# CODA

# Метрика в пространстве портретов процессов

Научный руководитель:
ст. преп. М.В.Баклановский

Лозов Пётр Алексеевич
371 группа

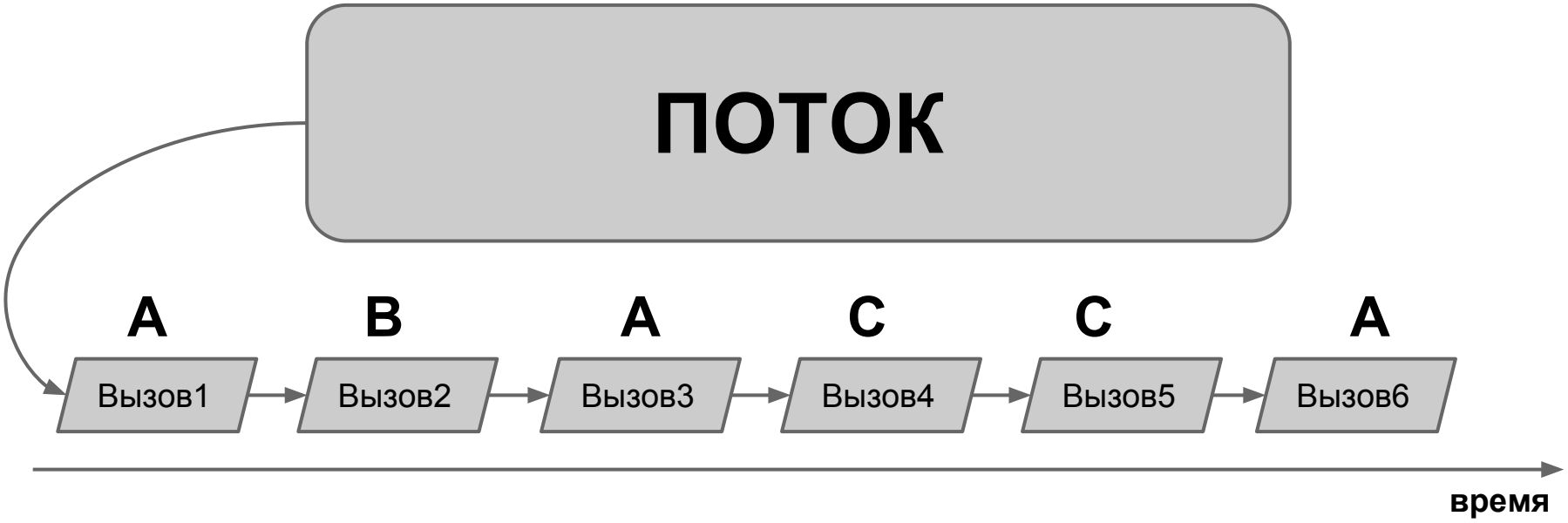
СПбГУ
2015

# Проект CODA

- Система противодействия вредоносным программам
- Анализ процессов, а не файлов
- Принцип “чужой среди своих”
- Нечёткая реакция на угрозы

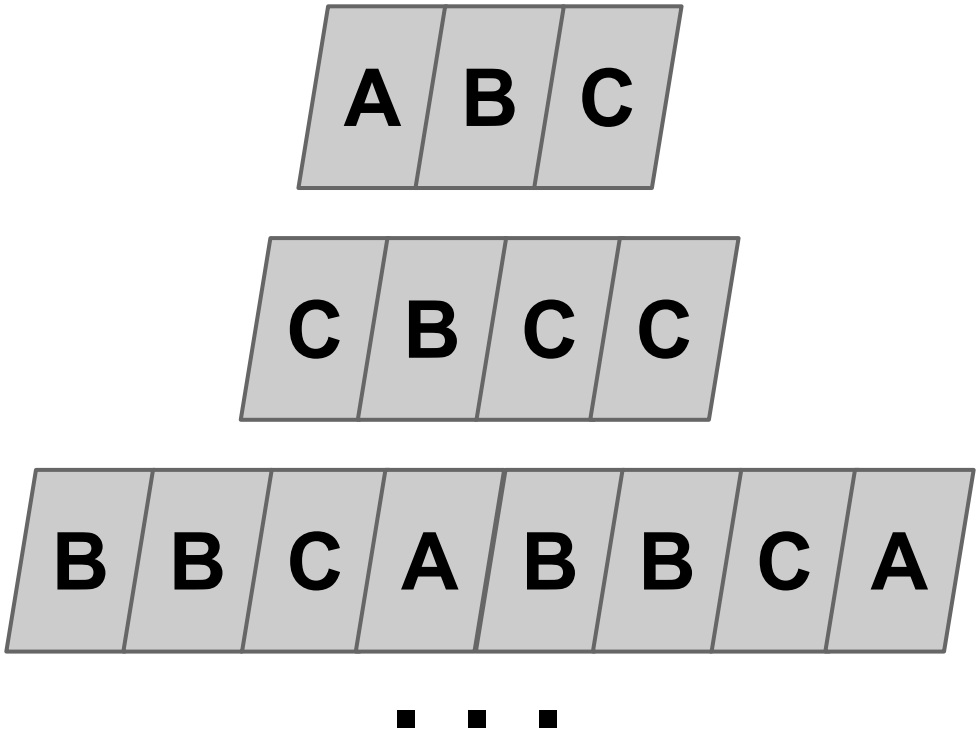
# След потока

Упорядоченный набор системных вызовов потока процесса



# Портрет процесса

Набор часто повторяющихся подстрок
в следах процесса



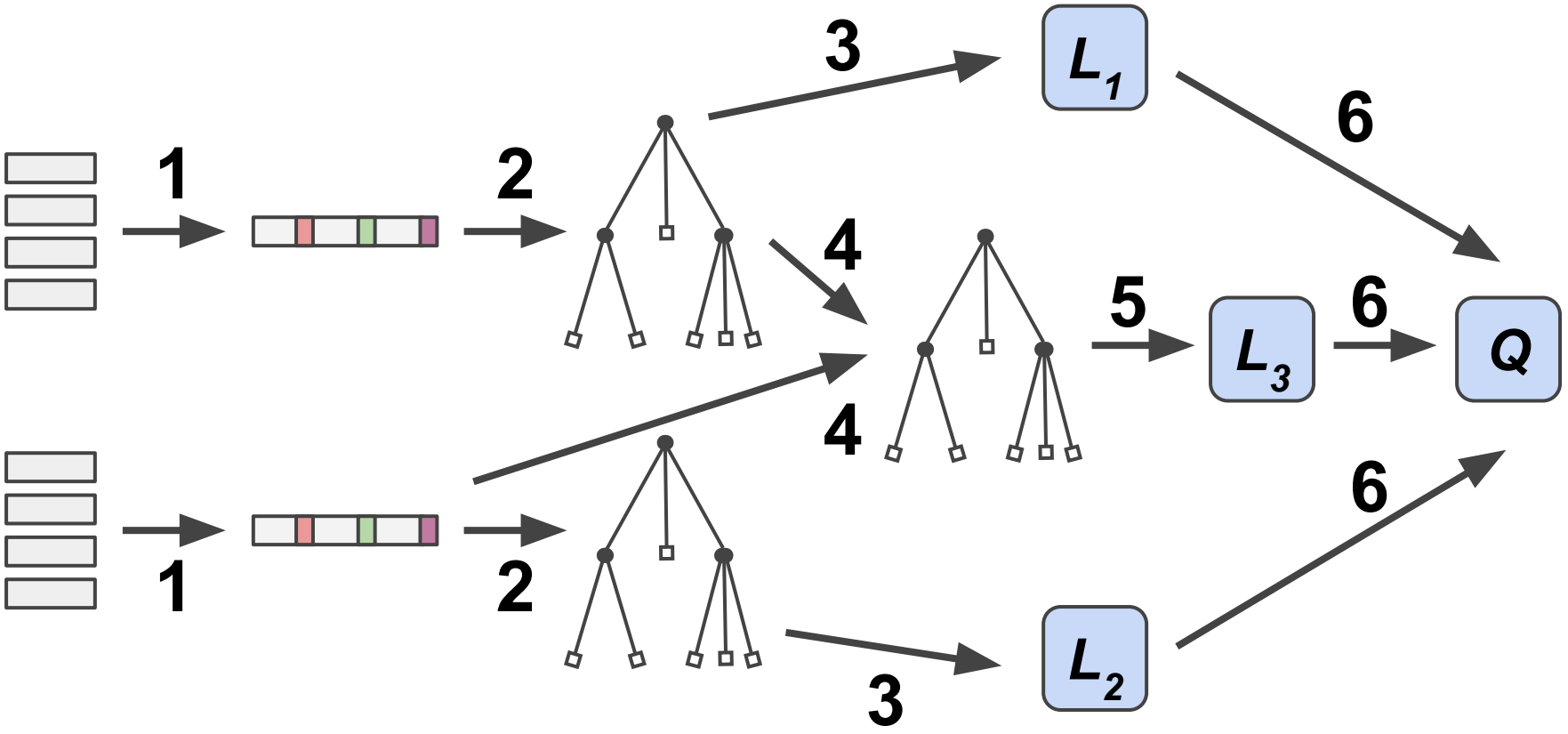
# Задачи

- Собрать базу портретов
- Разработать алгоритм сравнения портретов
- Провести тестирование алгоритма на собранных портретах

# Выбор алгоритма

- Частоты символов
- Общие строки
- Общие подпоследовательности
- Общие замкнутые подстроки

# Реализация



# Реализация

N — сумма длин всех шаблонов

M — общий размер портретов

- Память: O(N)
- Время: O(N * logM)

# Тестирование (1)

## Различные процессы

| | Explorer | Opera | Mine Sweeper | Task Manager | Paint W7 | Note Pad ++ | WinRAR | Calculator W7 | VS 2012 | Word Pad |
|---|---|---|---|---|---|---|---|---|---|---|
| Explorer | **63** | **0** | **3** | **2** | **2** | **3** | **5** | **3** | **3** | **3** |
| Opera | **0** | **52** | **8** | **0** | **1** | **0** | **1** | **1** | **1** | **0** |
| Mine Sweeper | **2** | **5** | **88** | **2** | **2** | **2** | **3** | **3** | **1** | **2** |
| Task Manager | **2** | **0** | **3** | **34** | **2** | **2** | **7** | **5** | **1** | **1** |
| Paint W7 | **4** | **0** | **2** | **2** | **47** | **5** | **4** | **3** | **2** | **15** |
| Note Pad ++ | **3** | **0** | **3** | **2** | **2** | **59** | **6** | **4** | **2** | **1** |
| WinRAR | **5** | **1** | **5** | **6** | **3** | **5** | **40** | **6** | **3** | **4** |
| Calculator W7 | **2** | **1** | **3** | **4** | **2** | **3** | **3** | **67** | **1** | **1** |
| VS 2012 | **2** | **1** | **1** | **1** | **2** | **2** | **2** | **1** | **50** | **2** |
| Word Pad | **4** | **0** | **2** | **1** | **12** | **2** | **4** | **2** | **2** | **12** |

# Тестирование (2)

## Различные поведения процесса Word Pad

| | Просмотр | Вставка текста | Изображение | Курсив | Всё вместе |
|---|---|---|---|---|---|
| Просмотр | **49** | **7** | **9** | **6** | **16** |
| Вставка текста | **5** | **51** | **2** | **2** | **19** |
| Изображение | **5** | **2** | **94** | **2** | **21** |
| Курсив | **5** | **3** | **2** | **99** | **99** |
| Всё вместе | **8** | **22** | **15** | **71** | **97** |

# Тестирование (3)

## Различные поведения процесса Opera

| | Google | Wikipedia | Google map | Youtube | Всё вместе |
|---|---|---|---|---|---|
| Google | **75** | **53** | **13** | **23** | **51** |
| Wikipedia | **51** | **71** | **14** | **20** | **36** |
| Google map | **17** | **14** | **61** | **14** | **21** |
| Youtube | **25** | **29** | **11** | **54** | **61** |
| Всё вместе | **46** | **41** | **22** | **58** | **69** |

# Тестирование (4)
## Текстовые редакторы

| | Word Pad | Note Pad | Note Pad ++ | Far Manager | Sublime Text | VS 2012 |
|---|---|---|---|---|---|---|
| Word Pad | **93** | **9** | **12** | **1** | **1** | **4** |
| Note Pad | **13** | **92** | **17** | **1** | **1** | **10** |
| Note Pad ++ | **14** | **15** | **73** | **2** | **1** | **10** |
| Far Manager | **1** | **1** | **2** | **99** | **0** | **3** |
| Sublime Text | **1** | **1** | **2** | **0** | **91** | **1** |
| VS 2012 | **13** | **18** | **20** | **3** | **1** | **81** |

# Результаты

- Собрана база портретов (> 100)
- Разработан алгоритм сравнения портретов
- Проведено тестирование алгоритма на собранных портретах