Конфигурируемая модульная система мониторинга поведения транспортного протокола на уровне ядра операционной системы

- В. А. Пономарев
- О. Ю. Богоявленская
- Ю. А. Богоявленский

{vadim,olbgvl,ybgv}@cs.karelia.ru

Петрозаводский Государственный Университет

Введение

- Перехват сетевого трафика используется при организации мониторинга сети, учета трафика, выяснении способов несанкционированного воздействия, решении исследовательских задач
- Существует большое количество утилит для перехвата сетевого трафика: tcpdump, wireshark (бывший Ethereal), netfilter ULOG + fprobe-ulog и т.д.

Введение

- Для решения некоторых исследовательских задач, а также при несанкционированных воздействиях, подобных описанным в Alexandar Kuzmanovic, Edward W. Knightly, Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. The Mice and Elephants), ACM SIGCOMM 2003, требуется доступ к внутренним переменным ядра ОС
- Традиционные утилиты перехвата трафика не предоставляют такую возможность

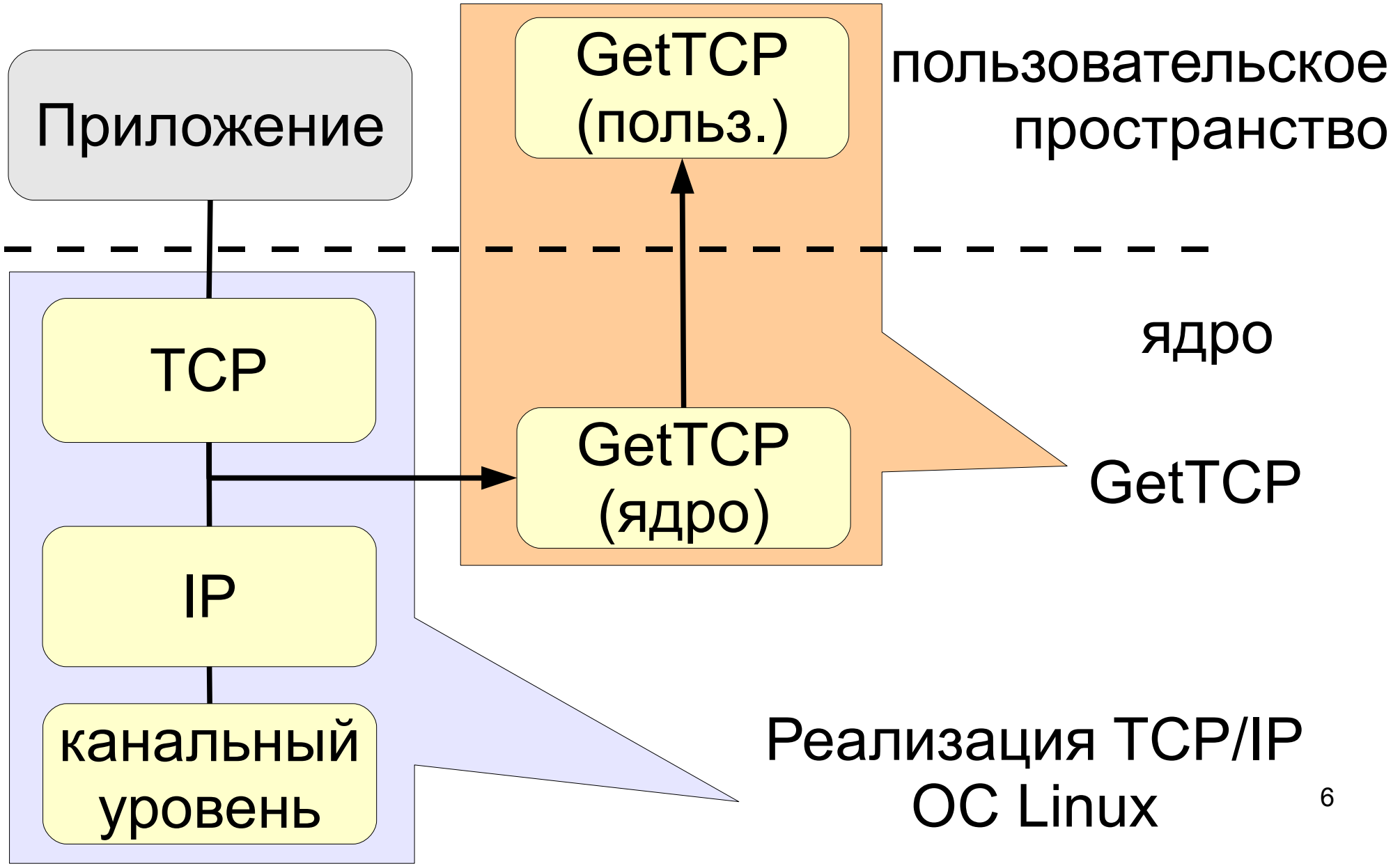
Введение

- SystemTap (Red Hat, IBM, Intel, Hitachi, Oracle): предоставляет возможность доступа к внутренним данным ядра, слишком громоздкая, высокие накладные расходы, нет возможности интеграции с существующими утилитами перехвата трафика

Первая версия GetTCP

- На МаБИТ 2006 авторами была представлена первая версия системы перехвата GetTCP
- GetTCP позволяет получать локализованные в ядре ОС Linux данные о состоянии внутренних переменных, отражающих поведение соединений TCP
- Приняты меры для уменьшения накладных расходов

Первая версия GetTCP



Первая версия GetTCP

- Система успешно применялась для сбора данных, необходимых для проверки адекватности модели TCP (труды международного семинара DCCN 2007)
- Вместе с тем, первоначальный вариант системы GetTCP обладал рядом недостатков
- Отсутствие полноценной библиотеки пользовательского уровня, обеспечивающей доступ к возможностям системы
- Необходимость перекомпиляции ядра

Получение управления

- Для получения внутренних данных ядра ОС часть системы должна действовать в адресном пространстве ядра и получать управление при отправлении каждого сегмента TCP, дейтаграммы IP и т.п.
- В первой версии в исходный код ядра ОС Linux, осуществляющий передачу сегмента TCP, была добавлена передача управления системе GetTCP

Получение управления

- В современном ядре ОС Linux существует возможность динамической установки «контрольных точек» Kprobes
- Была исследована одна из разновидностей: Jprobes
- Выяснилось, что получение управления с использованием Jprobes на тестовой ЭВМ требует минимум 3185 тактов процессора, что составляет около 1мкс

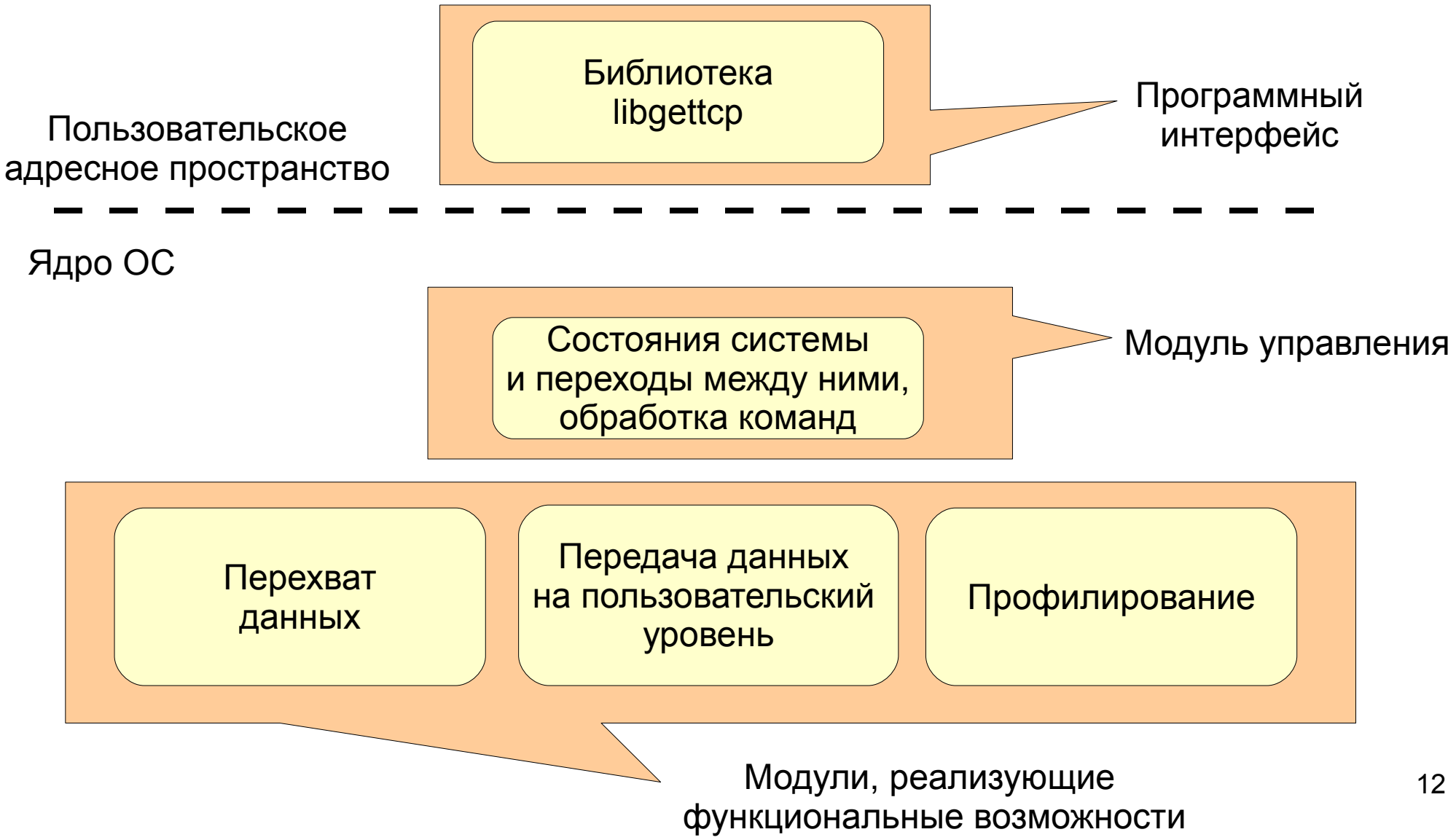
Получение управления

- В первой версии системы GetTCP накладные расходы в 94.02% случаев не превышали 0.3 мкс (на той же самой тестовой ЭВМ). Было принято решение отказаться от использования Kprobes
- Kernel markers: включен в «официальное» ядро ОС Linux начиная с версии 2.6.24
- Для получения управления с помощью kernel markers требуется 138 тактов процессора (около 0.05 мкс)

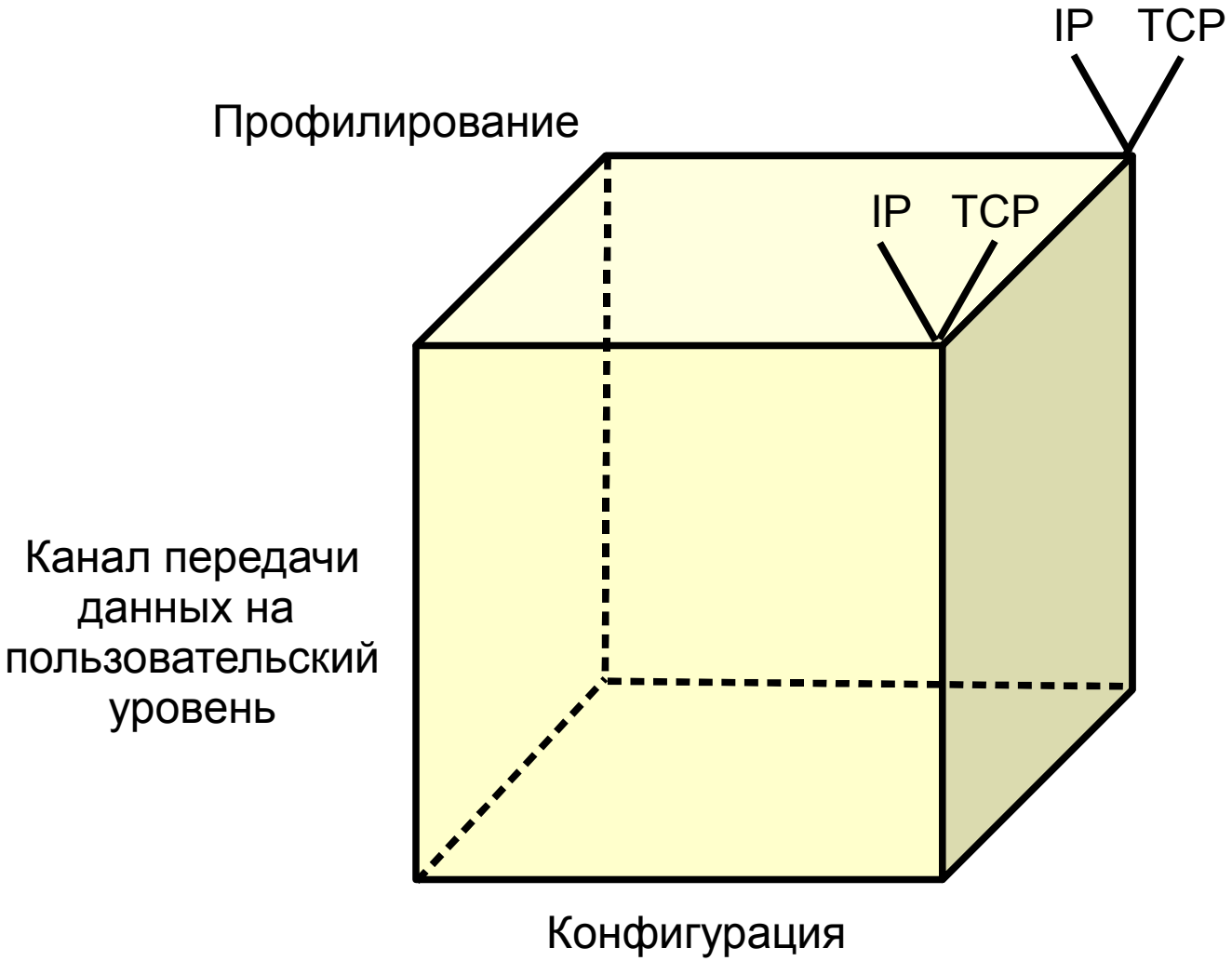
Получение управления

- Было принято решение об использовании механизма kernel markers
- Необходимость внесения изменений в исходный код ядра и последующей перекомпиляции ядра были признаны неизбежными т.к. доступные механизмы, не требующие перекомпиляции (Kprobes) приводят к недопустимому увеличению накладных расходов

Архитектура



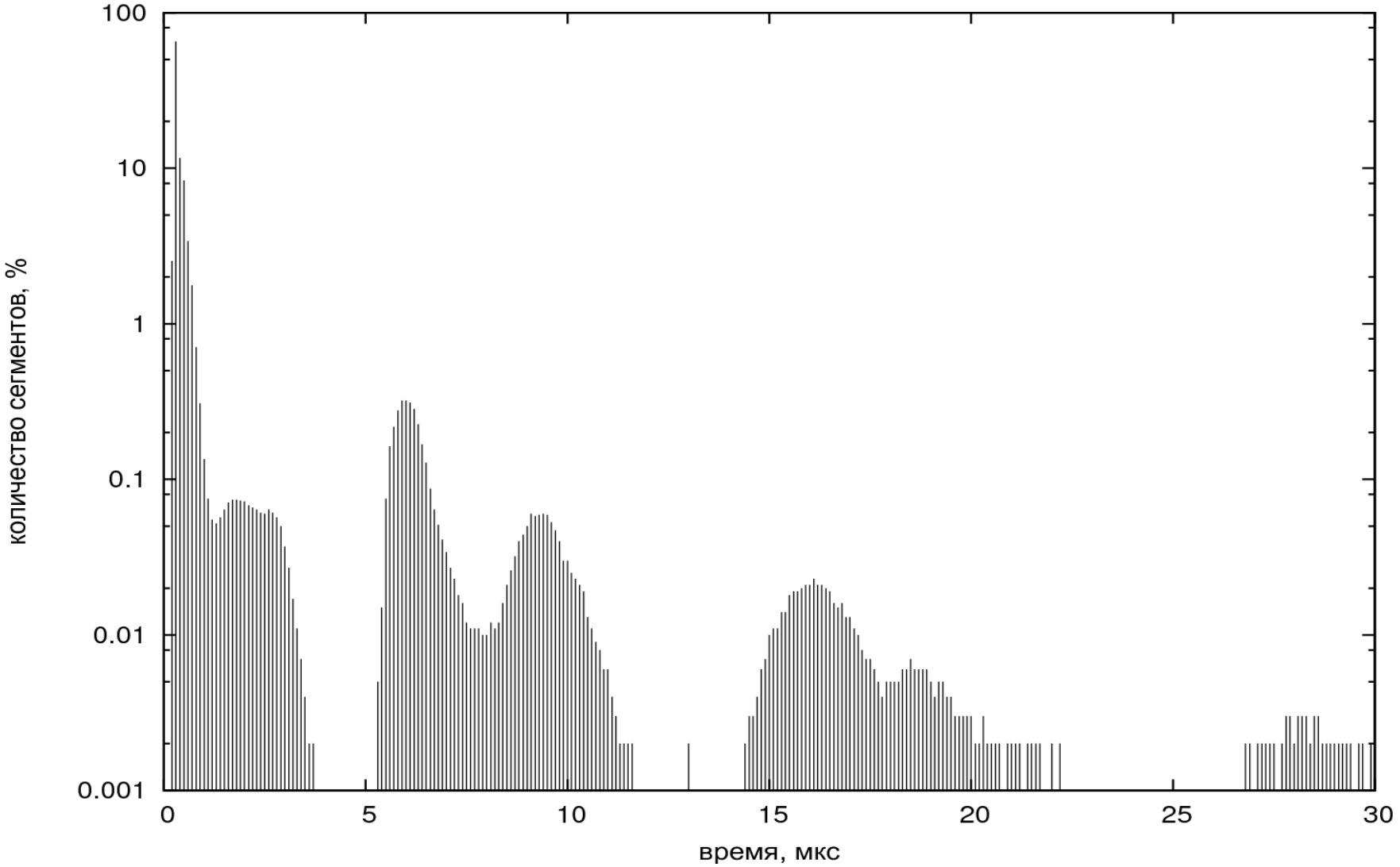
Состояния


IP TCP
Профилирование
IP TCP
Канал передачи данных на пользовательский уровень
Конфигурация

Реактивность

- Передавался максимально возможный объем данных за фиксированный интервал времени (120 секунд) при фиксированном размере сегмента (50 байт)
- Для 94% сегментов задержка не превышает 1 мкс

Реактивность



Результаты и текущее состояние

- По сравнению со старой версией улучшена архитектура и реализация части системы, действующей в адресном пространстве ядра
- Реализована библиотека libgettcp, предоставляющая доступ к возможностям системы
- Выполнена модификация утилиты fprobe-ulog для работы с использованием библиотеки libgettcp

Результаты и текущее состояние

- Уточняются накладные расходы, возникающие при работе системы, для различного оборудования и условий работы
- Идет тестирование и отладка
- Возможно применение в качестве инструментального средства для решения задач безопасности