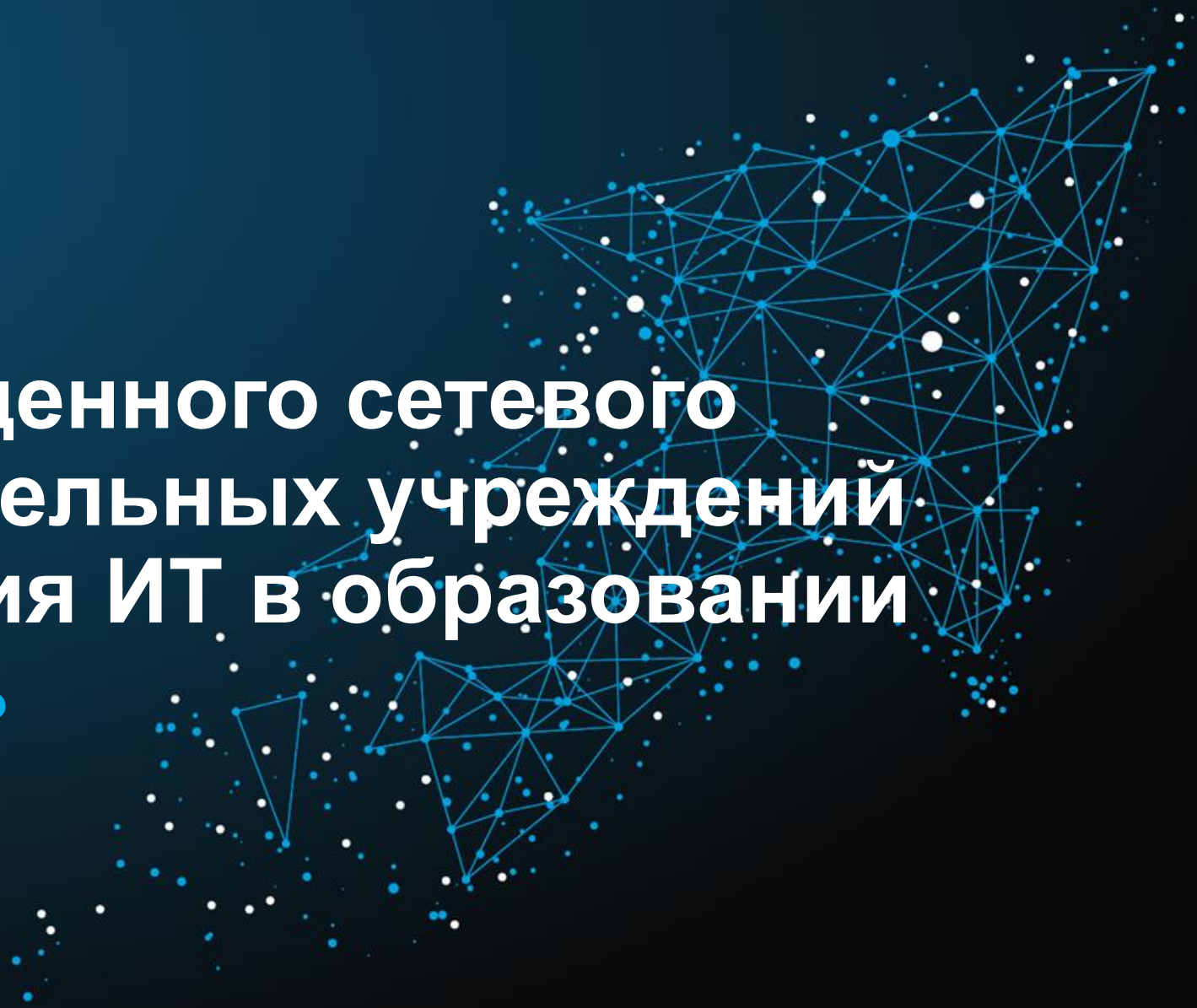
Ростелеком



Построение защищенного сетевого контура образовательных учреждений как основа развития ИТ в образовании

Сервисная модель в действии

ПРОБЛЕМЫ ДАЛЬНЕЙШЕГО РАЗВИТИЯ ИБ

Постоянный рост числа эксплуатируемых СЗИ
Новая проблема/ИТ-система – новое СЗИ (новый контракт/проект). Высокие сроки поставки. Необходимость прогноза на 3-5 лет. Высокие капитальные затраты.

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

Нехватка квалифицированного персонала
Универсальных специалистов мало, стоят они дорого, постоянная текучка

ИБ не успевает за ИТ
Постоянно меняющаяся инфраструктура. ИТ уходят в облако. Новые угрозы, вектора атак.

Возрастающее реальное влияние кибер-рисков
Вирусы шифровальщики, таргетированные атаки, хактивисты, хулиганы.

Enemy Inside. Необходимо ловить «врага» внутри.
Высокая стоимость собственной службы мониторинга инцидентов 24\7\365

ПОЧЕМУ СЕРВИСЫ ИБ ОТ РОСТЕЛЕКОМ

Аттестованная и сертифицированная Национальная облачная платформа
Размещение ИСПДН (до УЗ-1), ГИС (до К1), и 1Г по РД ГТК.
Сертификат соответствия PCI DSS v3.2

Защищенный канал передачи (в т.ч. ГОСТ VPN)
С-Терра (в т.ч. виртуальный шлюз), ViPNet, Континент, Фактор-ТС

Замена капитальных затрат (CAPEX) на операционные (OPEX)
Быстрое включение сервиса. Вы платите только за те сервисы, которые нужны именно Вам.

Группы мониторинга, расследования и реагирования, администрирования СЗИ (24/7/365) (*InHouse*)
35 человек в SOC. Более 100 в ИБ. Постоянное развитие и рост. Инфраструктура по всей РФ.

Успешные реализованные проекты
Более 5 лет на страже ЭП, Госуслуги, Выборы, ЕГЭ, Прямая линия с Президентом, Клиенты НОП, SOC, антиDDOS

«Переложите обязанность по обеспечению безопасности на Ростелеком»
Поручение обеспечения безопасности ПДн, ГИС Ростелекому.

MSSP: ПОДХОД РОСТЕЛЕКОМ

Дата-центр (основной или резервный) в ВЦОД оператора.
Оператор предоставляет инфраструктуру и её защиту

Сетевая безопасность

- Защита от DDoS-атак
- Межсетевой экран канального уровня (FW)
- Предотвращение компьютерных атак (IPS/IDS)
- Межсетевой экран уровня приложений (WAF)
- Контроль приложений (App control)
- Web-фильтрация
- Защита от APT-атак

Security Operations Center

- Мониторинг и анализ событий ИБ
- Поиск реальных угроз (Threat Detection\Hunting)
- Реагирование на инциденты (IR)
- Расследование инцидентов
- Услуги Корпоративного центра ГосСОПКА

Endpoint security

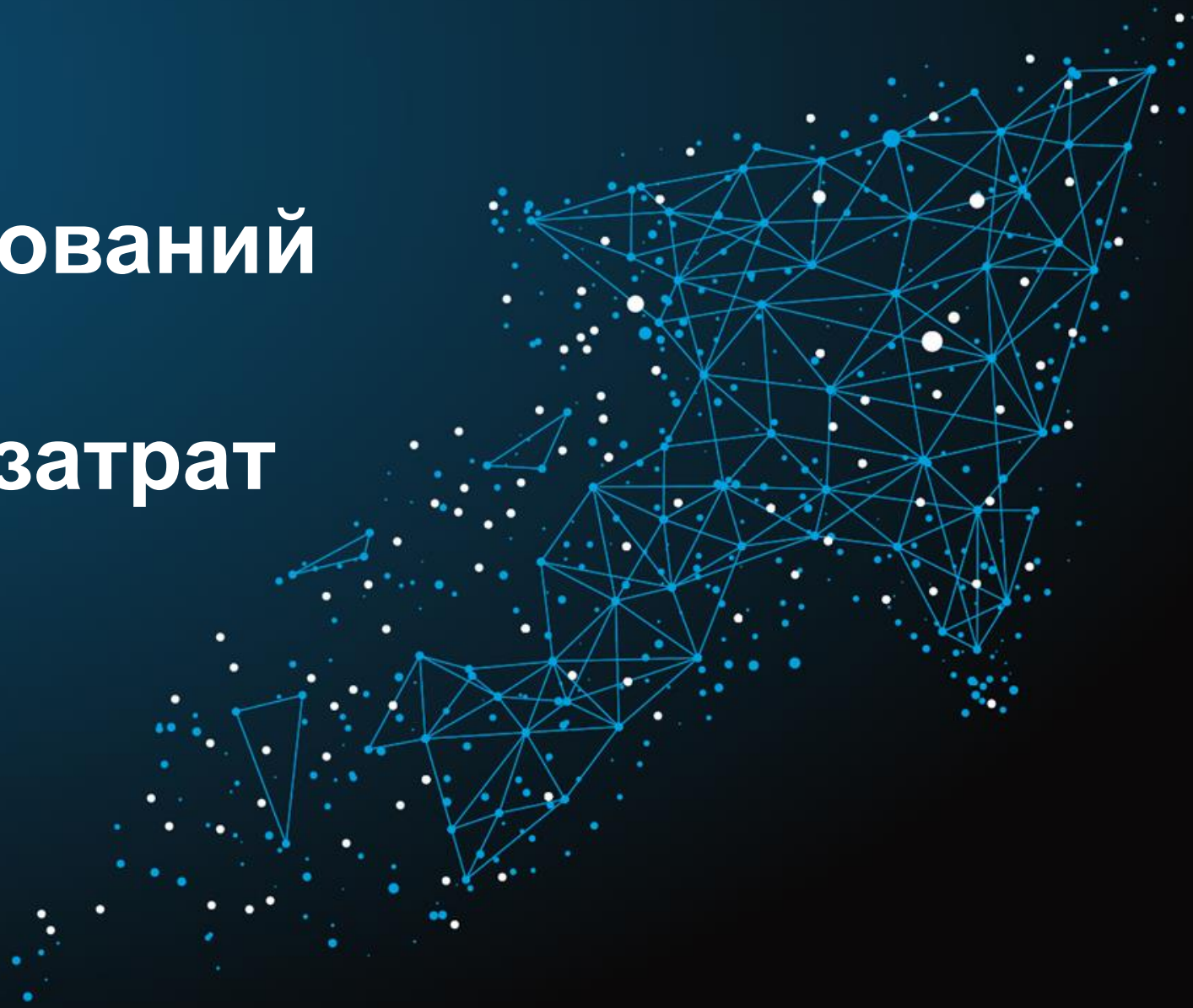
- Управление мобильностью предприятия (EMM)
- Anti-Virus/Anti-Malware
- Защита электронной почты (e-mail security)

Аналитика и тестирование

- Анализ и управление уязвимостями
- Тестирование на проникновение
- Управление навыками информационной безопасности
- Compliance 152-ФЗ
- Аттестация (ГИС, ИСПДн, АС)

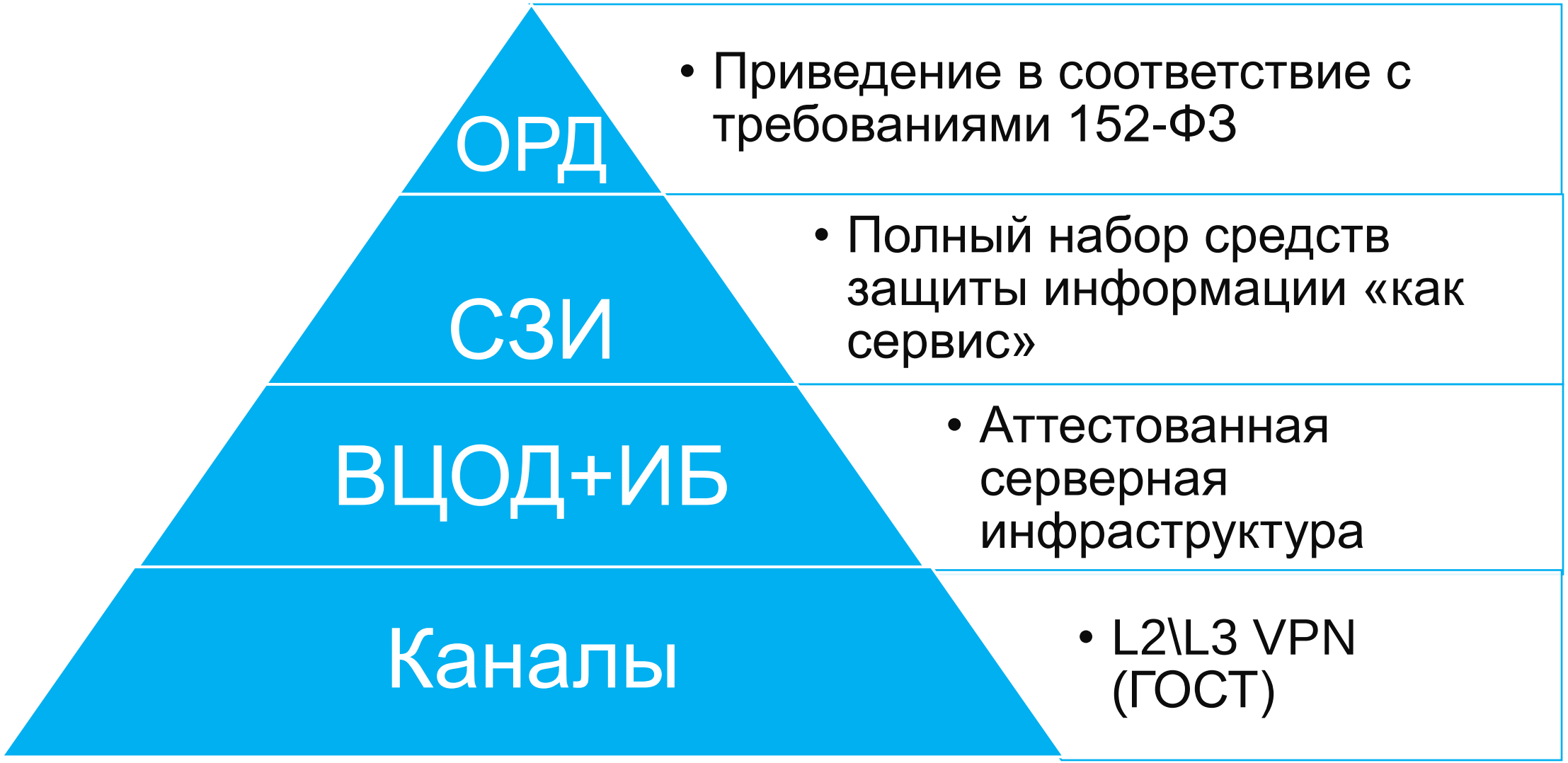
Ростелеком

Выполнение требований 152-ФЗ без капитальных затрат



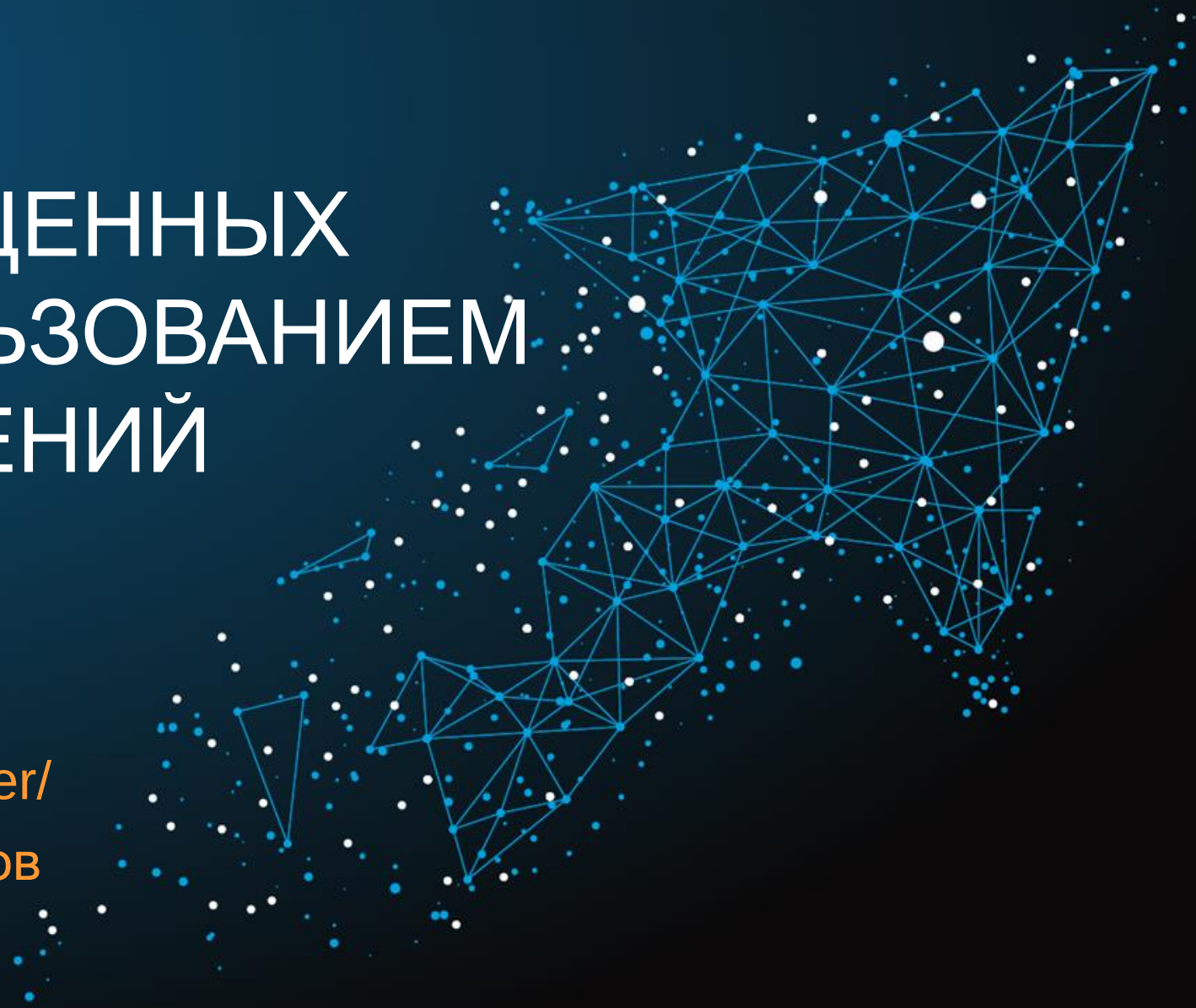
Широкие возможности
для организации защищенных
инфраструктур с выполнением
требований законодательства

ИНФРАСТРУКТУРА «152-ФЗ» ОТ РОСТЕЛЕКОМ



Ростелеком

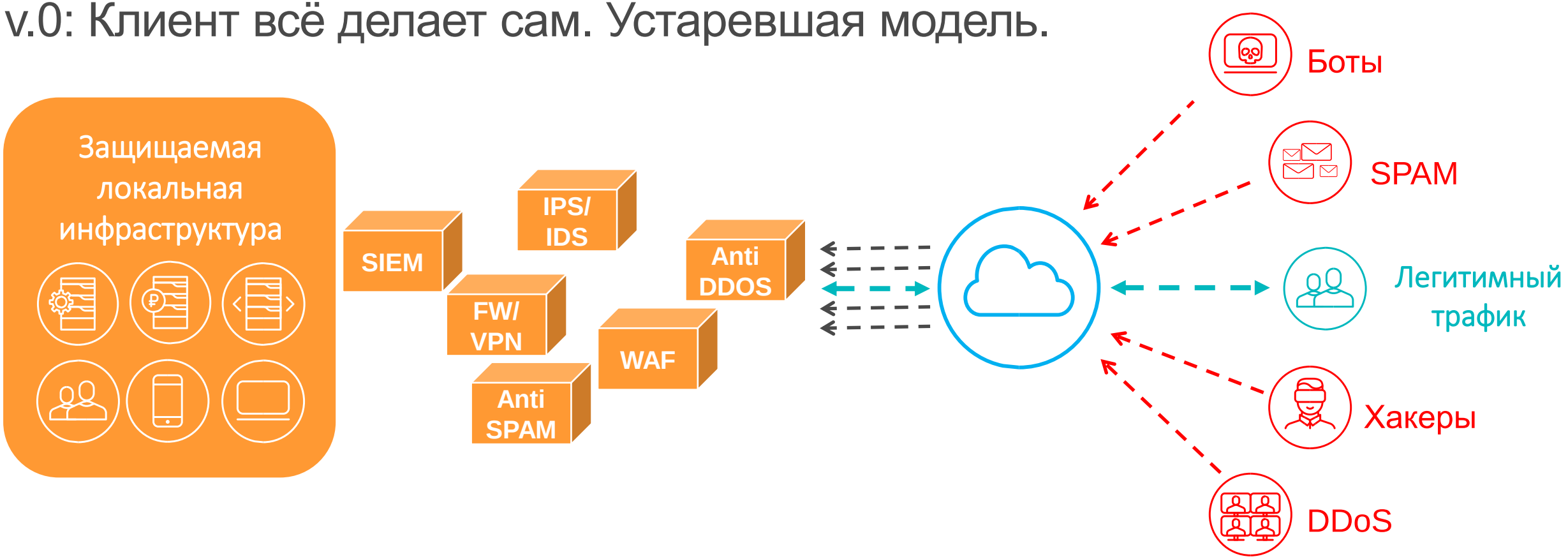
СОЗДАНИЕ ЗАЩИЩЕННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ СЕРВИСНЫХ РЕШЕНИЙ (MSSP: TelcoCloud)



Managed Security Services Provider/
Провайдер управляемых сервисов безопасности

ТРАДИЦИОННЫЙ ПОДХОД К ИБ

v.0: Клиент всё делает сам. Устаревшая модель.

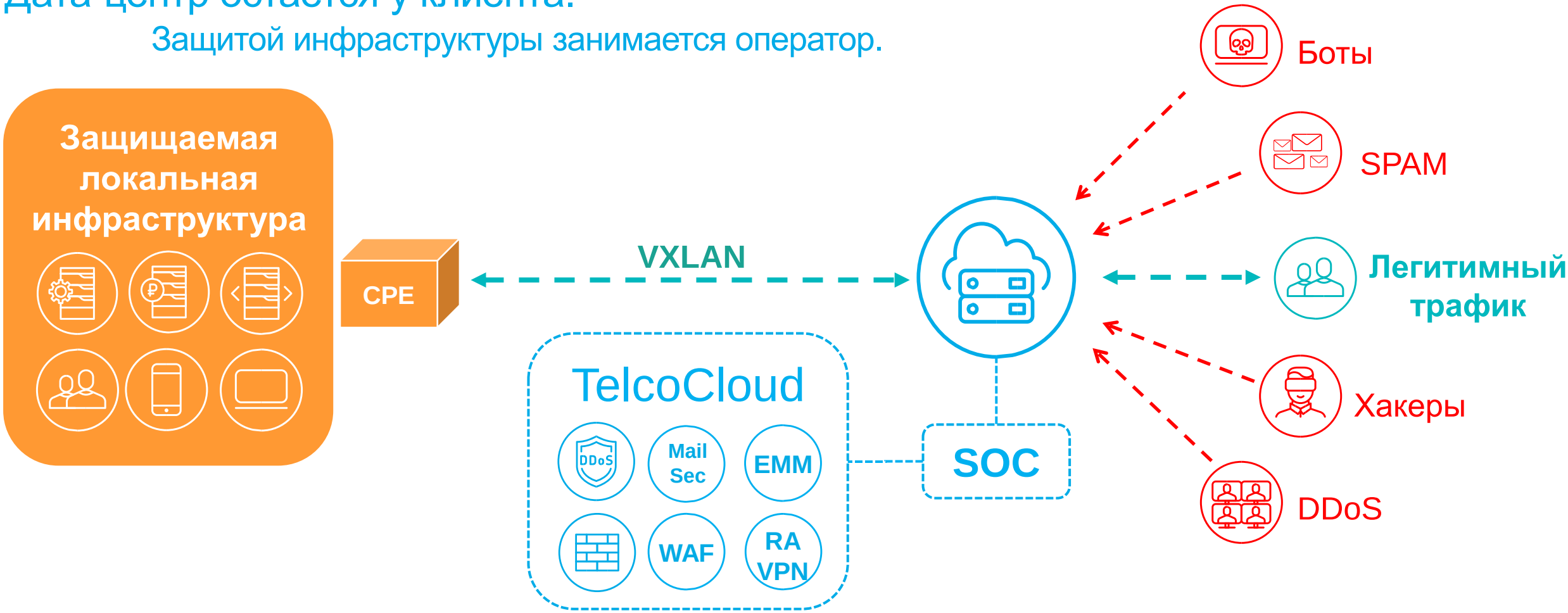


Сегмент ИС Клиента | Сеть провайдера | Интернет

MSSP: TELCOCLOUD+SOC

Дата-центр остается у клиента.

Защитой инфраструктуры занимается оператор.



Сегмент ИС Клиента | Сеть провайдера | Интернет

Ростелеком

МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ (РТК SOC)

Security Operation Center/
Оперативный центр мониторинга информационной безопасности

ПОДРОБНЕЕ ПРО SOC

СБОР СОБЫТИЙ

- SIEM
- FW
- IPS/IDS
- WAF
- VPN
- AV
- Anti DDoS
- Vulnerability scanners/management
- SandBox
- Сканеры кода

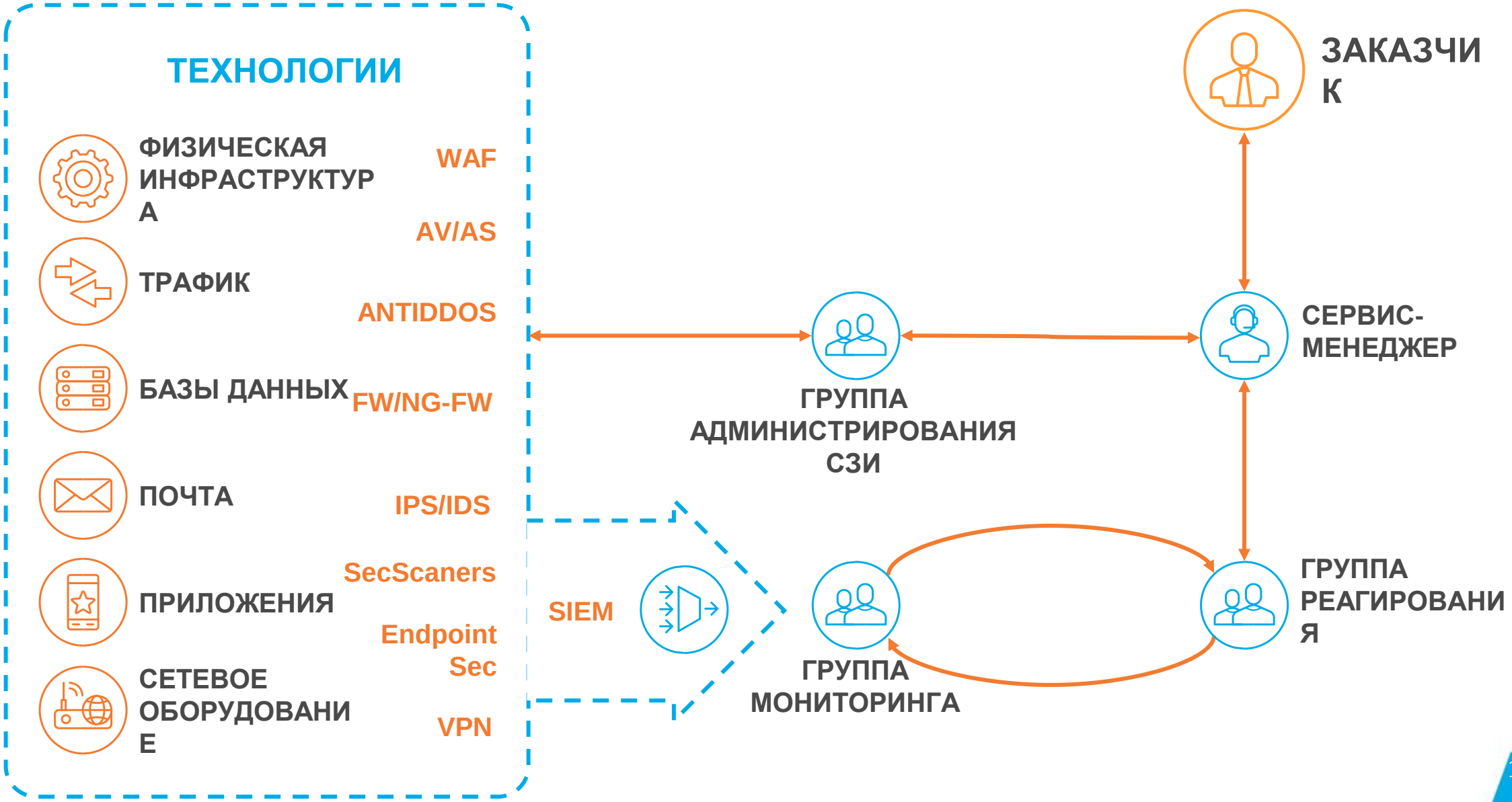
АНАЛИЗ СОБЫТИЙ

- мониторинг поступающих событий безопасности в режиме 24x7x365;
- обработка входящих данных и выделение инцидентов;
- мониторинг работоспособности подключенных услуг по обеспечению информационной безопасности;
- сбор необходимых данных для обработки инцидента;
- уведомление Заказчика об инциденте.

РЕАКЦИЯ НА ОБНАРУЖЕННЫЕ ИНЦИДЕНТЫ

- анализ инцидентов на основании информации, поступившей из разных источников
- определение информационных активов, пострадавших в результате инцидентов ИБ
- координация устранения инцидента в рамках всех оказываемых услуг
- принятие необходимых мер для устранения инцидента

SOC: ТЕХНОЛОГИИ-ПРОЦЕССЫ-ЛЮДИ



Ростелеком

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ (Compliance)

Платформа оценки, контроля и управления соответствием требованиям регуляторов в области ИБ (ПДн, ГИС, СТО БР, ОТИ)

ЦИКЛ СЕРВИСА COMPLIANCE

Пошаговое заполнение check-листа

Классификация ИС. Генерация пакета документов, в т.ч. Модели угроз

Разработка Технического решения в т.ч. С участием специалистов Ростелеком

Выезд или удаленная доработка документов и аттестация ИС (при необходимости)

Периодическая актуализация


По интересующим Вас вопросам
обращайтесь по телефону
8(4812)303303
Ростелеком
С НАМИ НАДЁЖНО!