Санкт-Петербургский государственный политехнический университет
Кафедра прикладной математики

Разработка генератора виртуальных машин для предотвращения обратного проектирования программного обеспечения, поставляемого в виде машинных кодов

Диссертация на соискание ученой степени магистра

Выполнила студентка гр. 6057/2 Ю.П. Кириллова
Научный руководитель В.Ю. Аранов

2012 г.

Основные понятия

Виртуальная машина – программа, имитирующая систему команд некоторой вычислительной машины

Реинжиниринг – восстановление структуры и алгоритма программы по ее исполняемому коду

Протектор – программа, преобразующая приложение в форму, защищенную от анализа и реинжиниринга

Дизассемблирование – перевод программы из машинного кода на язык ассемблера

Машинный код – двоичный код программы на языке команд компьютера

Цели и задачи

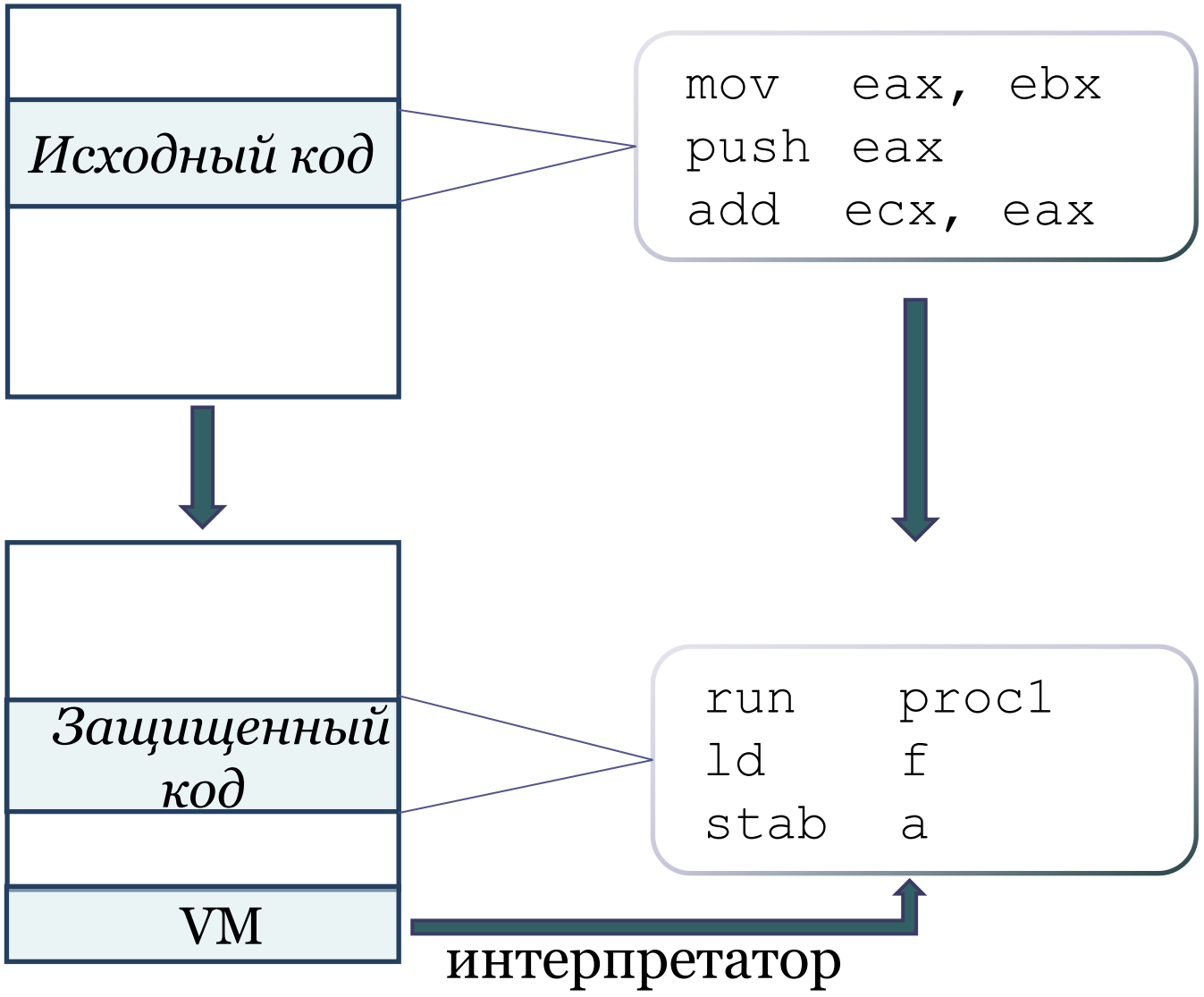
Цель: Защита алгоритмов от реинжиниринга

Исполняемый файл → Дизассемблер → Исходный код (Ассемблер)

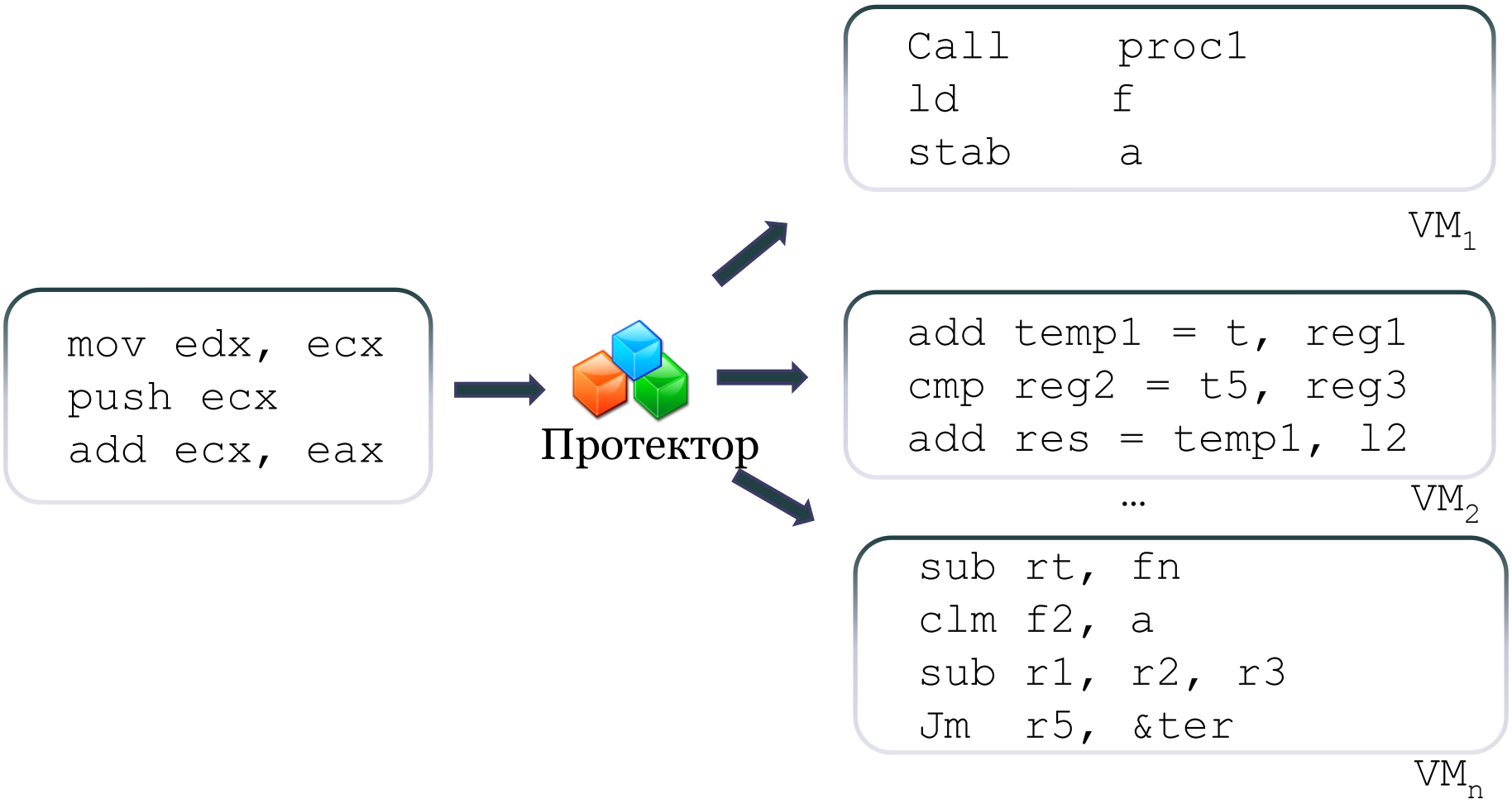
Задачи:

- Разработка генератора виртуальных машин, как мультиплатформенного протектора
- Разработка вариативной системы команд виртуальных машин

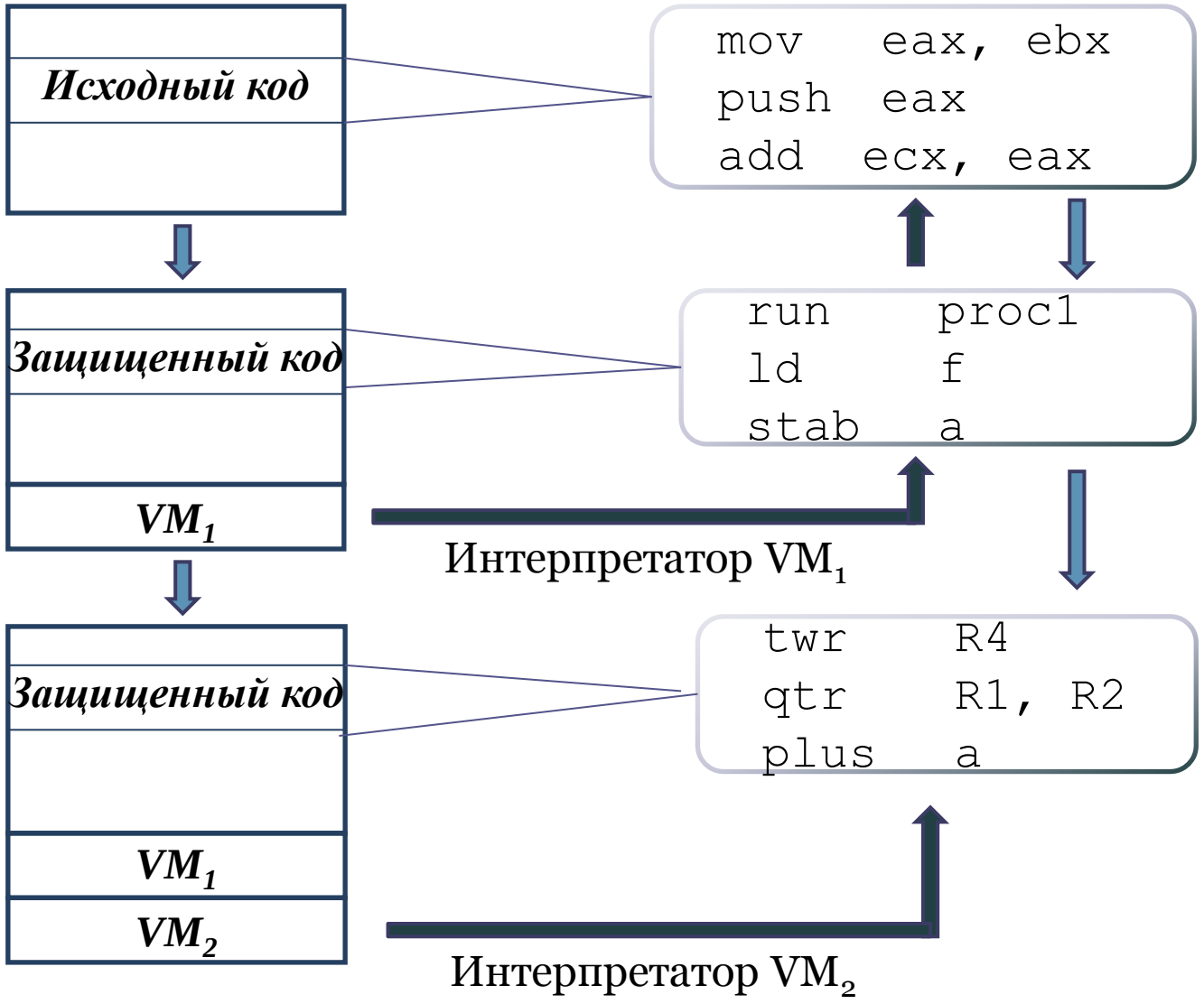
Виртуальная машина



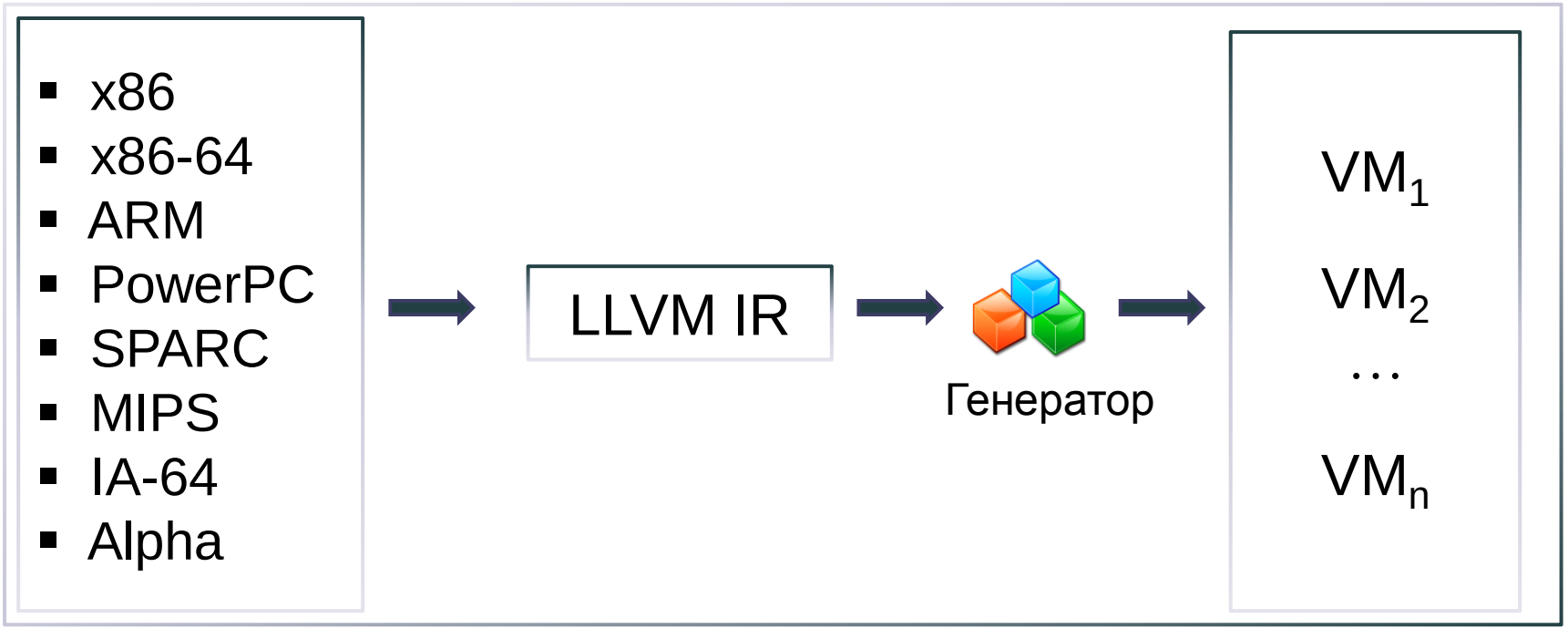
Генератор виртуальных машин



Многоуровневая защита



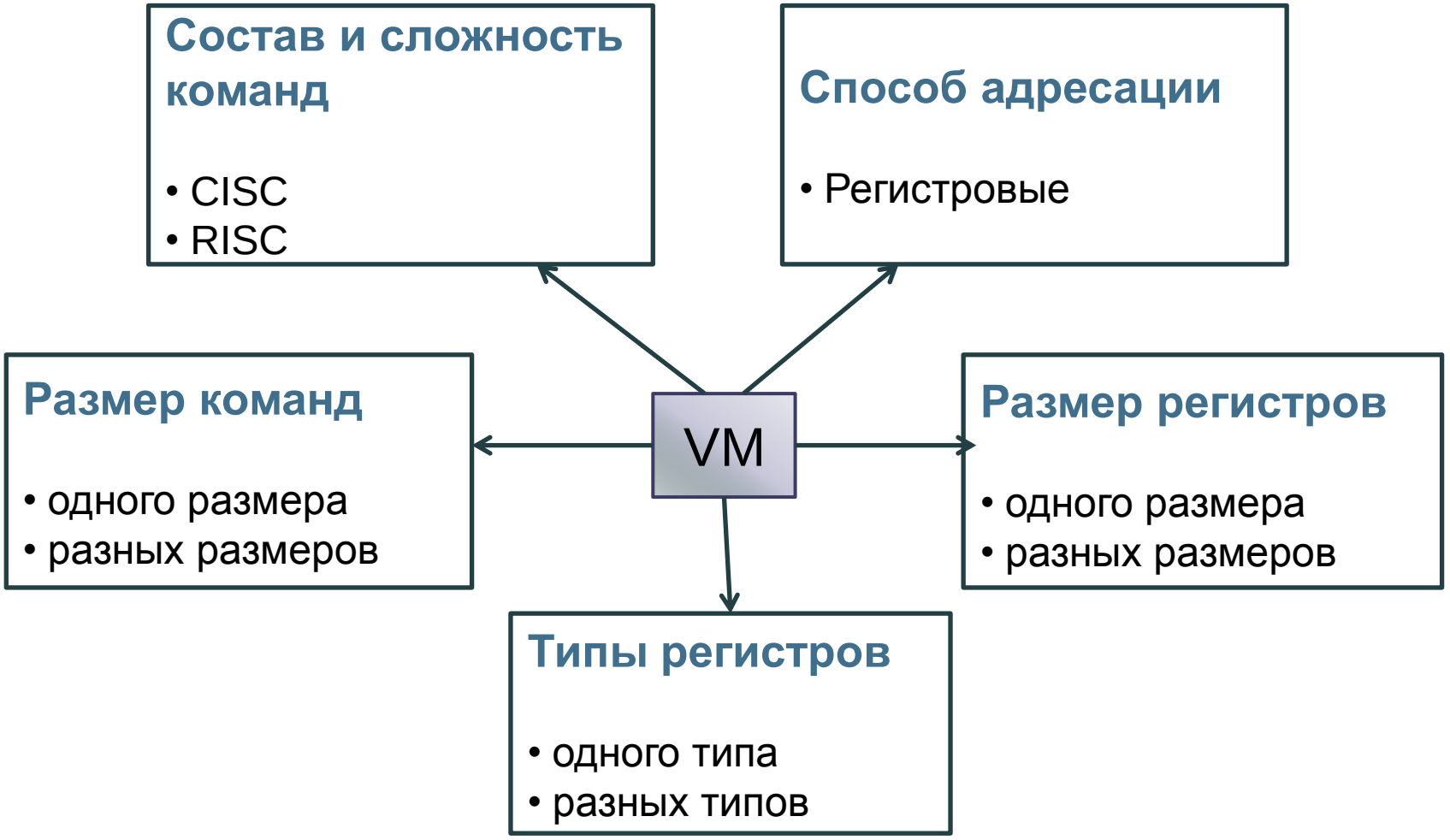
Мультиплатформенность протектора



LLVM *- Low Level Virtual Machine*

LLVM IR *– LLVM Intermediate Representation*

Типы виртуальных машин



Многообразие команд виртуальных машин

Типы команды

знаковые
беззнаковые

целочисленные
веществ. чисел

двухоперандные
трехоперандные

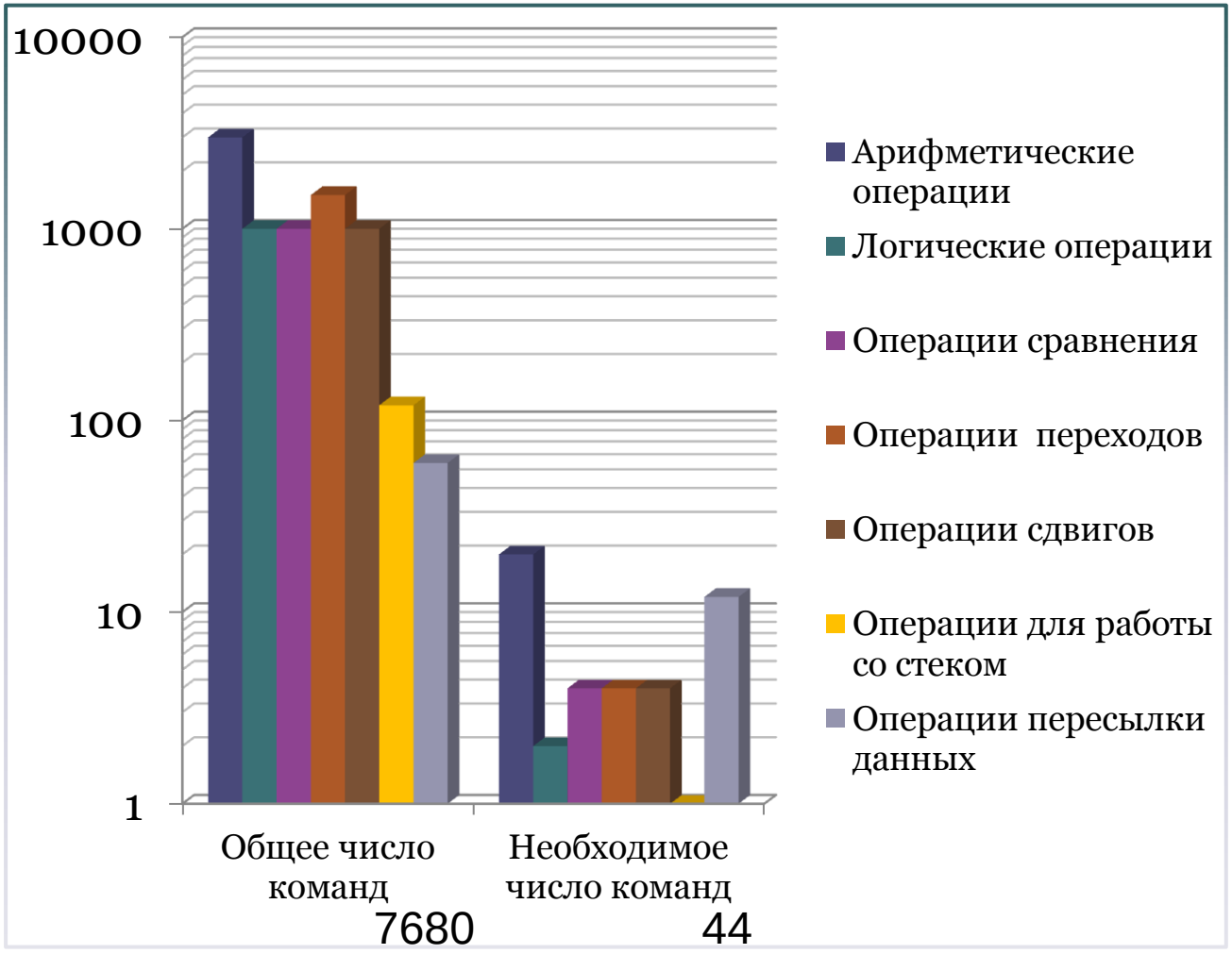
Операнды

Размер
- 8/16/32/64/80 бит

Тип

- регистр
- ссылка на ячейку памяти
- непосредственное значение
- регистр, с адресом ячейки памяти

Функционально - полные наборы команд

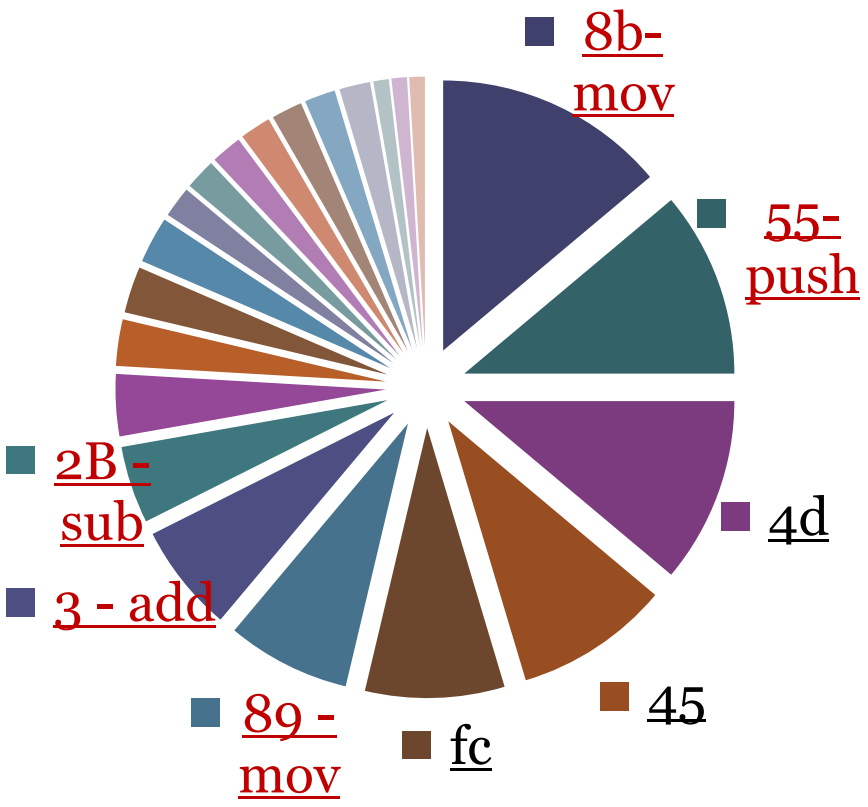


- 200 команд
- Число наборов команд превышает

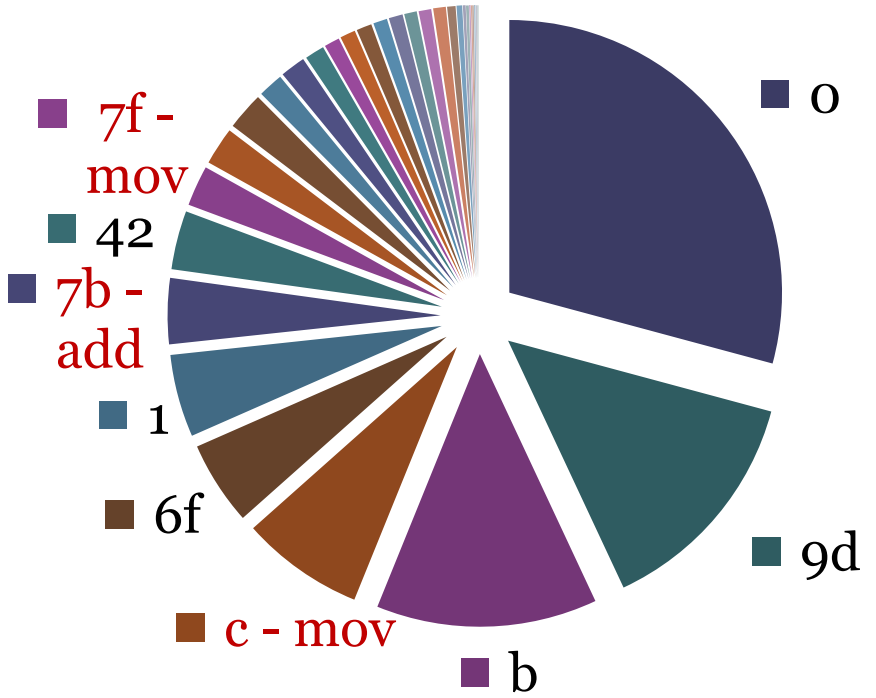
$$C_{7636}^{156} \cong 6 \cdot 10^{329}$$

Частотный анализ байт-кода

Машинные коды x86



Машинные коды VM



Результаты

- Определено множество свойств виртуальных машин варьируя которые, создаются конкретные виртуальные машины.

- Разработана вариативная система наборов команд виртуальных машин, которая
  - состоит более чем из 10^329 различных наборов команд
  - не поддается частотному анализу

- Разработан и реализован генератор виртуальных машин, который
  - является мультиплатформенным протектором
  - позволяет производить многоуровневую защиту ПО

Спасибо за внимание