Анализ программного кода

Введение

доц. Нестеренко В.А.

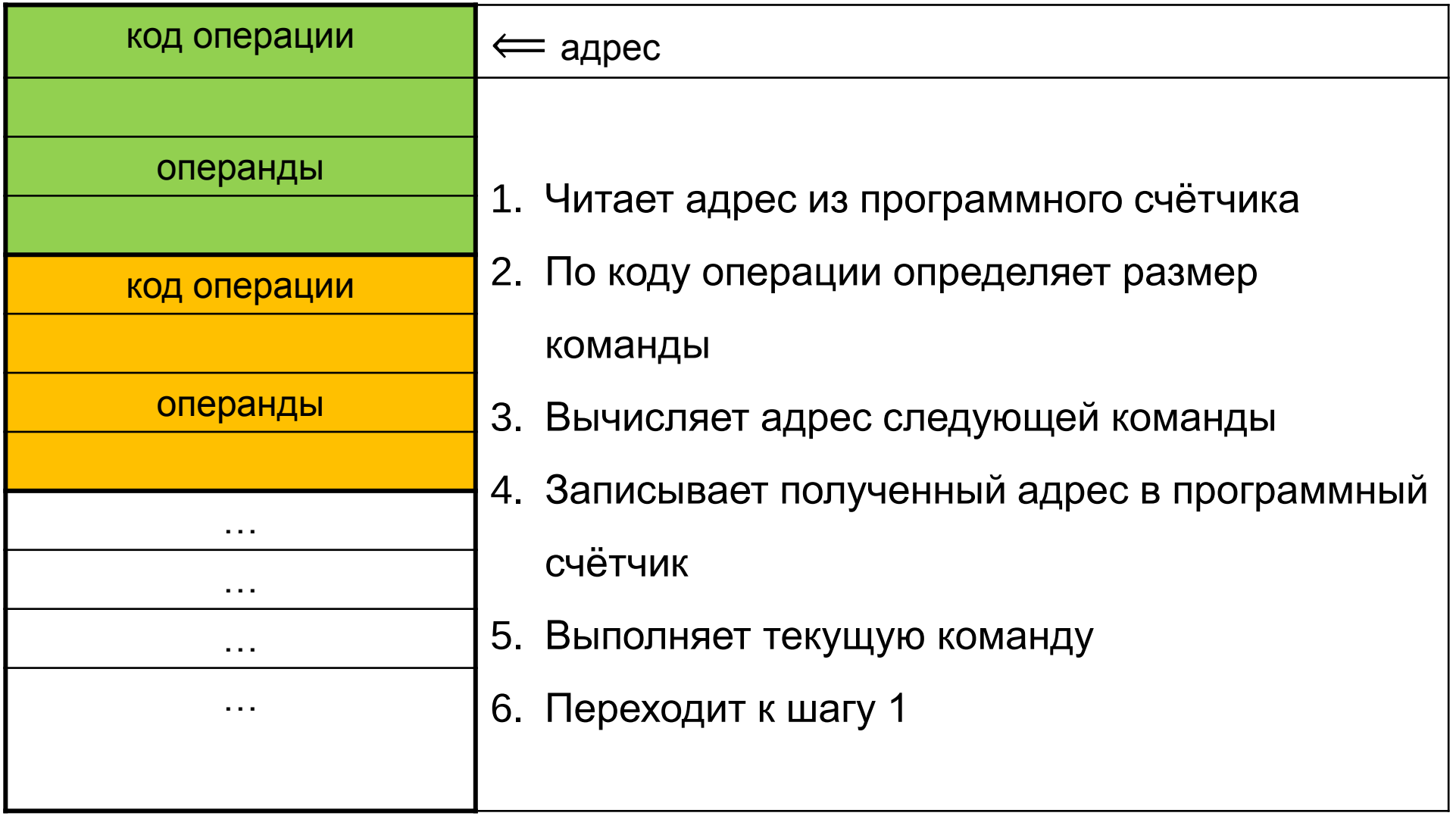
Цель и содержание курса

Знакомство с основными принципами и деталями размещения и исполнения программного кода на персональном компьютере с целью его анализа, улучшения и защиты.

Задачи:

- знакомство с общими принципами разбора анализа программного кода как в виде исходных текстов так и в виде исполнимых модулей;
- изучение основных инструментов анализа исполнимых программных модулей (отладчик, дизассемблер, профайлер, ...);
- изучение методов выявления подозрительных и вредоносных участков кода и изучение возможности защиты программ от средств анализа.

Исполнение кода



Регистры процессора

Регистры – основное (единственное) средство общения программы с процессором.

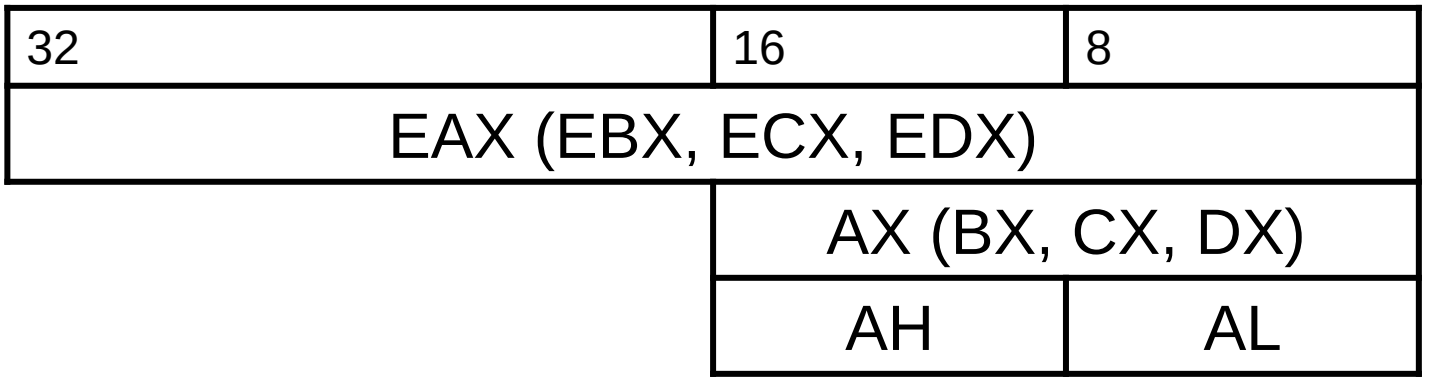
Обращение к регистрам по имени (не по адресу как в случае с ячейками памяти).

Группы регистров:

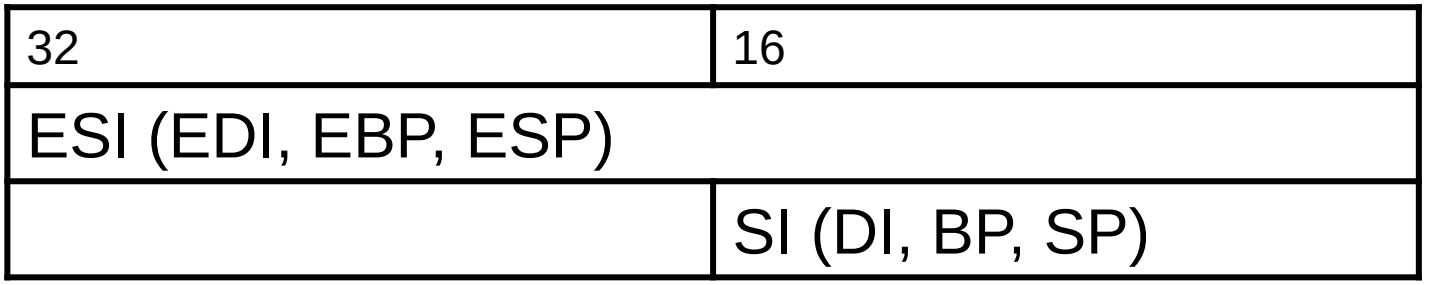
- *Регистры общего назначения* (РОН) используются для хранения и модификации данных и адресов.
- *Сегментные регистры* используются для работы с памятью.
- *Регистры состояния и управления* содержат информацию о состоянии процессора и исполняемой команде программы.

Регистры общего назначения

EAX, EBX, ECX, EDX



ESI, EDI, EBP, ESP

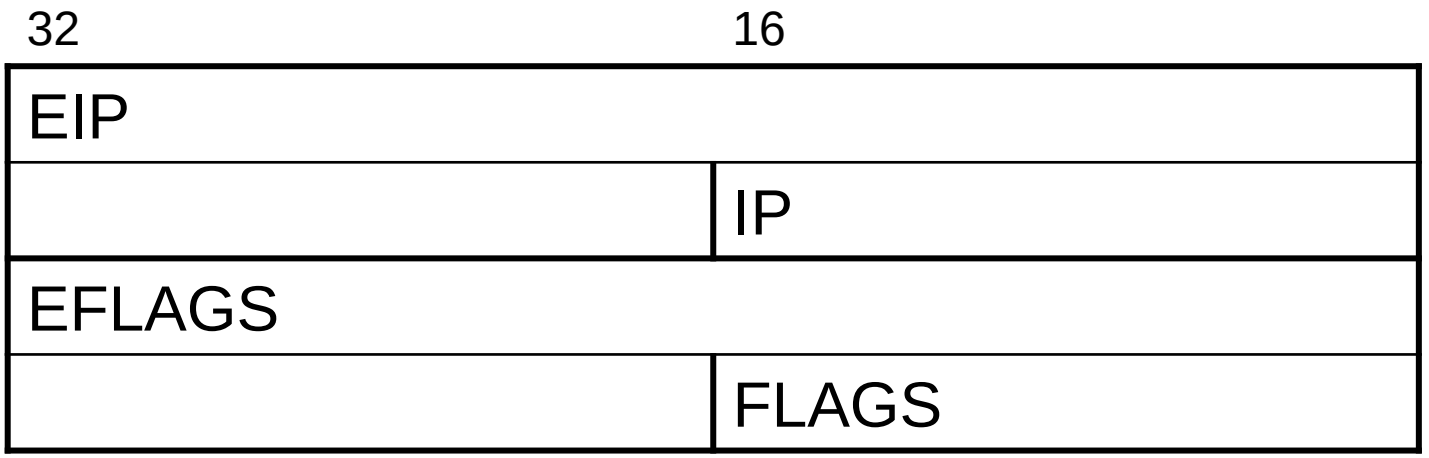


Сегментные регистры

16

CS – *команды*
SS – *стек*
DS – *данные*
ES – *данные*
FS – *данные*
GS – *данные*

Регистры состояния и управления



Модель память

Адресное пространство программы

Линейная модель
Сегментная модель
Страничная модель

Физическое адресное пространство

Машинный код, Язык Ассемблера

…