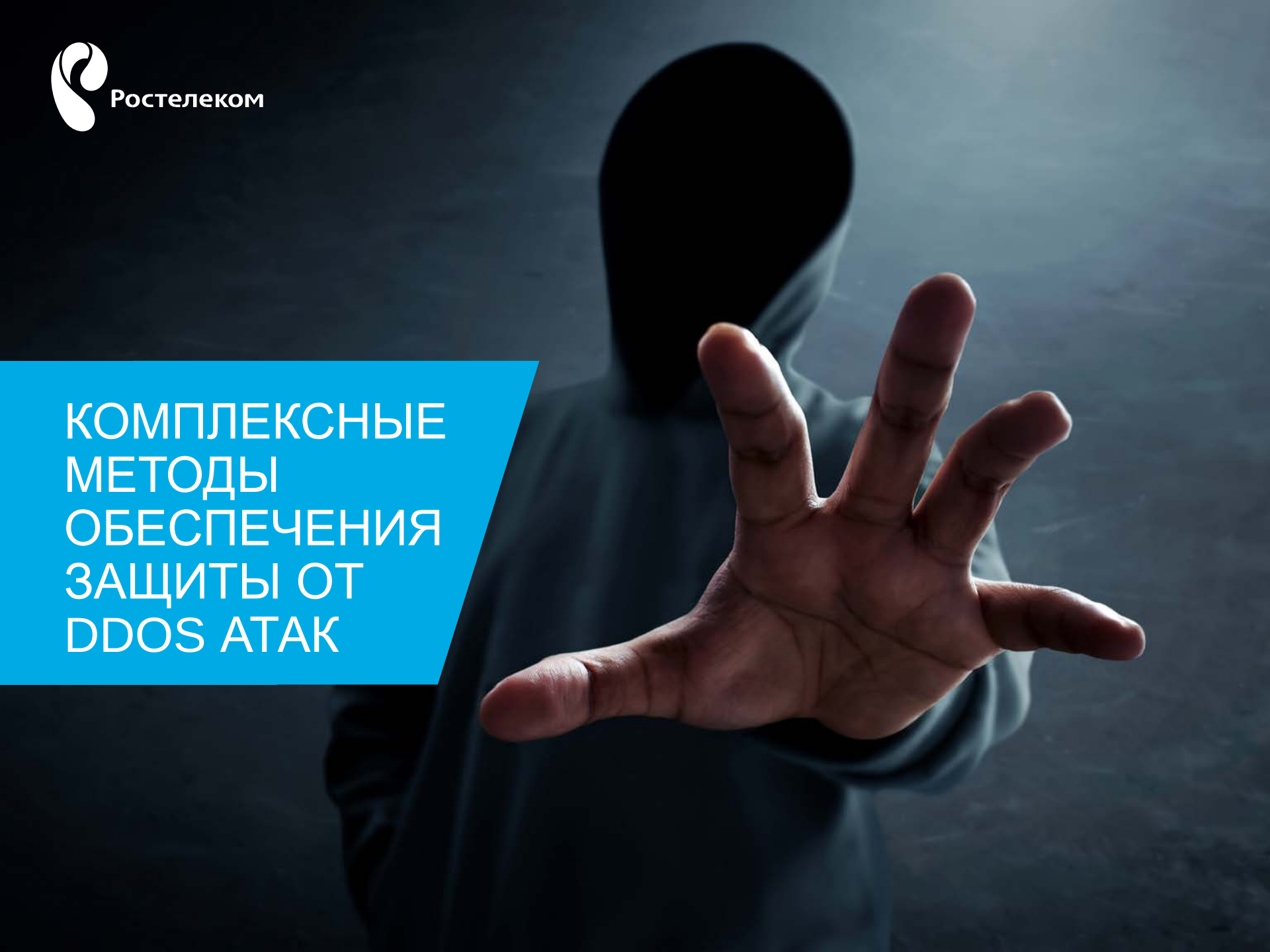
Ростелеком

КОМПЛЕКСНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ DDOS АТАК

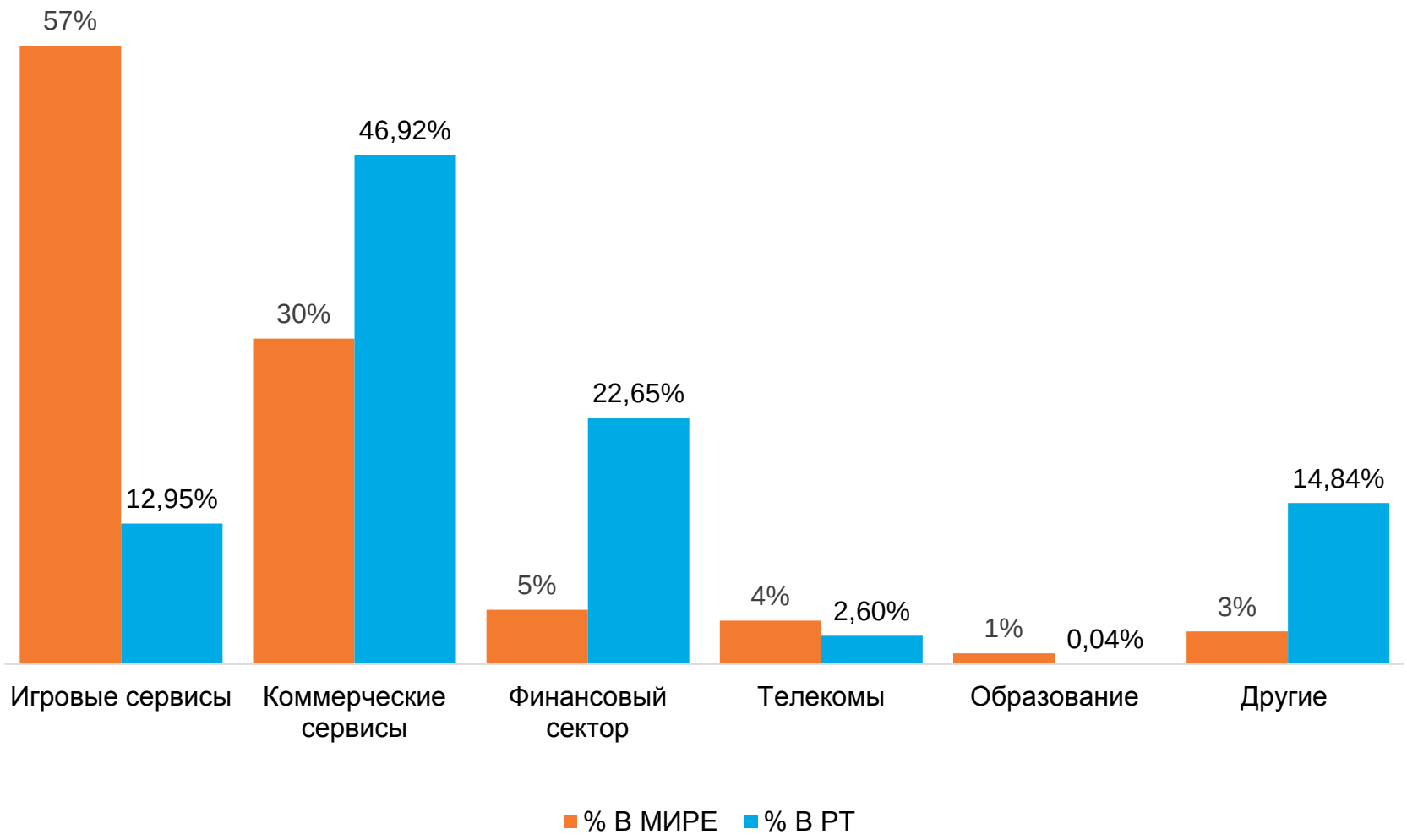


РОСТЕЛЕКОМ В ЦИФРАХ

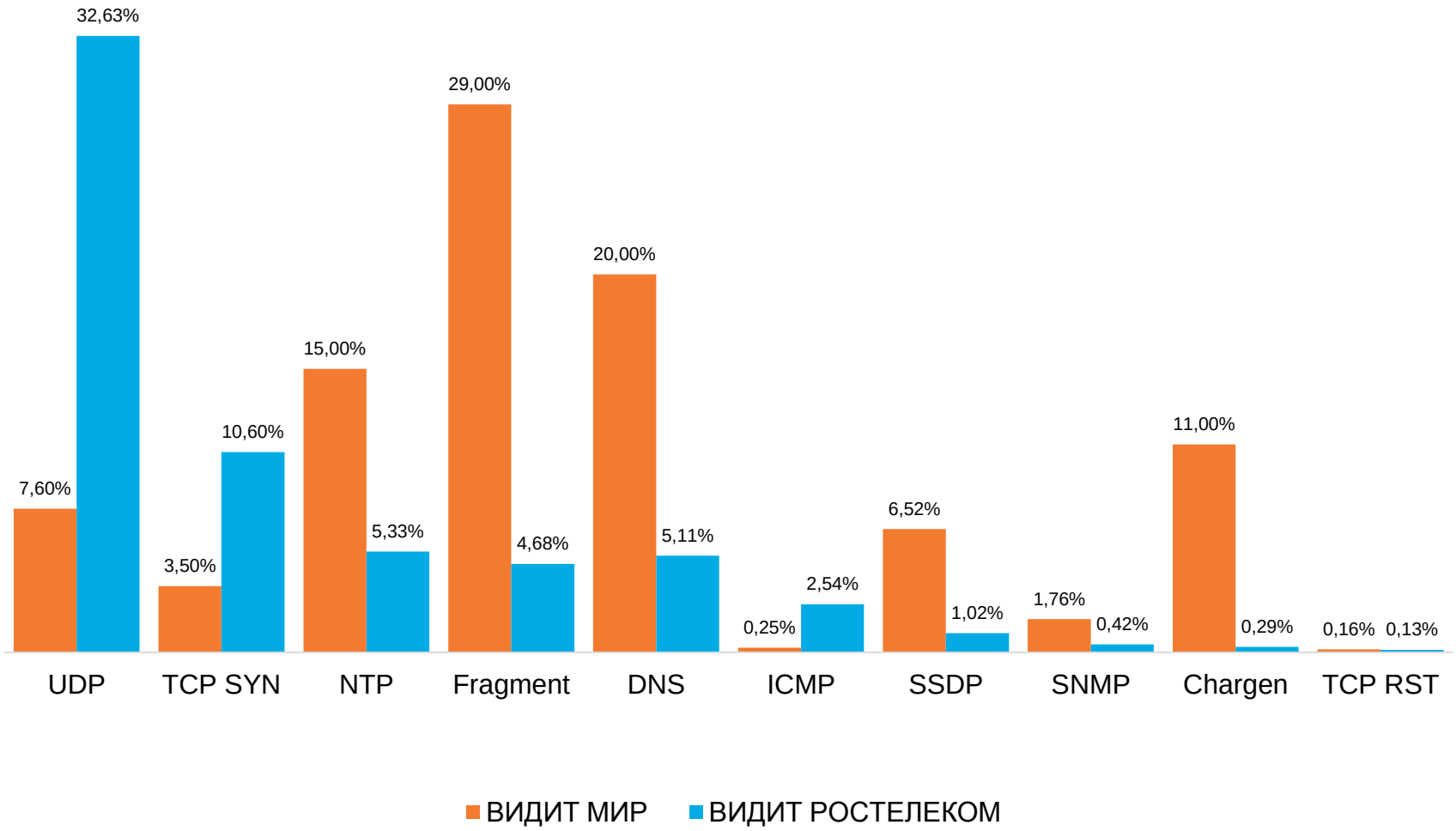
Ростелеком

28 000 000	АБОНЕНТОВ ФИКСИРОВАННОЙ ГОЛОСОВОЙ СВЯЗИ
12 500 000	АБОНЕНТОВ ШИРОКОПОЛОСНОГО ДОСТУПА В ИНТЕРНЕТ
8 200 000	АБОНЕНТОВ ПЛАТНОГО ТЕЛЕВИДЕНИЯ
80	РЕГИОНАЛЬНЫХ ФИЛИАЛОВ
2 500	ТОЧЕК ПРОДАЖ И ОБСЛУЖИВАНИЯ
160 000	СОТРУДНИКОВ
БОЛЕЕ 50%	АКЦИЙ КОМПАНИИ КОНТРОЛИРУЕТ ГОСУДАРСТВО

МИРОВЫЕ ТРЕНДЫ DDOS АТАК ПО СЕКТОРАМ



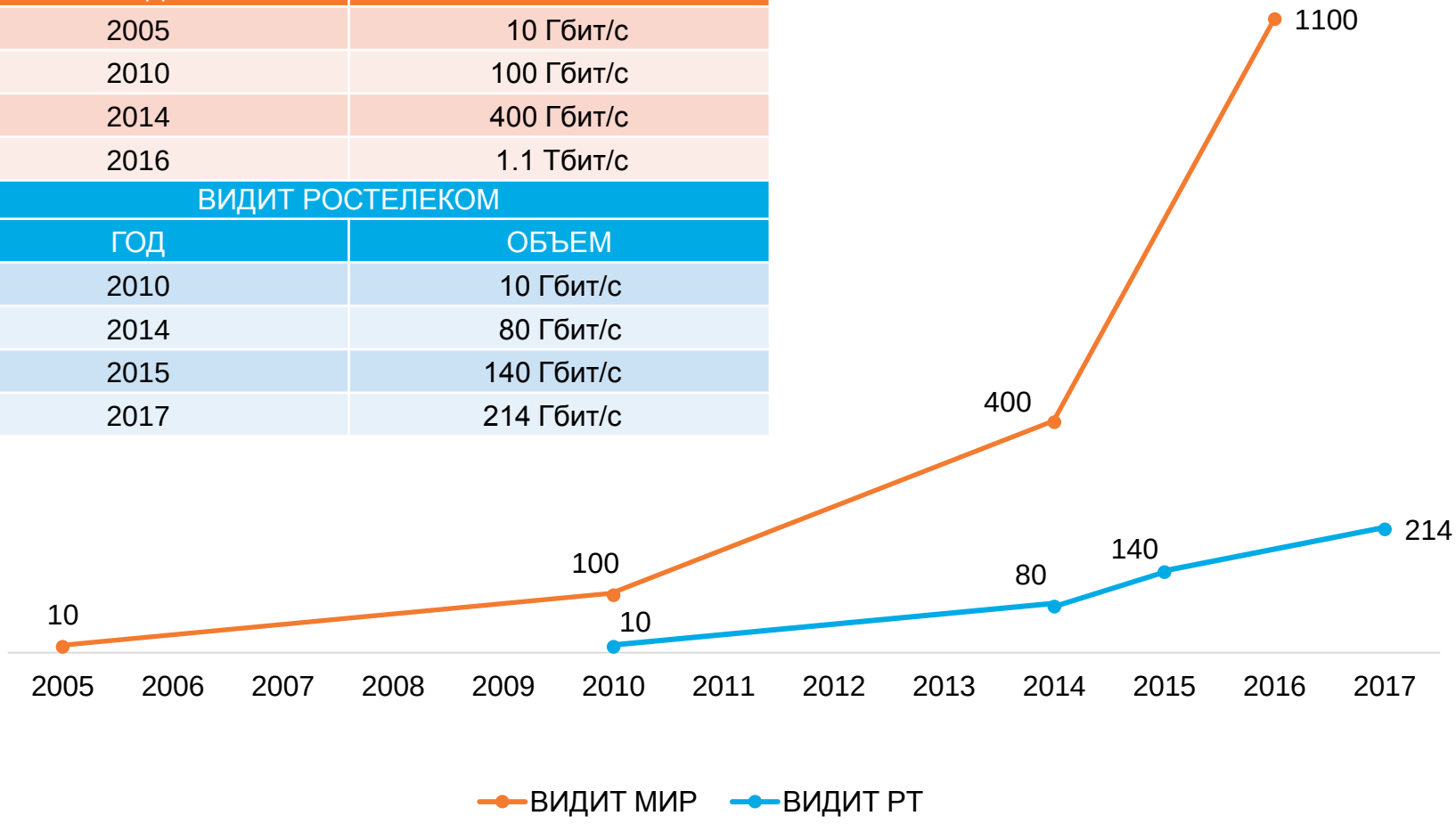
АТАКИ ПО ТИПАМ



ОБЪЕМЫ АТАК

ВИДИТ МИР	
ГОД	ОБЪЕМ
2005	10 Гбит/с
2010	100 Гбит/с
2014	400 Гбит/с
2016	1.1 Тбит/с

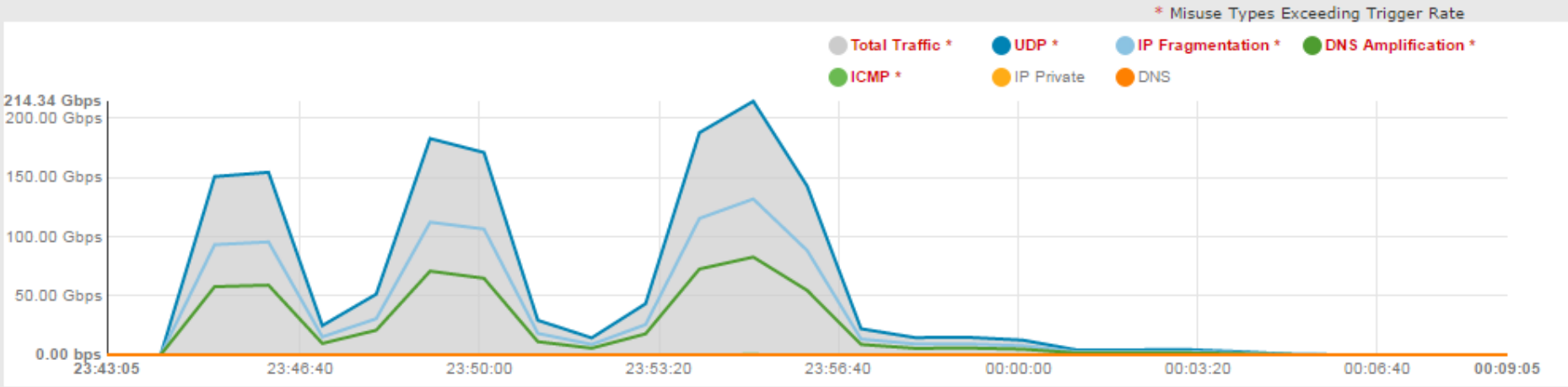
ВИДИТ РОСТЕЛЕКОМ	
ГОД	ОБЪЕМ
2010	10 Гбит/с
2014	80 Гбит/с
2015	140 Гбит/с
2017	214 Гбит/с



РОСТЕЛЕКОМ В КАРТИНКАХ

Ростелеком

Alert Traffic



Top Traffic Patterns (last 5 minutes)

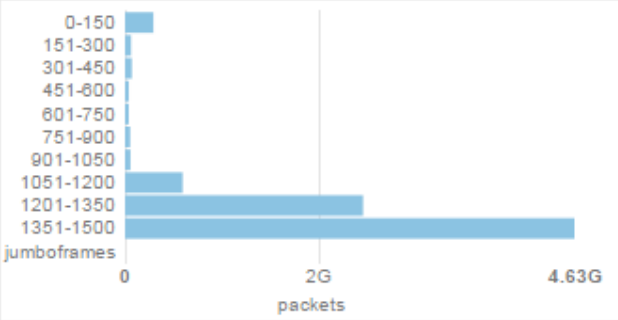
Download All Patterns

No patterns found in the last 5 minutes of the selected timeframe.

Alert Characterization

Misuse Types	Total Traffic (7)	100.00%
Destination IP Addresses		100.00%
Source IP Addresses	Highly Distributed	99.00%
Protocols	udp (17)	99.00%
Misuse Types	UDP (9)	99.00%
Destination UDP Ports	0	61.00%
Source UDP Ports	0	61.00%
Misuse Types	IP Fragmentation (1)	61.00%
Source UDP Ports	53 (domain)	38.00%
Destination UDP Ports	4444 (nv-video)	36.00%
Source Countries	Russian Federation	29.00%

Packet Size Distribution



ЗАЩИТА ОТ DDOS ВНУТРИ КОМПАНИИ

Ростелеком

ПЛЮСЫ

- «Сор не выходит из избы»
- Своя внутренняя компетенция
- Системы ИБ, которые нужны именно вам, а не те, которые «есть в наличии»

МИНУСЫ

- Возможности отражения атак ограничены возможностями защищаемой инфраструктуры
- Капитальные вложения (CAPEX)
- Операционные затраты (OPEX)
- Зарплаты сотрудникам (ФОТ)

АУТСОРСИНГ ЗАЩИТЫ ОТ DDOS

Ростелеком

ПЛЮСЫ

- Экономия CAPEX, OPEX, ФОТ
- Подбор сервиса по своим потребностям с возможностью улучшения
- Профессиональная команда людей
- Широкие (часто) возможности и внешние каналы оператора (облачного или магистрального)

МИНУСЫ

- Нет полного контроля за ситуацией, понимания происходящего
- Нет возможностей мобилизоваться компании для решения возникшей проблемы
- Иногда ценник в конце месяца может неприятно удивить
- Может оставаться ощущение «незащищенности»

ИНОГДА DDOS НЕ ТО, ЧЕМ КАЖЕТСЯ

Ростелеком

По данным опроса компаний, после DDoS,

ЦЕЛЬ – ФИНАНСОВЫЕ ОРГАНИЗАЦИИ

Ростелеком

- По данным Neustar в среднем банки теряют $100,000 в час. При этом более 1/3 опрошенных фирм заявили, о потерях гораздо выше.
- По оценке Сбербанка, ежегодные суммарные потери российской экономики от киберпреступников составляют 600 млрд рублей. Мировые потери от киберпреступности в 2015 году составили $500 млрд.
- С середины 2015 по май 2016 года хакеры похитили у клиентов российских банков более 3 млрд рублей.
- За второе полугодие 2016 года было зафиксировано более 20 кибератак на платежные системы российских финансовых организаций. Мошенники пытались похитить со счетов кредитных организаций более 2,87 млрд рублей.

ЦЕННОСТЬ – ЦЕЛЕВОЙ РЕСУРС

Ростелеком

ПОВЫШЕНИЕ УСТОЙЧИВОСТИ

- Защита сервера приложения
  - Межсетевое экранирование
  - Отключение ненужных сервисов
- Правильная архитектура
  - Масштабируемость компонентов
  - Тюнинг характеристик платформы
- SDLC
- Периодический анализ защищенности

ЭШЕЛОН БЕЗОПАСНОСТИ И ДОСТУПНОСТИ

Ростелеком

ЭШЕЛОН №1

- Межсетевое экранирование на сети
- Межсетевое экранирование на уровне приложения (WAF)
- Защита от DDoS каналов с вышестоящими операторами
- Балансировка

ЭШЕЛОН ОПЕРАТОРА СВЯЗИ

Ростелеком

ЭШЕЛОН №2

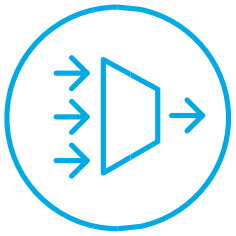
Анализ HTTP(S) трафика,
отражение прикладных атак,
защита от DDoS
с использованием WAF
(Web Application Firewall)

ЭШЕЛОН №3

Защита от DDoS атак
до уровня приложения
на устройстве операторского
класса

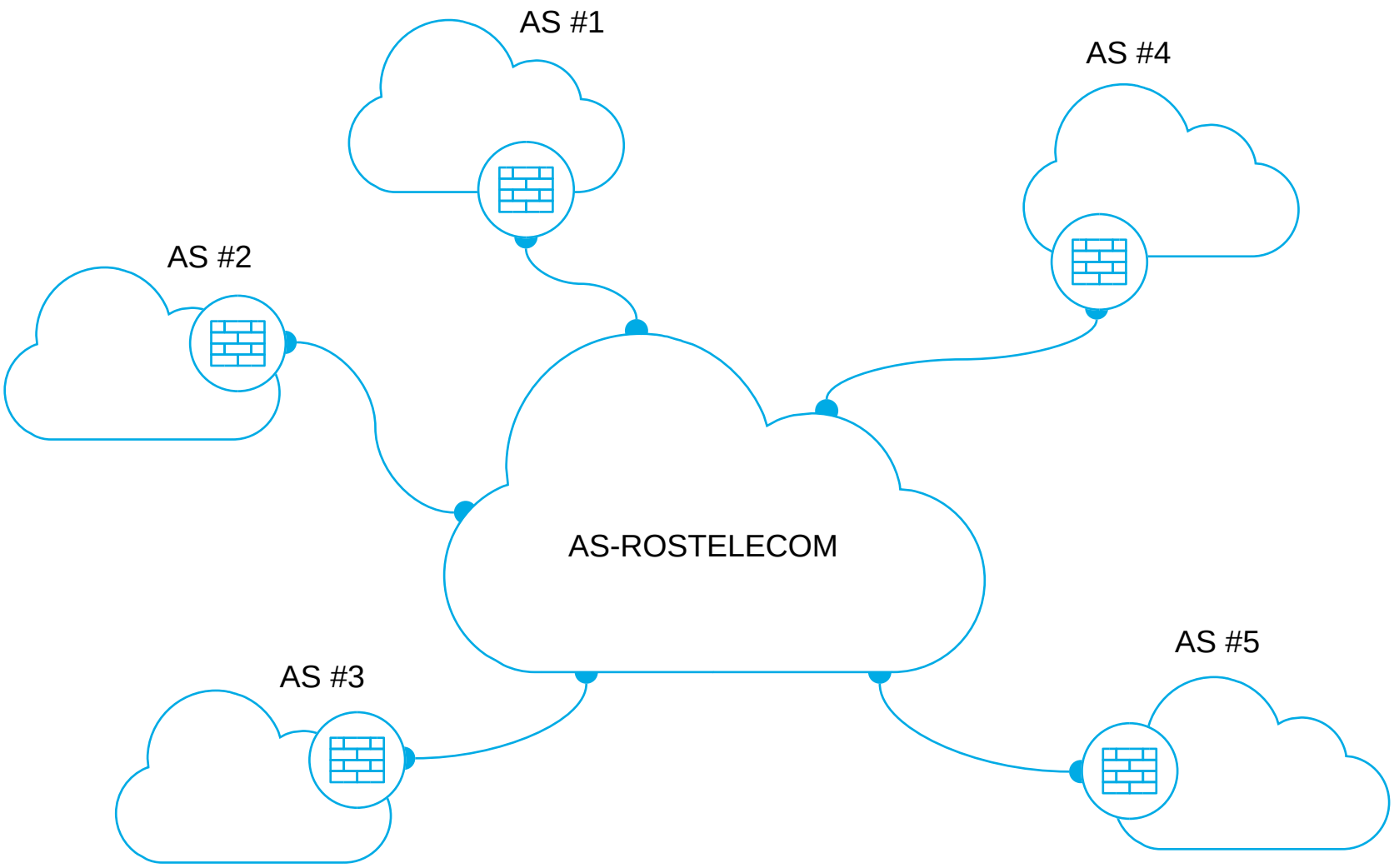
ЭШЕЛОН №4

Очистка трафика на границе
сети вплоть
до транспортного уровня
модели OSI



ЭШЕЛОН ОПЕРАТОРОВ ОПЕРАТОРА

Ростелеком



ЗАЩИТА ОТ DDOS ОТ РОСТЕЛЕКОМ В ЦИФРАХ

Ростелеком

КРУПНЕЙШАЯ В ЕВРОПЕ ИНСТАЛЛЯЦИЯ ОПЕРАТОРСКОГО КОМПЛЕКСА ЗАЩИТЫ ARBOR PEAKFLOW

- Позволяет отражать атаки емкостью 160 Гбит/с до уровня приложений
- Позволяет отражать атаки емкостью более 5 Тбит/с на пограничных маршрутизаторах
- 50 инженеров обученных Arbor Peakflow
- Опыт отражения атак пиковой производительностью более 200 Гбит/с
- Ежедневная фильтрация более 15 инцидентов емкостью более 10 Гбит/с
- Опыт успешной защиты информационных ресурсов Крупных мероприятий федерального и мирового масштаба

ЗАЩИТА ОТ DDOS ОТ РОСТЕЛЕКОМ В ЦИФРАХ

Ростелеком

Особенности услуги

- Всем клиентам предоставляется доступ в личный кабинет по управлению услугой
- Выделенная круглосуточная смена по отражению DDoS атак
- Стоимость услуги не зависит от мощности и количества DDoS-атак
- Оператор связи, имеющий опыт подключения клиентских устройств защиты от DDoS – Arbor Pravail (опция Cloud-signaling)

РАЗВИТИЕ УСЛУГИ

РОСТЕЛЕКОМ – ОБЛАЧНЫЙ ПРОВАЙДЕР УСЛУГ ЗАЩИТЫ ОТ DDOS АТАК

- Защита HTTP трафика проксированием
- Защита HTTP/HTTPS трафика с использованием WAF (в том числе PCI DSS)
- Управляемый Arbor Pravail APS
- TelcoCloud
- И другие…

Ростелеком

СПАСИБО
ЗА ВНИМАНИЕ

ДМИТРИЙ ЦАРЕВ
Dmitriy.Tsarev@rt.ru