Разработка профайлера уровня ядра Windows
Анализ блокировок и ожиданий.

СПбГУ, Кафедра системного программирования

Научный руководитель

Баклановский М.В.

Анисимов Константин

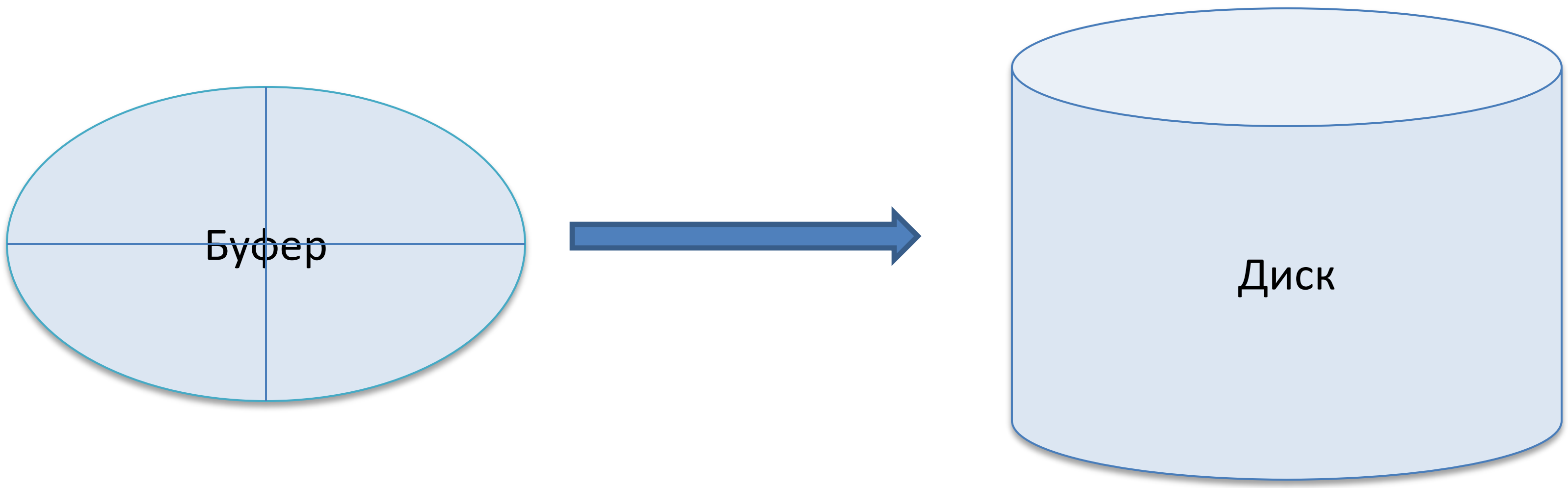
rrevenantt@gmail.com

Аналоги

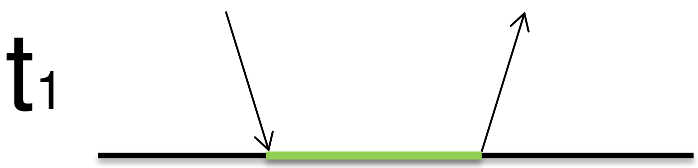
	xPerf	VTune
Семплирование (user mode)	+	+
Семплирование (kernel mode)	+	+
Инструментирование (user mode)	-	+
Инструментирование (kernel mode)	- (ETW)	-

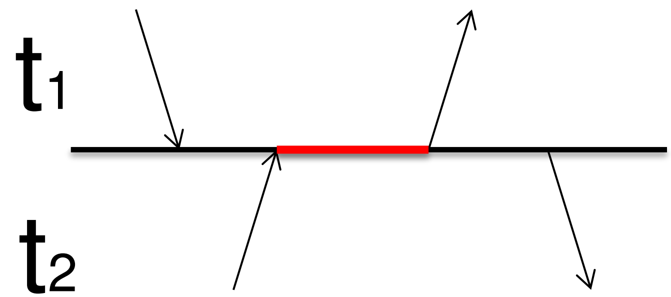
Архитектура

Захват / освобождение SpinLock'а



Полезные данные

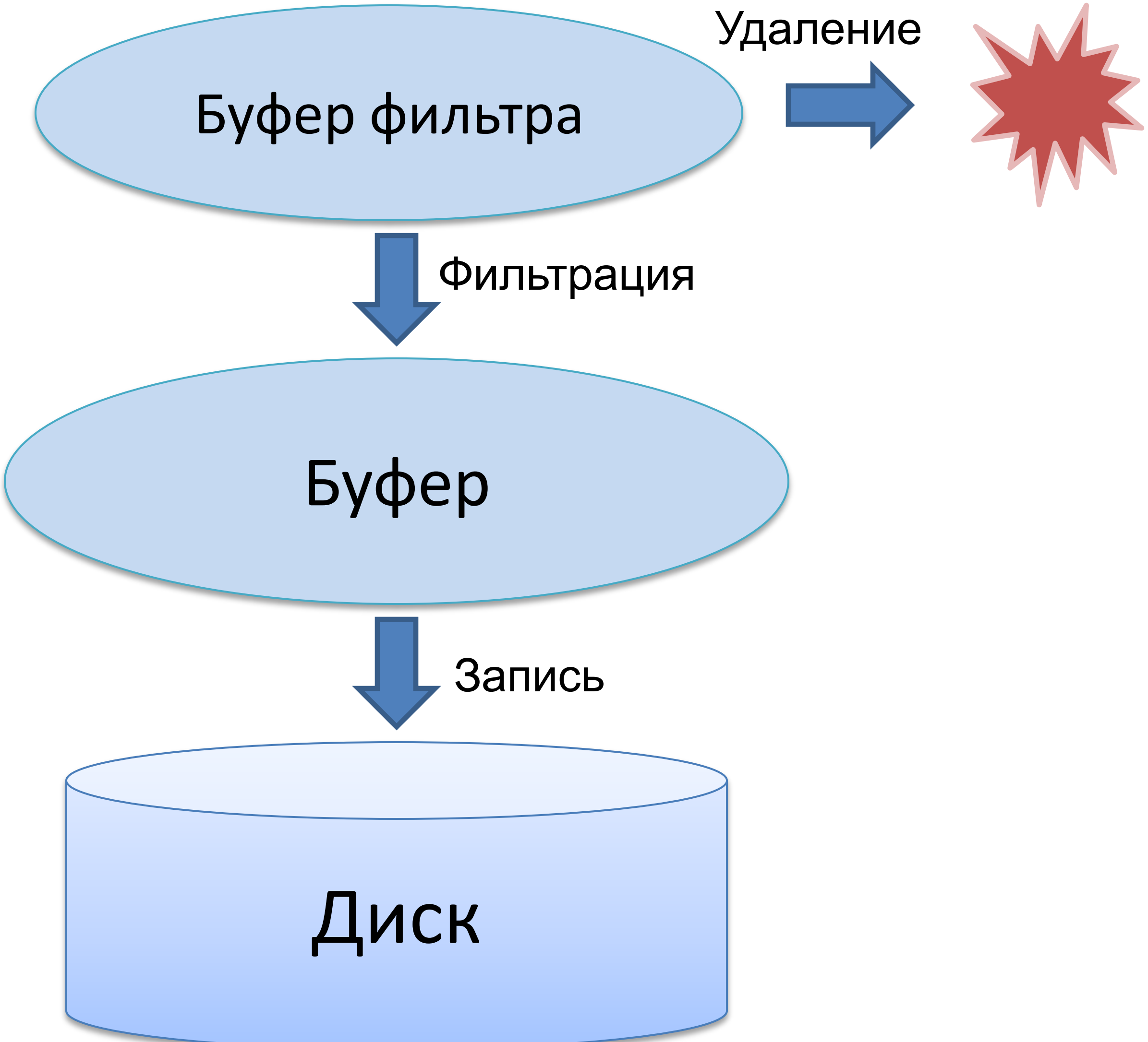




95%

5%

Предлагаемое решение

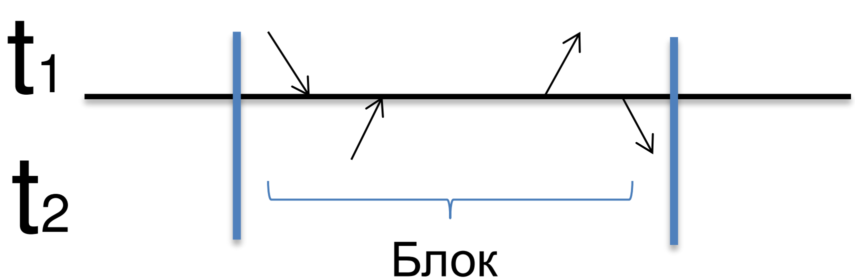


Проблемы

- Переполнение промежуточного буфера
- Определение окончания записи

Решение

- Отключение фильтрации
- Выделение блоков обращений к ресурсу

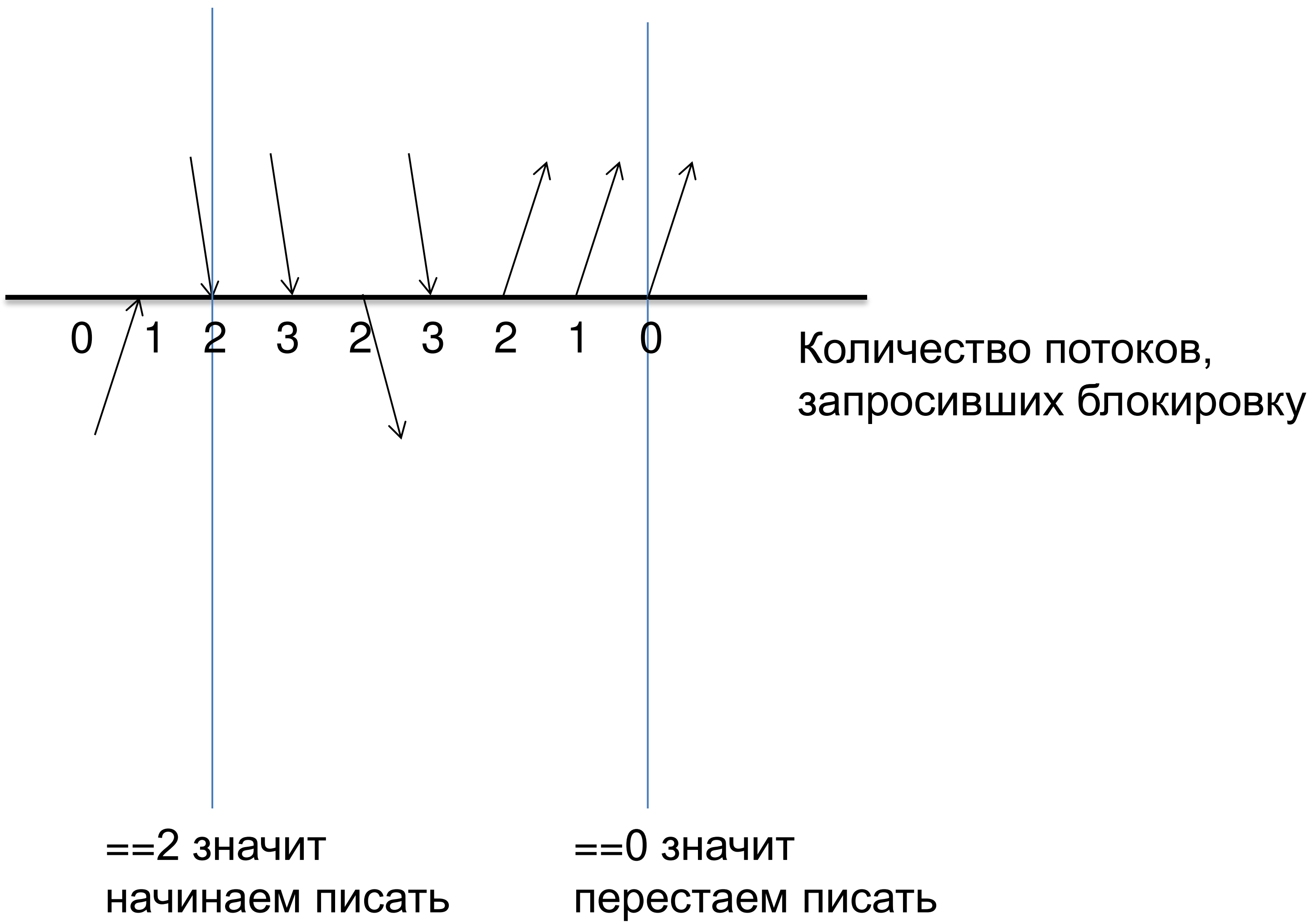


Счетчик

Для каждого ресурса(блокировки):

- Функция захвата – увеличение счетчика
- Функция освобождения – уменьшение счетчика
- Если сразу за захватом - освобождение тем же потоком , то не пишем в буфер.
- Если нет, меняем состояние записи и пишем все, пока счетчик не обнулится

Пример обработки



Не обработанные ситуации

- Начало записи
- Не один захват от одного потока
- Не одно освобождение от одного потока

Накладные расходы

– Без профайлера	500 тактов
– Без фильтрации	1500 тактов
– С фильтрацией	2500 тактов

```
rdtsc;
KeAquireSpinLock();
KeReleaseSpinLock();
rdtsc;
```