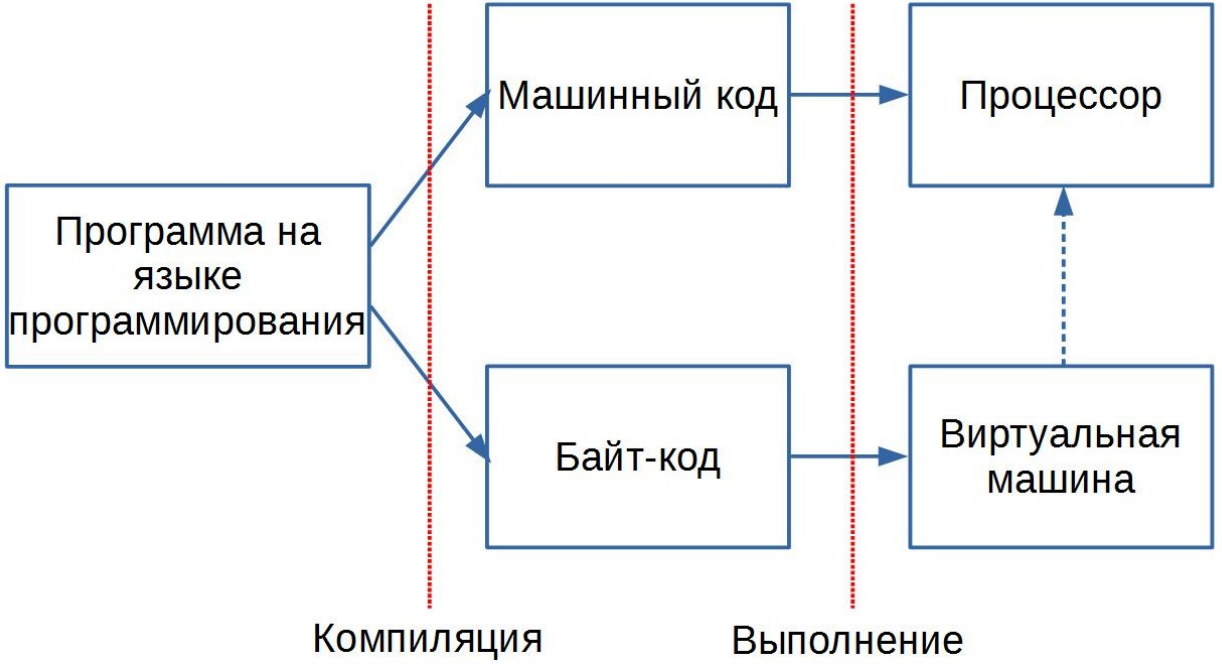
Математические основы информационной безопасности

Груздев Дмитрий Николаевич

Дизассемблирование программ

Компиляция программ

Компиляция – преобразование программы с предметно-ориентированного языка на машинно-ориентированный язык, байт-код или в машинный код.



Язык ассемблера

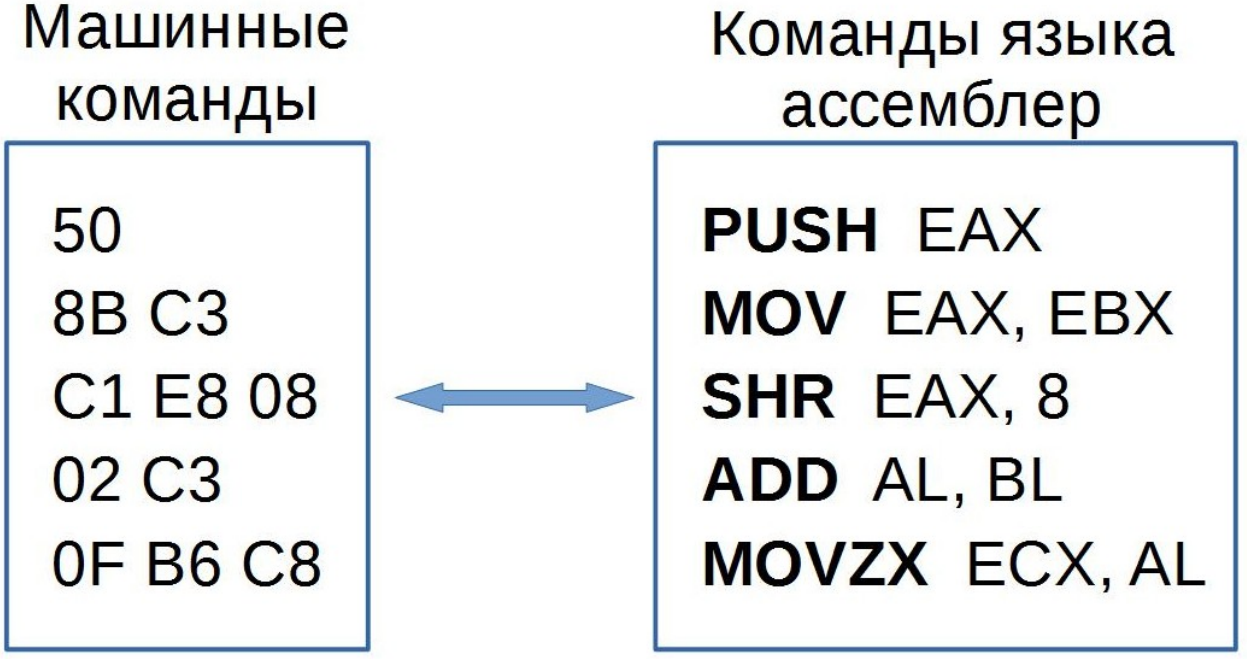
Язык ассемблера – машинно-ориентированный язык программирования низкого уровня. Его команды прямо соответствуют отдельным машинным командам или их последовательностям.

Используется для представления машинных программ в удобно читаемой форме.

Является платформо-зависимым.

Соответствие машинных команд и команд языка ассемблер

Машинный код: 508BC3C1E80802C30FB6C8

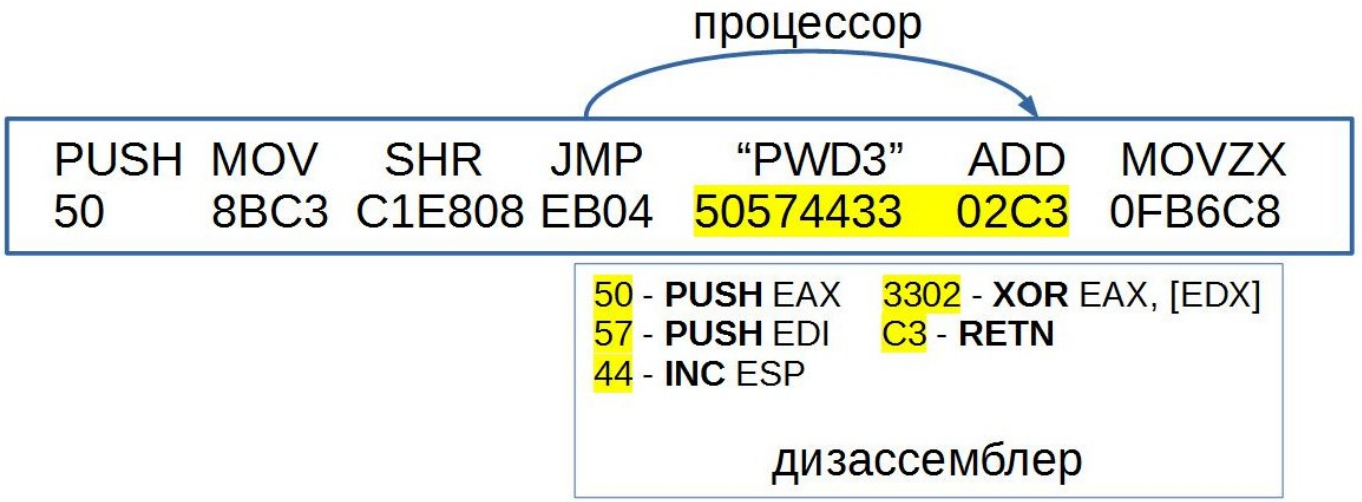


Для
Intel Pentium и
AMD Athlon

Дизассемблеры

Дизассемблер – транслятор, преобразующий машинный код в команды на языке ассемблера.

Основная трудность при работе дизассемблера – отличить данные от машинного кода.



Дизассемблер IDA

IDA является интерактивным дизассемблером – предоставляет пользователю интерактивную среду для модификации листинга программы (задание имен функций и переменных, доопределение участков данных и кода, добавление комментариев и др.).

https://www.hex-rays.com/products/ida/support/download_freeware.shtml - бесплатная версия с ограниченным функционалом

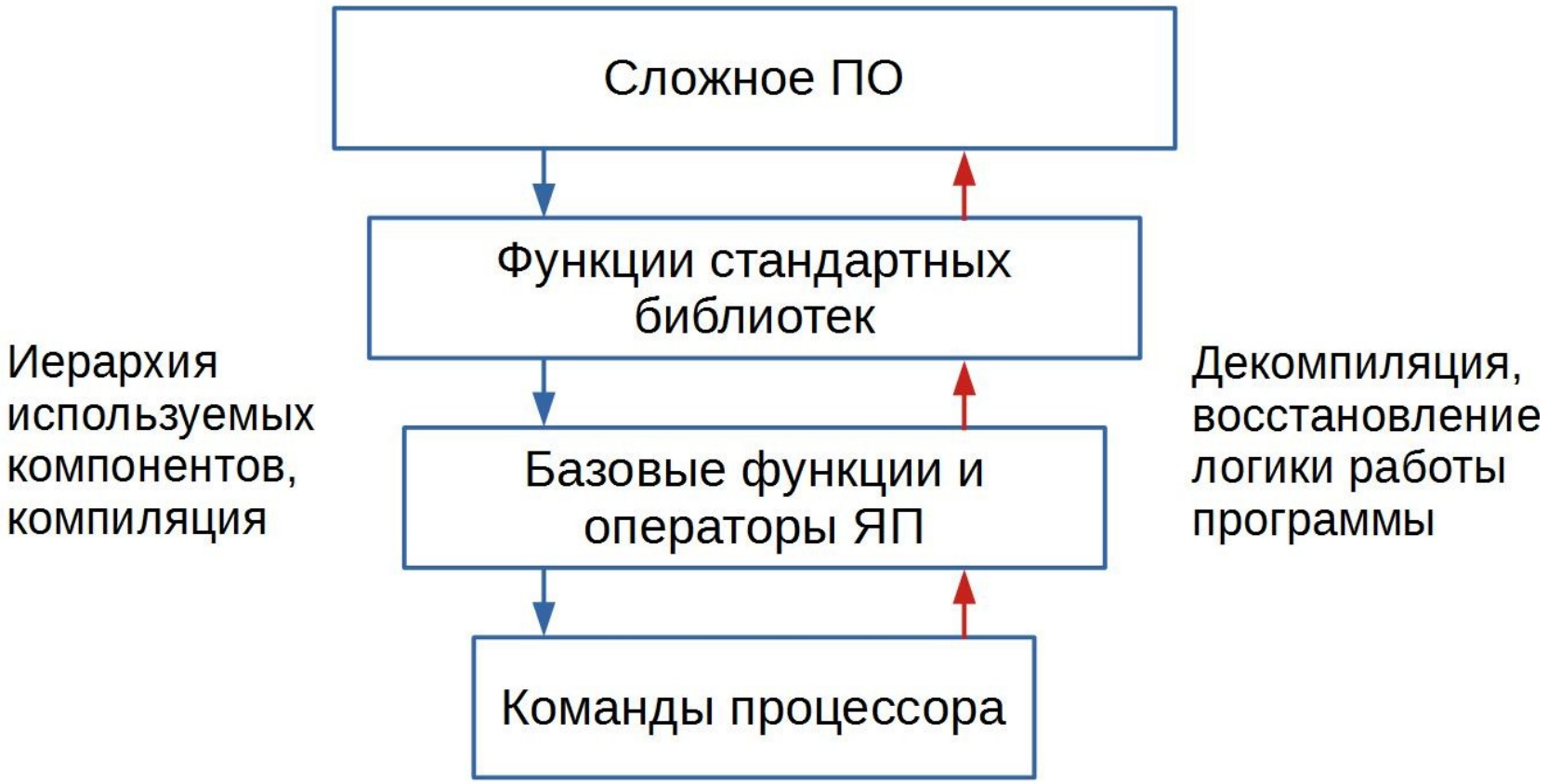
CheckPassword.exe

Статья 272 УК РФ

Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации наказывается…

Примечание: под компьютерной информацией понимаются сведения (сообщения, данные), предоставляемые а форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Декомпиляция



Типы команд процессора

Пересылки данных:

- работа с регистрами: mov, xchg
- работа со стеком: push, pop
- работа с памятью: mov, xchg

Арифметические:

- add, sub, div, mul, inc, dec

Логические:

- xor, and, or, not, test, shr

Передачи управления:

- ветвление: jz, jnz, ja, jnb
- безусловный переход: jmp
- вызов функций: call, pop

CheckLicense.exe

https://sesc-infosec.github.io/