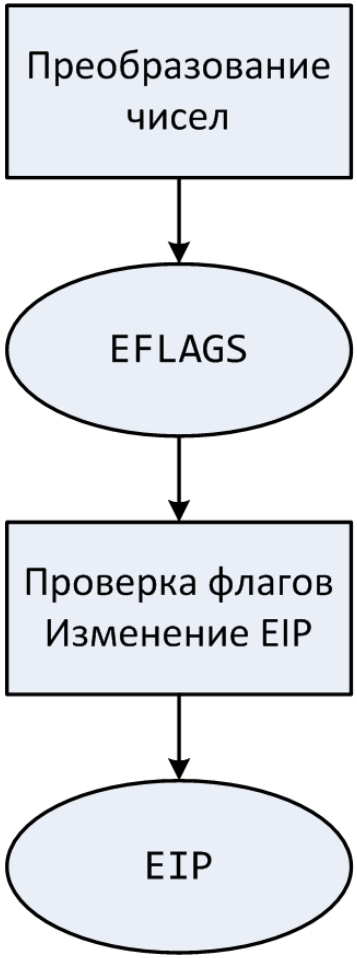
Лекция 4

16 февраля

Изменение естественного порядка выполнения программы

- Арифметические операции
- CMP
  - r/m 8/16/32, imm 8/16/32
  - r/m 8/16/32, r 8/16/32
  - r 8/16/32, r/m 8/16/32
- TEST
  - r/m 8/16/32, imm 8/16/32
  - r/m 8/16/32, r 8/16/32
- JMP
  - r/m/imm 32
- Jcc
  - imm32
- Переходы
  - Абсолютные
  - Относительные



	OF	SF	ZF	PF	CF
ADD	M	M	M	M	M
SUB	M	M	M	M	M
IMUL MUL	M	-	-	-	M
IDIV DIV	-	-	-	-	-
NEG	M	M	M	M	M
CMP	M	M	M	M	M
TEST	-	M	M	M	-

```
...
SECTION .text
GLOBAL CMAIN
CMAIN:
   MOV  EAX, DWORD [a]     ; (1)
   TEST EAX, EAX           ; (2)
   JE   .1                 ; (3)
   MOV  ECX, DWORD [b]     ; (4)
   TEST ECX, ECX           ; (5)
   JE   .1                 ; (6)
   CDQ                     ; (7)
   IDIV ECX                ; (8)
   SUB  DWORD [a], EDX     ; (9)
 .1:
   XOR  EAX, EAX           ; (10)
   RET                     ; (11)
```

Просмотр содержимого исполняемого файла

```
-bash-2.05b$ ./build_asm.sh backward.asm
-bash-2.05b$ objdump -d -M intel backward
```

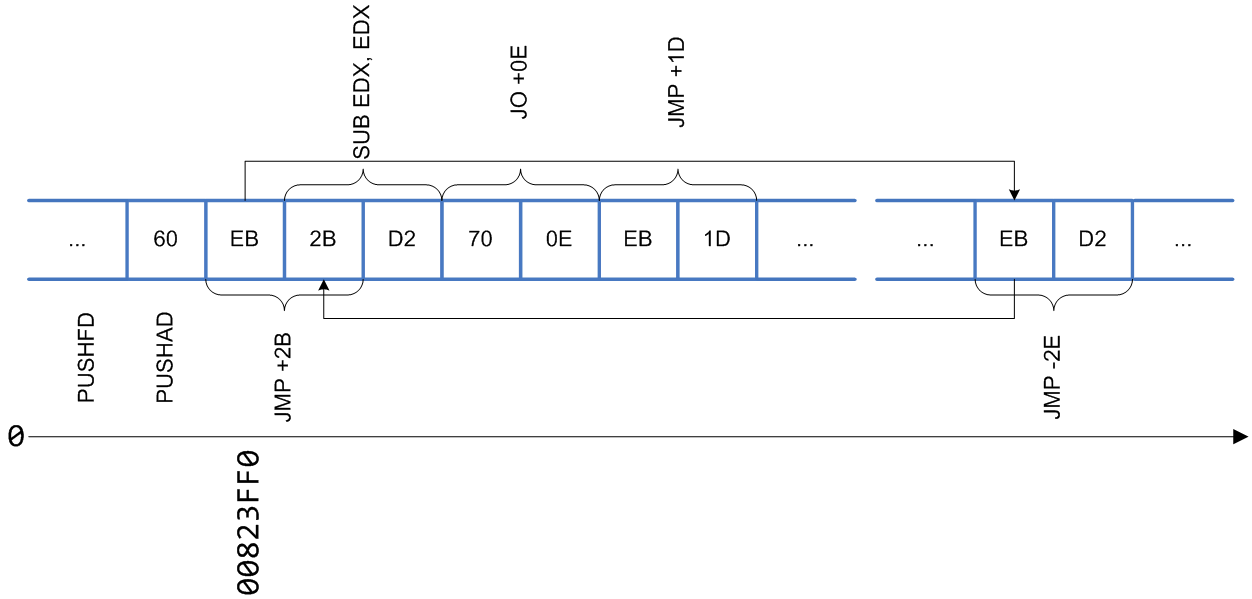
```
080483e0 <main>:
 80483e0:       a1 fc 94 04 08          mov    eax,ds:0x80494fc
 80483e5:       85 c0                   test   eax,eax
 80483e7:       74 13                   je     80483fc <main.1>
 80483e9:       8b 0d 00 95 04 08       mov    ecx,ds:0x8049500
 80483ef:       85 c9                   test   ecx,ecx
 80483f1:       74 09                   je     80483fc <main.1>
 80483f3:       99                      cdq
 80483f4:       f7 f9                   idiv   ecx
 80483f6:       29 15 fc 94 04 08       sub    ds:0x80494fc,edx

080483fc <main.1>:
 80483fc:       31 c0                   xor    eax,eax
 80483fe:       c3                      ret
 80483ff:       90                      nop
```

Противодействие дизассемблеру

Трасса выполнения

Адрес	Машинная команда	Ассемблерная инструкция	
00823FEF	60	PUSHAD	
00823FF0	EB2B	JMP	0082401Dh
0082401D	EBD2	JMP	00823FF1h
00823FF1	2BD2	SUB	EDX, EDX
00823FF3	700E	JO	00824003h
00823FF5	EB1D	JMP	00824014h

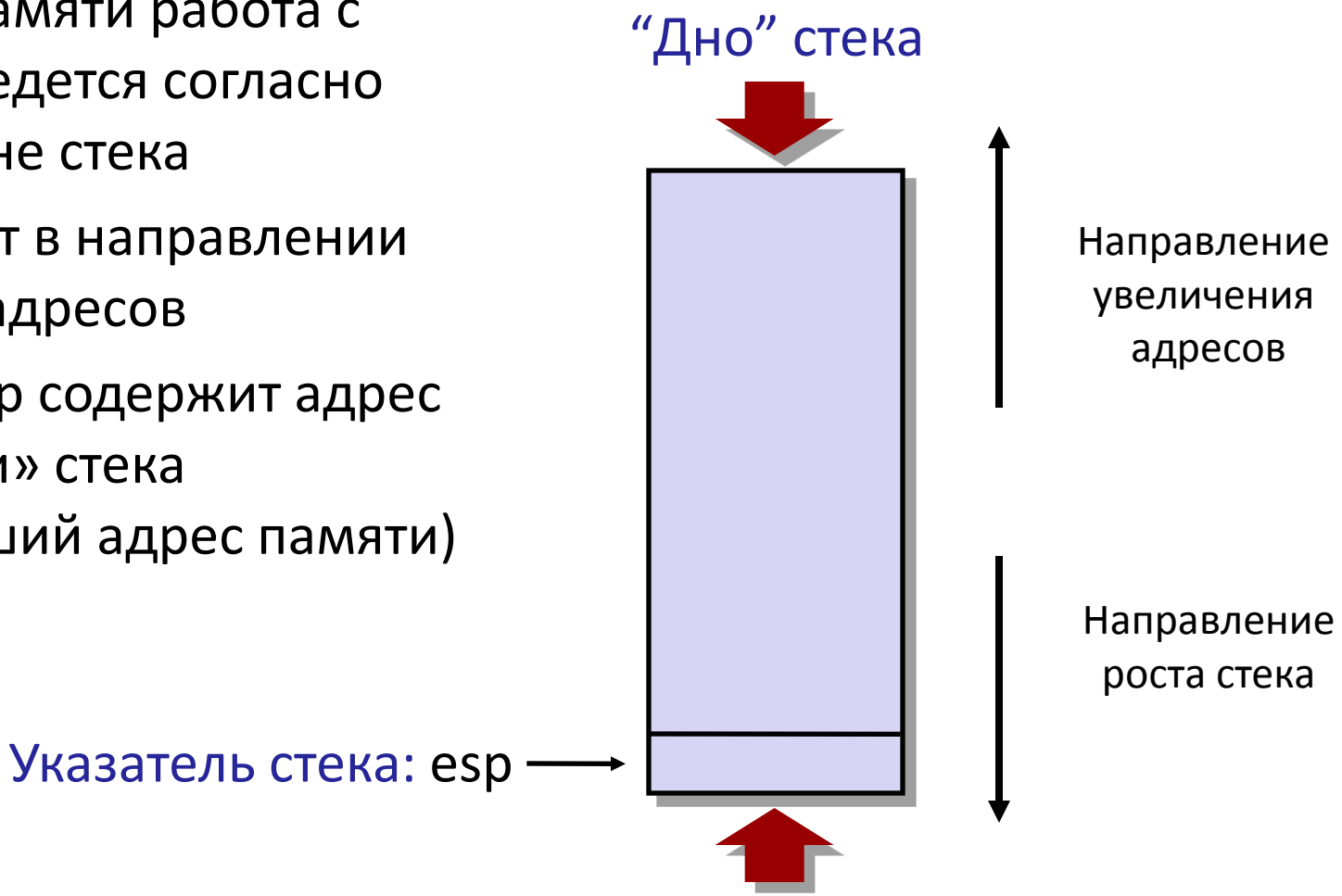


Организация вызова функций

- Вопросы
  - Передача управления и возвращение обратно
  - Вычисление значений фактических параметров и их размещение
  - Передача возвращаемого значения
  - Размещение автоматических локальных переменных
  - Порядок использование регистрового файла различными функциями
  - Какие именно машинные команды использовать для поддержки функций
- Ответы – Application Binary Interface (ABI)
  - Соглашение о вызовах (Calling Convention)

Аппаратный стек IA-32

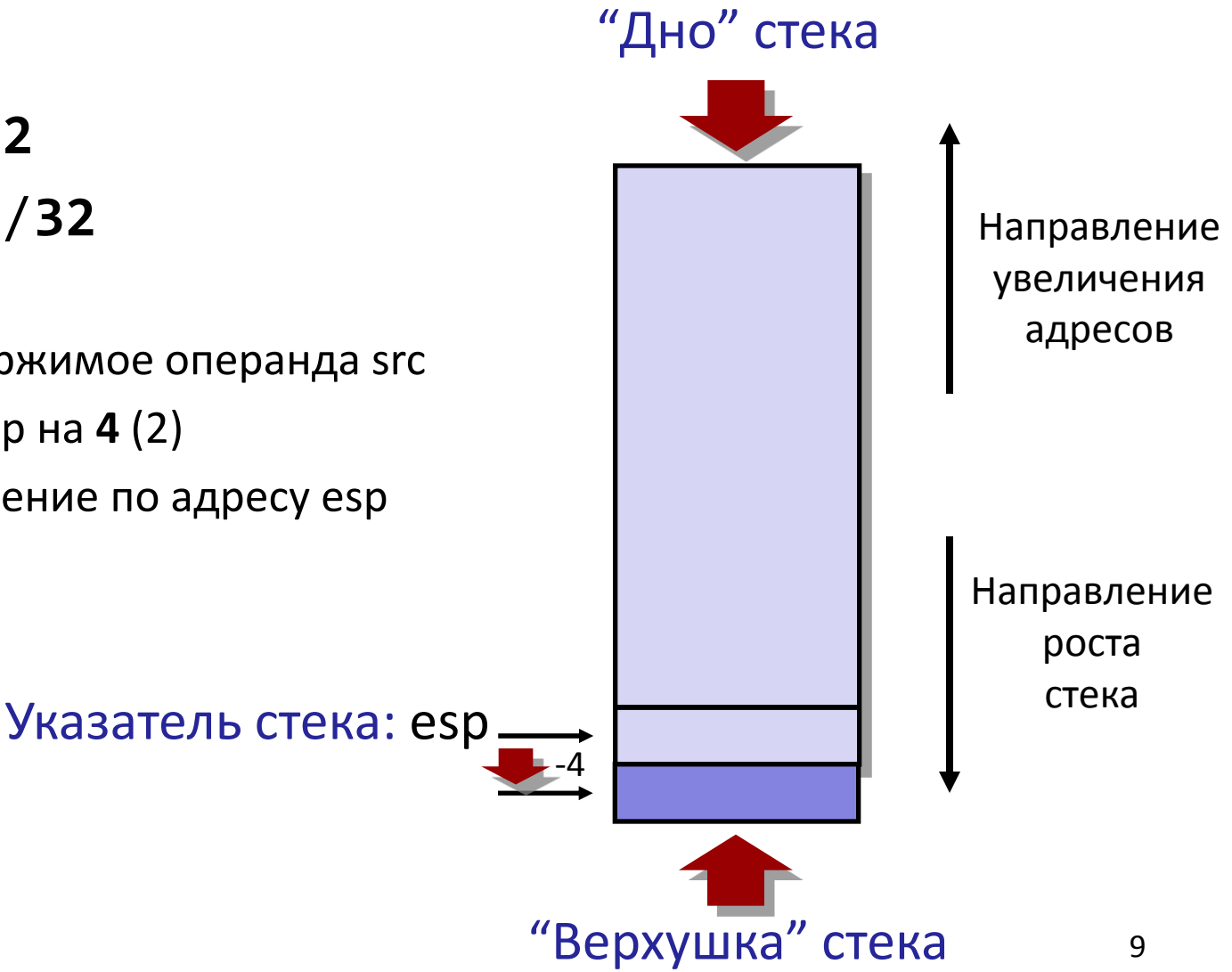
- Область памяти работа с которой ведется согласно дисциплине стека
- Стек растет в направлении меньших адресов
- Регистр esp содержит адрес «верхушки» стека (наименьший адрес памяти)



Загрузка данных в стек: Push

- `push src`
  - `r/m 16/32`
  - `imm 8/16/32`

  – Извлечь содержимое операнда src
  – Уменьшить esp на **4** (2)
  – Записать значение по адресу esp



Выгрузка данных из стека: Pop

- `pop dst`
  - `r/m 16/32`

  – Извлечь значение по адресу esp
  – Увеличить esp на **4** (2)
  – Записать содержимое операнда dst