Программирование на Ассемблер
к.т.н., доц. Красов А.В.
Лекция 1

Факультет	МТС
Курс	3
Семестр	6
Форма контроля	зачет
Лекции	14 часов
Лабораторные работы	12 часов

Автор курса

к.т.н., доцент Красов Андрей Владимирович
директор УИЦ ИТТ, доцент кафедры ИБТС
Куратор специальности
201800 «Защищенные системы связи»

Введение

Архитектура компьютера включает в себя:

- структурную схему компьютера;
- набор системных регистров;
- способ организации оперативной памяти;
- организацию и разрядность интерфейсов компьютера;
- способы представления и форматы данных компьютера;
- набор и форматы машинных команд;
- систему обработки прерываний.

Пятиступенчатый конвейер имеет следующие этапы:

- выборка команды из оперативной памяти;
- декодирование команды;
- вычисление адреса операндов;
- выполнение операции в арифметико-логическом устройством (АЛУ);
- запись результата.

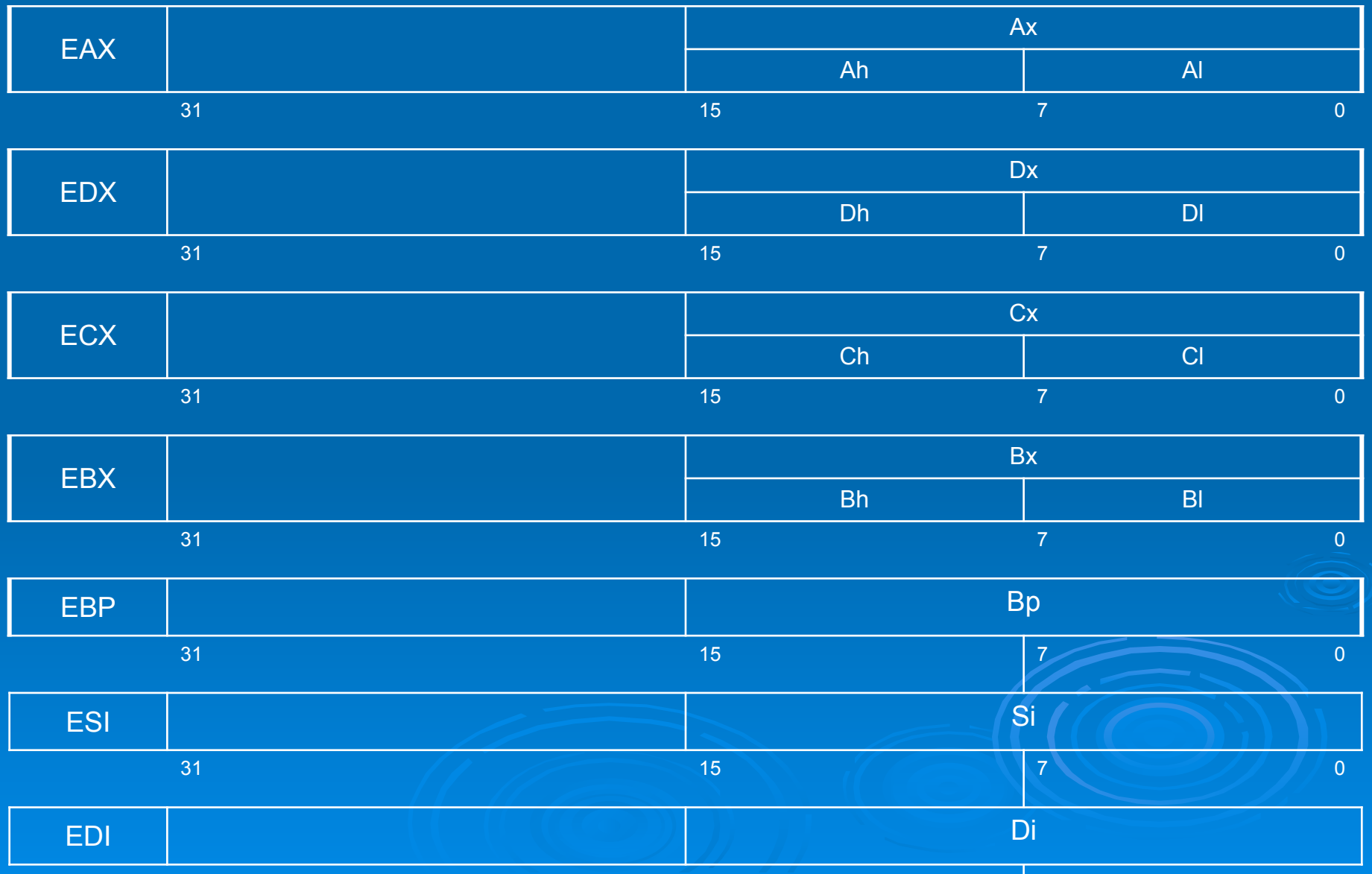
Суперскалярная архитектура имеет следующие особенности:

- раздельное кэширование кода и данных;
- предсказание правильного адреса перехода (сохранение 256 последних переходов, вероятность до 80%);
- усовершенствованный блок вычислений с плавающий точкой.

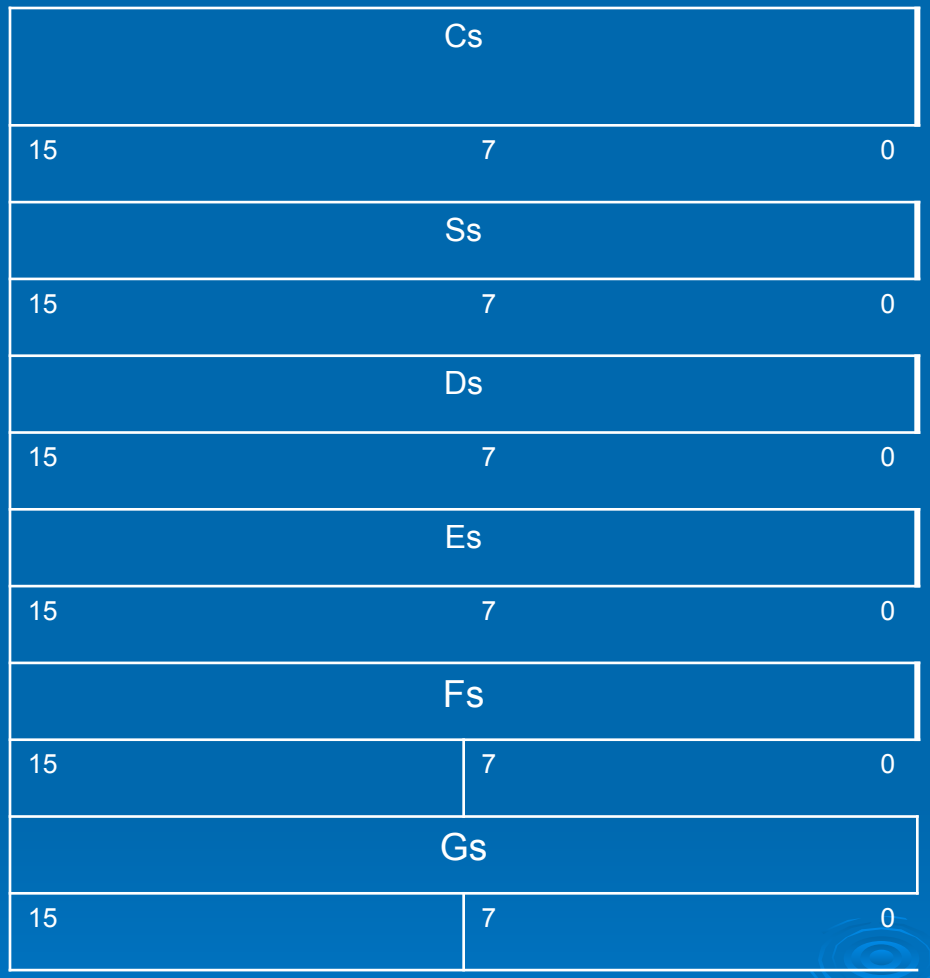
Набор регистров

Программная модель микропроцессора содержит 16 пользовательских и16 системных регистра.

Пользовательские регистры:



Сегментные регистры:



Регистры флагов и указателя команд:

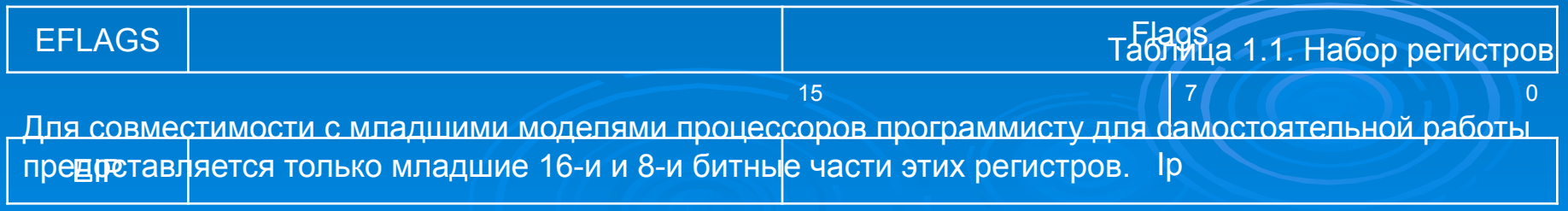


Таблица 1.1. Набор регистров

Для совместимости с младшими моделями процессоров программисту для самостоятельной работы предоставляется только младшие 16-и и 8-и битные части этих регистров.

Таблица 1.2. Назначение регистров общего назначения

eax/ax/ah/al	Аккумулятор – применяется для хранения промежуточных данных.
ebx/bx/bh/bl	Базовый регистр – применяется для хранения базового адреса объекта в памяти.
ecx/cx/ch/cl	Регистр-счетчик – применяется в командах организации циклов.
edx/dx/dh/dl	Регистр данных – применяется для хранения промежуточных данных.
Регистры для поддержки цепочных операций	
esi/si	Индекс источника – содержит текущий адрес элемента в цепочке-источнике.
edi/di	Индекс приемника – содержит текущий адрес в цепочке-приемнике.
Регистры для работы со стеком	
esp/sp	Указатель стека – содержит указатель на вершину стека.
ebp/bp	Указатель базы кадра стека – предназначен для организации доступа к данным из стека.

Сегментные регистры:

Процессор поддерживает следующие типы сегментов:

1. Сегмент кода. Содержит команды программ. Адрес сегмента содержится в регистре cs.
2. Сегмент данных. Содержит данные программы. Адрес сегмента содержится в регистре ds.
3. Сегмент стека. В данном сегменте размещается стек. Адрес сегмента содержится в регистре ss.
4. Дополнительный сегмент данных (адреса дополнительных сегментов в регистрах es, gs, fs).

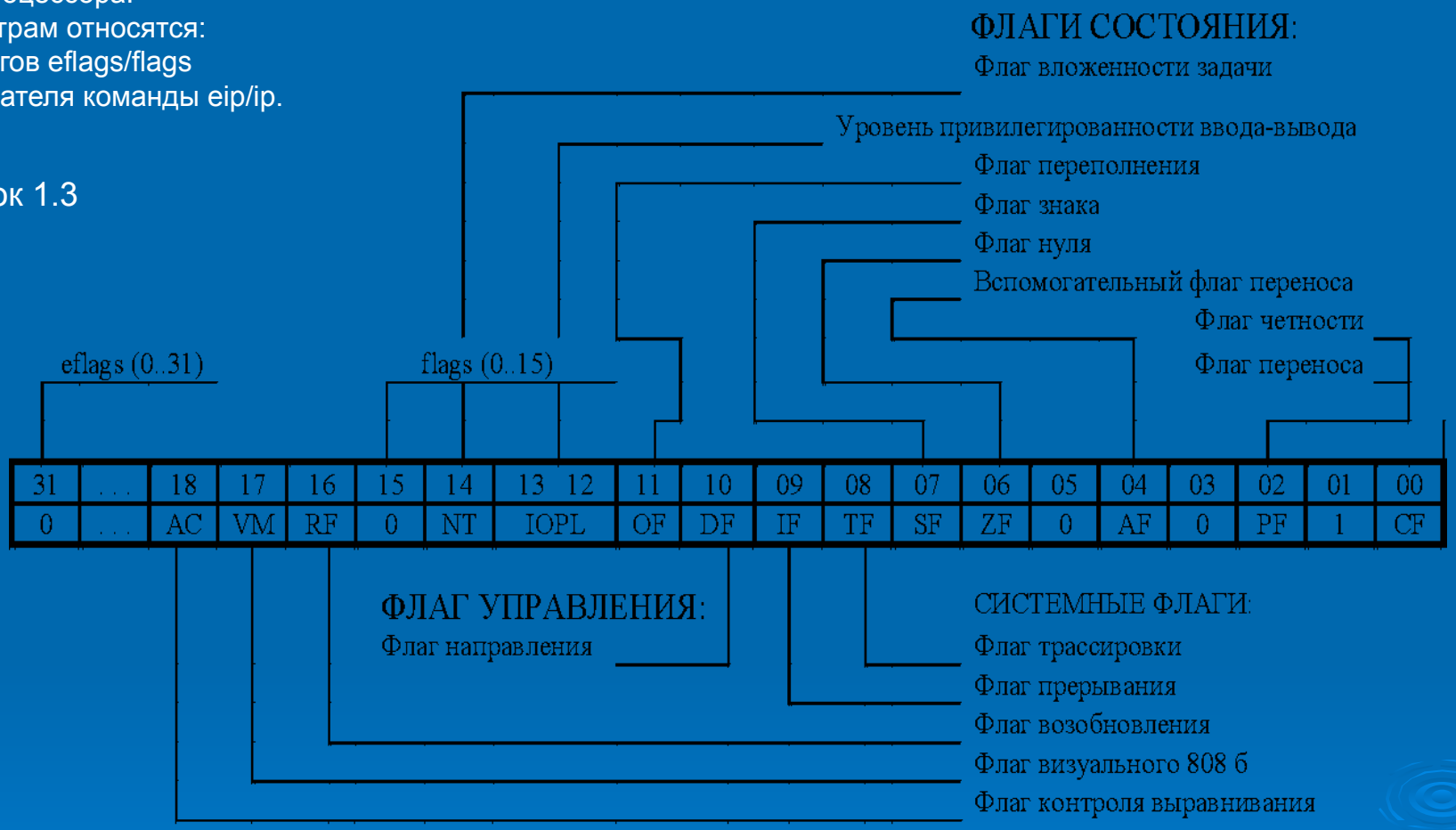
Регистры состояния:

В процессор включены несколько регистров, которые постоянно содержат информацию о результатах выполнения команд и состояния процессора.

К этим регистрам относятся:

- регистр флагов eflags/flags
- регистр указателя команды eip/ip.

Рисунок 1.3



Все флаги регистра флагов можно разделить на три группы:

8 флагов состояния. Данные флаги отражают результат исполнения команд процессора.

- 1 флаг управления. Данный флаг используется цепочными командами. Значение флага, обозначаемого как ds, определяет направление поэлементной обработки. Если df=0 обработка производится в прямом порядке, а если df=1 то в обратном. Работа с данным флагом возможна с помощью специальных команд (cld и std).
- 5 системных флагов. Системные флаги предназначены для управлением вводом/выводом, системой прерываний, режимом отладки, переключением задач. Без особой нужды модифицировать значение этих флагов нецелесообразно.

Организация памяти

Процессор поддерживает несколько режимов работы с оперативной памятью:

- реальный режим – режим, в котором работал процессор i8086, сохраняемый для преемственности с ранними моделями;
- защищенный режим – использование всех возможностей процессора;
- режим виртуального 8086 – предназначен для работы программ созданных с использованием реального режима адресации памяти, в защищенном режиме.

Сегментированная модель памяти

Сегментация – механизм адресации, обеспечивающий существование нескольких независимых адресных пространств.

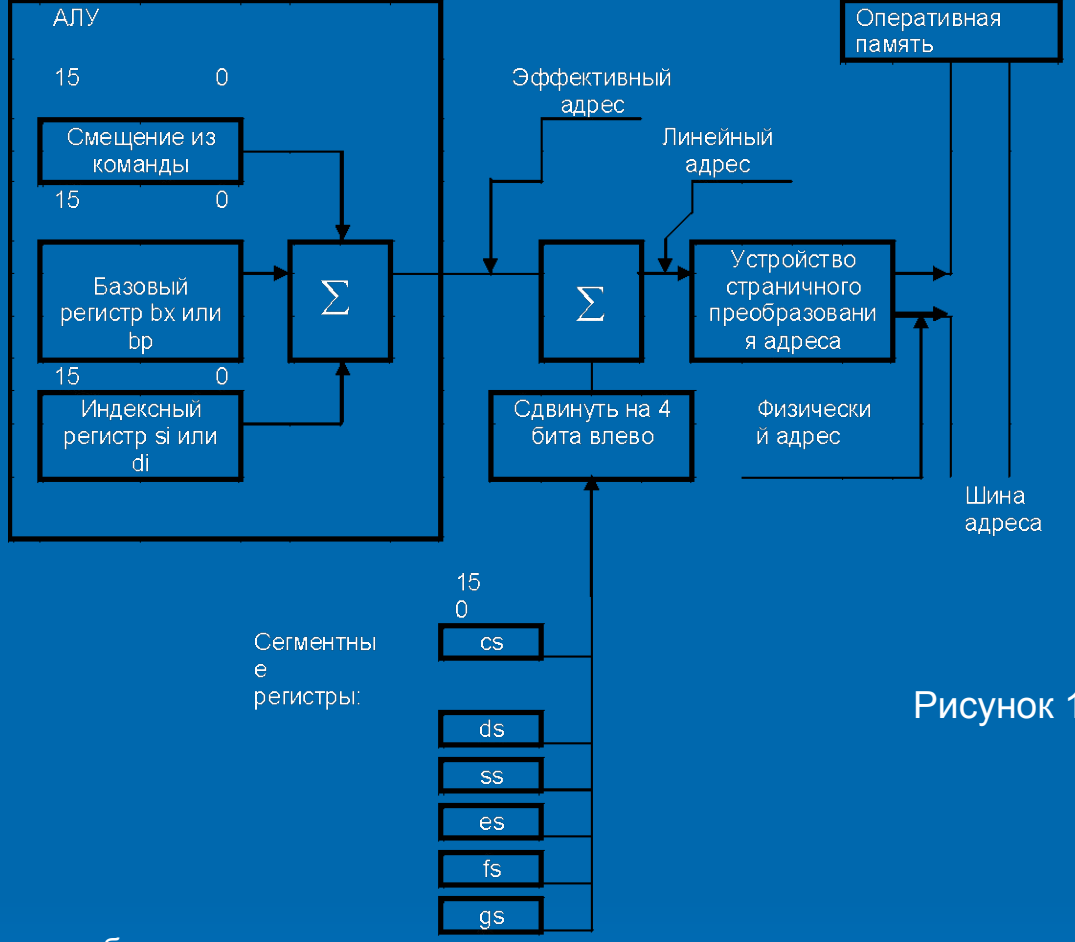


Рисунок 1.4

Используются следующие обозначения:

- Физический адрес и линейный адрес – адрес, выдаваемый на шину адреса процессора. В реальном режиме они одинаковы, при страничном режиме они отличаются.
- Эффективный адрес – значение адреса относительно текущего сегмента.

В реальном режиме памяти механизм адресации физической памяти имеет следующие параметры:

- Диапазон изменения физического адреса от 0 до 1 Мбайт (шина адреса в i8086 имела 20 линий).
- Размер сегмента - 64Кбайт. Эта величина определяется 16-и разрядной архитектурой.
- Сегментная составляющая адреса. В сегментных регистрах хранится только 16 разрядов адреса сегмента, для получения сегментной составляющий адреса, имеющий 20 разрядов, необходимо сдвинуть адрес из сегментного регистра на 4 разряда.

Недостатки сегментной организации памяти:

- максимальный размер сегмента 64 Кбайт;
- перекрытие сегментов.

Типы данных

На рис. 1.5, показаны аппаратно поддерживаемые процессором типы данных.

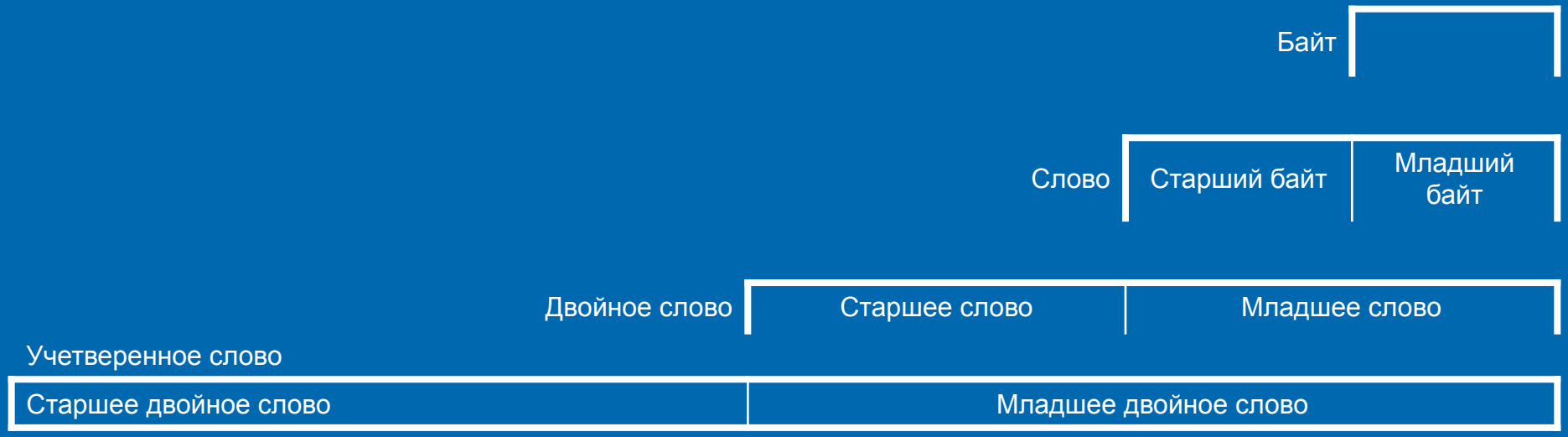


Рис.1.5. Типы данных процессора

На уровне команд процессор поддерживает логические типы данных, представленные на рис. 1.3.

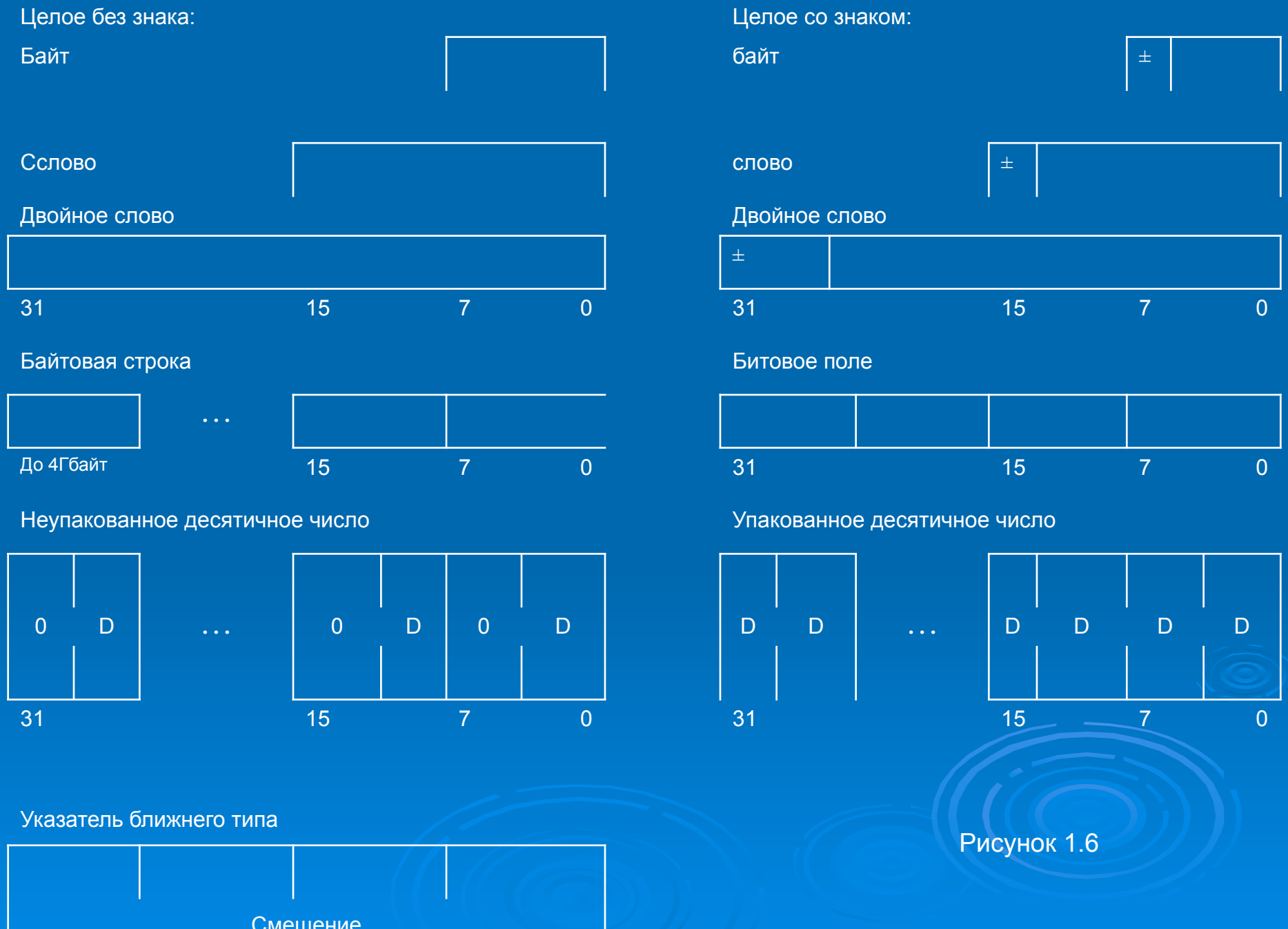


Рисунок 1.6

Таблица 1.7. Числовые диапазоны целых типов

Кол-во разрядов	Диапазон значений	
	Целое со знаком	Целое без знака
8	-128 . . 127	0 . . 255
16	-32768 . . 32767	0 . . 655535
32	-2^{31} . . $+2^{31} - 1$	0 . . $-2^{32} - 1$

Указатель на память. Указатель на память бывает двух типов:

- ближний тип – 32 разряда, отсчитываемый от начала сегмента;
- дальний тип – 48 (16 разрядов – адрес сегмента, 32 разряда – адрес смещения).

Цепочка. Цепочка представляет собой непрерывный набор байтов, слов, двойных слов. Максимальная длина цепочки составляет 4 Гбайта.

Битовое поле. Битовое поле представляет собой непрерывную последовательность до 32 бит. Каждый бит последовательности может адресоваться отдельно.

Неупакованный двоично-десятичный тип. Данный тип представляет собой двоичное представление десятичных чисел. Старшие разряды в этом случае всегда равны 0.

Упакованный двоично-десятичный тип. Данный тип размещает две десятичные цифры в одном байте.

Формат Команд

Машинная команда процессора имеет следующую структуру:

- поле префиксов;
- поле кода операции;
- поле операндов.

Поле префиксов – элемент команды который модифицирует действие этой команды, например: замена сегмента, изменение размерности адреса, изменение размерности операнда, циклическое выполнение команды.

Поле кода операции – числовой код команды.

Поле операндов – определяет с какими ячейками работает команда и куда помещает результат. Поле операндов может содержать от 0 до 2-х операндов. Возможны следующие сочетания операндов в команде:

- регистр – регистр;
- регистр – память;
- память – регистр;
- значение – регистр;
- значение – память.

Построение программы на ассемблере

На рис. 1.8, представлен порядок действий по компиляции построению исполнимого файла по ассемблерной программе.

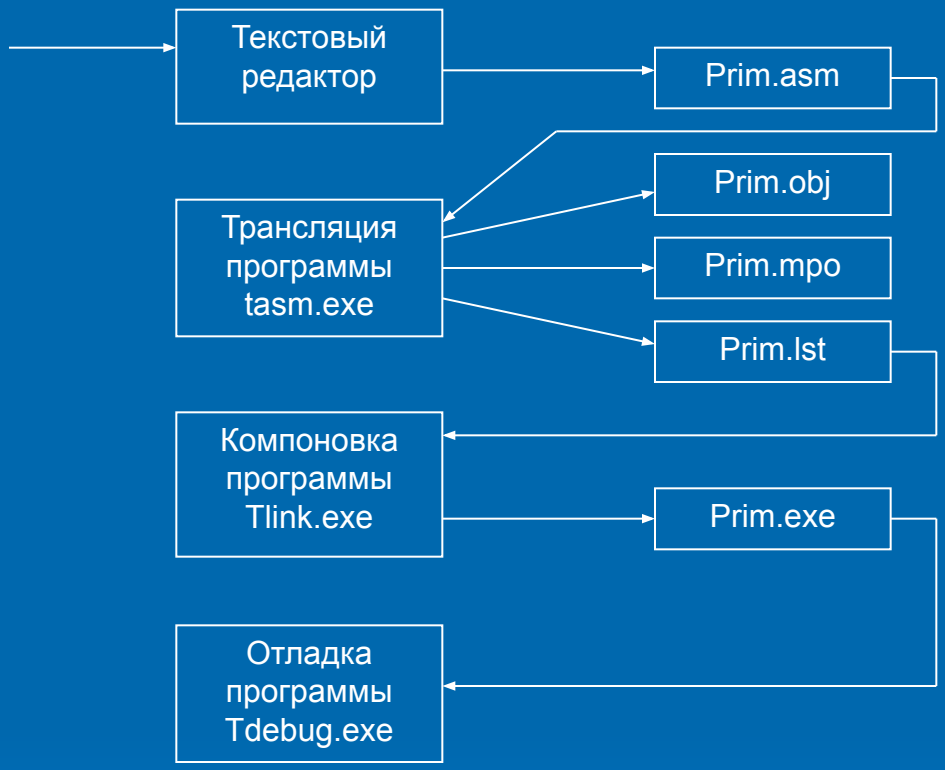


Рисунок 1.8
Иллюстрация построения программы на ассемблере