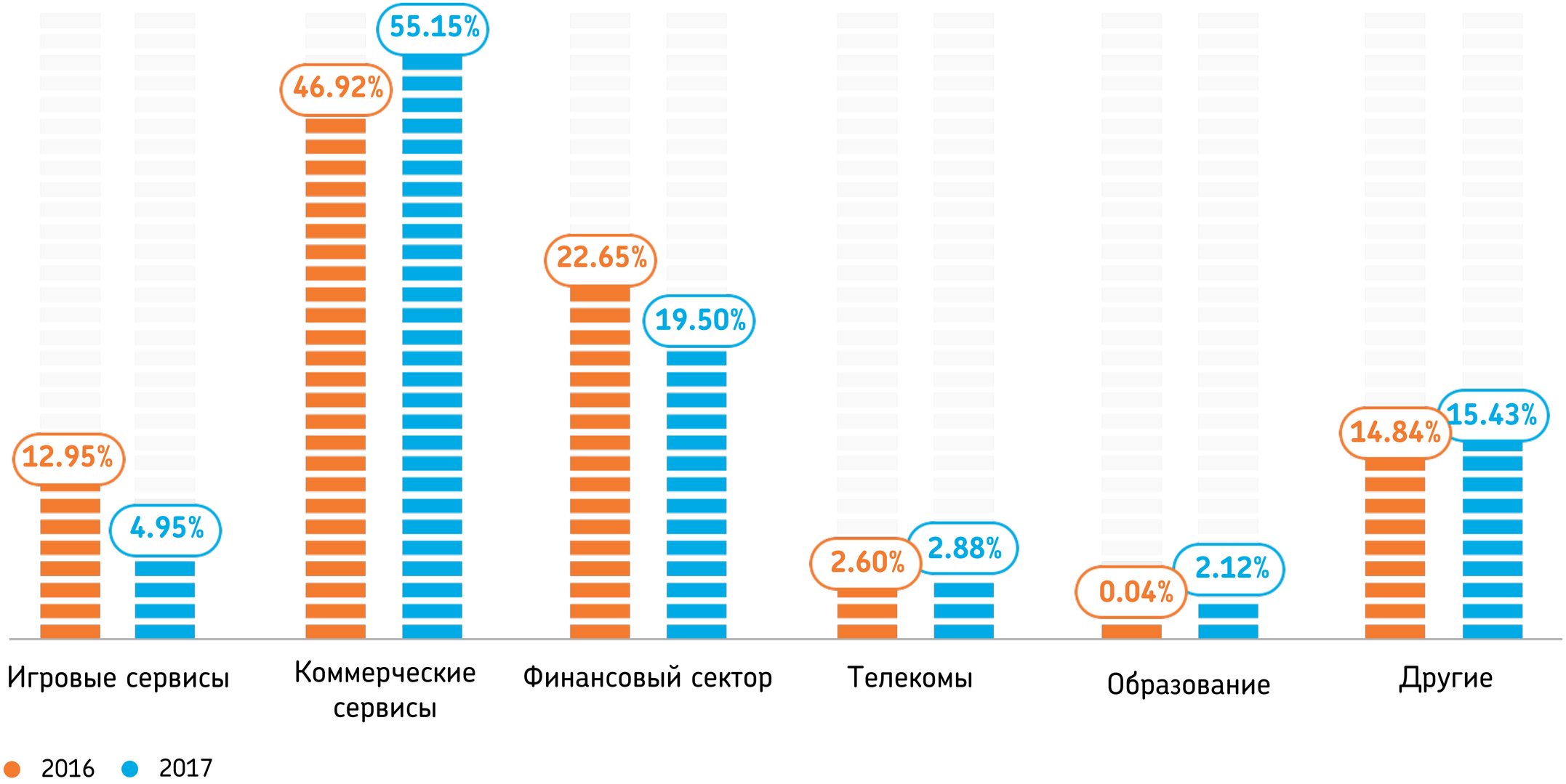
Ростелеком

ОБЛАЧНАЯ БЕЗОПАСНОСТЬ ДЛЯ ФИНАНСОВЫХ СЕРВИСОВ

ТРЕНДЫ DDOS АТАК ПО СЕКТОРАМ

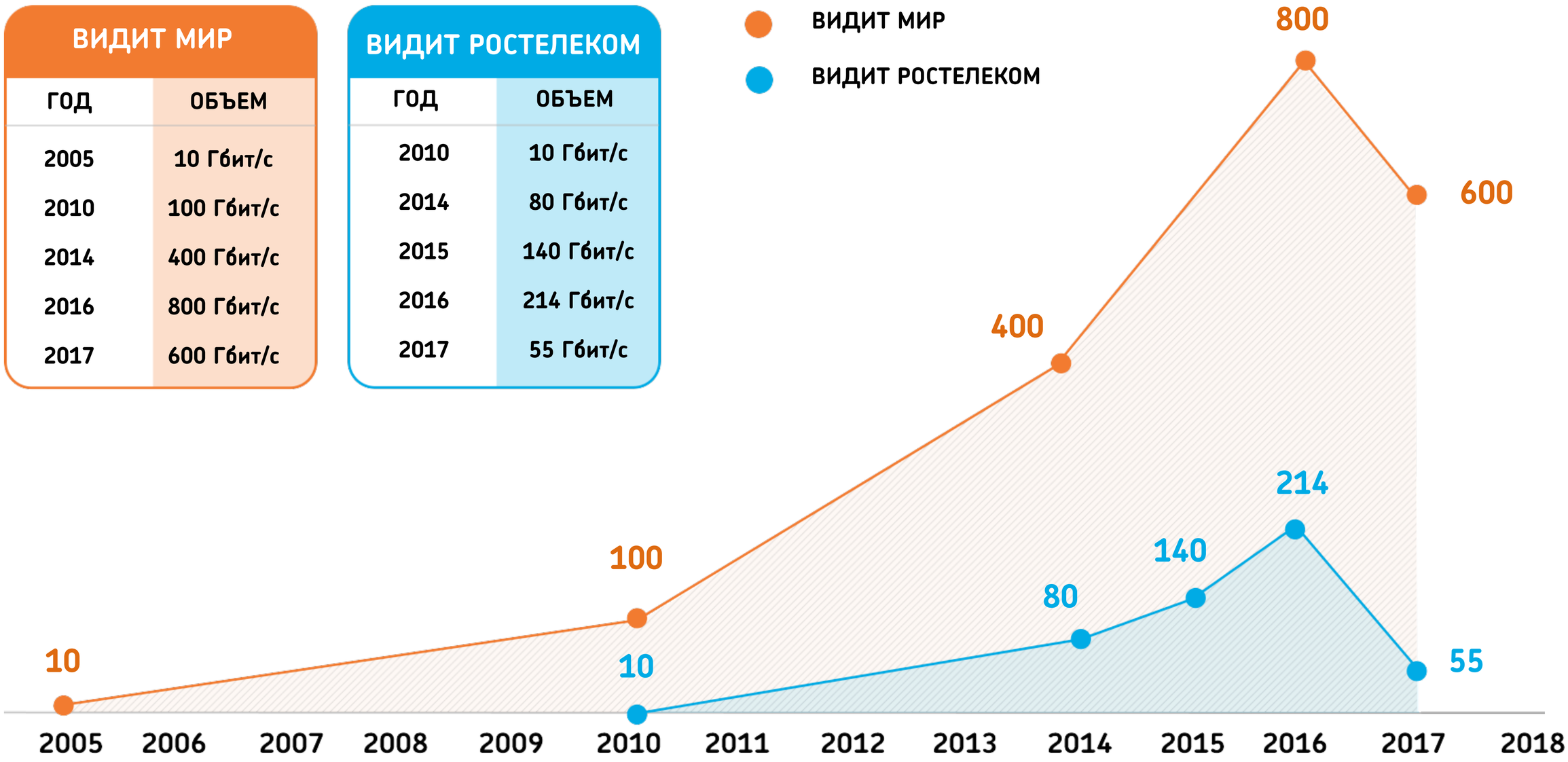
Ростелеком



ОБЪЕМЫ АТАК

ВИДИТ МИР	
ГОД	ОБЪЕМ
2005	10 Гбит/с
2010	100 Гбит/с
2014	400 Гбит/с
2016	800 Гбит/с
2017	600 Гбит/с

ВИДИТ РОСТЕЛЕКОМ	
ГОД	ОБЪЕМ
2010	10 Гбит/с
2014	80 Гбит/с
2015	140 Гбит/с
2016	214 Гбит/с
2017	55 Гбит/с



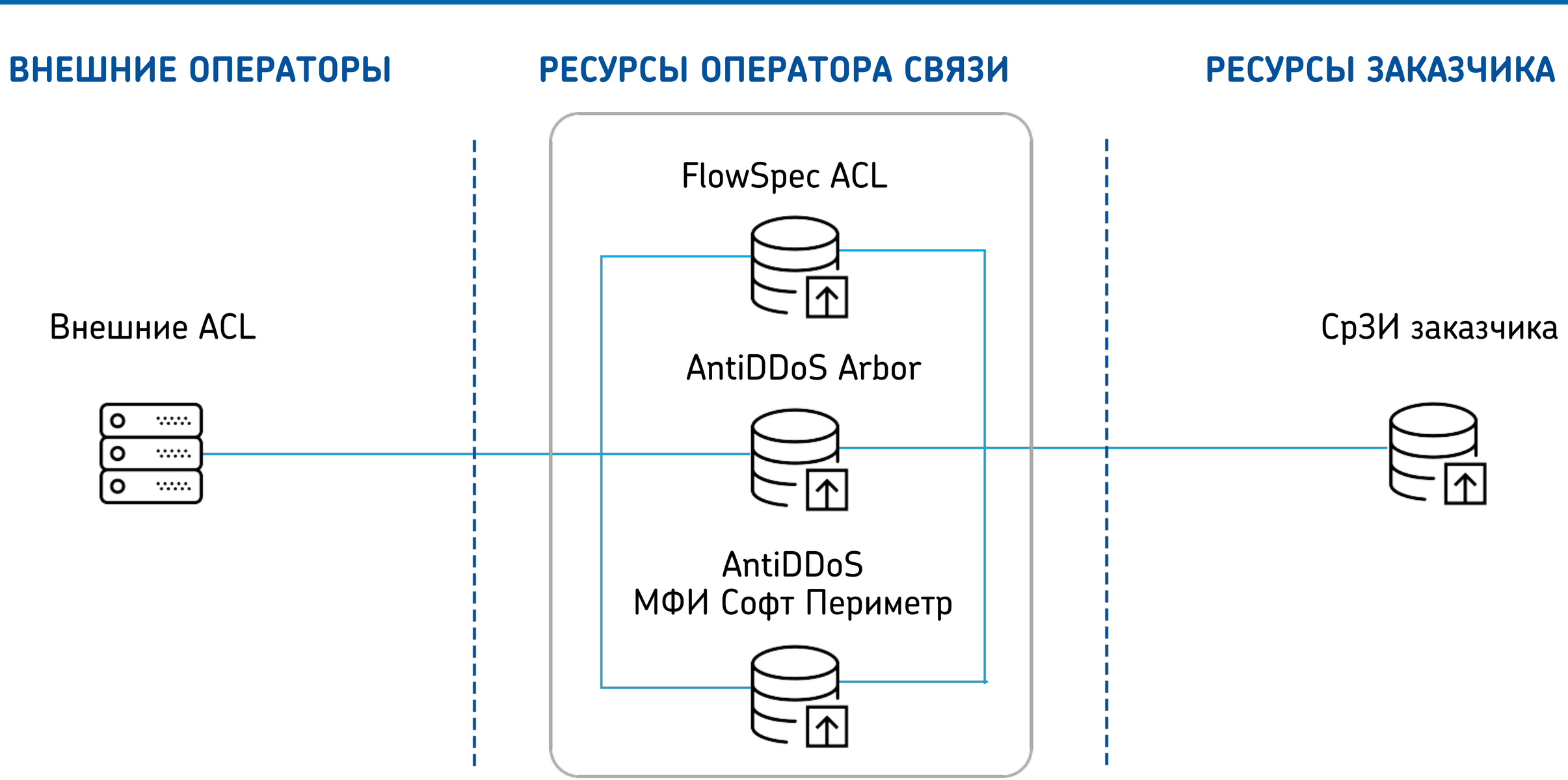
ЦЕЛЬ – ФИНАНСОВЫЕ ОРГАНИЗАЦИИ

ПОТЕРИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ
В 2017 ГОДУ ВЫРОСЛИ

В СРЕДНЕМ НА 9%

ПО СРАВНЕНИЮ С 2016 ГОДОМ.

ЭШЕЛОН ОПЕРАТОРА СВЯЗИ



ВОЗМОЖНОСТИ ЗАЩИТЫ ОПЕРАТОРА

Ростелеком

	ARBOR NETWORKS	МФИ СОФТ ПЕРИМЕТР
Отслеживание TCP сессий (Slow GET/POST)	✓	✓
Проверка HTTP на RFC	✓	✓
Регулярные выражения	✓	✓
Нелегитимное поведение	✓	✓
Расстояние Левенштейна		✓
Байес		✓
Возможность получать и анализировать логи web серверов		✓

РАЗВИТИЕ УСЛУГИ: ЦЕЛИ

РОСТЕЛЕКОМ – ОБЛАЧНЫЙ ПРОВАЙДЕР УСЛУГ ЗАЩИТЫ ОТ DDOS АТАК

В 2017 году мы видели свое развитие в:

- Защита HTTP трафика проксированием
- Защита HTTP/HTTPS трафика с использованием WAF (в том числе PCI DSS)
- Управление Arbor Pravail APS

РАЗВИТИЕ УСЛУГИ: ИТОГИ

ЗАЩИТА HTTP ТРАФИКА. Совместный продукт с NGENIX.

ЗАЩИТА HTTP/HTTPS ТРАФИКА С ИСПОЛЬЗОВАНИЕМ WAF (В ТОМ ЧИСЛЕ PCI DSS). Сертифицированная облачная платформа для защиты ресурсов.

УПРАВЛЯЕМЫЙ ARBOR PRAVAIL APS. Возможность управлять оборудованием заказчика.

РОССИЙСКИЙ ПРОВАЙДЕР ОБЛАЧНЫХ СЕРВИСОВ ДЛЯ ВЕБ-РЕСУРСОВ

NGENIX

ОКАЗЫВАЕТ УСЛУГИ С 2008 ГОДА. ВХОДИТ В ГК РОСТЕЛЕКОМ С 2015 ГОДА.

СРЕДИ КЛИЕНТОВ:

Яндекс, ВГТРК, Олимпийский комитет России, ozon.ru выбирайте, Азбука вкуса, CarPrice

САМАЯ БОЛЬШАЯ РАСПРЕДЕЛЕННАЯ ОБЛАЧНАЯ ПЛАТФОРМА В РФ:

- 1 Тбит/с в РФ с возможностью расширения до 10 Тбит/с за пределами РФ;
- 20 узлов в 14 точках присутствия в РФ, Казахстане и Украине;
- Прямое подключение к 500+ операторам (87% пользователей РФ).

ТРИ КЛЮЧЕВЫХ ПРОДУКТА:

- NGENIX Secure Cloud. Комплексная защита и ускорение веб-сайта.
- NGENIX Content Delivery Network. Распределенная доставка файлов и вещание онлайн-видео.
- NGENIX Cloud Storage. Хранение «горячих» данных.

УСЛУГА ЗАЩИТЫ И УСКОРЕНИЯ ВЕБ-САЙТА

NGENIX

ЗАЩИТА ОТ DDOS

- На базе Arbor PeakFlow на сети Ростелеком
- Быстрое подключение под атакой
- Демпфирование атак с первых секунд

ВЕБ-АКСЕЛЕРАЦИЯ

- Кэширование статического контента
- Ускорение динамики на уровне сети
- Сервис хранения объектов (S3)

WAF

- PT Application Firewall
- Wallarm WAF
- SolidWall WAF

ЗАЩИЩЕННЫЙ DNS

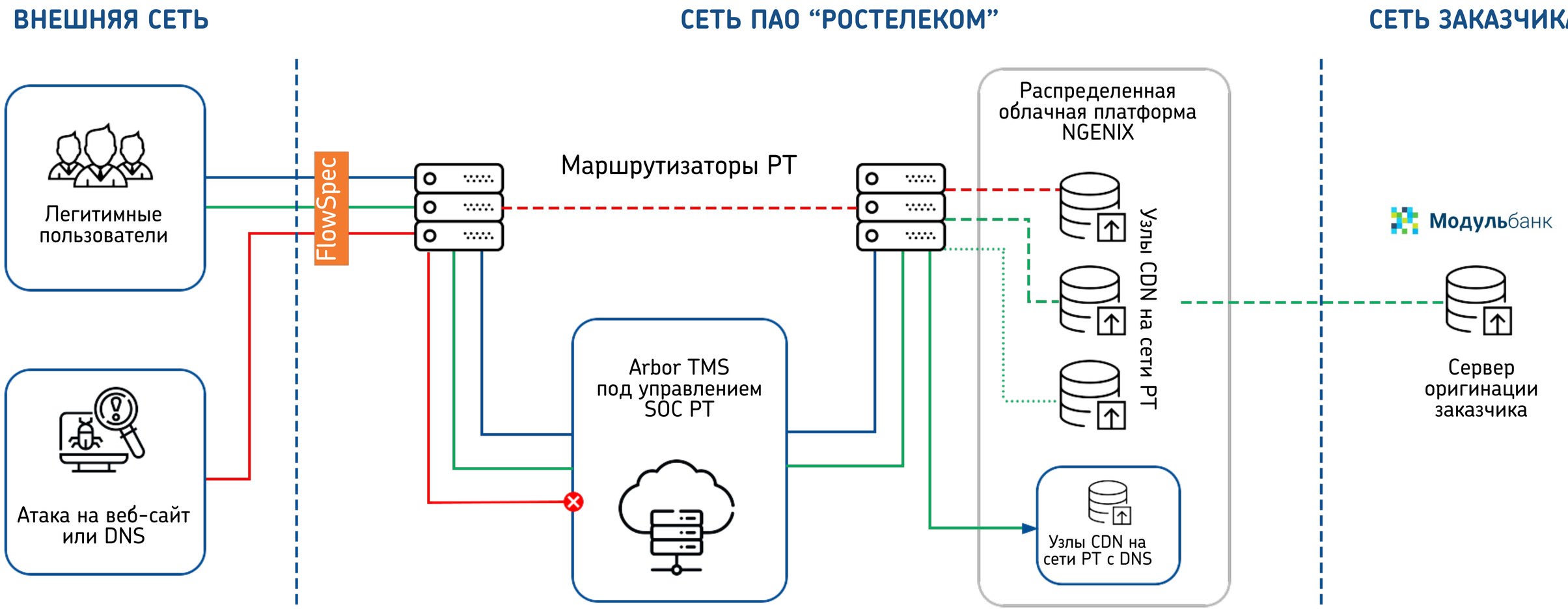
- Высокопроизводительный (100M RPS)
- Географически распределенный
- Защищен от DDoS-атак

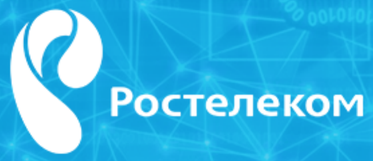
ПОГРУЖЕНИЕ В ОБЛАЧНУЮ БЕЗОПАСНОСТЬ

Эффект от внедрения в зависимости от уровня интеграции

ДЕЙСТВИЕ	ЭФФЕКТ
Разместить весь статический контент в S3-облаке и организовать к нему доступ через CDN	Снижение нагрузки на инфраструктуру в среднем до 90%. Скорость доступа к статическому контенту сайта выше до 4 раз.
Перенести обработку DNS-запросов на распределенный отказоустойчивый сервис DNS	Сокращения времени первого запроса. Полная защита DNS от DDoS-атак.
Перевести обработку всех запросов к публичным веб-ресурсам (корп. сайт, промо-страницы и лэндинги) на CDN с функцией мониторинга и фильтрации атак.	Защита от кибератак сайтов и обеспечение непрерывного потока новых клиентов. Скорость доступа к веб-сайту в любой точке РФ менее 2 сек.
Внедрить шифрование «чувствительных» данных, передаваемых по WebSockets. Перевести обработку всех запросов к закрытым сервисам (интернет-банк) на распределенную облачную платформу с функцией мониторинга и фильтрации атак.	Ускорение работы и защита от атак всех предоставляемых через интернет сервисов без затрат на инфраструктуру и без раскрытия «чувствительных» данных.

КЕЙС: МОДУЛЬБАНК





СПАСИБО ЗА ВНИМАНИЕ

ДМИТРИЙ ЦАРЕВ
dmitriy.tsarev@rt.ru

КОНСТАНТИН АНОХИН
k.anokhin@ngenix.net