Информационная безопасность от Ростелеком

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

Почему кибер-безопасность?

Ростелеком

ПОЯВЛЕНИЕ НОВЫХ ТЕХНОЛОГИЙ И БИЗНЕС МОДЕЛЕЙ

- Использование мобильных устройств / BYOD
- Виртуализация и облачные технологии
- Обширная IT инфраструктура
- Internet of Things

ПОЯВЛЕНИЕ НОВЫХ КИБЕР-УГРОЗ

- Инсайдеры
- Script-kiddies
- Организованная преступность
- Конкуренты/хактивисты
- Таргетированные атаки

НОВЫЕ ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА

- Приказы ФСТЭК
- Требования ЦБ
- Требования ФСБ
- PCI/DSS
- ISO 27001

ГРОМКИЕ ИНЦИДЕНТЫ ИБ

ЗАРАЖЕНИЕ ВРЕДОНОСНЫМ КОДОМ

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

ПРОВЕРКИ РЕГУЛЯТОРОВ

КРАЖА МОБИЛЬНЫХ УСТРОЙСТВ

УТЕЧКА ДАННЫХ

DDOS АТАКИ

Проблемы дальнейшего развития ИБ

Ростелеком

Постоянный рост числа эксплуатируемых СЗИ

Новая проблема/ИТ-система – новое СЗИ (новый контракт/проект). Высокие сроки поставки. Зависимость от производителя СЗИ. Необходимость прогноза на 3-5 лет. CAPEX.

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, векторы атак.

Возрастающее реальное влияние кибер-рисков на бизнес

Нужна реальная безопасность, а не только на бумаге.

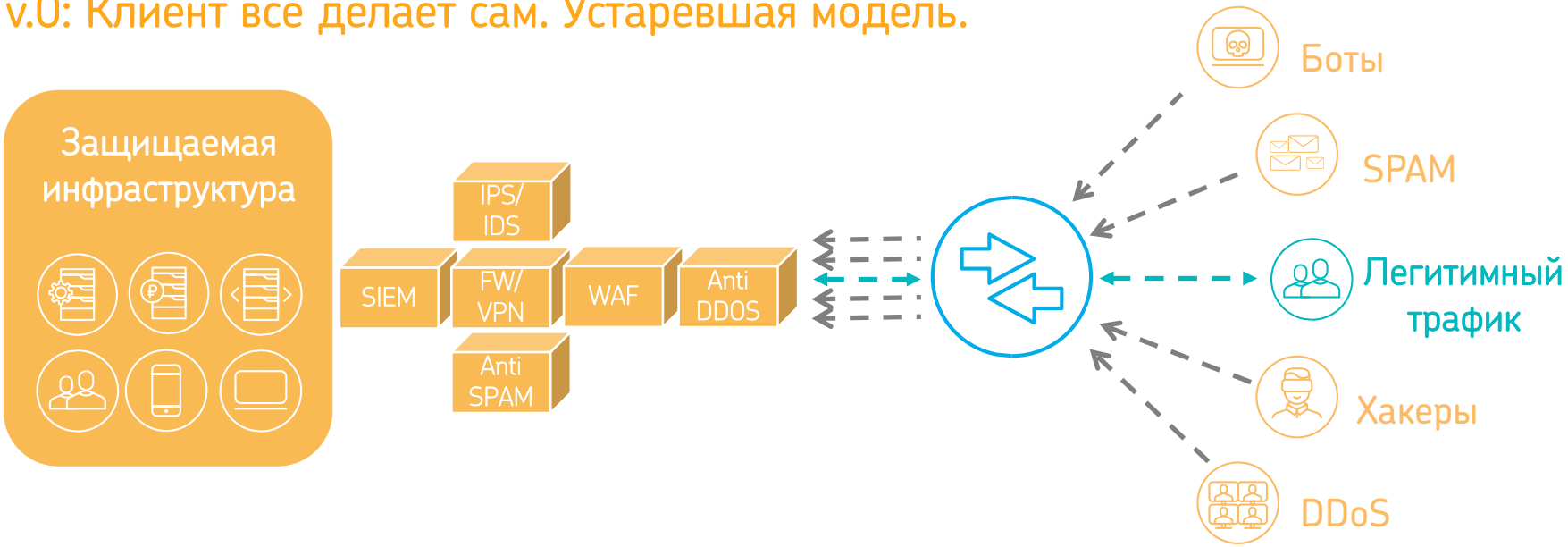
Enemy Inside. Первый рубеж создан. Необходимо ловить «врага» внутри своей сети

Высокая стоимость собственной 24/7/365 службы мониторинга и расследования инцидентов

Традиционный подход к ИБ

Ростелеком

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

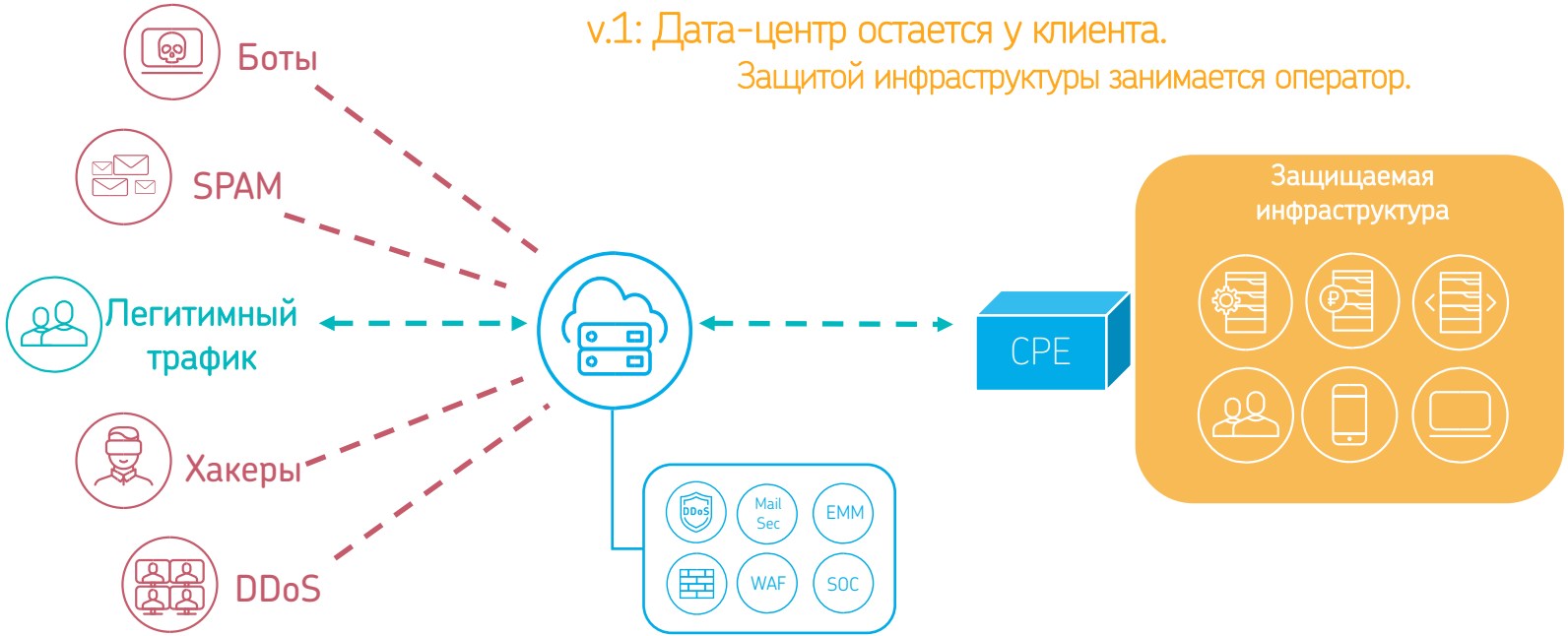


Сегмент ИС Клиента | Сеть провайдера | Интернет

Сервисная модель построения системы защиты информации

Ростелеком

v.1: Дата-центр остается у клиента.
Защитой инфраструктуры занимается оператор.

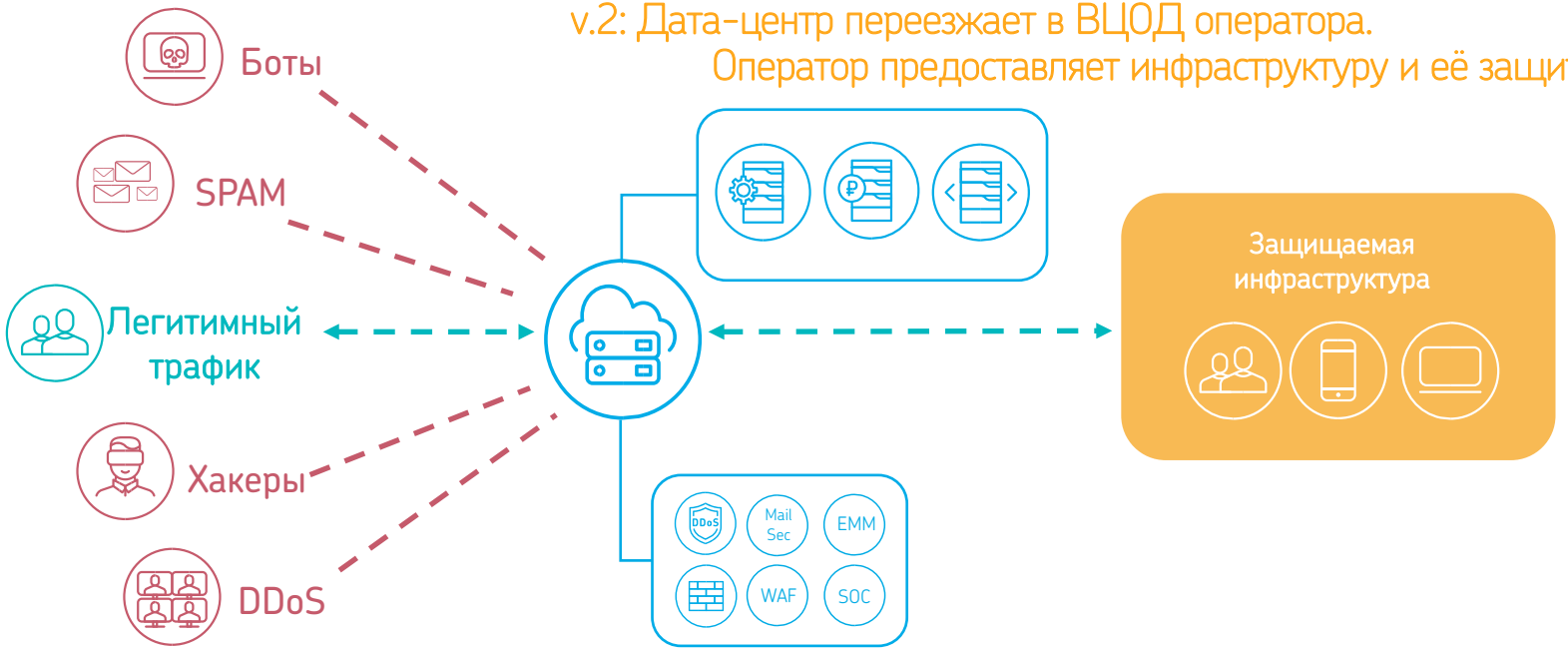


Интернет	Облако Ростелеком	Сегмент ИС

Сервисная модель построения системы защиты информации

Ростелеком

v.2: Дата-центр переезжает в ВЦОД оператора.
Оператор предоставляет инфраструктуру и её защиту



Интернет	Облако Ростелеком	Сегмент ИС

Существующие сервисы по ИБ

Ростелеком

UTM

Предотвращение сетевых угроз, URL фильтрация и выявление бот-сетей

WAF

Защита веб-приложений от комплексных угроз безопасности, исходящих из сети Интернет

Anti DDoS

Выявление и предотвращение DDoS-атак из сети Интернет

SOC

Мониторинг, выявление и реагирование на инциденты информационной безопасности

EMM

контроль и защита мобильных устройств, используемых организацией и её сотрудниками

Email Security

Защита корпоративной почты с использованием специализированного устройства Оператора для проверки почтовых сообщений на вирусы и другие известные угрозы

Преимущества сервисной модели услуг ИБ

- Гибкость конфигурации и возможность быстрого наращивания или сокращения мощностей
- Единое окно управления всеми средствами защиты
- Эксплуатация системы защиты силами квалифицированных специалистов поставщика услуг
- Мониторинг и реагирование на инциденты ИБ в режиме 24x7
- Отсутствует необходимость в большом собственном штате дорогостоящих инженеров ИБ
- Форма затрат – OPEX

Подробнее про Security Operations Center

Что это такое?

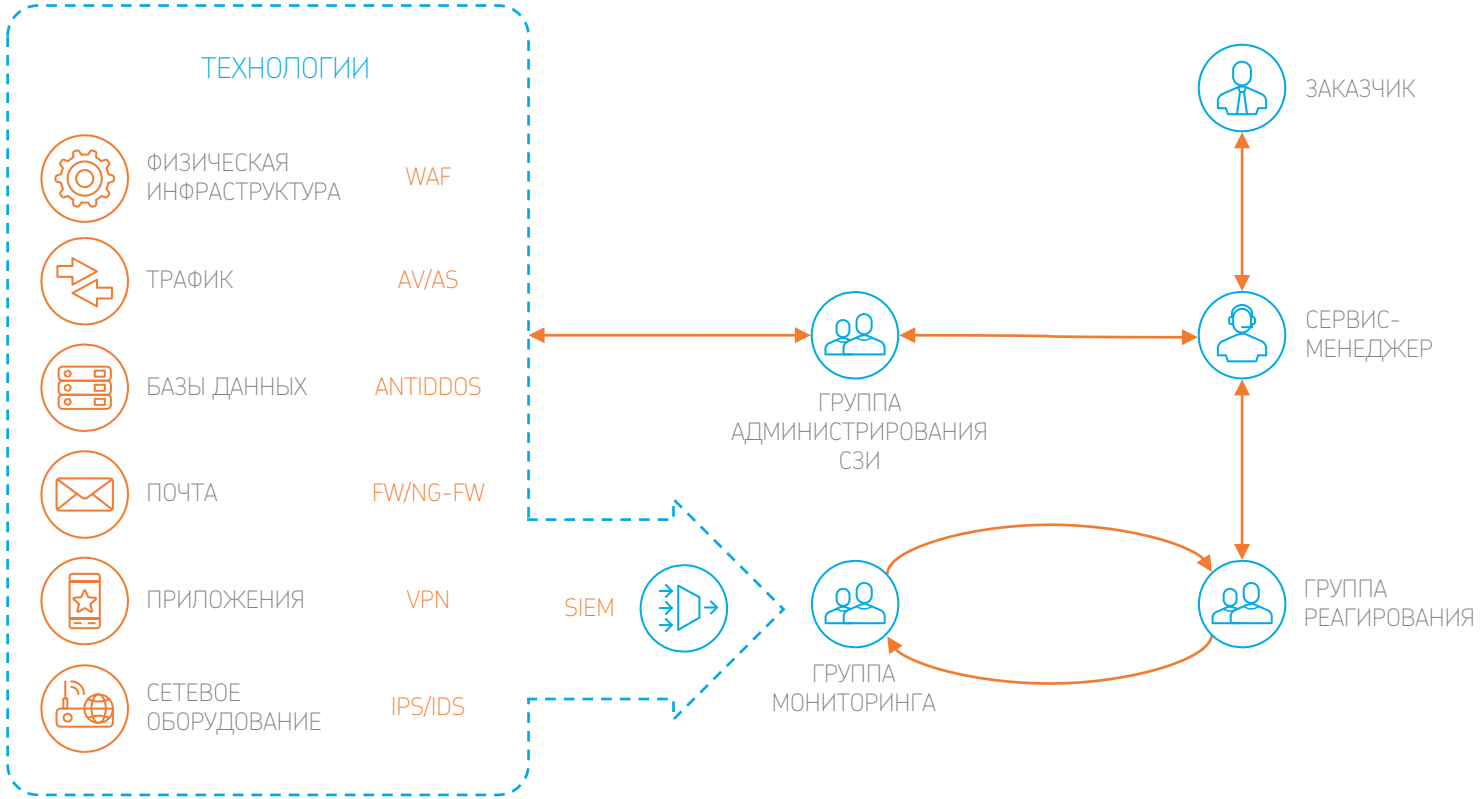
Ростелеком

Security Operations Center (SOC) – Центр мониторинга и оперативного реагирования на инциденты информационной безопасности

Подробнее про Security Operations Center

Как все устроено?

Ростелеком



Подробнее про Security Operations Center

Как это работает?

Ростелеком

СБОР СОБЫТИЙ

- FW
- IPS/IDS
- WAF
- AV
- Anti DDoS
- Vulnerability scanners

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

SLA

Период предоставления Услуг	24x7	
Обнаружение инцидента ИБ, Регистрация инцидента ИБ	1 – Критический 2 – Высокий 3 – Средний	до 15 минут
Проверка ложного срабатывания, Уведомление Заказчика об инциденте ИБ	1 – Критический 2 – Высокий 3 – Средний	до 30 минут до 120 минут до 120 минут
Время выдачи рекомендаций по противодействию	1 – Критический 2 – Высокий 3 – Средний	до 2 часов до 6 часов до 12 часов

Тарифы

Ростелеком

Скорость канала	100 Мбит/с	1 Гбит/с
UTM (FW,IPS, RAVPN)	от 15 000 руб/мес	от 70 000руб/мес
MailSec (за одного пользователя)	от 100 руб/мес	от 100 руб/мес
Мониторинг и реагирование на инциденты	От 35 000 руб/мес	

Выгоды для заказчика

Ростелеком

- Высокий уровень устойчивости к кибер-угрозам
- Оптимизация затрат на ИБ за счет сервисной модели
- Быстрая масштабируемость
- Решение кадрового вопроса
- Качественный сервис вместо коробки

Почему кибер-безопасность от Ростелекома?

Ростелеком

Более 5 лет опыта в защите:
- Инфраструктуры систем «Электронного правительства»
- Клиентов «Национальной облачной платформы Ростелеком»

Около 100 человек в команде обеспечения кибер-безопасности.

Инфраструктура распределена от Калининграда до Владивостока

Непрерывно развиваемся
- Ориентируемся на мировой опыт
- Привлекаем консультантов с признанным в мире опытом

Ростелеком

Спасибо за внимание

Схема работы Telco Cloud