Кибербезопасность ближе, чем кажется

Екатерина Митюкова
Директор по продуктам МРФ «Сибирь»
+7 953-777-4649

Каким вы видите мир ИБ через 10 лет?

УГРОЗЫ, ВЫЗОВЫ, РЕШЕНИЯ

ПОЯВЛЕНИЕ НОВЫХ
КИБЕР-УГРОЗ

НОВЫЕ
ТРЕБОВАНИЯ
ЗАКОНОДАТЕЛЬСТВА
И ОТРАСЛИ

ПОЯВЛЕНИЕ НОВЫХ
ТЕХНОЛОГИЙ И
БИЗНЕС МОДЕЛЕЙ

Причем здесь РТК-SOLAR?

Ростелеком-Solar – крупнейший поставщик на рынке информационной безопасности

#1

НА РЫНКЕ СЕРВИСОВ ИБ

350+

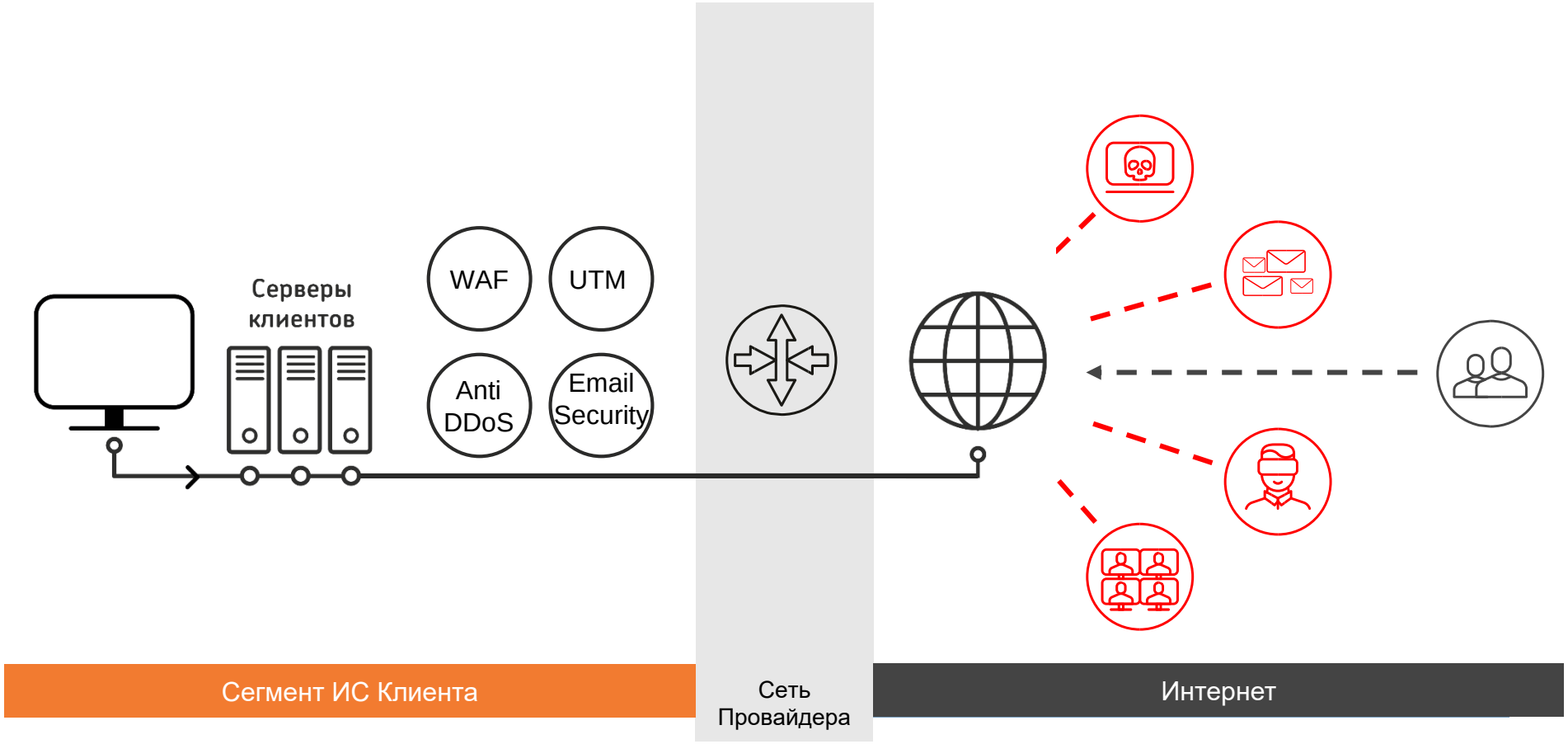
ЭКСПЕРТОВ КИБЕРБЕЗОПАСНОСТИ

Ключевые преимущества

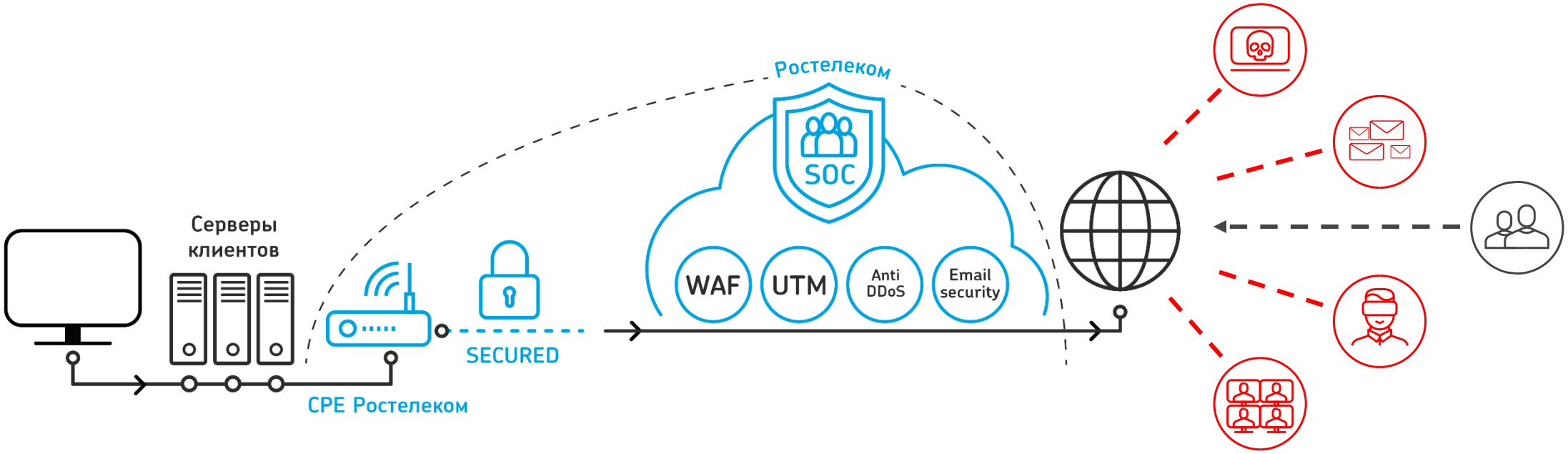
- Сервисное end-to-end предложение от инфраструктуры безопасности до управления ИБ
- Сервисы ИБ, поставляемые из сети и ЦОДов Ростелеком
- Сквозной SLA и единая точка ответственности за ИБ

ИНФРАСТРУКТУРА ОТ РОСТЕЛЕКОМ БЕЗ CAPEX

Традиционный подход к ИБ



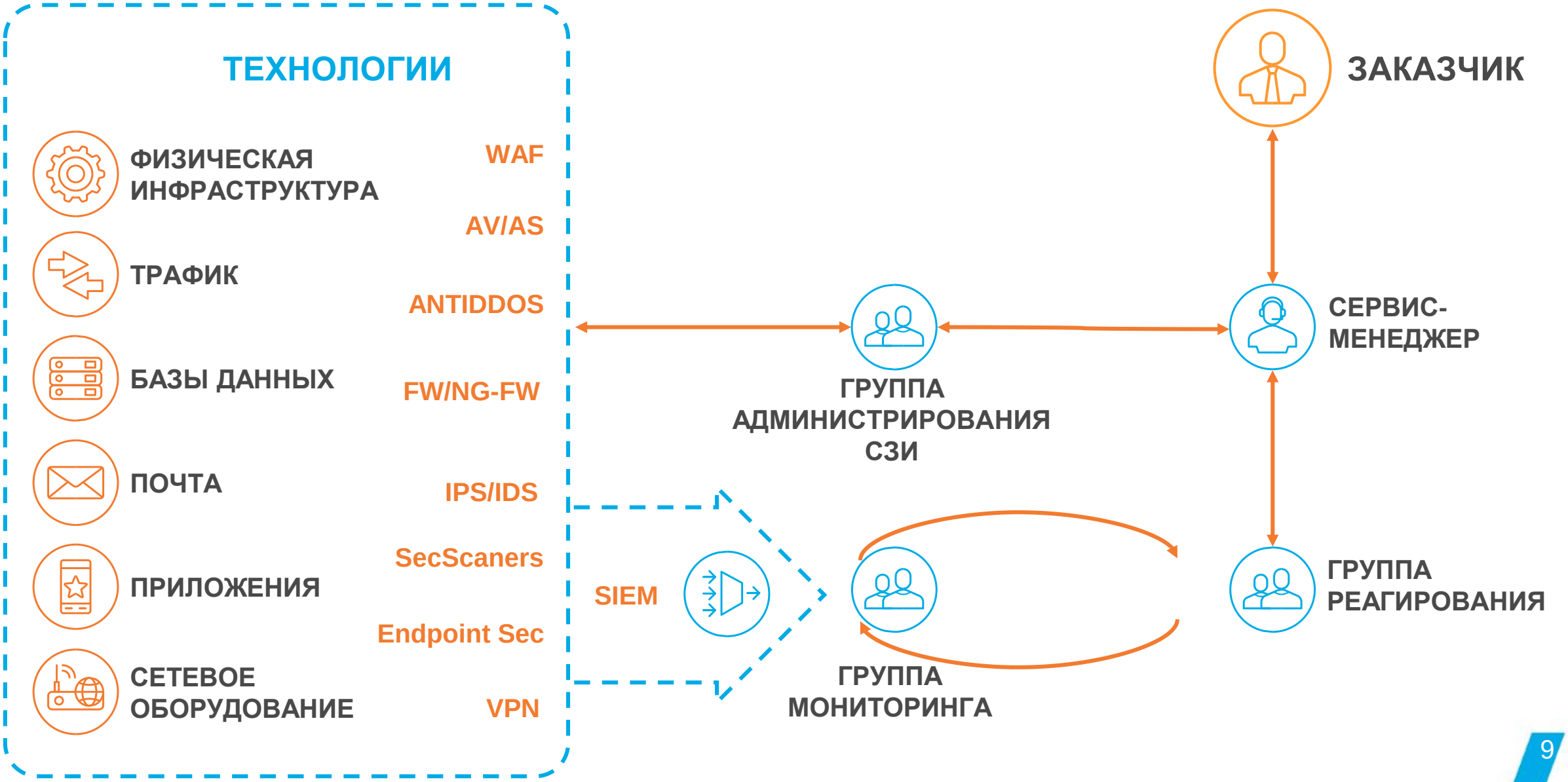
Сервисная модель предоставления услуг ИБ



Сегмент ИС Клиента | Облако Ростелеком | Интернет

Solar JSOC

SOC: ТЕХНОЛОГИИ-ПРОЦЕССЫ-ЛЮДИ



Про SOC

Функции SOC:

- Мониторинг, выявление и анализ инцидентов информационной безопасности
- Техническое противодействие атакам
- Контроль состояния защищенности, выявление уязвимостей, ошибок настройки
- Техническое расследование возникающих критичных инцидентов
- Аналитика по выявляемым инцидентам, их причинам для принятия решений

Ростелеком Solar JSOC сейчас

80+
Крупных клиентов под защитой

90+
Специалистов по ИБ в штате

6
Лет оказания услуг

99,4%
Общая доступность сервиса

10 мин
Время реакции на инцидент

30 мин
Время анализа/ противодействия

- Первый коммерческий центр сервисов ИБ-аутсорсинга в России
- Лидер направлений мониторинга инцидентов и построения центров ГосСОПКА
- Первая компания в России, ориентированная на бизнес в сервисах ИБ

Преимущества ситуационного центра

- ✓ Агрегация и оптимизация капитальных вложений при закупках оборудования и лицензий
- ✓ Прозрачный план развития ИБ и ИТ (road map) на основе реальных измеримых данных
- ✓ Оптимизация затрат на персонал
- ✓ Возможность предоставления сервисов внутри компании – столько сколько необходимо, тем кому необходимо, тогда когда необходимо
- ✓ Единая система контроля ИБ процессов – метрики, контроли, SLA
- ✓ Гибкое управление рисками – современный ландшафт угроз слишком динамичный для «обычного» проектного подхода
- ✓ Унификация технологий ИБ и экспертных ресурсов с повышением их эффективности

Уже под защитой:

МТС Банк

Почта Банк

media

НСПК
Национальная система платежных карт

Тинькофф

Министерство информационных технологий и связи Хабаровского края

Конструкторское бюро навигационных систем НАВИС

Ростелеком

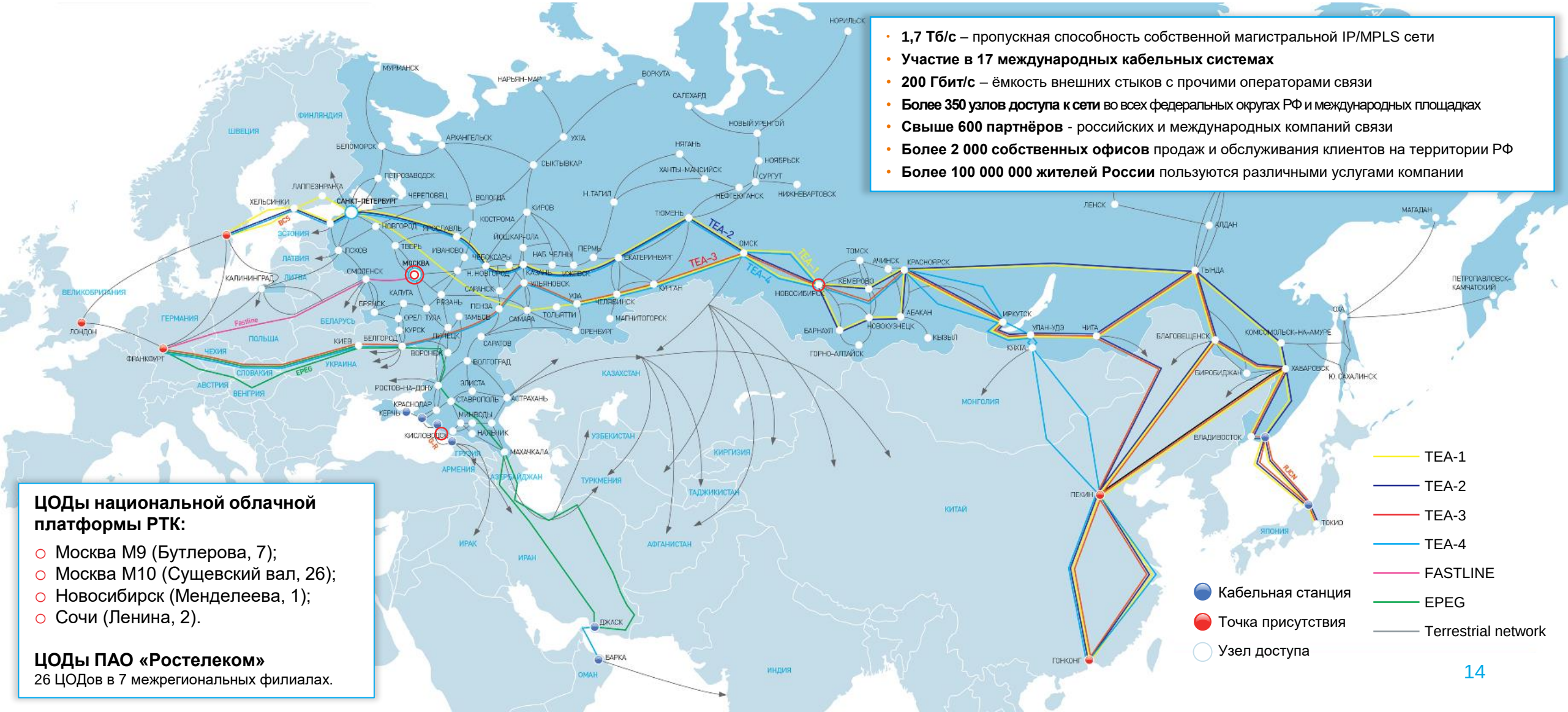
Департамент развития информационного общества Ивановской области

МСП Банк

Корпорация МСП

Сервисы по аренде и эксплуатации ИБ инфраструктуры

СЕТЬ КОМПАНИИ РОСТЕЛЕКОМ



- **1,7 Тб/с** – пропускная способность собственной магистральной IP/MPLS сети
- **Участие в 17 международных кабельных системах**
- **200 Гбит/с** – ёмкость внешних стыков с прочими операторами связи
- **Более 350 узлов доступа к сети** во всех федеральных округах РФ и международных площадках
- **Свыше 600 партнёров** - российских и международных компаний связи
- **Более 2 000 собственных офисов** продаж и обслуживания клиентов на территории РФ
- **Более 100 000 000 жителей России** пользуются различными услугами компании

ЦОДы национальной облачной платформы РТК:

- Москва М9 (Бутлерова, 7);
- Москва М10 (Сущевский вал, 26);
- Новосибирск (Менделеева, 1);
- Сочи (Ленина, 2).

ЦОДы ПАО «Ростелеком»

26 ЦОДов в 7 межрегиональных филиалах.

Кабельная станция
Точка присутствия
Узел доступа

TEA-1
TEA-2
TEA-3
TEA-4
FASTLINE
EPEG
Terrestrial network

Облачные сервисы

Защита электронной почты

В основе услуги лежит решение класса Secure Email Gateway, предоставляющее эффективные механизмы противодействия распространению СПАМа, вредоносного программного обеспечения и фишинга по почтовому каналу коммуникаций.

Защита от сетевых угроз (UTM).

- межсетевое экранирование FW;
- межсетевое экранирование и обнаружение/предотвращение вторжений (FW + IPS);
- комплексное решение (UTM), включающее в себя:
  - межсетевое экранирование на уровне сети
  - обнаружение/предотвращение вторжений
  - фильтрацию трафика веб-приложений
  - контроль использования приложений
  - защиту от вредоносного ПО

Облачные сервисы

Защита Веб-приложений (WAF)

Межсетевой экран уровня приложений, позволяющий детектировать и блокировать атаки, направленные на веб-приложения.

- Фильтрация сетевого трафика Веб-приложений Клиента на стороне Оператора с целью его анализа на прикладном уровне.
- Создание индивидуального профиля защиты для каждого Веб-приложения Клиента, обучение и настройка WAF для обеспечения корректной фильтрации трафика.
- Корректировка индивидуальных профилей защиты в случае выявления некорректных срабатываний, изменения состава/функционала Веб-приложений или по запросу Клиента.

Защита от DDoS - атак

Выявление и предотвращение DDoS-атак из сети Интернет или региональной сети на защищаемые информационные ресурсы.
Индивидуальный профиль защиты для каждого клиента.

Особенности услуги:

- Выделенная круглосуточная смена по отражению DDoS атак (возможность отражения атак в автоматическом и ручном режиме)
- Индивидуальный профиль защиты для каждого клиента
- Стоимость услуги не зависит от мощности и количества DDoS-атак
- Интеграция с защитным комплексом операторского класса Ростелеком Arbor Peakflow - опция Cloud-signaling

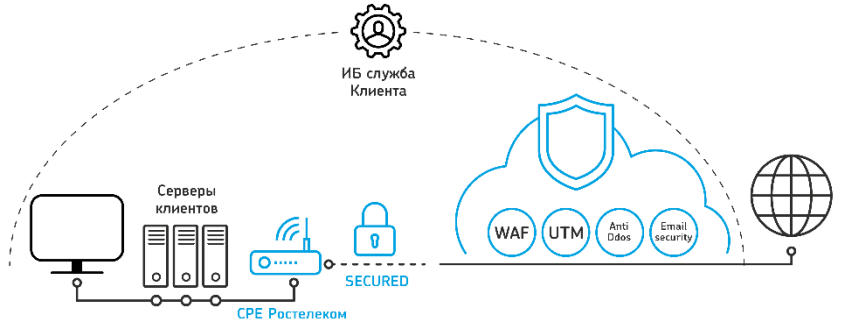
Варианты подключения услуги:

Комплексный подход:

Информационные системы и инфраструктура заказчика располагаются в виртуальном ЦОД Ростелекома.

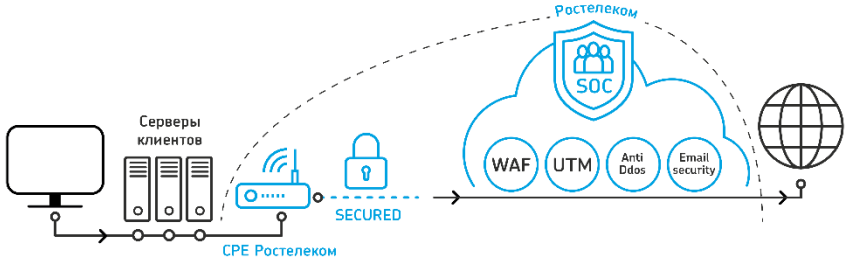
Аренда (Самообслуживание):

Информационные системы и инфраструктура располагаются на площадке заказчика, а защита — в Telco Cloud, под управлением службы информационной безопасности заказчика.



Управляемые сервисы безопасности (Эксплуатация сотрудниками Ростелеком):

Информационные системы и инфраструктура располагаются на площадке заказчика, а защита — в Telco Cloud.



Security Awareness

Управление навыками информационной безопасности

Почему сотрудники открывают письма?

Векторные атаки:

Корпоративные

- Приглашение на социальные/профессиональные активности внутри компании
- Реалистичные корпоративные письма
- Шаблоны «от партнеров» и т.д.

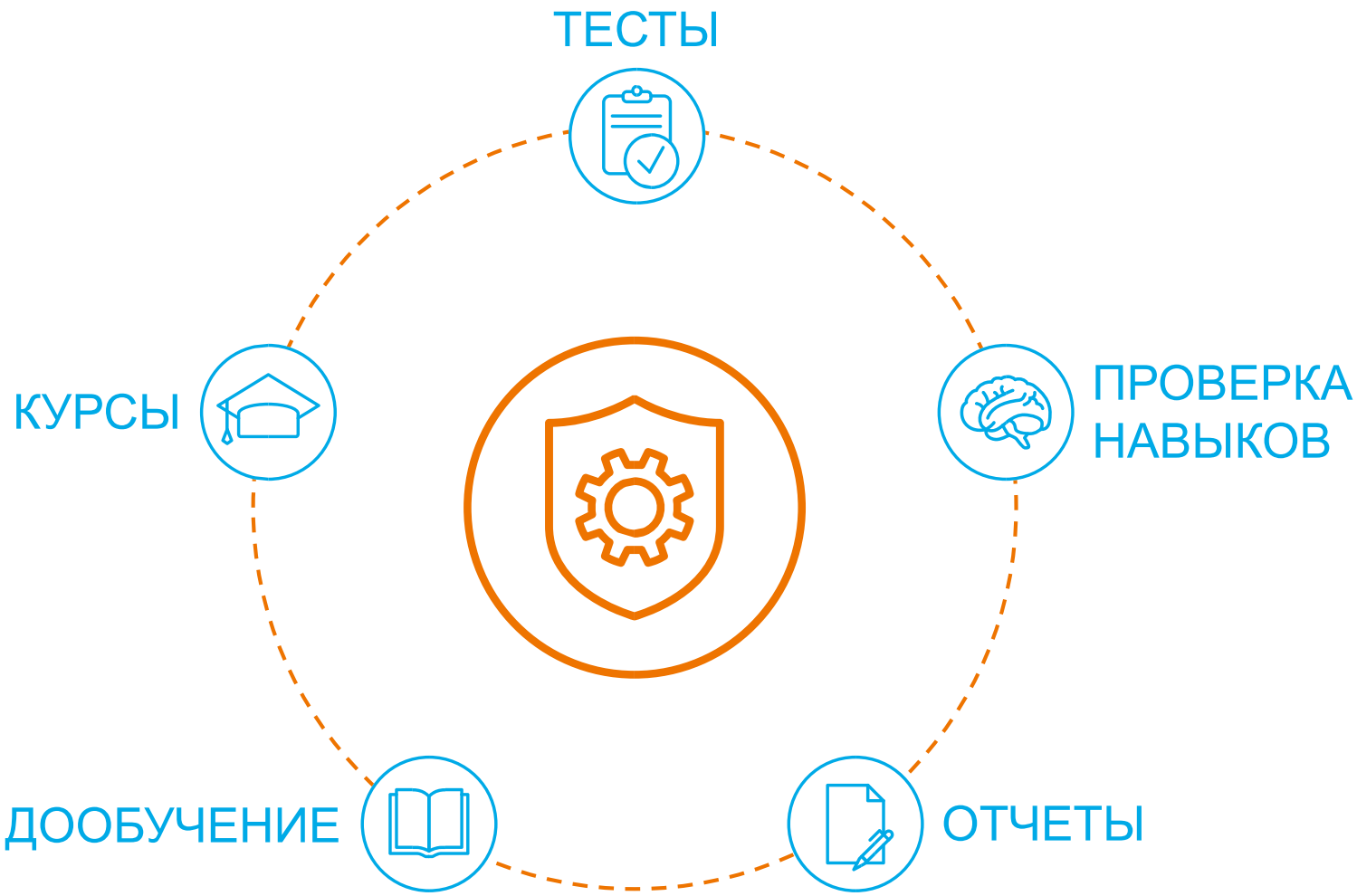
Организационные

- Уведомление из «налоговой»
- Обучение в профессиональной области
- «Уведомление» об изменении законодательства и т.д.

Личные

- Уведомление о штрафе
- Розыгрыш билетов
- «Отписка» от спам-рассылки

Решение: Обучить пользователей и контролировать их навыки в учебных атаках



СОСТАВ ПРЕДЛАГАЕМОГО СЕРВИСА

ПЕРВИЧНОЕ ТЕСТИРОВАНИЕ И СТАТИСТИКА

Предоставление отчёта по уязвимостям пользовательского программного обеспечения, которые идентифицируются в результате действий персонала во время тестирования и могут эксплуатироваться злоумышленником для развития атаки

ПЛАНИРОВАНИЕ И ОБУЧЕНИЕ

Согласование значимых действий с выделенными сотрудниками заказчика, обучение навыкам работы с платформой повышения осведомленности

АКТУАЛИЗАЦИЯ

Ежемесячная разработка четырех шаблонов имитации атак на пользователей с учётом особенностей и должностных обязанностей каждой группы тестируемых пользователей

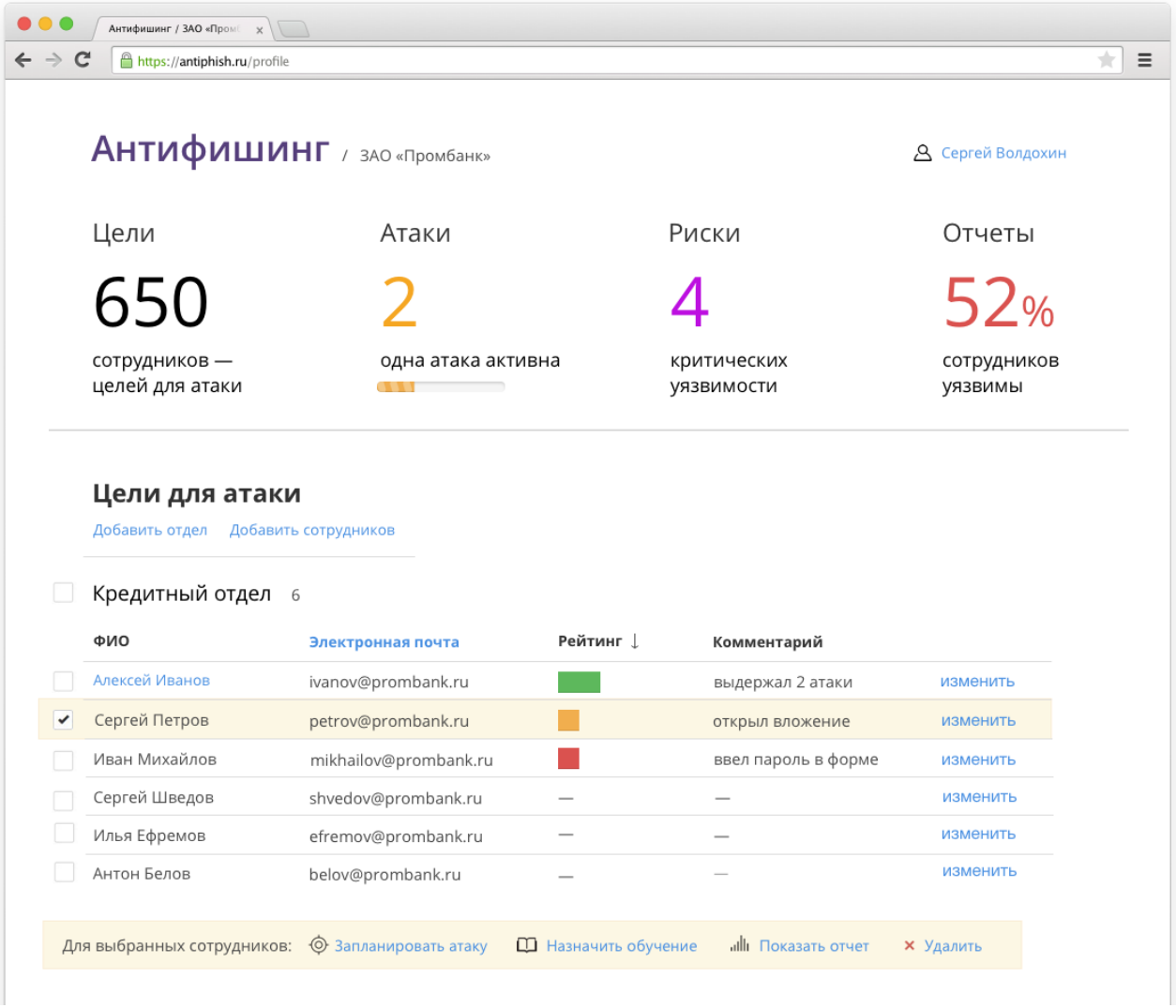
ПОДДЕРЖКА

Автоматизация и поддержка процесса дистанционного обучения и тестирования навыков выбранных групп пользователей с учётом изменений, происходящих в организации

ОТЧЕТНОСТЬ

Предоставление ежемесячной отчётности по текущему уровню навыков персонала и их изменениям с учётом предыдущих периодов

Итоги


Антифишинг / ЗАО «Промбанк»
https://antiphish.ru/profile
Антифишинг / ЗАО «Промбанк»
Сергей Волдохин
Цели
650
сотрудников — целей для атаки
Атаки
2
одна атака активна
Риски
4
критических уязвимости
Отчеты
52%
сотрудников уязвимы
Цели для атаки
Добавить отдел
Добавить сотрудников
Кредитный отдел 6
ФИО
Электронная почта
Рейтинг
Комментарий
Алексей Иванов ivanov@prombank.ru выдержал 2 атаки изменить
Сергей Петров petrov@prombank.ru открыл вложение изменить
Иван Михайлов mikhailov@prombank.ru ввел пароль в форме изменить
Сергей Шведов shvedov@prombank.ru — — изменить
Илья Ефремов efremov@prombank.ru — — изменить
Антон Белов belov@prombank.ru — — изменить
Для выбранных сотрудников:
Запланировать атаку
Назначить обучение
Показать отчет
Удалить

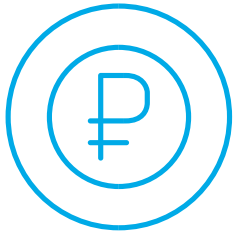
Зачем?

БЕЗОПАСНОСТЬ

Обученные сотрудники действуют правильно в случае реальной атаки

КОНТРОЛЬ РИСКОВ

Служба безопасности видит точный процент и список уязвимых сотрудников



ЭКОНОМИЯ

Без ущерба при взломах и затрат на восстановление данных

КИИ (187-ФЗ)

Объекты и субъекты КИИ

КИИ – критическая информационная инфраструктура

Согласно п. 7 и 8 ст. 2 187 ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Субъекты КИИ

- Государственные органы
- Государственные учреждения
- Юридические лица
- ИП

Объекты КИИ

- Информационные системы
- Информационно-телекоммуникационные сети
- Автоматизированные системы управления

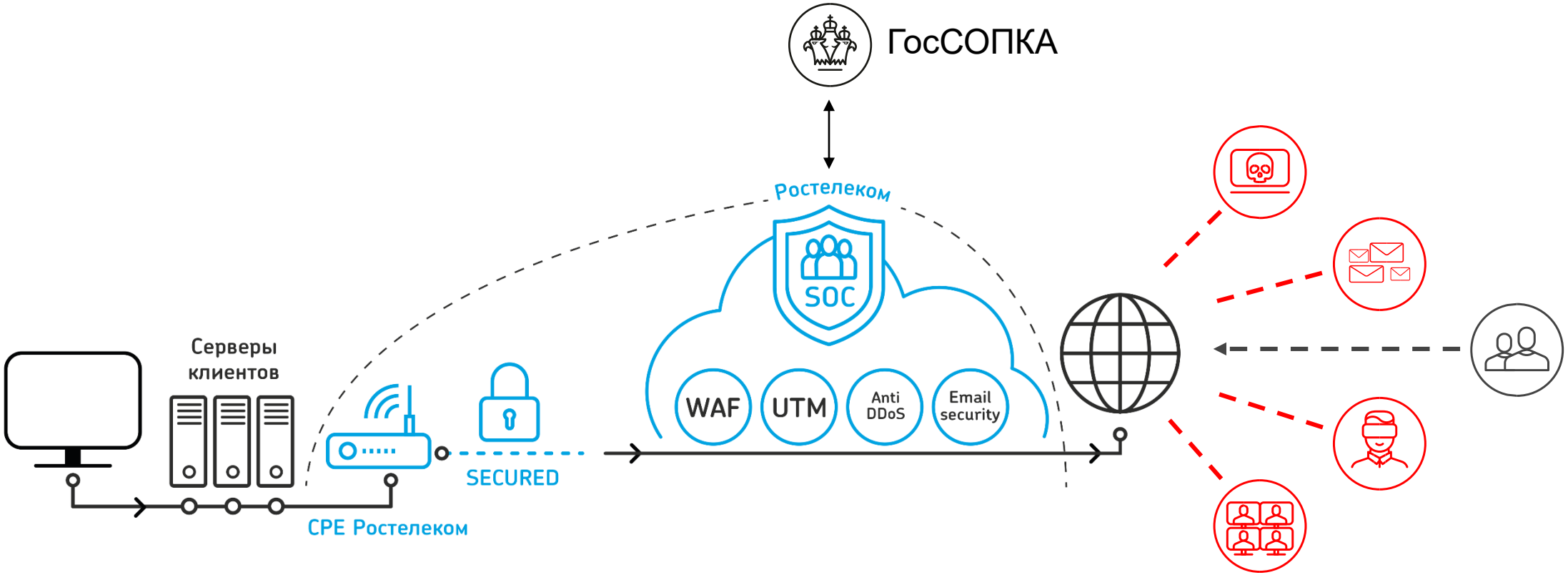
Работающие в отраслях

- Оборонная
- Ракетно-космическая
- Горно-добывающая
- Металлургическая
- Химическая
- Энергетика
- Атомная энергетика
- ТЭК
- Связь
- Банки
- Финансовая сфера
- Наука
- Транспорт
- Здравоохранение

Услуги по созданию системы безопасности

- Обследование (аудит) инфраструктуры
- Категорирование объектов КИИ
- Создание системы безопасности значимых объектов КИИ
- Оценка соответствия значимых КИИ
- Подключение всех объектов КИИ к ГосСОПКА

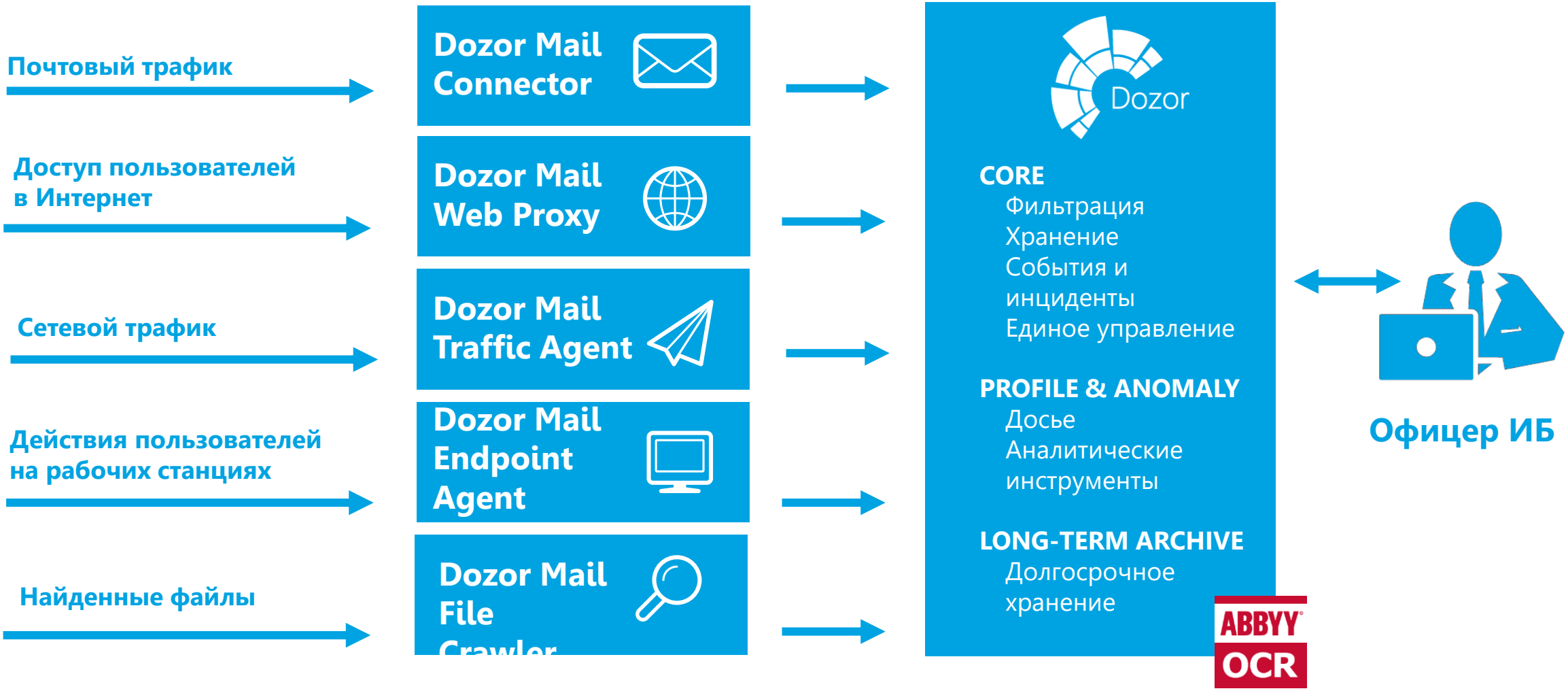
Подключение к ГосСОПКА через РТК SOC



DLP Solar Dozor

Что делает Solar Dozor?

Средство информационной безопасности для предотвращения утечек конфиденциальной информации за пределы корпоративной сети



Solar inRights

Solar inRights. Предпосылки

IGA – Identity Governance & Administration, системы **управления** цифровыми Id и **доступом**, развитие систем IdM

IGA-платформа для **автоматизации** полного спектра **процессов** управления жизненным циклом **пользователей**, **ролей**, **ресурсов**, оргструктуры

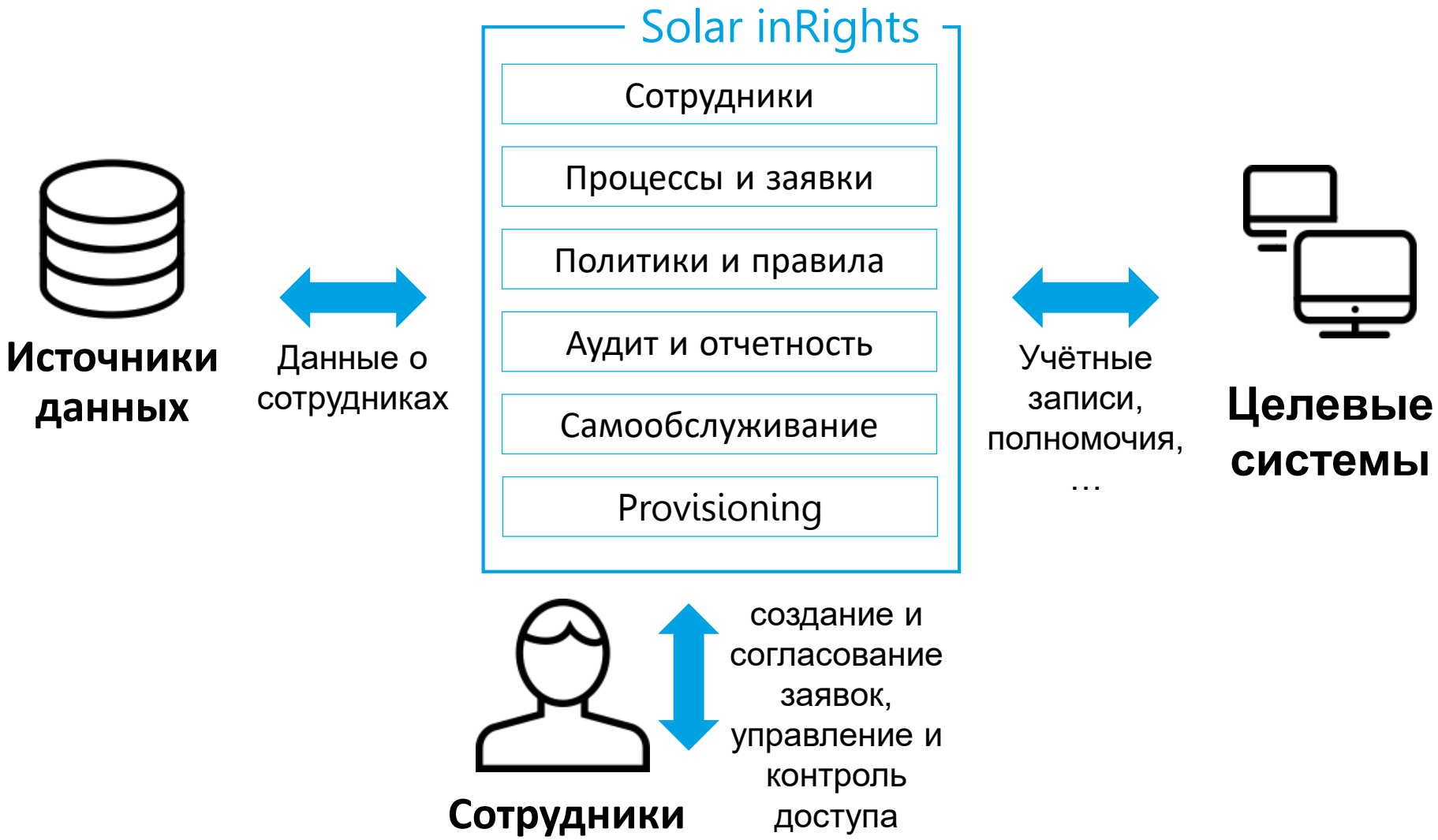
- Большой штат сотрудников
- Развитая инфраструктура
- Сложные бизнес-процессы

делают ручное управление и контроль доступа неэффективным и непрозрачным

Возможности

	Solar inRights	Системы IdM
Подача,согласование и автоматическое исполнение заявок на доступ	+	+
Управление заявками: групповые заявки, разбиение заявок, частичное согласование	+	+/-
Добавление новых типов процессов/заявок,например, процесс управления паролями	+	-
Управление правами совместителей отдельно для каждой совмещаемой должности	+	-
Управление учётными записями в информационных системах	+	+
Управление папками,группами и другими объектами информационных систем	+	-
Управление технологическими учётными записями	+	-

Как это работает?



Достоинства

прозрачный процесс управления доступом

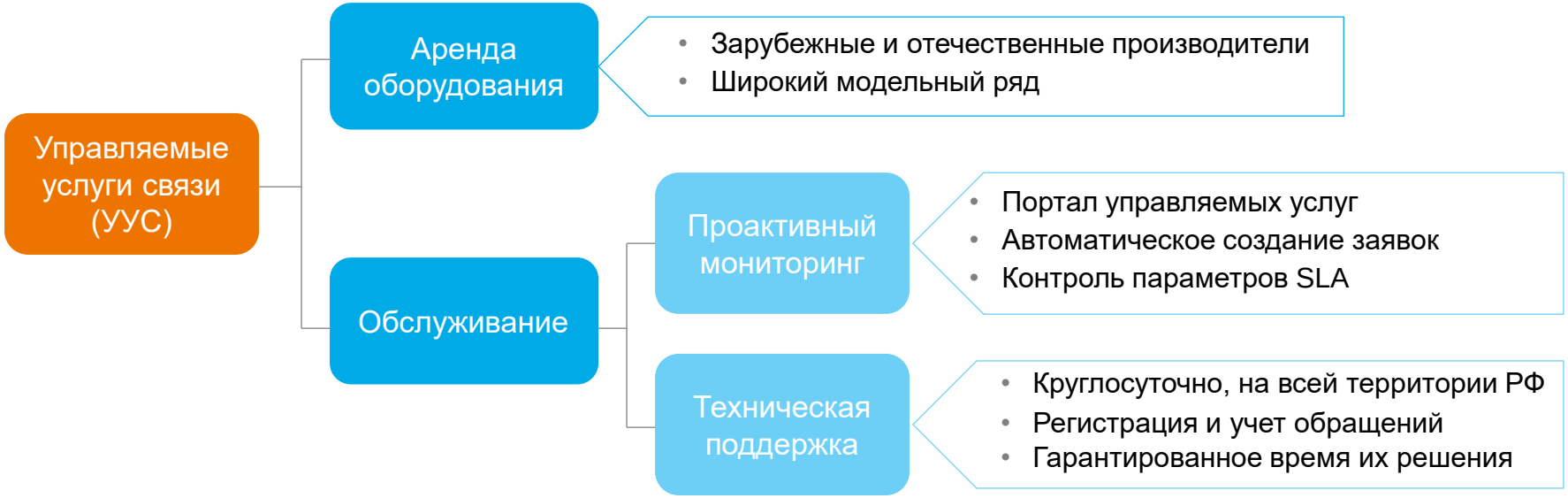
порядок в информационных системах

автоматизация большого объёма ручного труда по управлению доступом и аудиту

yyc

Что такое УУС?

Это комплексное решение, включающее в себя аренду сетевого оборудования,
а также услуги по управлению оборудованием, на котором строится вся сетевая инфраструктура.



CISCO

hp

JUNIPER NETWORKS

FORTINET

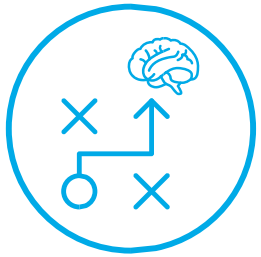
Check Point SOFTWARE TECHNOLOGIES LTD.

infotecs

КОД БЕЗОПАСНОСТИ

Pentest

Pentest



Что это?

Тестирование на проникновение

Как?

- Сбор информации об ИС Заказчика
- Поиск и анализ уязвимостей
- Атака, эксплуатация уязвимостей с целью получить доступ к системе или повысить привилегии пользователя
- Отчет о результатах тестирования

Да, кому это все интересно…

Актуальные тенденции

Уязвимостей и атак все больше

- Целевые и массовые атаки (WANNACRY, NOTPETYA и пр.)
- Утечки данных (UBER, HBO, EQUIFAX и пр.)
- Вредоносный майнинг
- DDoS – атаки
- IoT/Big Data/Blockchain

Усиливаются требования к ИБ

- Защита государственных информационных систем
- Защита КИИ и ГосСОПКА
- Импортозамещение
- Цифровая экономика (направление ИБ)

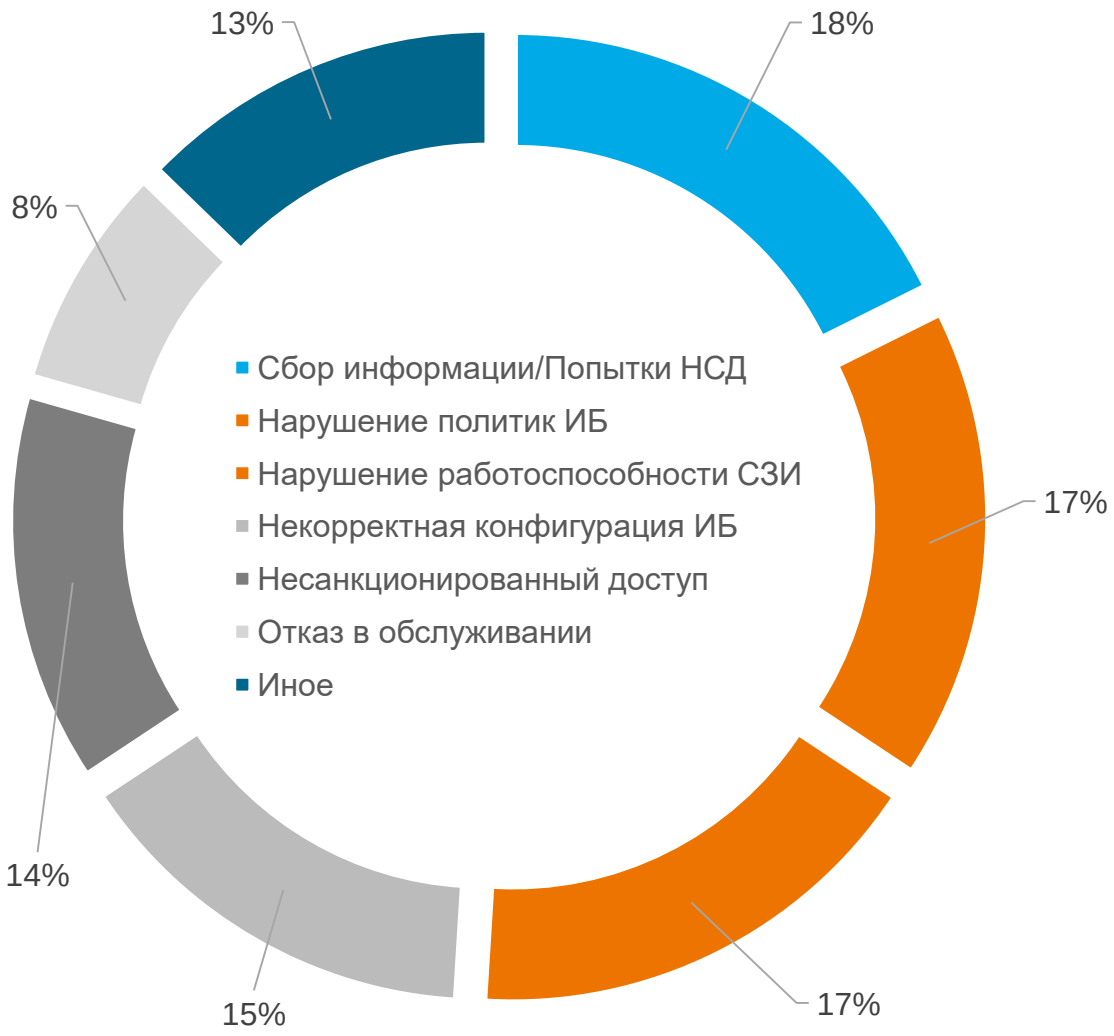
Сводная статистика за отчетный период

2,5 млрд

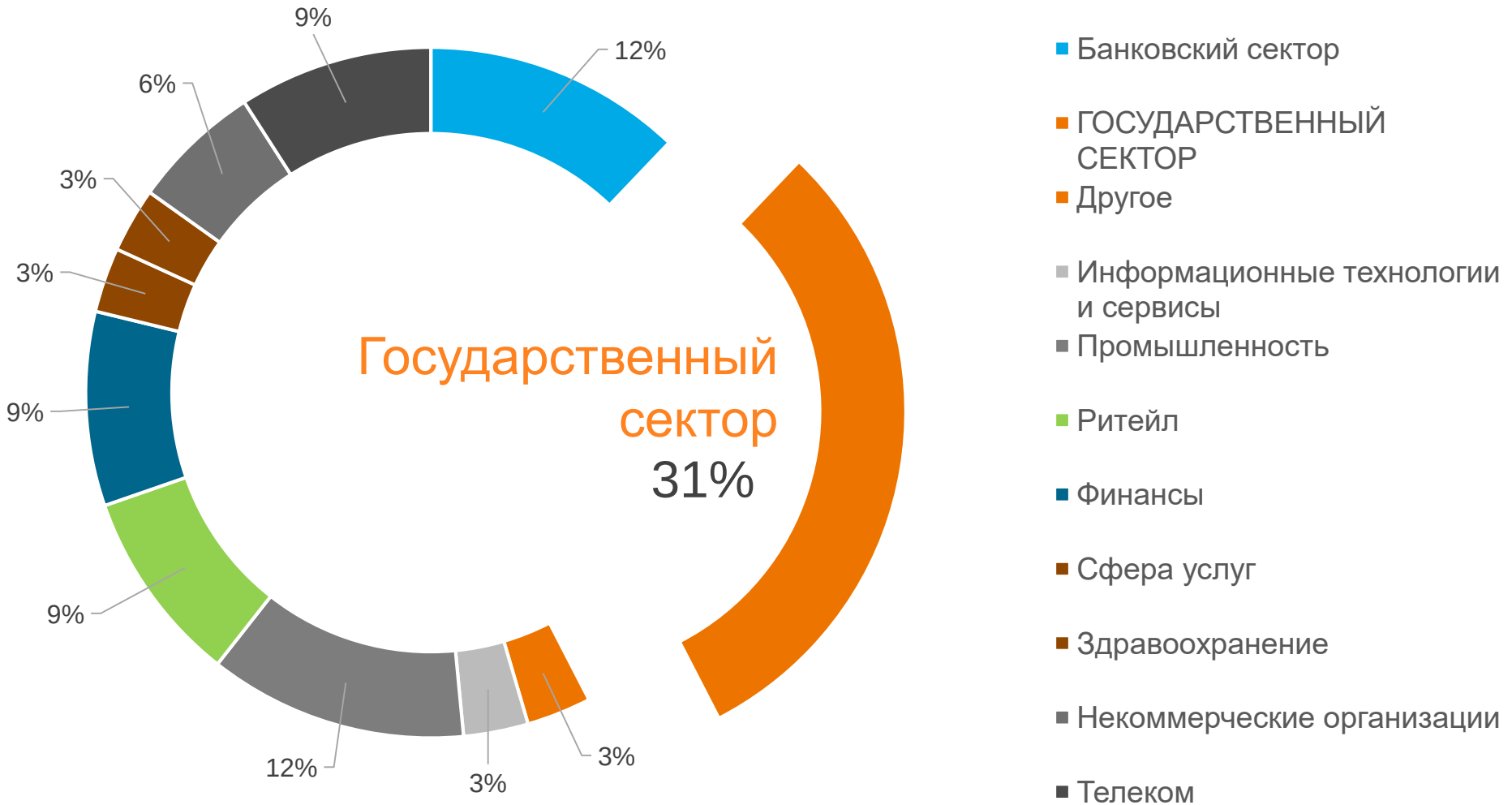
Среднесуточное число подозрительных событий ИБ, обрабатываемых SIEM-системами ПАО “Ростелеком”

1137

Инцидентов ИБ зафиксированных за первый квартал 2018 года в ПАО “Ростелеком”



Распределение инцидентов по отраслям



Сервисы информационной безопасности

Security Operations Center

Защита веб ресурсов

Compliance

Security awareness

Облачные сервисы ИБ

Защита каналов передачи данных

Защита мобильный устройств

Тестирование на проникновение

РОСТЕЛЕКОМ — ПРОВОДНИК В ТЕМНЫХ ТУННЕЛЯХ ЦИФРОВОЙ ЭКОНОМИКИ