЕСТЕРЕ). УБИТЬ –

означает сделать так, чтобы ТЕЛО ПЕРЕСТАЛО ИСПОЛНЯТЬ СВОЙ ФУНКЦИОНАЛ,

**Вопрос 10**

**Ответ:** Если речь идет о макрокоманде MoveFPos FHandle 0eh, то ее макрорасширение будет выглядеть следующим образом:

MoveFPos macro F\_Handle, FPos

mov ax, 4200h

mov bx, F\_Handle

xor cx, cx

mov dx, FPos

int 21h

endm

**Вопрос 11**

**Ответ:** Если речь идет о командах в исходном тексте антивируса, то push ds и pop es используются для сохранения и восстановления значений сегментных регистров ds и es.

**Вопрос 12**

**Ответ:** Если речь идет о фрагменте исходного текста антивируса, то префикс repe означает "repeat while equal" (повторять, пока равно), и он применяется перед инструкцией сравнения cmpsb. Этот префикс указывает процессору повторять инструкцию cmpsb, пока значения в si и di равны и флаг ZF (Zero Flag) установлен. В результате выполнения repe cmpsb происходит следующее:

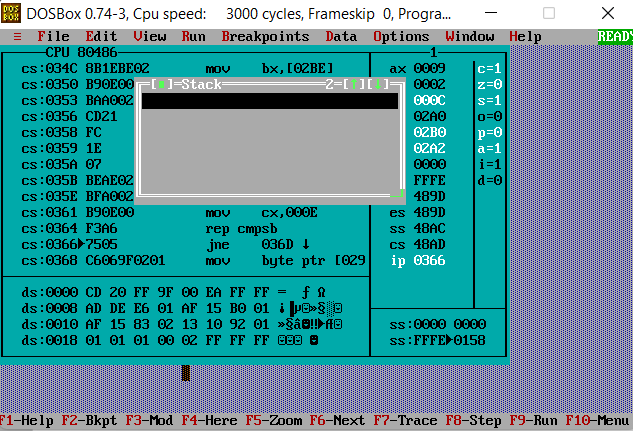
Происходит сравнение байтов, начиная с адресов, указанных в si и di, если значения байтов равны, флаг ZF устанавливается, счетчик cx уменьшается на 1, если значения байтов не равны или счетчик cx достигает 0, цикл прерывается.

Результат сравнения можно определить по состоянию флага ZF.

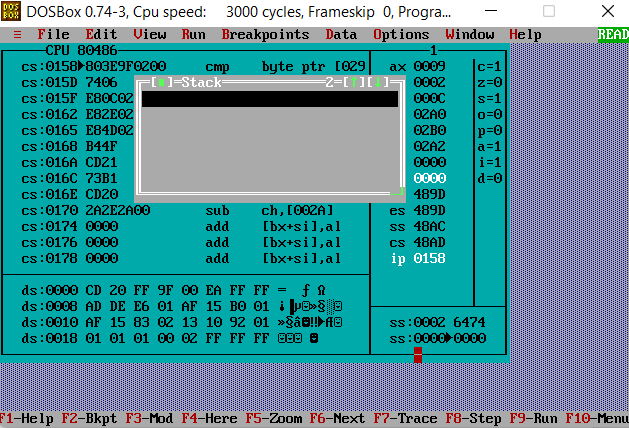
**Вопрос 13**

**Ответ:**

До выполнения:



После выполнения ret:



**Вопрос 14**

**Ответ:** Если речь идет о процедуре KillExecutable из исходного текста антивируса, то при вызове процедуры KillExecutable, записывается 2 байта в файл, дескриптор которого содержится в регистре bx, используя функцию int 21h с функцией 40h.

**Вопрос 15**

**Ответ:** Если речь идет о командах lodsb, stosb, которые являются инструкциями процессора, то команда lodsb загружает байт данных из памяти по адресу, указанному в регистре si, в аккумуляторный регистр al. Затем регистр si автоматически увеличивается или уменьшается в зависимости от флага направления DF. Команда stosb записывает байт данных из аккумуляторного регистра al в память по адресу, указанному в регистре di. Затем регистр di автоматически увеличивается или уменьшается в зависимости от флага направления DF.

**Вопрос 16**

**Ответ:** Если речь идет о директиве End start из исходного текста антивируса, то транслятор генерирует метку, обозначающую конец процедуры start. Эта метка может быть использована в других частях программы для определения места, куда можно перейти после выполнения процедуры start.ожно перейти после выполнения процедуры start.