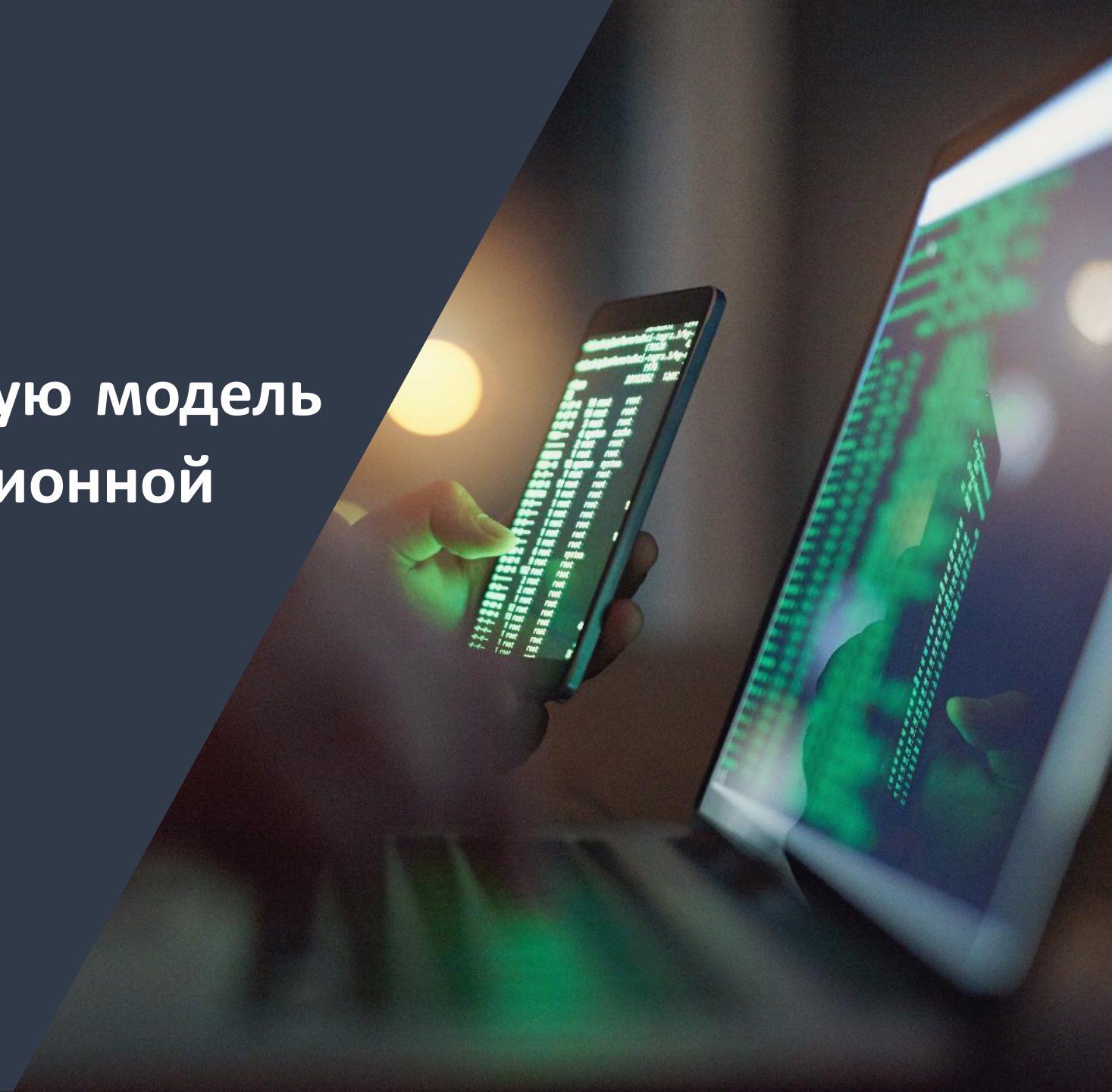
Ростелеком

Как перейти на сервисную модель обеспечения информационной безопасности?



Алексей Богданов
Макрорегиональный филиал «Волга»
ПАО «Ростелеком»
Директор по развитию бизнеса по информационной безопасности

Насколько Вы знакомы с сервисной моделью в ИБ?

1. Знаком, использую,
это действительно удобно и выгодно
2. Знаком, использую,
но есть шероховатости…
3. Сам не использую,
Но знаю тех, кто использует
4. Слышал только в теории,
На практике не встречал

Зачем нужна информационная безопасность?

Защита от кибер-угроз

- Вирусы шифровальщики (WannaCry, NotPetya)
- Майнеры
- Инсайдеры
- Готовые пакеты для хаккинга (Script-kiddies)
- Организованная преступность
- Конкуренты/хактивисты
- Таргетированные (целевые) атаки

Защита технологий и бизнес моделей

- Переход на мобильные и web-технологии
- Использование мобильных устройств / BYOD
- Виртуализация и облачные технологии
- Обширная IT инфраструктура
- Интернет вещей

Выполнение требований законодательства и отрасли

- Приказы ФСТЭК и ФСБ России (КИИ, ИСПДн, ГИС)
- Требования ЦБ России
- Требования Минздрава (ЕГИСЗ)
- PCI/DSS
- ISO 27001

ЗАРАЖЕНИЕ ВРЕДОНОСНЫМ КОДОМ

УТЕЧКА ДАННЫХ

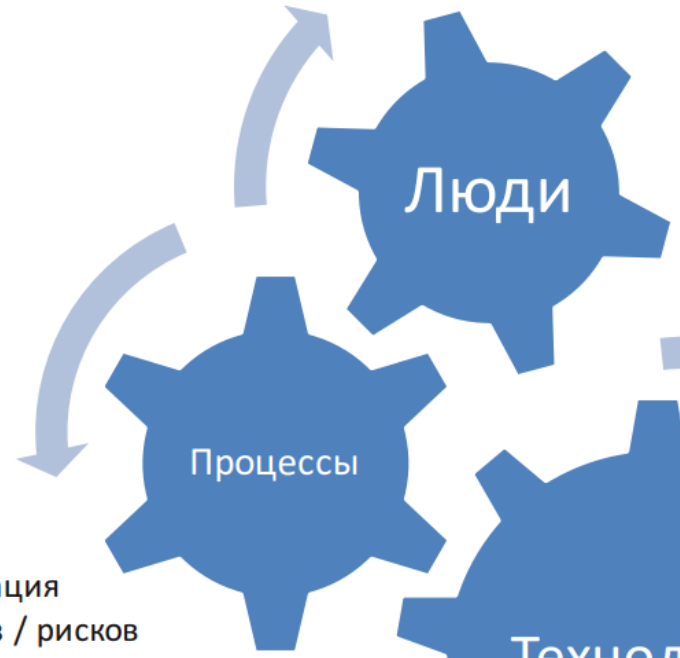
DDOS АТАКИ

КРАЖА МОБИЛЬНЫХ УСТРОЙСТВ

ПРОВЕРКИ РЕГУЛЯТОРОВ

Ростелеком

Теория всем давно известна



- 1я линия (обнаружение)
- 2я линия (расследование и реагирование)
- 3я линия (экспертная поддержка, руководство, юр.вопросы)

- Инвентаризация
- Анализ угроз / рисков
- Выявление уязвимостей
- Тестирование на проникновение
- Контроль устранения ранее выявленных уязвимостей
- Контроль выполнения требований (аудит)
- Анализ кода приложений
- Обучение и повышение осведомленности
- Управление событиями ИБ
- Управление инцидентами
- …

Технологии, обеспечивающие:

- Взаимодействие персонала
- Инвентаризацию ИС и контроль конфигурации
- Выявление уязвимостей
- Анализ событий ИБ
- Учет и обработку инцидентов
- Управления знаниями

- Анализ кода (прикладное ПО, вредоносное ПО)
- Сбор цифровых доказательств

- СЗИ (МСЭ, IPS, DLP, Sandbox, и пр.)
- …

ГЛОБАЛЬНЫЕ ТРЕНДЫ

Технологии определяют бизнес

Бизнесу нужен новый темп

Цифровизация бизнеса и производства

Бизнес осознает уязвимость ИТ

ВЫЗОВЫ ДЛЯ ИБ

- Динамика внешних угроз
- Скорость изменений в ИТ
- Сложные ИБ-технологии, которыми нужно управлять
- Дефицит кадров
- Необходимость защиты ядра бизнеса

Ростелеком

СЕРВИСНАЯ МОДЕЛЬ КАК ИДЕОЛОГИЯ

БЕЗОПАСНОСТЬ КАК СЕРВИС – ЭТО:

– БЕЗОПАСНОСТЬ КАК ФУНКЦИЯ, А НЕ КОНСТРУКТОР ИЗ ТЕХНОЛОГИЙ

– БЕЗОПАСНОСТЬ В ТЕМПЕ – ЗДЕСЬ И СЕЙЧАС

– БЕЗОПАСНОСТЬ БЕЗ КАДРОВЫХ ОГРАНИЧЕНИЙ

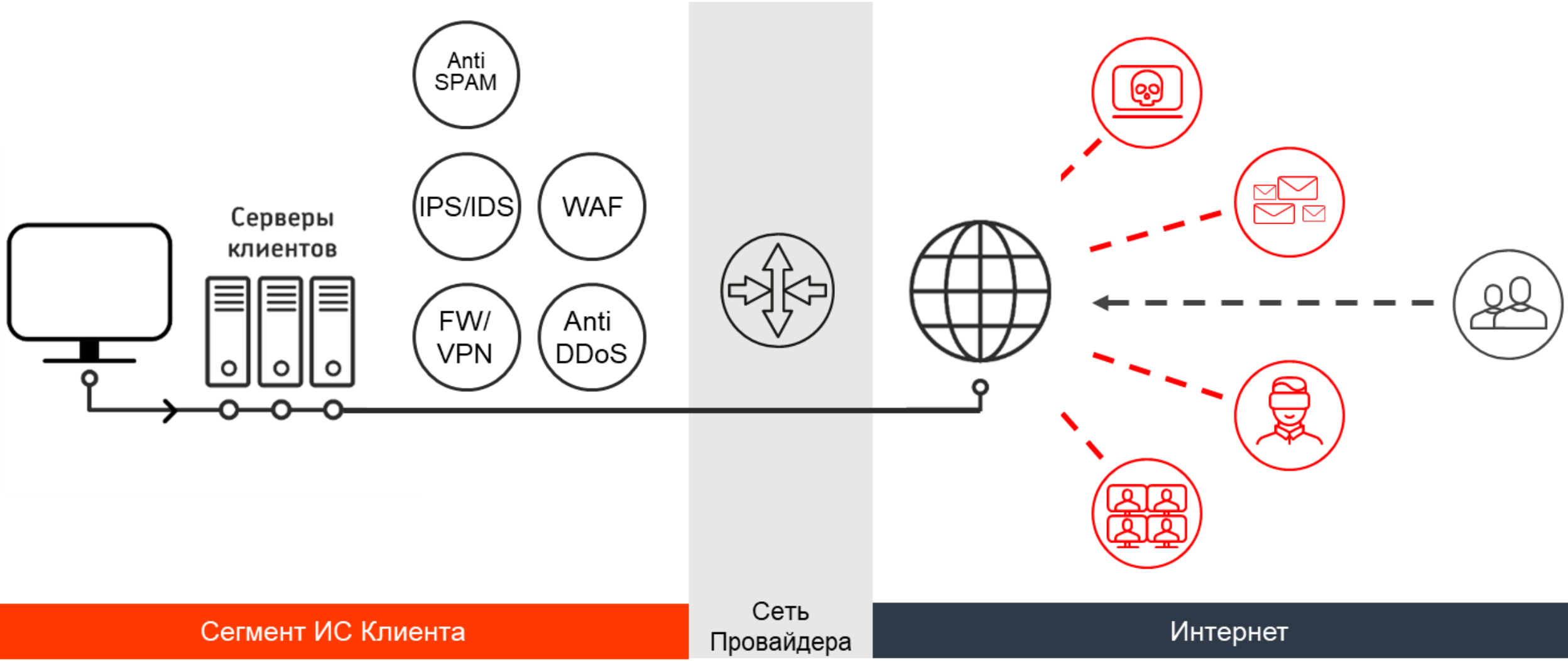
И ЭТО МИРОВОЙ ТРЕНД

15% ДОЛЯ РЫНКА MSS-СЕРВИСОВ НА МИРОВОМ РЫНКЕ ИБ СЕГОДНЯ

X3,6 ИНВЕСТИЦИИ В ТЕХНОЛОГИИ, ПРЕДОСТАВЛЯЕМЫЕ В СЕРВИСНОЙ МОДЕЛИ, БОЛЬШЕ, ЧЕМ В ТРАДИЦИОННОЙ

*Gartner

Традиционный подход к средствам защиты



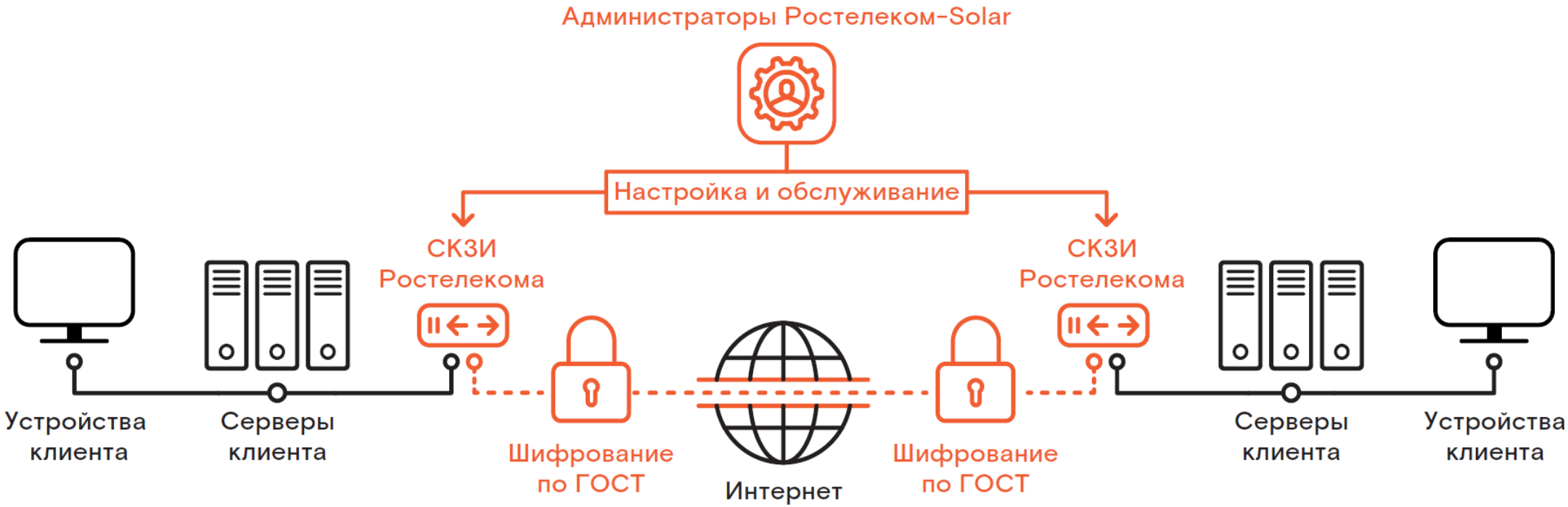
Сервисы сетевой безопасности

- Защита от сетевых угроз (UTM)
- Защита веб-приложений (WAF)
- Защита электронной почты (SEG)
- Защита от DDoS-атак (Anti-DDoS)

- Единая точка управления всей инфраструктурой (SD-WAN)
- Автоматическая настройка CPE (Zero Touch Provisioning)
- Виртуализация вместо ПАК (Network Functions Virtualization)
- Мониторинг и реагирование в режиме 24×7

Ростелеком

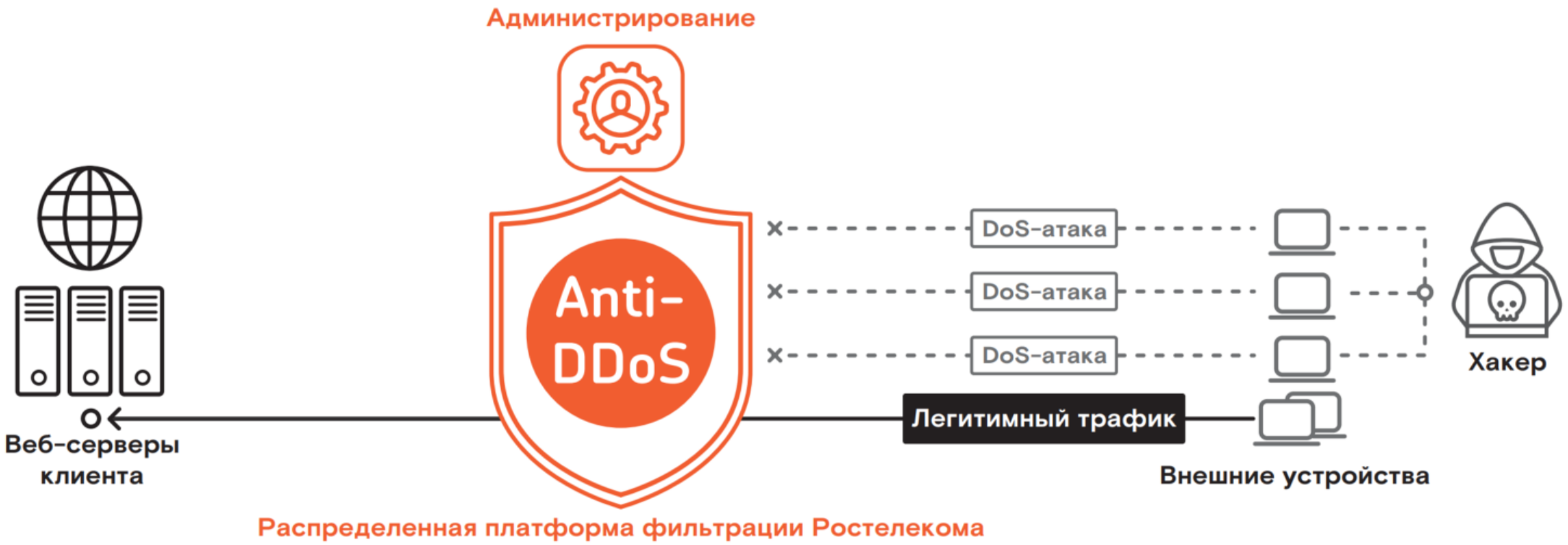
ГОСТ VPN по сервисной модели



- Масштабируемость и быстрое подключение к сервису
- Настройка и реагирование в режиме 24x7
- Перемещение ответственности за систему криптозащиты на сторону компании-провайдера
- Возможность выбора вендора СКЗИ

Ростелеком

Сервисы Anti-DDoS

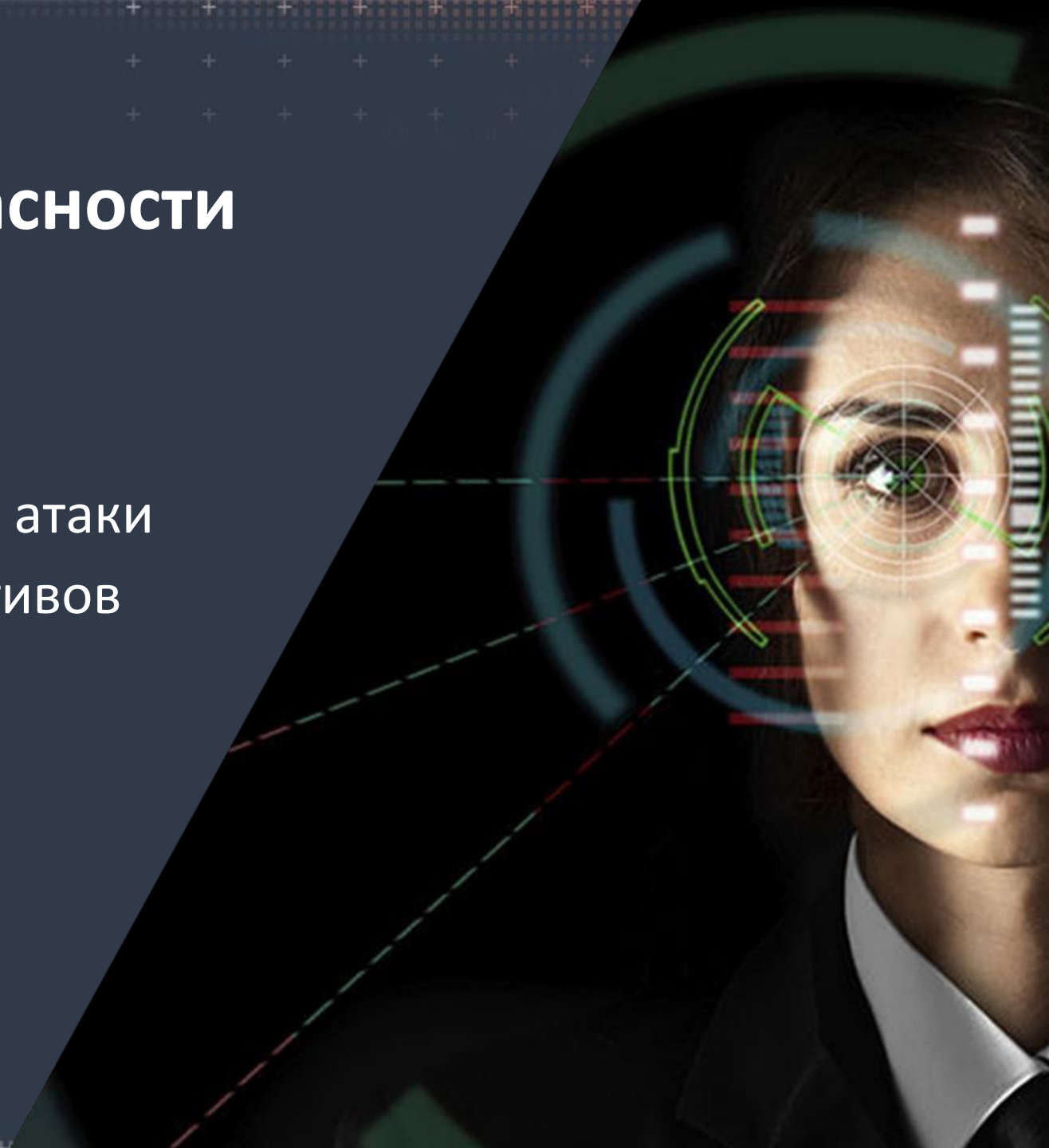


Ростелеком
Солар

Контроль информационной безопасности

БЕЗОПАСНОСТИ НУЖНЫ ГЛАЗА

1. Мониторинг и реагирование на атаки
2. Контроль защищенности ИТ-активов
3. Расследование инцидентов

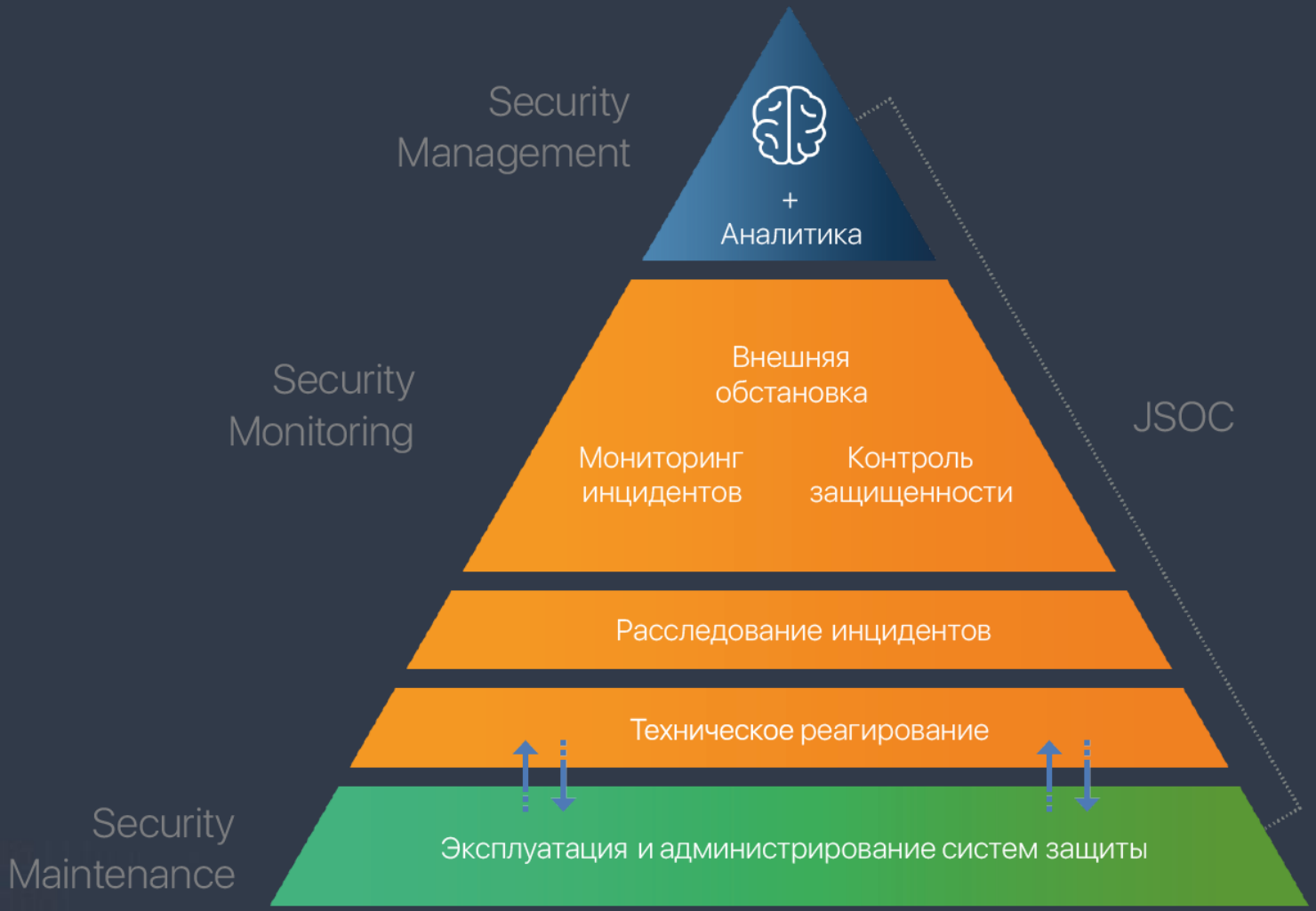


Ростелеком

Ситуационный центр информационной безопасности

Security Operations Center (SOC)

SOC: Архитектура, задачи и функции



Ростелеком

Из чего состоит SOC

Инфраструктура

- SIEM, Security Scanner, IRP…
- Система аналитики, отчетности и визуализации

Процессы

- Концепция, архитектура, документирование
- Реагирование на инциденты
- Внутренние SLA и KPI

Сотрудники

- 1 линия мониторинга 24/7
- Команда реагирования
- Обучение, развитие, тестирование

Дополнительные задачи

- Процессы Threat Intelligence
- Forensics
- Проверка эффективности

Что дает сервисная модель?

Преимущества сервисной модели

Экономия и эффективность

Снижение стоимости владения

Совокупная стоимость владения сервисами дешевле покупки, внедрения и последующей поддержки ИБ-решений

Устранение дефицита кадров

Отсутствие необходимости создания отдела из высококвалифицированных ИБ-специалистов

Экономия

Снижение затрат на оборудование и персонал, перевод капитальных издержек в операционные

Профессиональная команда

Настройка, обслуживание и разбор инцидентов безопасности лучшими специалистами отрасли

Технологичность и надежность

Доступность

Защита и мониторинг 24 часа в сутки без перерывов и выходных

Надежность

Эксплуатация распределенной отказоустойчивой инфраструктуры

Гибкость

Простая масштабируемость и быстрое изменение параметров услуги

Скорость

Быстрое подключение к сервисам и оперативное реагирование на инциденты

Соблюдение законодательства

Соответствие требованиям

Выполнение требований информационной безопасности

Оптимальные средства защиты

Эксплуатация сертифицированных решений лидирующих вендоров

Лицензии регуляторов

Компания является лицензиатом ФСТЭК России, ФСБ России и Минобороны России

Отслеживание изменений

Меры защиты всегда соответствуют новым законам и регламентам

Как выбрать сервис-провайдера по ИБ?

На что обратить внимание

1. Наличие инфраструктуры для обеспечения сервисов
2. Штат специалистов, их квалификация, география присутствия
3. Технологии и опыт применения
4. SLA

\+ тесты – наше все. Проводите пилотные проекты!

Будьте под защитой Ростелеком

ib@volga.rt.ru