КОД БЕЗОПАСНОСТИ

10 ЛЕТ

Высокоскоростной шифратор

КОД БЕЗОПАСНОСТИ

Необходимость в средствах шифрования с высокой пропускной способностью

Проблемы

Захват пакетов сетевым адаптером и обработка прерываний => большое

количество прерываний и переключений контекста ЦП на прерывания

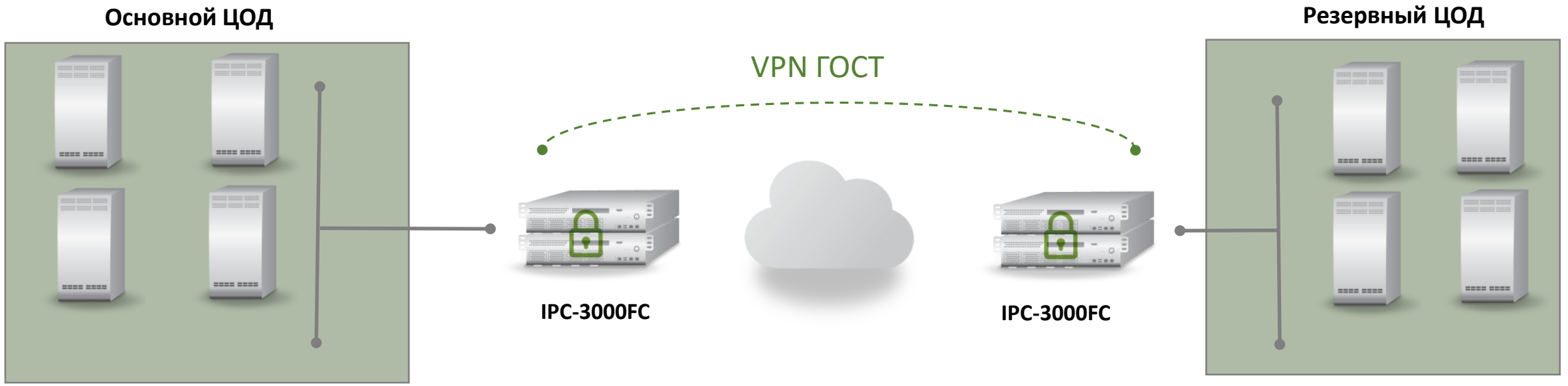
Обработка пакетов в сетевом стеке ядра ОС => большой объем кода, большой объем ветвлений, блокировки, копирования

Архитектура x86 плохо подходит для шифрования по ГОСТ 28147-89 => низкая производительность VPN

- **Требования регуляторов к межсетевому экранированию и шифрованию трафика**
- **Вертикально-ориентированная структура государственных учреждений**
- **Электронный документооборот, СМЭВ**
- **Ежегодно увеличивающиеся объемы трафика**

КОД БЕЗОПАСНОСТИ

Объединение сетей ЦОД



КОД БЕЗОПАСНОСТИ

Требования к каналам между ЦОД

- Производительность 10Гбит/с
- Отказоустойчивость
- Минимальные задержки при обработке трафика
  - Высоконагруженные БД
  - All flash СХД
  - Software Defined Storage
  - Виртуальная инфраструктура
- Масштабируемость

КОД БЕЗОПАСНОСТИ

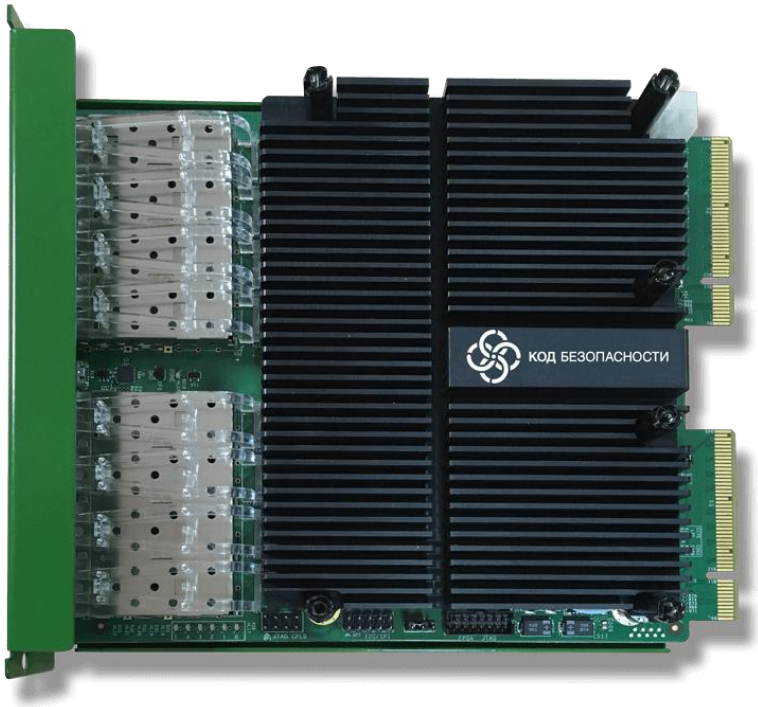
Недостатки стандартного подхода к шифрованию трафика

Недостаток	Недостатки обычных x86 серверов	Причина
Недостаточная производительность шифрования	Рост частоты процессора и числа ядер или процессоров не приводит к соответствующему увеличению производительности	• Тактовая частота ограничена технологически • Необходимость распределения задач между процессорами «компенсирует» увеличение запаса по производительности
Высокие задержки при обработке	Пакеты обрабатываются в порядке живой очереди на процессоре и сетевой плате	• Необходимость разделения ресурсов компьютера с другими процессами • «Универсальность» сетевой подсистемы ОС
Недостаточная стабильность	Утечки памяти и другие некритичные ошибки влияют на производительность ОС	• Неизбежность ошибок в системном и прикладном ПО

КОД БЕЗОПАСНОСТИ

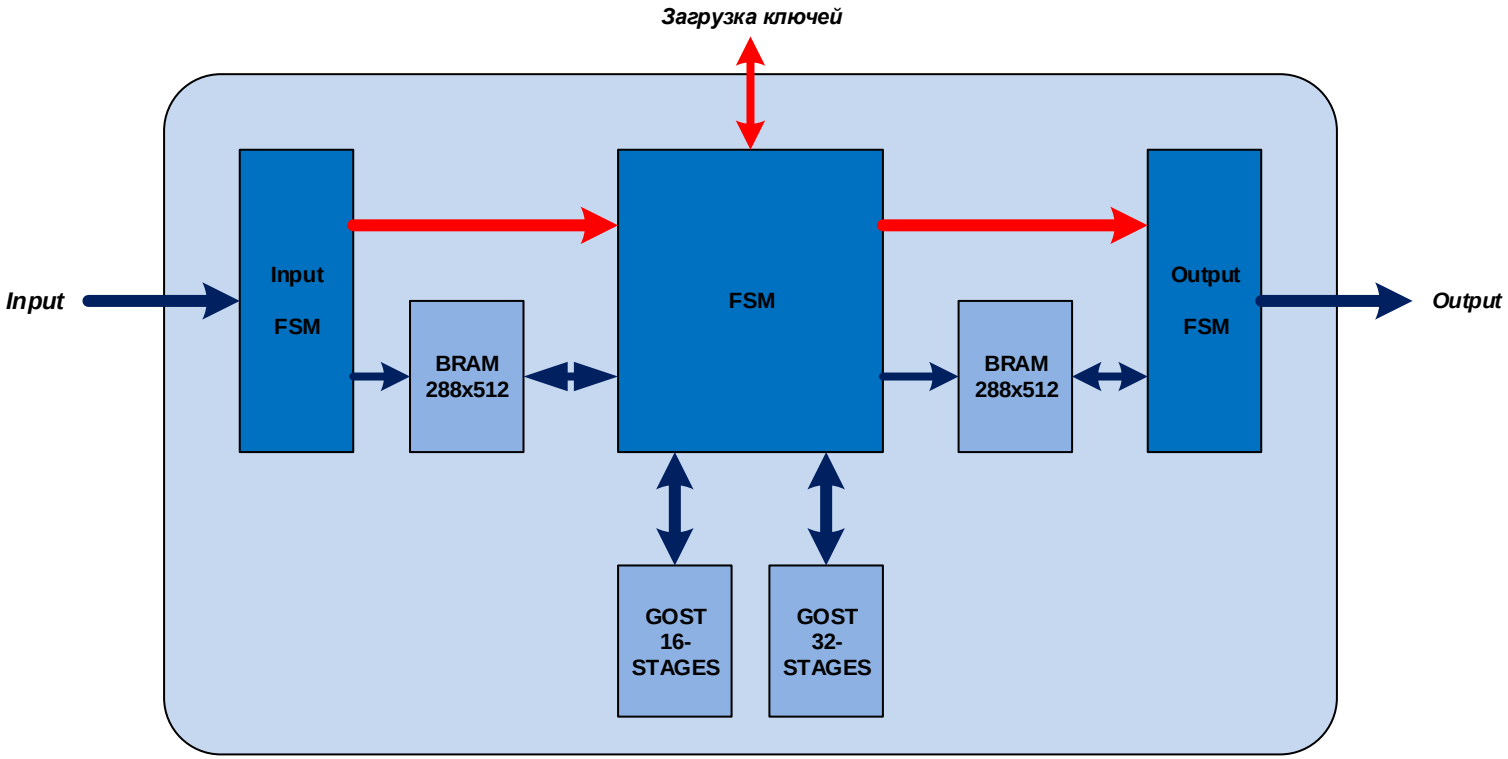
Аппаратное шифрование

Задача	Преимущество FPGA
Высокая производительность	Чип проектируется под реализацию конкретного алгоритма шифрования
Низкая задержка	Пакеты не обрабатываются на центральном процессоре и не стоят в очередях сетевого адаптера
Устойчивость к ошибкам ОС	Независимость от задержек, создаваемых ОС

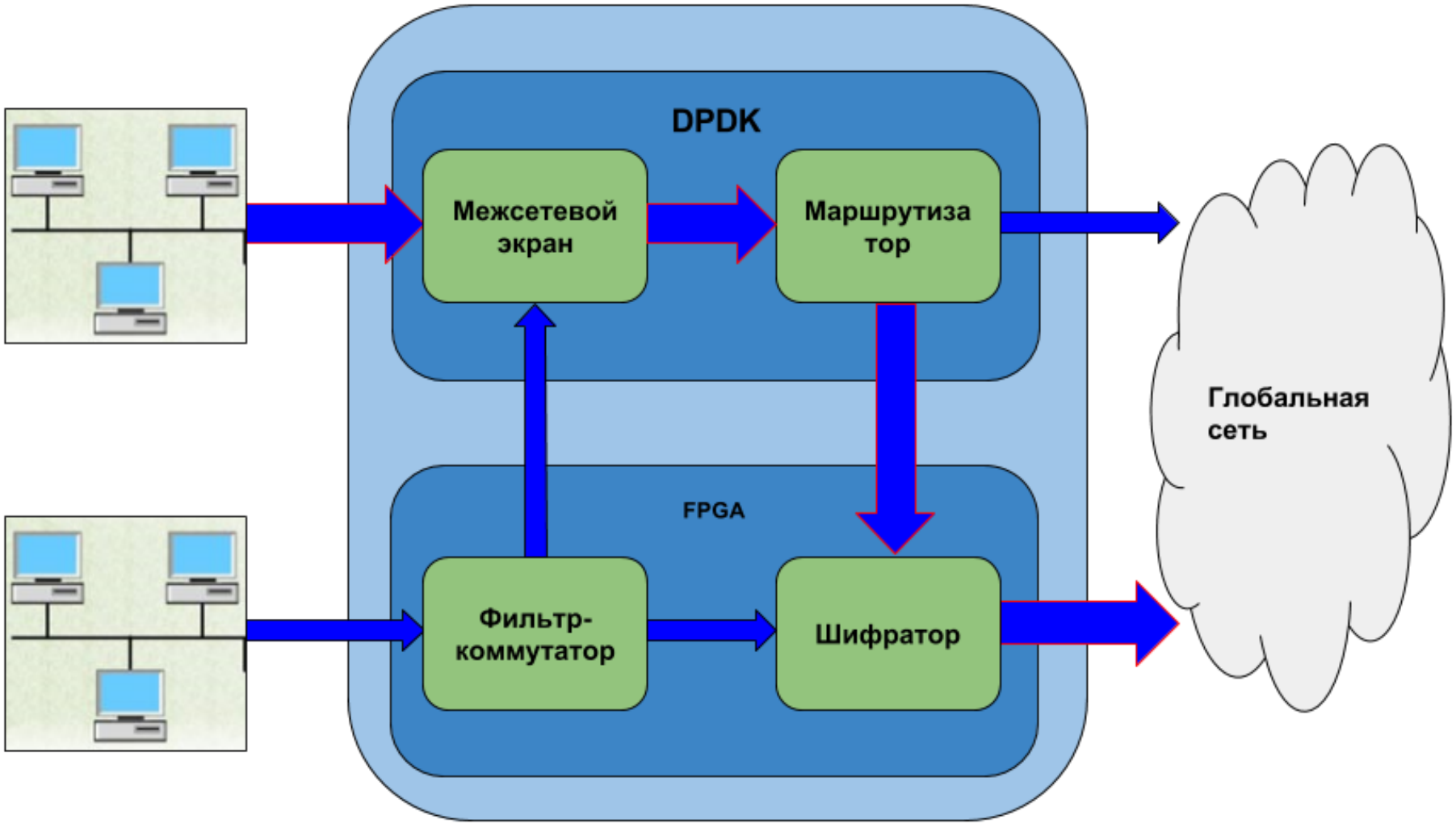


КОД БЕЗОПАСНОСТИ

Логика работы шифратора

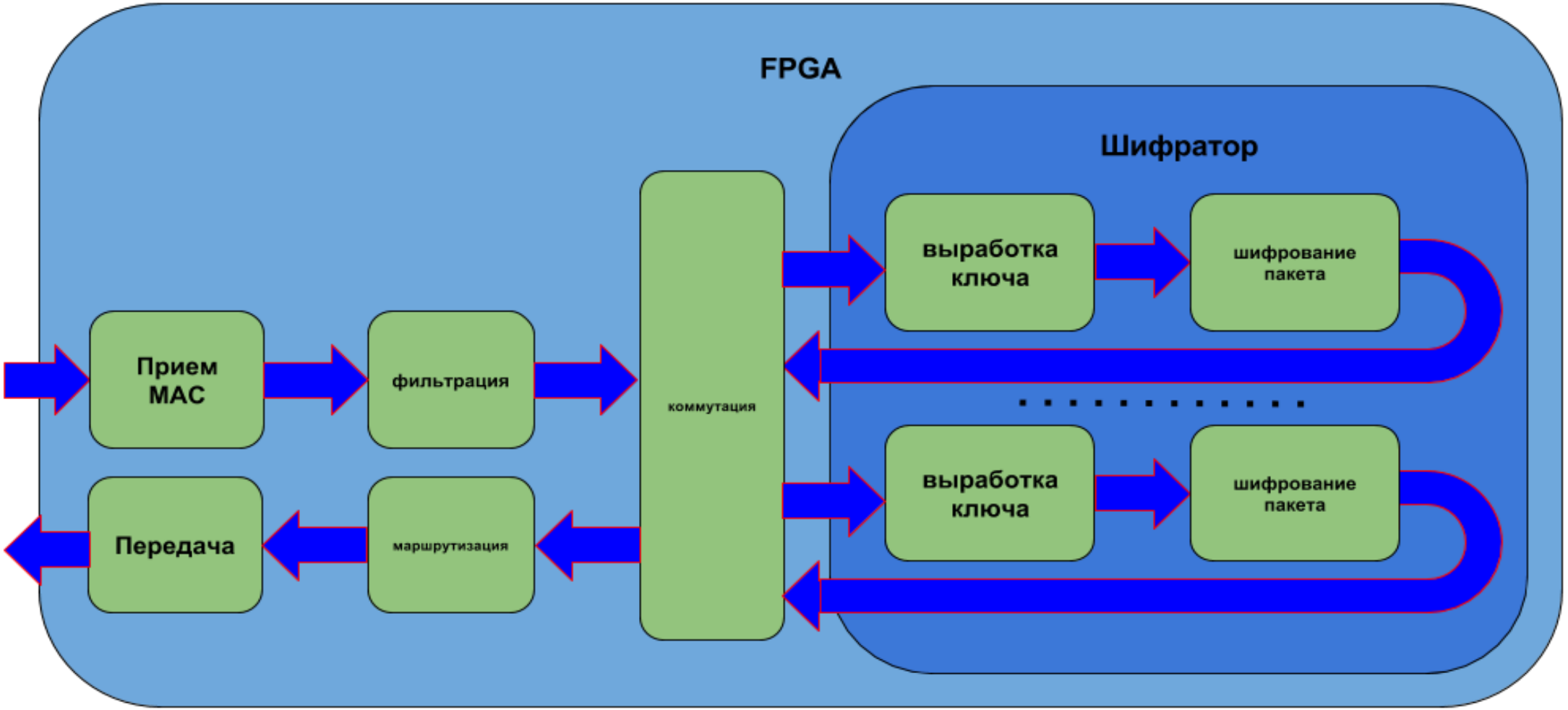


Сценарии обработки трафика



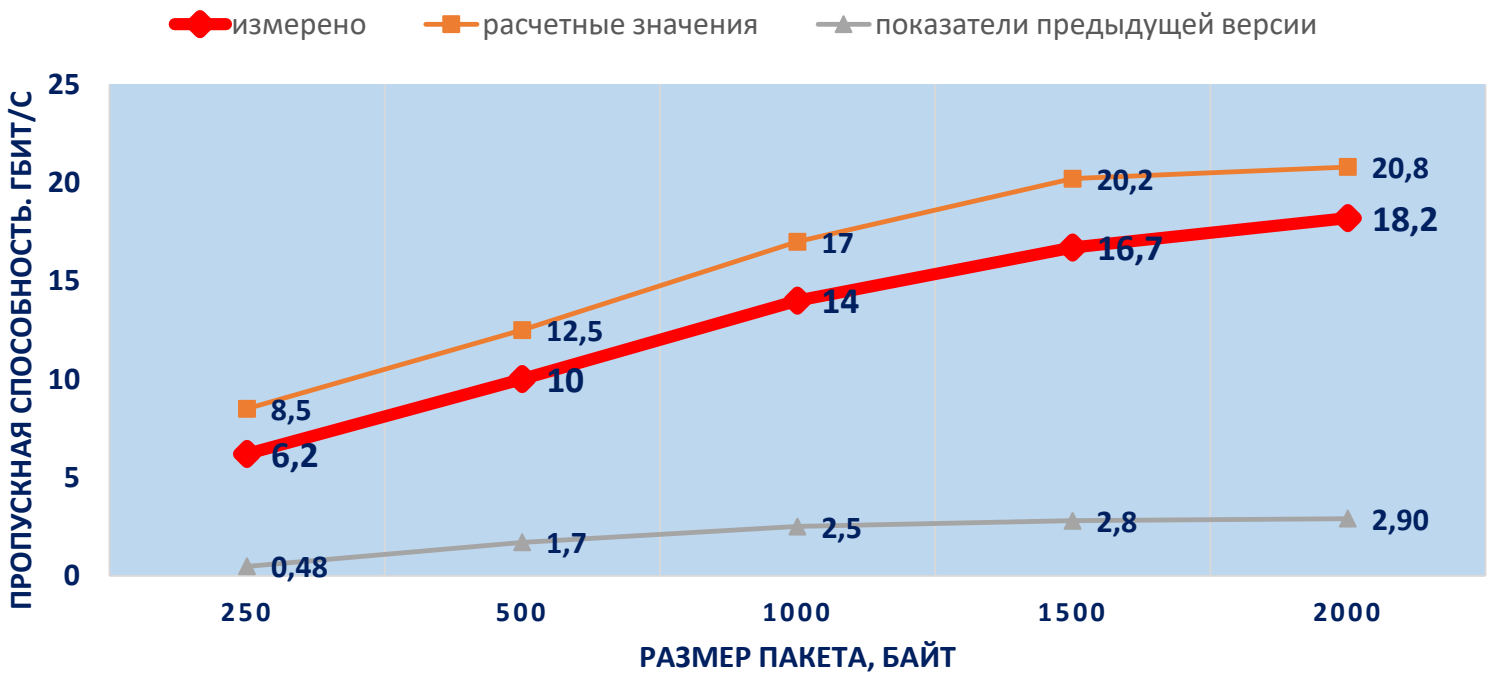
КОД БЕЗОПАСНОСТИ

Схема обработки пакетов



КОД БЕЗОПАСНОСТИ

Режимы работы: шифрование + МЭ



Алгоритм тестирования

- Длительность тестирования – не менее 1000 секунд
- Средство для тестирования Ixia BreakingPoint
- Порог потерь 0%
- Двунаправленный поток
- Не менее 100 клиентов с каждой стороны
- Не менее 10 серверов с каждой стороны

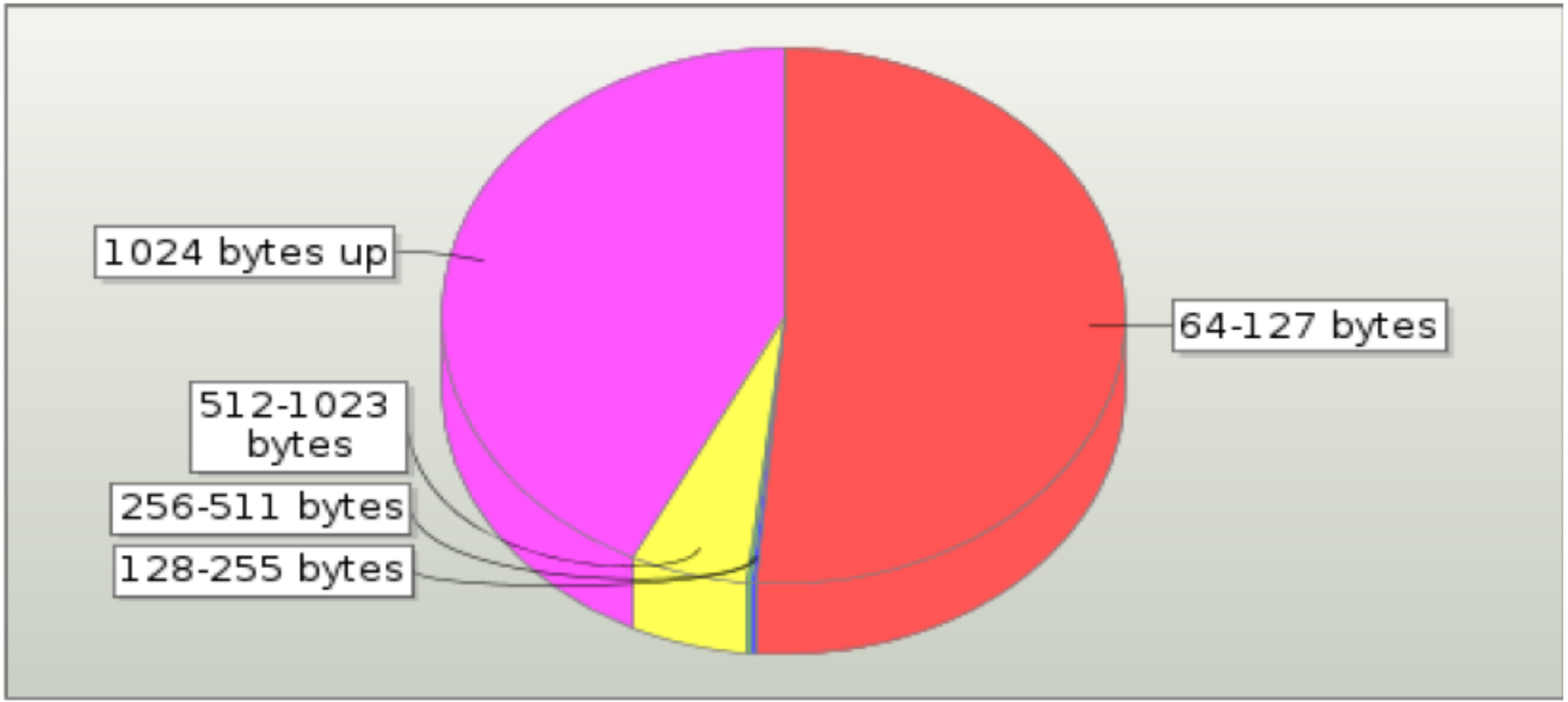
КОД БЕЗОПАСНОСТИ

Набор приложений в Real World методике

Приложение	Процент от полосы пропускания	Количество МБ в одном сеансе приложения
HTTPS	17,12	1,1
HTTP audio, video, text, bandwith	19,81	9/2/1,4/0,5
Facebook	16,98	0,6
Amazon S3	10,94	1,2
Bittorent	8,84	0,9
Yahoo Mail	5,47	0,1
FTP	4,72	0,3
Gmail	3,96	7
AOL Chat	3,28	0,4
Twitter	2,92	0,02
SMTP	2,73	0,02
Raw	2,26	5
SSH	0,57	0,01
Oracle	0,35	0,01
Youtube	0,05	23

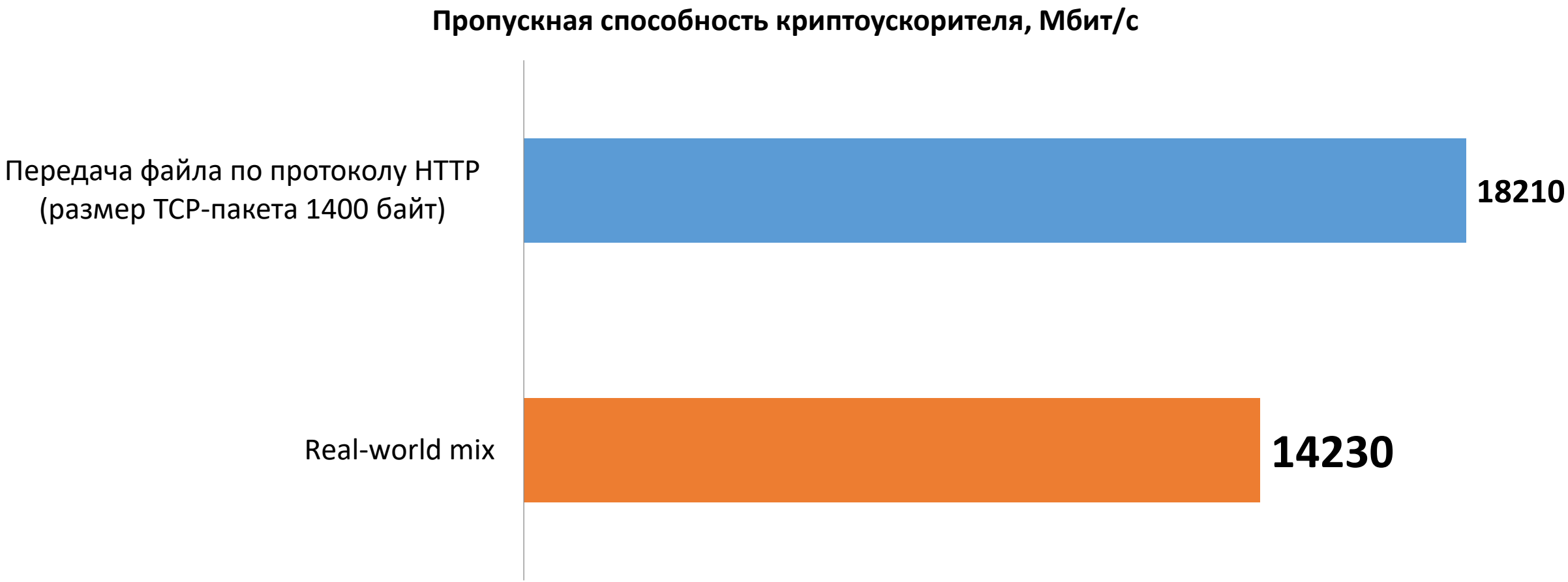
Распределение размеров пакетов в Real World методике

- В среднем – 700 байт



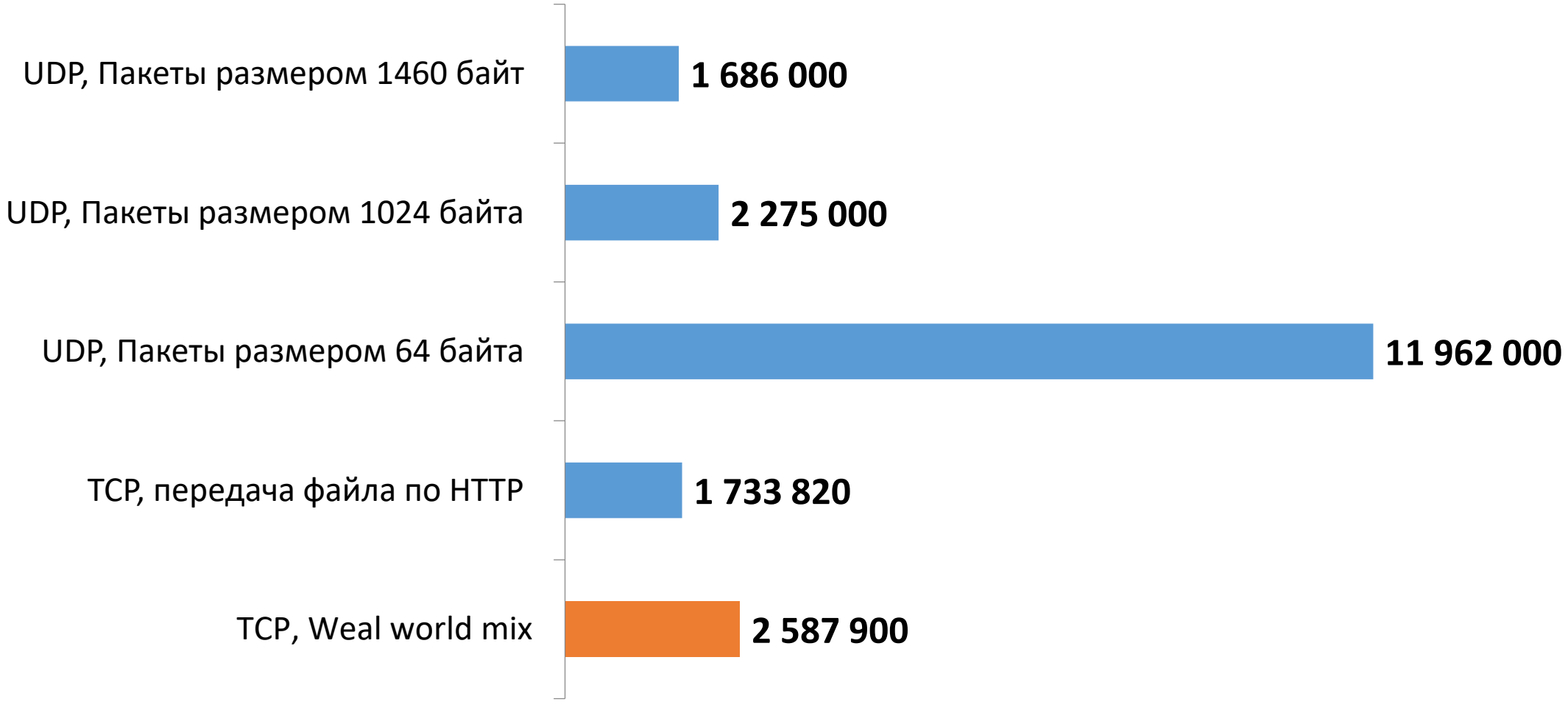
КОД БЕЗОПАСНОСТИ

Сравнение производительности TCP и Real–world mix



КОД БЕЗОПАСНОСТИ

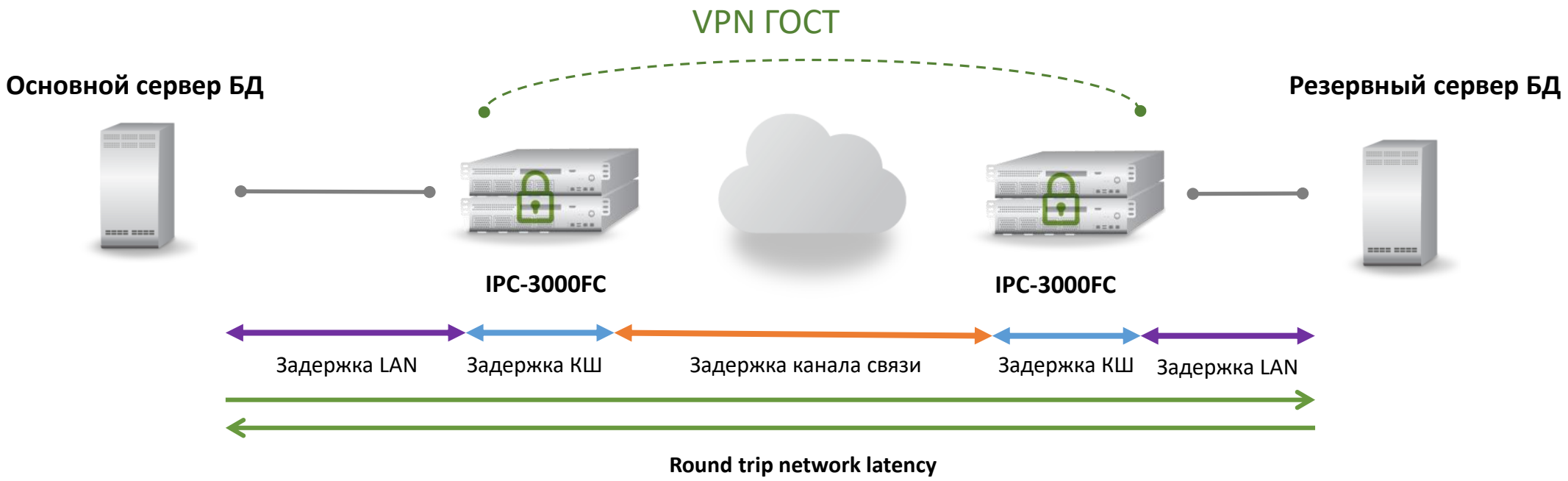
Количество обрабатываемых кадров в секунду



На обычной платформе минимум **в два раза меньше!**

КОД БЕЗОПАСНОСТИ

Важность задержки при резервировании СУБД



Для архитектора высоконагруженной БД очень важен параметр **Round trip network latency.** Это время затраченное на передачу пакета плюс время до получения пакета-подтверждения.

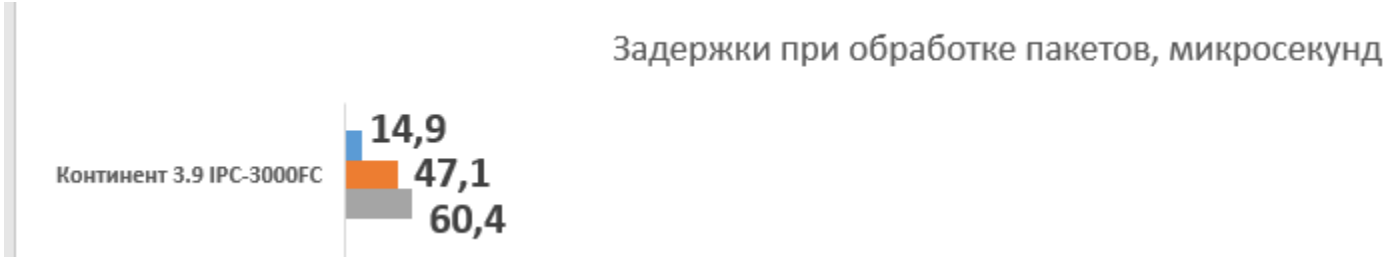
Он состоит из:

- задержка криптошлюза
- задержка локальной сети
- задержка канала связи

Задержка криптошлюза должна минимально влиять на общую задержку передачи данных

КОД БЕЗОПАСНОСТИ

Данные о задержках в высокопроизводительных решениях



Резюме

Аппаратный криптоускоритель – единственный способ обеспечить защиту трафика крупных ЦОДов и обеспечить оптимальные условия для работы гео-распределенных БД и приложений

СПАСИБО!

КОНТАКТЫ:

+7 (495) 982-30-20

info@securitycode.ru

www.securitycode.ru

КОД БЕЗОПАСНОСТИ