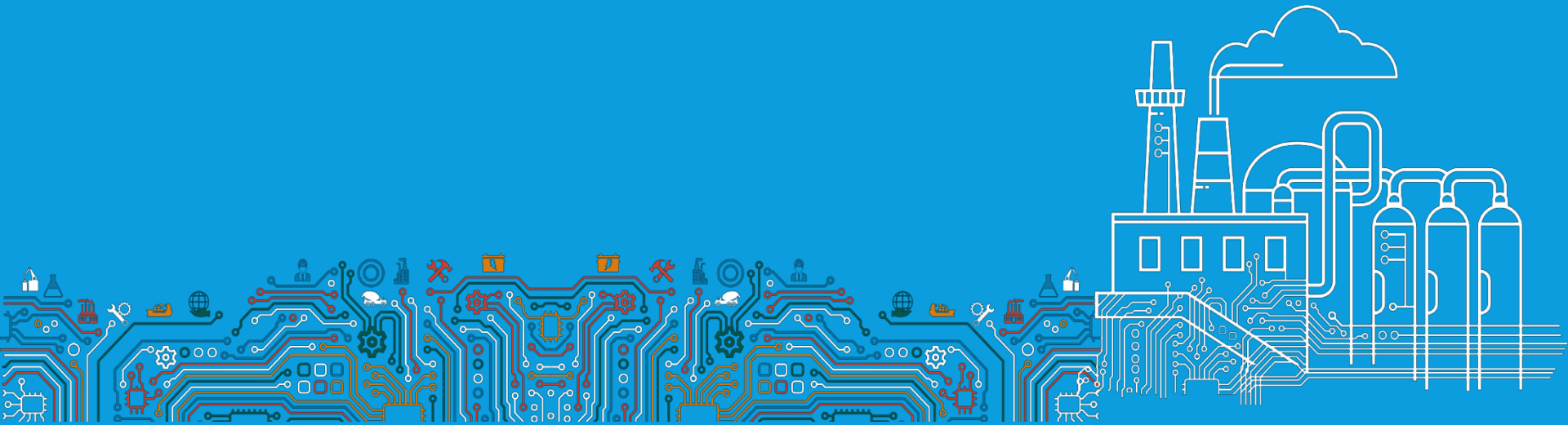
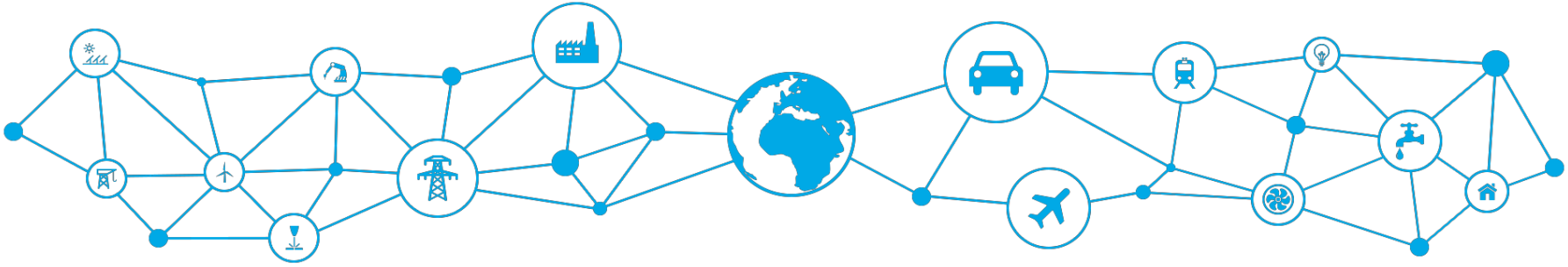
БЕЗОПАСНОСТЬ ИНДУСТРИАЛЬНОГО ИНТЕРНЕТА: РЕШЕНИЯ ПАО «РОСТЕЛЕКОМ»

18, 19 сентября 2017 / Региональный семинар МСЭ / Узбекистан, Ташкент



ИНДУСТРИАЛЬНЫЙ ИНТЕРНЕТ (IIOT)

«Индустриальный интернет» (Industrial Internet of Things, IIoT) – единая сеть любых небытовых устройств, оборудования, датчиков, систем, способных изменять свои параметры или параметры внешней среды, собирать информацию и передавать ее на другие устройства



1	Сквозная оптимизация производственных и логистических цепочек предприятий
2	Оптимизация использования активов и их сервисного обслуживания
3	Создание интеллектуальной функциональности для существующих продуктов («умные» продукты)
4	Предоставление продуктов по сервисной модели, новые способы тарификации

СТОП-ФАКТОРЫ РАЗВИТИЯ ИНДУСТРИАЛЬНОГО ИНТЕРНЕТА

Ростелеком

- Стирание грани между ОТ и ИТ: «Обмен угрозами»
- Недостаток экспертизы и опыта в разработке бизнес-сценариев индустриального Интернета вещей
- Неопределенность в выборе поставщиков (необходим надежный поставщик безопасной IIoT платформы)
- Недостаточное количество средств в ИТ-бюджетах на освоение новых технологий.
- Отсутствие единых стандартов для отраслей и кросс-платформенных решений
- Сопротивление конечных пользователей: IIoT повышает объективный контроль.

ПРОБЛЕМЫ ДАЛЬНЕЙШЕГО РАЗВИТИЯ ИБ

Ростелеком

Постоянный рост числа эксплуатируемых СЗИ

Новая проблема/ИТ-система – новое СЗИ. В среднем на мероприятии по ИБ представлено порядка 50-70 брэндов СЗИ

Необходимость автоматизации ИБ

Реальное управление «зоопарком» СЗИ и документирование ИБ возможно только с существенной автоматизацией процессов

Высокая стоимость собственной 24/7/365 службы мониторинга

Необходим круглосуточный контроль, но издержки на его содержание сложно обосновать

Нехватка квалифицированного персонала

Универсальных специалистов мало, стоят они дорого, постоянная текучка

Необходимость адаптации процессов ИБ к изменениям ИТ ландшафта

ИТ уходят в облака

Возрастающее влияние кибер-рисков на бизнес

Для промышленности это наиболее очевидно

ОСНОВНЫЕ ИСТОЧНИКИ УГРОЗ ИБ В АСУ ТП

Ростелеком

APT-хакеры (Целевые атаки)

Промышленный шпионаж, терроризм, конкуренция, политические «войны»

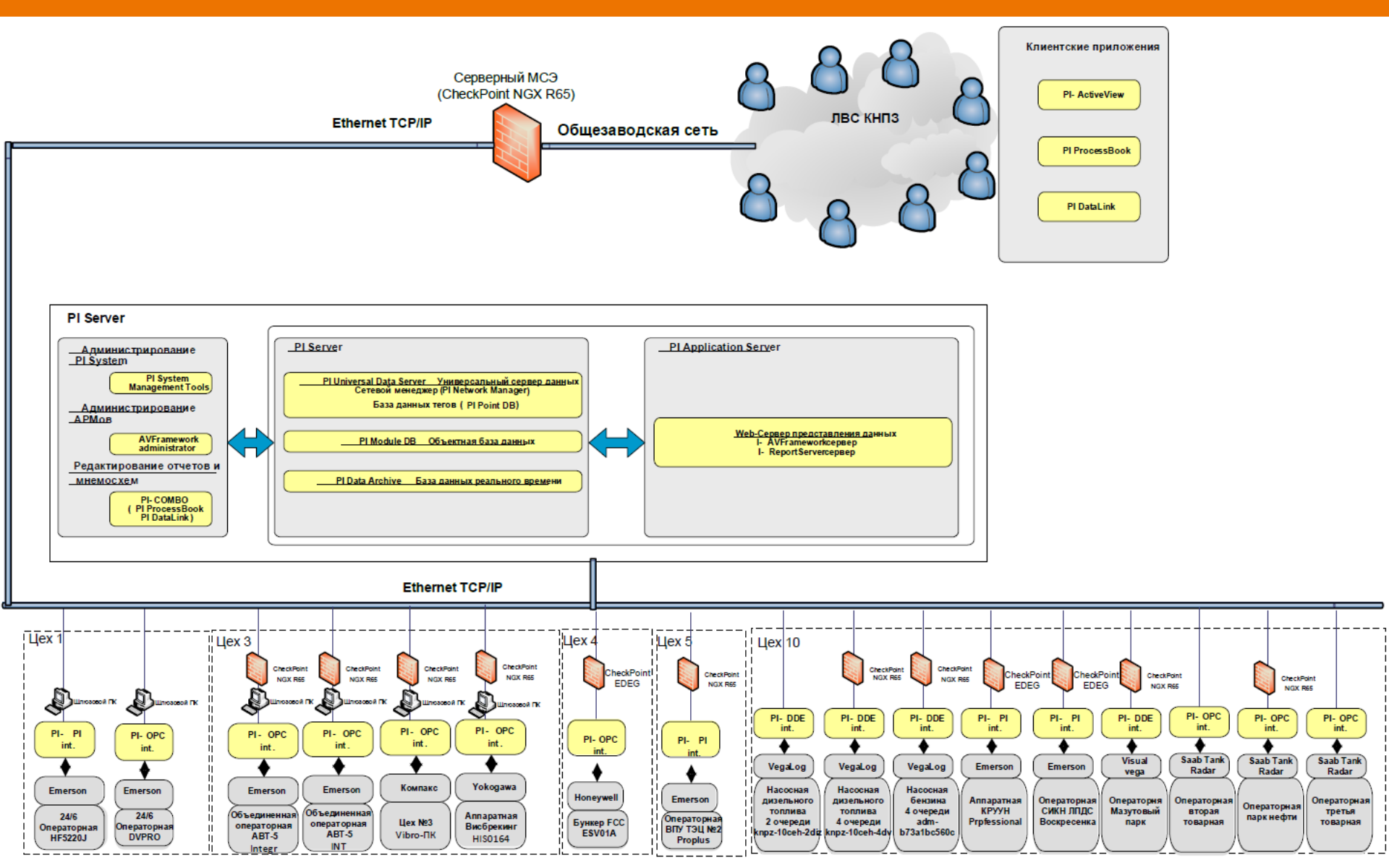
Внутренние пользователи

Злой умысел (мошенничество, месть), ошибки, социальная инженерия (внешнее влияние)

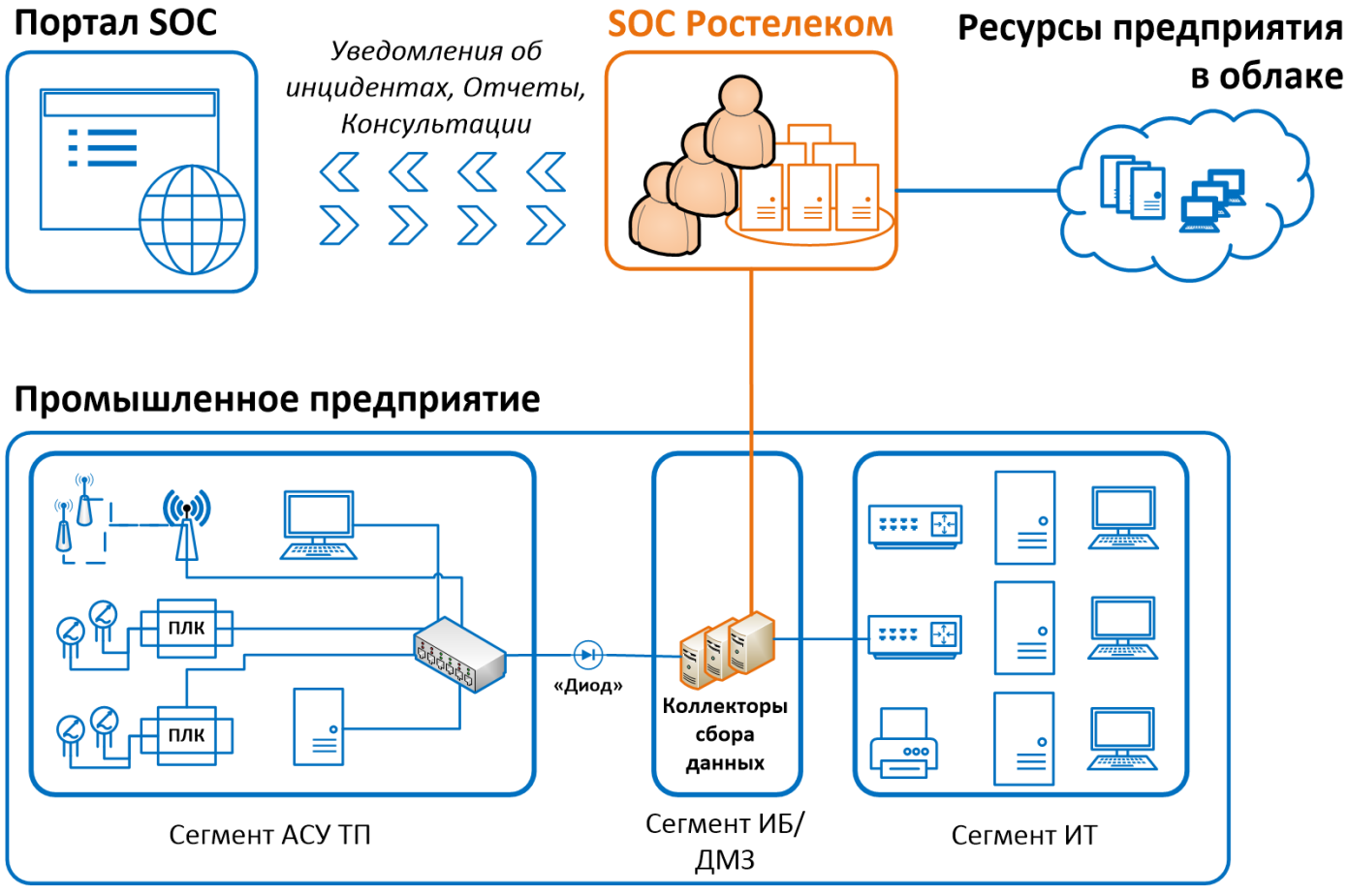
Производители оборудования

Неограниченный удаленный доступ с использованием 3G/4G каналов.

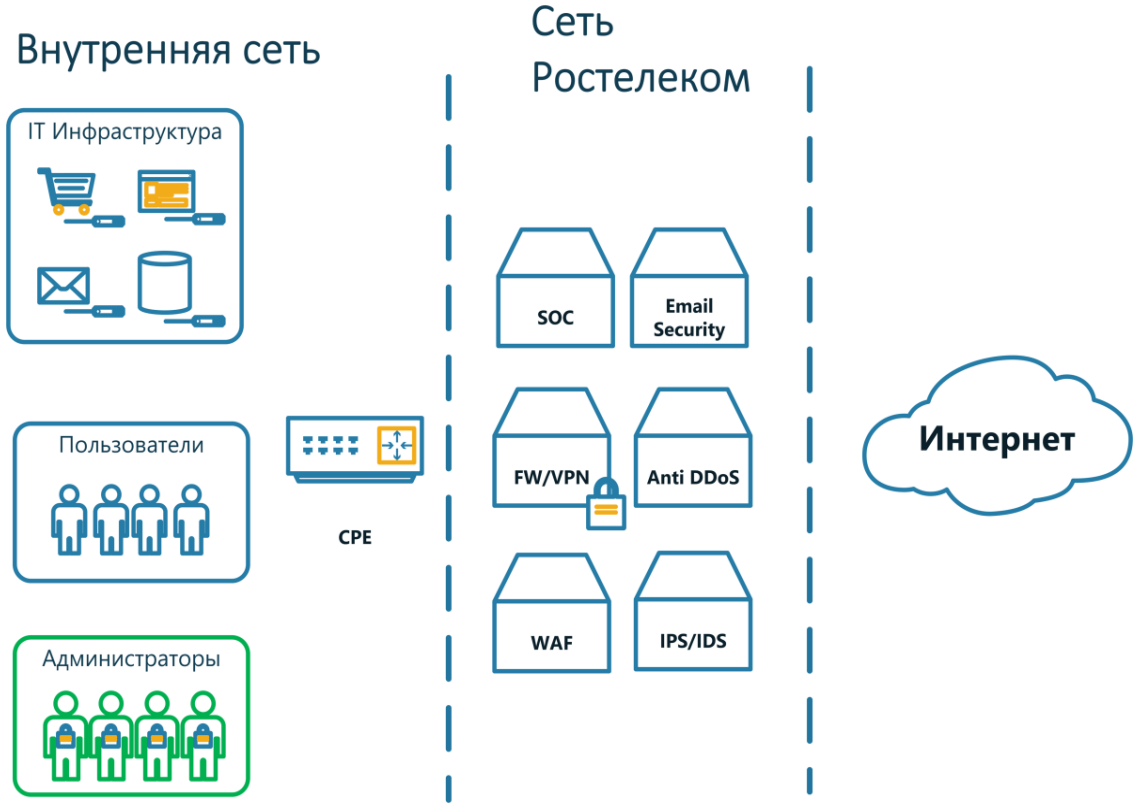
Нейтрализовать угрозы, исходящие от данных источников, штатными методами и средствами службы ИБ/ИТ невозможно


Серверный МСЭ
(CheckPoint NGX R65)
Ethernet TCP/IP
Общезаводская сеть
ЛВС КНПЗ
Клиентские приложения
PI- ActiveView
PI ProcessBook
PI DataLink
PI Server
Администрирование PI System
PI System Management Tools
Администрирование АРМов
AVFramework administrator
Редактирование отчетов и мнемосхем
PI- COMBO (PI ProcessBook PI DataLink)
PI Server
PI Universal Data Server Универсальный сервер данных
Сетевой менеджер (PI Network Manager)
База данных тегов (PI Point DB)
PI Module DB Объектная база данных
PI Data Archive База данных реального времени
PI Application Server
Web-Сервер представления данных
I- AVFrameworkсервер
I- ReportServerсервер
Ethernet TCP/IP
Цех 1
Шлюзовой ПК
PI- PI int.
PI- OPC int.
Emerson
24/6 Операторная HF5220J
24/6 Операторная DVPRO
Цех 3
CheckPoint NGX R65
Шлюзовой ПК
PI- OPC int.
Emerson
Объединенная операторная ABT-5 Integr
Объединенная операторная ABT-5 INT
Компакс
Цех №3 Vibro-ПК
Yokogawa
Аппаратная Висбрекинг HIS0164
Цех 4
CheckPoint EDEG
PI- OPC int.
Honeywell
Бункер FCC ESV01A
Цех 5
CheckPoint NGX R65
PI- PI int.
Emerson
Операторная ВПУ ТЭЦ №2 Proplus
Цех 10
CheckPoint NGX R65
CheckPoint EDEG
PI- DDE int.
PI- PI int.
PI- OPC int.
VegaLog
Emerson
Visual vega
Saab Tank Radar
Насосная дизельного топлива 2 очереди knpz-10ceh-2diz
Насосная дизельного топлива 4 очереди knpz-10ceh-4dv
Насосная бензина 4 очереди adm-b73a1bc560c
Аппаратная КРУУН Prpfessional
Операторная СИКН ЛПДС Воскресенка
Операторня Мазутовый парк
Операторная вторая товарная
Операторная парк нефти
Операторная третья товарная

РЕШЕНИЕ РОСТЕЛЕКОМ ПО МОНИТОРИНГУ ИБ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ



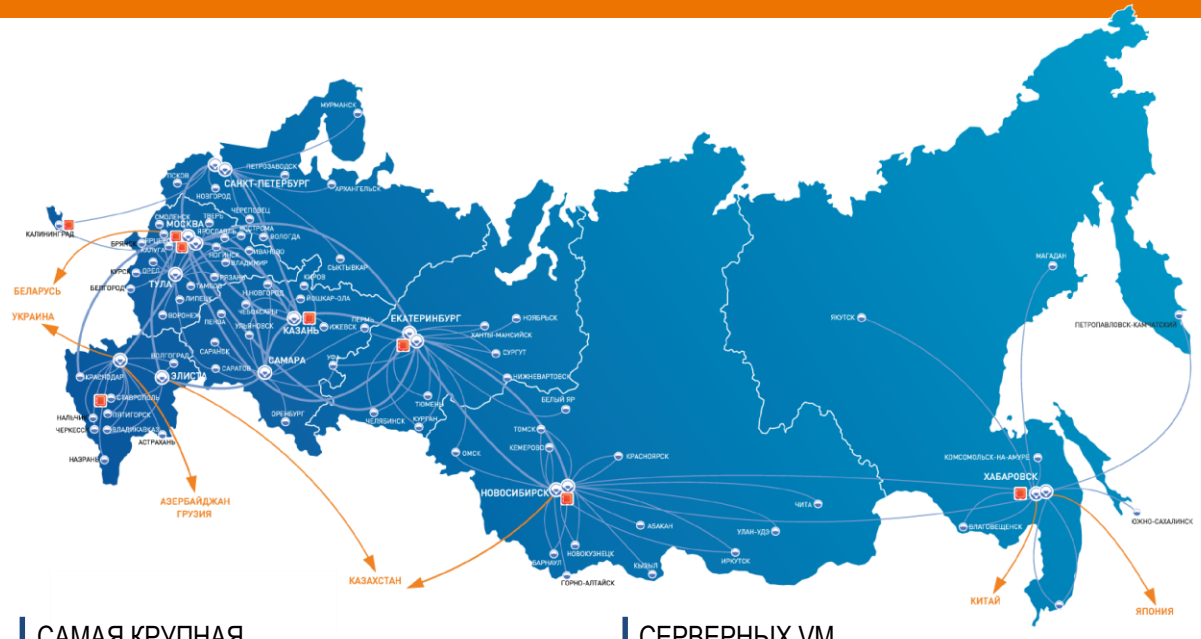
СЕРВИСНАЯ МОДЕЛЬ РЕШЕНИЙ ИБ РОСТЕЛЕКОМ (TELCOCLOUD)



Особенности

- Сервисная модель оказания услуг
- Гибкость конфигурации и возможность быстрого наращивания или сокращения мощностей
- Единое окно управления всеми СЗИ
- Эксплуатация системы защиты силами квалифицированных специалистов поставщика услуг
- Мониторинг и реагирование на инциденты ИБ в режиме 24x7
- Отсутствует необходимость в большом штате дорогостоящих инженеров ИБ
- Форма затрат – OPEX
- Возможность использования услуги мониторинга и анализа событий ИБ SOC RTK

SOC РОСТЕЛЕКОМ В ЦИФРАХ



214 Гбит/с — САМАЯ КРУПНАЯ ОТРАЖЕННАЯ DDOS АТАКА

> 3 000 — СЕРВЕРНЫХ VM НАХОДИТСЯ ПОД ЗАЩИТОЙ

2 272 369 584 — СОБЫТИЙ БЕЗОПАСНОСТИ АНАЛИЗИРУЕТСЯ ЕЖЕДНЕВНО

18 — БАНКОВ ИЗ ТОП50 УЖЕ СТОИТ У НАС НА ЗАЩИТЕ

70 — DDOS АТАК НА КЛИЕНТОВ ОТРАЖАЕТСЯ ЕЖЕДНЕВНО

600-700 — DDOS АТАК РЕГИСТРИРУЕТСЯ НА СЕТИ ЕЖЕДНЕВНО

ЦИФРОВОЕ ЛИДЕРСТВО РОСТЕЛЕКОМ

ПОЧЕМУ IIOT ВМЕСТЕ С РОСТЕЛЕКОМ

Ростелеком

Безусловный технологический лидер рынка ИКТ услуг (B2B/B2G)

Все виды связи, центры обработки данных, облачные услуги и крупные гос. проекты.
Инновационные решения в области электронного правительства, облачных вычислений, здравоохранения, образования, безопасности, ЖКХ.

НАПИ
industrial internet CONSORTIUM

Соучредитель «Национального консорциума Промышленного Интернета» и Член IIC (Индустриального интернет-консорциума)

Разработка стандартов IIoT

Совместно с профильными техническими комитетами Росстандарта (разработка российских стандартов и гармонизация международных для России, комитеты: «ТК 194. Кибер-физические системы», «ТК 22. Информационные технологии», «ТК 016. Электроэнергетика» и другие).
Участвуем в работе профильных комитетов ISO/IEC, ITU, IIC при разработке международных стандартов

Разработка собственной платформы IIoT

С учетом дальнейшего использования ее партнерами при разработке отраслевых платформ (энергетика, машиностроение, нефтегаз и т. д.)

В соответствии с последними решениями Совета директоров стратегическими направлениями развития ПАО «Ростелеком» определены «Индустриальный интернет» и «Информационная безопасности»

ПОЧЕМУ SOC ОТ РОСТЕЛЕКОМ

Ростелеком

Аттестованная Национальная облачная платформа

Размещение ГИС (до К1), ИСПДН (до УЗ-1) и 1Г по РД ГТК

Защищенный канал передачи (в т.ч. ГОСТ VPN)

С-Терра (в т.ч. виртуальный шлюз), ViPNet, Континент

Гарантированный однонаправленный канал

«Гальваническая развязка» между сетью Заказчика и CPE

Группа администрирования СЗИ (*InHouse*)

Обеспечивает работоспособность СЗИ, оценивая необходимости внесения изменений в них

Группа мониторинга (24/7/365) (*InHouse*)

Проводит постоянный мониторинг событий ИБ, классифицирует и ранжирует инциденты и оповещает Клиента о них

Группа реагирования на инциденты (*InHouse*)

Проводит анализ и расследования инцидентов, «закрывает» инциденты и формулирует рекомендации для Клиента

КИБЕРБЕЗОПАСНОСТЬ ОТ РОСТЕЛЕКОМ

ЕДИНСТВЕННЫЙ ПРОВАЙДЕР КИБЕРБЕЗОПАСНОСТИ (MSSP:TELCO+SOC)

ЗАЩИТА ОТ DDoS-АТАК (МАГИСТРАЛЬНАЯ И В ОБЛАКЕ)

ПЛАТФОРМА ПО КУЛЬТУРЕ КИБЕРБЕЗОПАСНОСТИ (Security Awareness) - ИЮЛЬ 2017

СТРАХОВАНИЕ ОТ КИБЕРУГРОЗ - ИЮЛЬ 2017

Спасибо за внимание!

Ростелеком