new way to secure your business

Алексей Станкус
CEO

Анатомия DDoS-атак. Что такое DDOS?

Как и какие части сетевой инфраструктуры атакуют?

TCP State-Exhausting Attacks

- ✓ Атака **направленная на устройства** связи с контролем состояний (load balancers, firewalls, application servers)
- ✓ Нацелена на традиционную структуру **сетевой безопасности**

Volumetric Attacks

- ✓ **Переполняет** каналы связи:
- ✓ Во внутренних сетях цели
- ✓Между сетями провайдера и атакуемой сетью

Application Layer Attacks

- ✓ **Малозаметные** атаки на приложения
- ✓ Нацелены на определённые уязвимости приложений

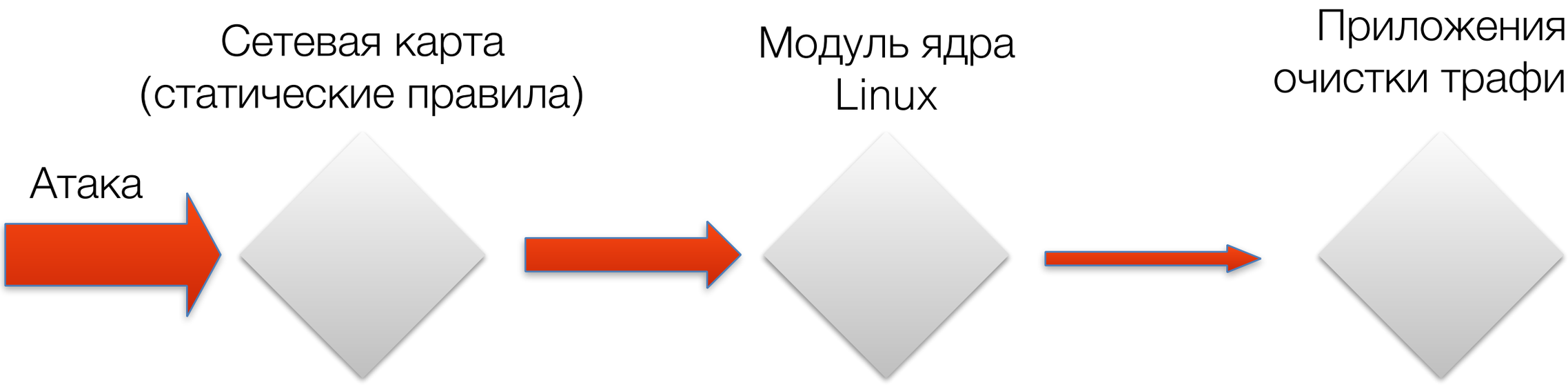
Возможности комплекса

- ✓ **Active Bot Protection**
- ✓ **Защита от DDoS layer 7**
- ✓ **Защита от DDoS layer 3**
- ✓ Защита HTTPS
- ✓ Защищенный хостинг DNS
- ✓ Определение ботов без CAPTCHA
- ✓ WAF
- ✓ IDS
- ✓ IPS
- ✓ Zero Day
- ✓ Белые и черные списки
- ✓ Ускорение сайта (кэширование, оптимизация, SPDY)
- ✓ Улучшение индексирования поисковыми системами
- ✓ Балансировка сайта (в том числе на несколько площадок)
- ✓ Оптимизация (под мобильного клиента через сжатие трафика)
- ✓ Мониторинг и статистика сайта
- ✓ IPv6
- ✓ Сохранение копий сайта
- ✓ Кастомные страницы ошибок

Защита от DDoS L3

Особенности реализации:

- ✓ Многоуровневая обработка трафика с различной глубиной анализа;
- ✓ Управление трафиком через аппаратную часть сетевой карты Intel X520;
- ✓ Использование модуля ядра Linux для обхода узкого места Linux - реализация стэка TCP/IP;
- ✓ Математические алгоритмы для определения вредоносного трафика;
- ✓ Корректная настройка стандартных возможностей системы;

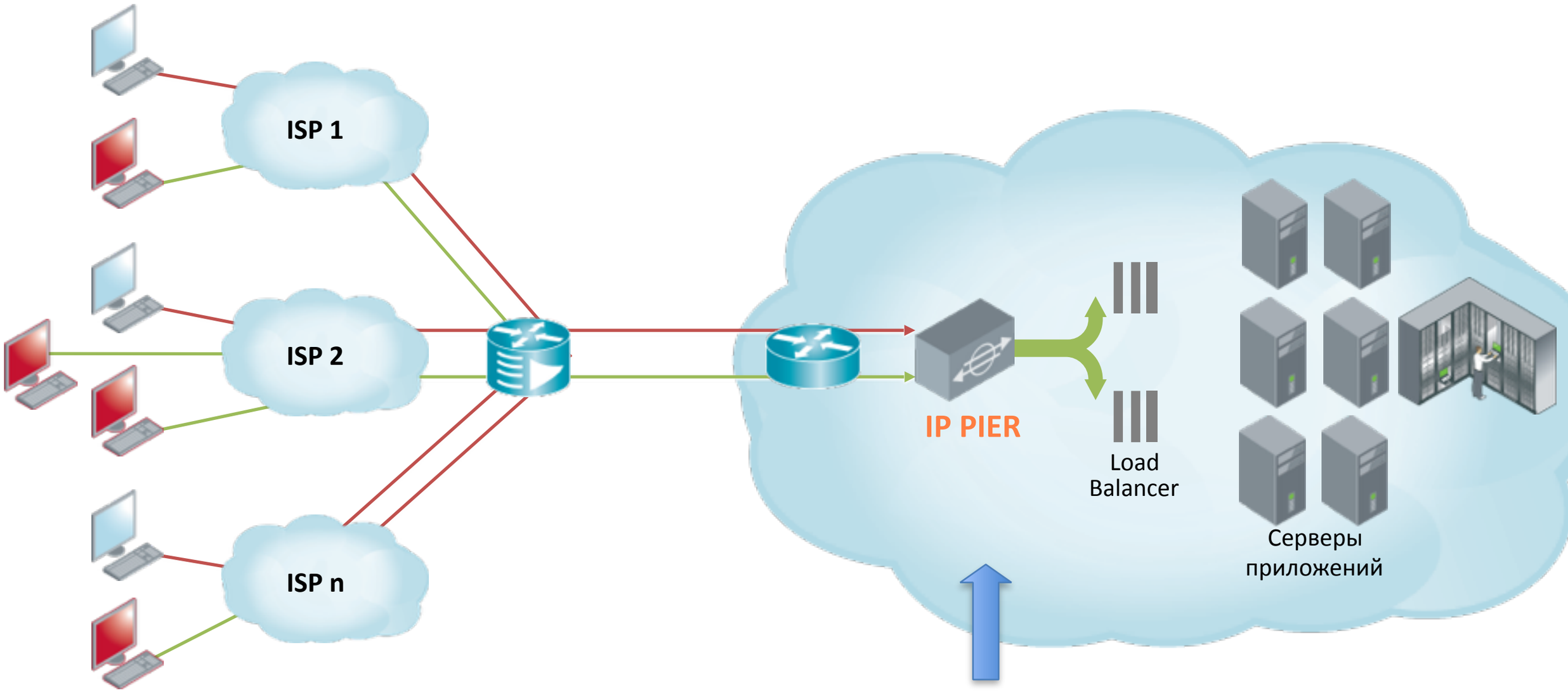


Защита от DDoS L7 (Active Bot Protection)

Особенности реализации:

- ✓ Применение математических алгоритмов для определения атак L7 на L3;
- ✓ Использование собственного backend и для обработки WEB;
- ✓ Система автоматического управления уровнями защиты;
- ✓ Возможны одновременно различные уровни защиты для различных URL;
- ✓ Объем общения с ботами 0,2 - 64 KB;
- ✓ Система противодействия ботам (постановка ресурсозатратной задачи на атакующий копьютер);

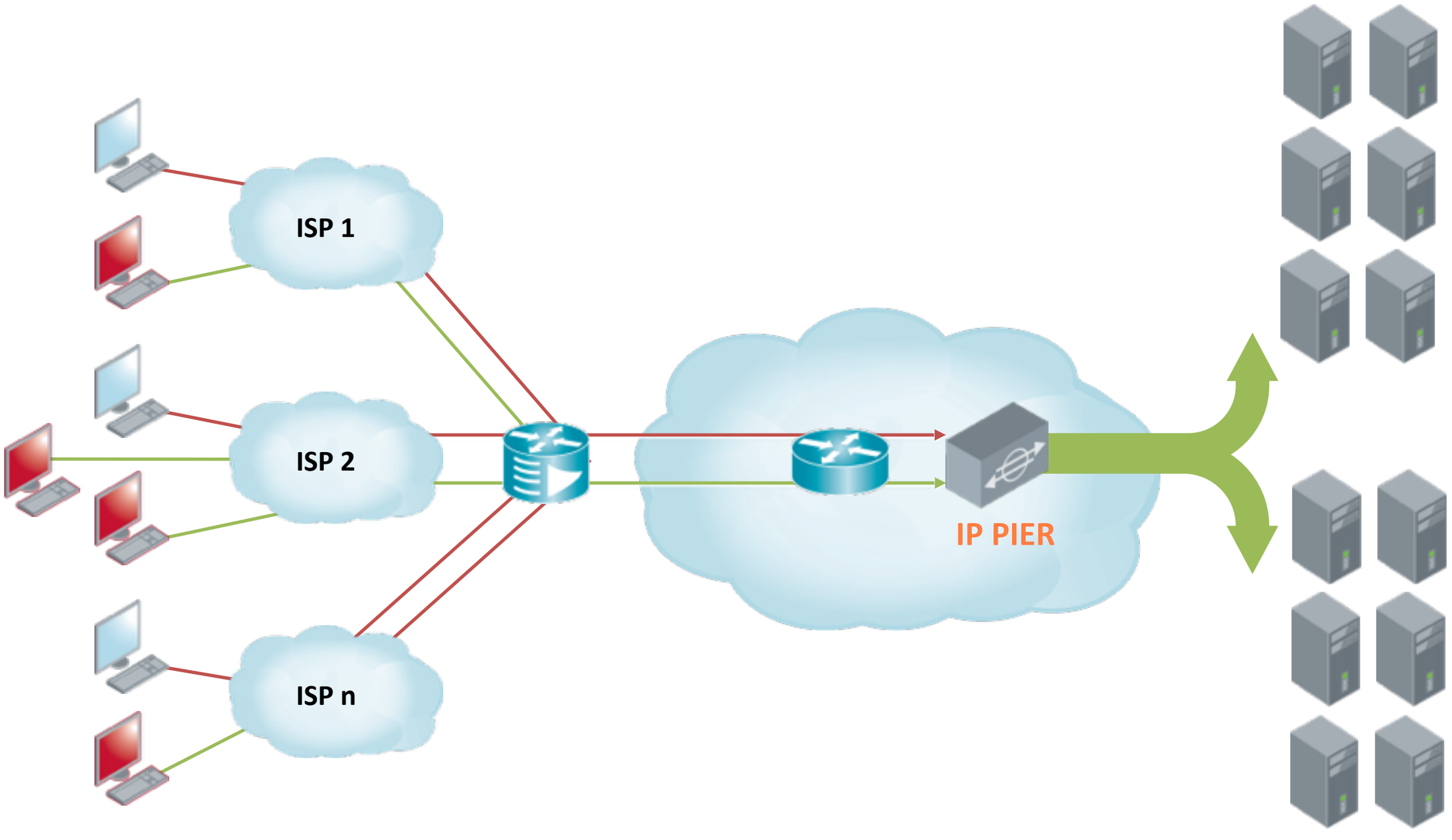
Подключение на площадке заказчика



Особенности

Может использоваться как border proxy для увеличения производительности основных web серверов

Совместное облако IP PIER - SkyparkCDN



Конкуренты

сервис/ компания	IP PIER	Incapsula	CloudFlare	Kaspersky	Qurator	Arbor
Active Bot Protection	+	-	-	-	-	-
WAF	+	+	+	-	+	+
IDS	+	+	+	+	-	+
IPS	+	+	+	+	-	+
DDoS L7	+	+-	+	+-	+-	-
DDoS L3	+*	+	-+	+*	+	+*
Оптими-зация	+-	+	+-	-	-	-

*Скорость обработки трафика на одном устройстве:

IP PIER - до 10 Gb/s & 14M pps

Kaspersky - до 5 Gb/s & 600K pps

Arbor Pravail - до 10 Gb/s & 8M pps

Спасибо за Ваше внимание

Алексей Станкус
alexey.stankus@ippier.com