

# Лекции по ассембелру модуль 4

Андрей Тищенко

2023/2024 гг.

## Лекция 6 апреля.

Организационные вопросы

См. в презентации (в телеграмм канале).

Мотивация

- Проблема 1. Свойства чисел. Свойства математических абстракций при выполнении вычислительной техникой несколько меняются.
- Проблема 2. Отладка. Где размещаются переменные, в каком порядке, что происходит при попадании в UB или в реализационно зависимое поведение. Как сделать отладчик?
- Проблема 3. Производительность. Понятие сложности с точки зрения математики.
- Проблема 4. Безопасность. Что на самом деле выполняется компьютером. Зачастую проблемы безопасности = ошибки в коде. Сейчас продвинутые эксполиты мимикрируют под ошибки в коде.

История первых компьютеров

Смотри презентацию.

Принципы фон Неймана

1. Двоичное кодирование информации.

В дополнительном коде данные хранятся в виде  $\vec{x} = 2^{n-1}x_{n-1} + \sum_{i=0}^{n-2} 2^i x_i$

2. Неразличимость команд и данных.  
Команды хранятся в памяти в виде:  
Код операции, Операнд<sub>1</sub>, Операнд<sub>2</sub>

3. Адресуемость памяти.

4. Последовательное выполнение команд.

#### (Модельный) цикл работы ЭВМ

1. Извлечение инструкции из памяти. Используя текущее положение счётчика команд, процессор извлекает некоторое количество байт из памяти и помещает их в буфер команд.
2. Декодирование команды. Процессор просматривает содержимое буфера команд и определяет код операции и ее операнды. Длина декодированной команды прибавляется к текущему значению счётчика команд.
3. Загрузка операндов. Извлекаются значения операндов. Если операнд размещен в ячейках памяти - вычисляется исполнительный адрес.
4. Выполнение операции над данными.
5. Запись результата. Результат может быть записан в том числе и в счётчиках команд для изменения естественного порядка выполнения. Возвращаемся в пункт 1.  
Интересный факт: взятие данных из регистра происходит быстрее, чем из памяти, потому что из регистра до процессора ток идёт быстрее.

#### Промежуточные итоги

1. Регистр, имя регистра, значение регистра, разрядность регистра, машинное слово.
2. Память ячейка памяти, адрес ячейки памяти, время доступа к памяти.
3. Цикл, тактовая частота, счётчик команд (указывает на очередную команду).

4. Машинная команда, код операции, операнд, адресность команды (сколько операндов в команде. 2 операнда - двухадресная, 1 - одноадресная, 0 - безадресная, 3 - трёхадресная), исполнительный (действительный адрес)
5. Способ адресации: прямая, непосредственная, косвенная.