SOLAR Rostelecom

Ростелеком

Анализ поведения пользователей

Что это и как это работает?

Санкт-Петербург

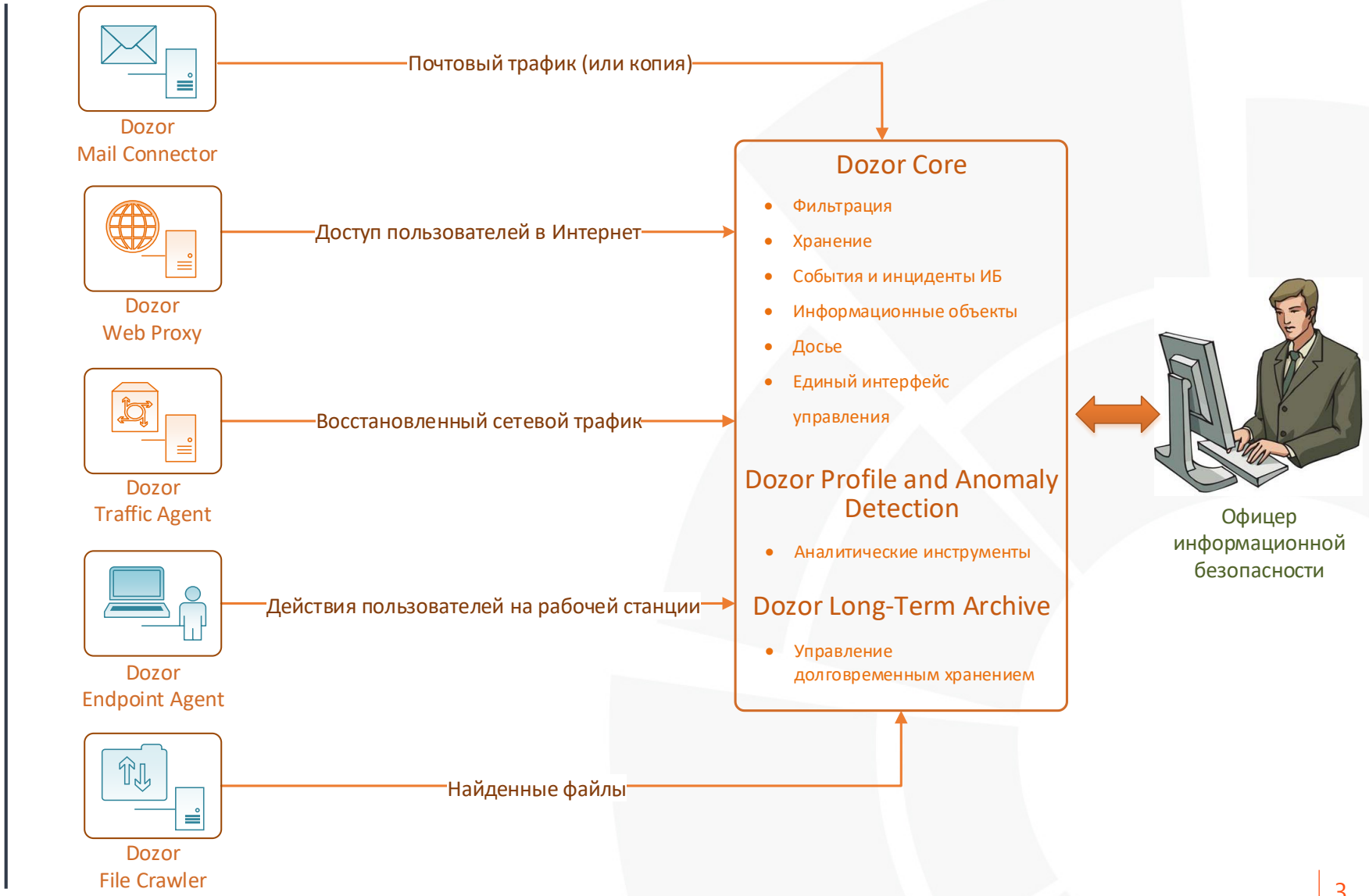
12 ноября, 2018

Все знают, что такое DLP

- Защита от утечек данных
- Контроль корпоративных коммуникаций

Концептуальная архитектура

Стандартные задачи DLP



Концептуальная архитектура

Стандартные задачи DLP

+

Аналитика

Dozor
Mail Connector

Почтовый трафик (или копия)

Dozor
Web Proxy

Доступ пользователей в Интернет

Dozor
Traffic Agent

Восстановленный сетевой трафик

Dozor
Endpoint Agent

Действия пользователей на рабочей станции

Dozor
File Crawler

Найденные файлы

Dozor Core

- Фильтрация
- Хранение
- События и инциденты ИБ
- Информационные объекты
- Досье
- Единый интерфейс управления

Dozor Profile and Anomaly Detection

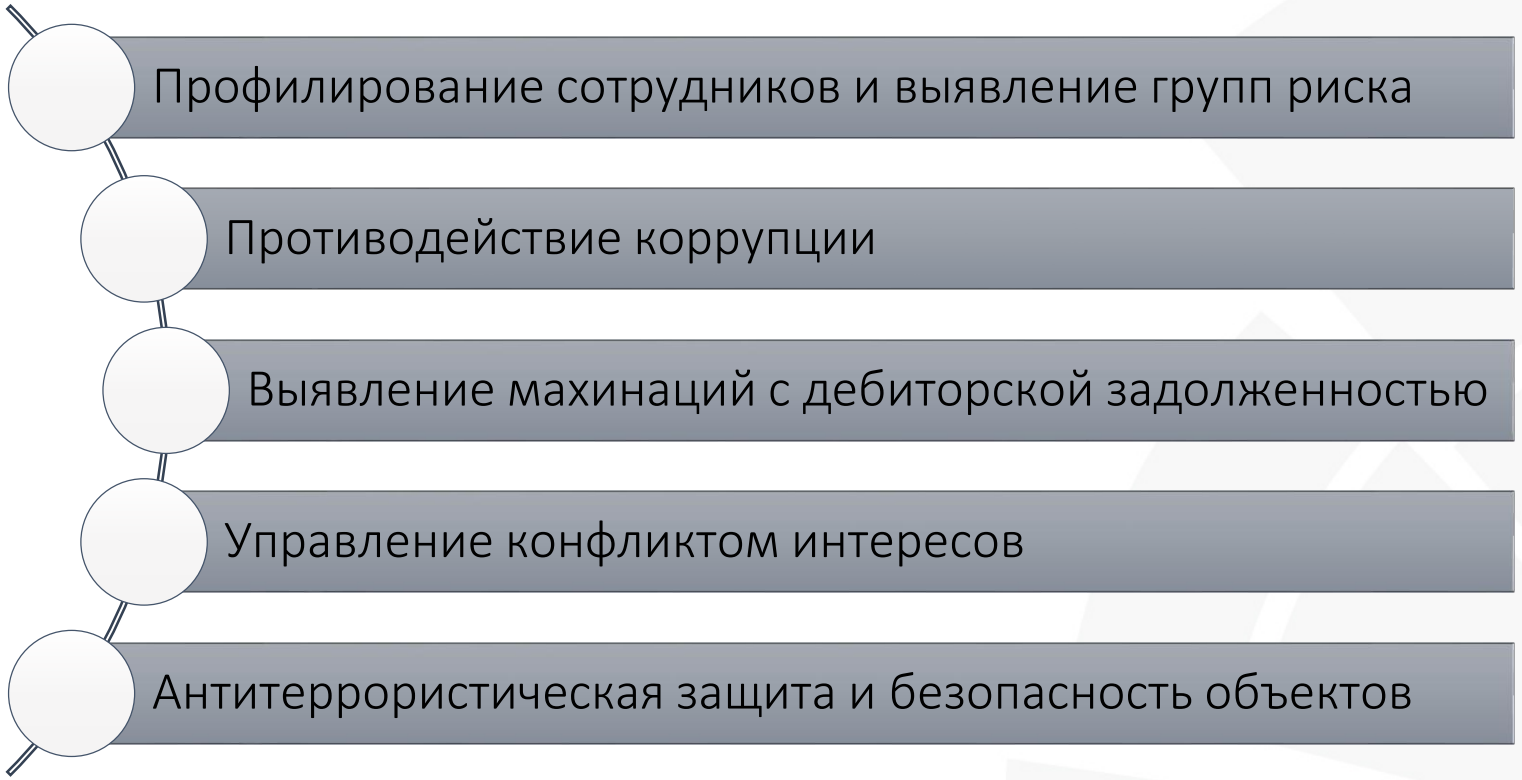
- Аналитические инструменты

Dozor Long-Term Archive

- Управление долговременным хранением

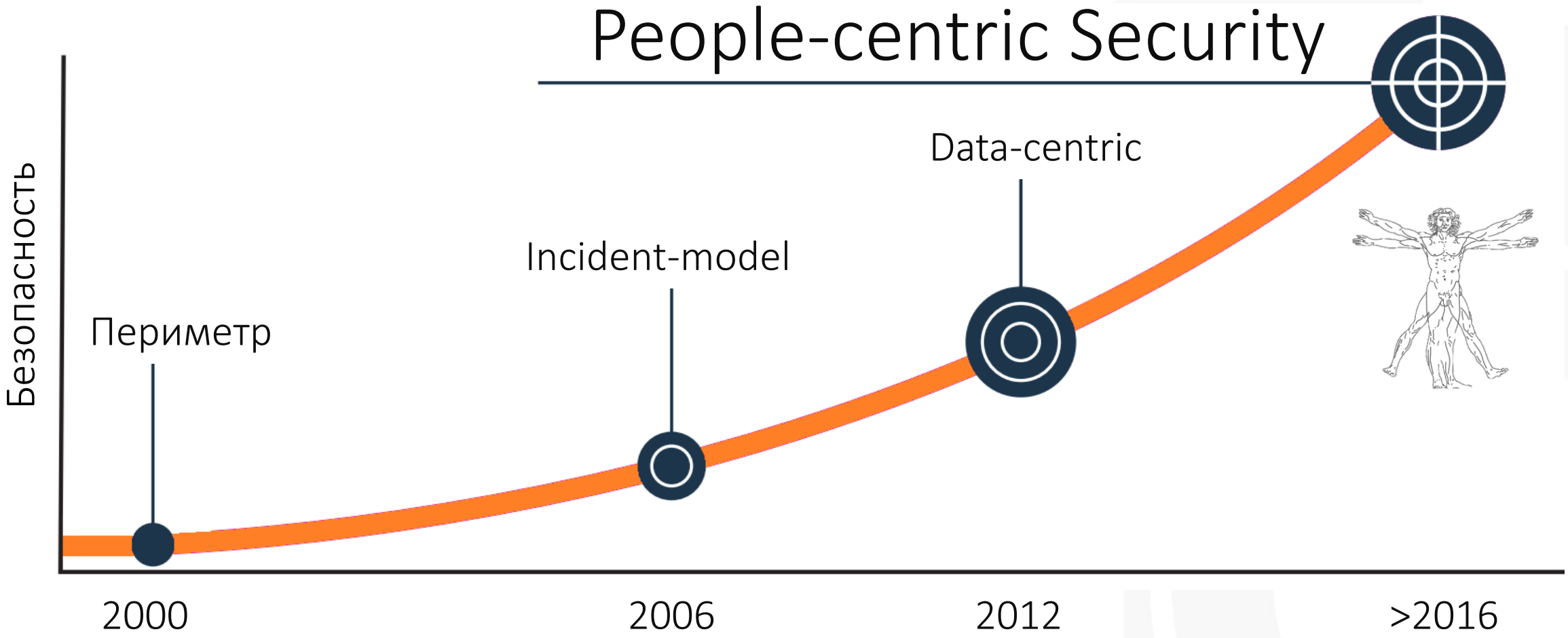
Офицер информационной безопасности

Новые области применения DLP

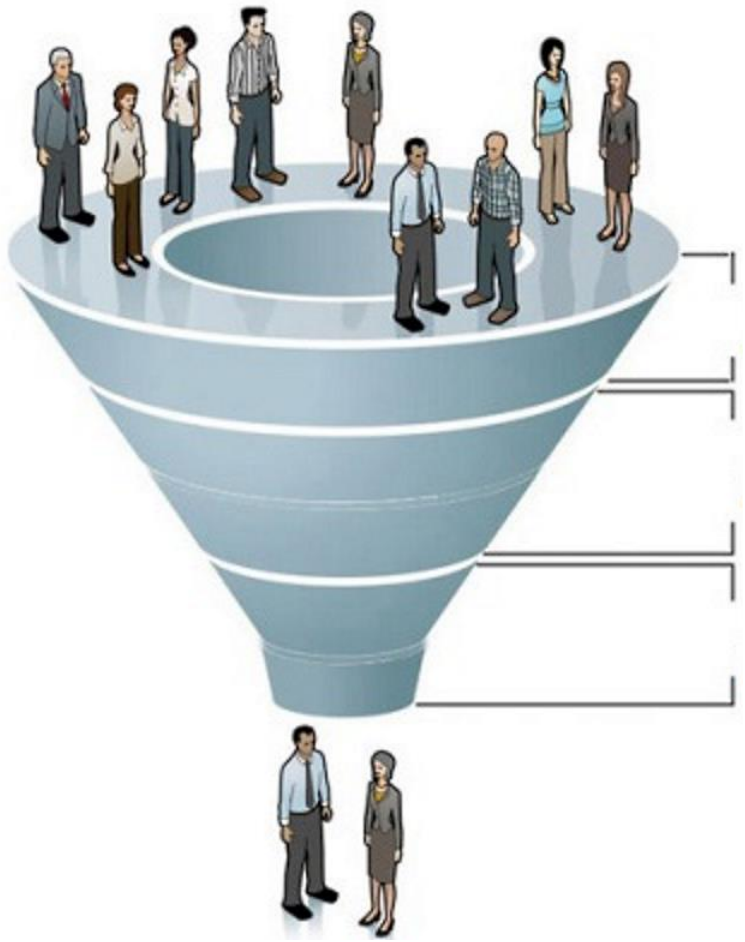


2 безопасника на 3000 сотрудников!

Next Generation DLP



Воронка профилактики



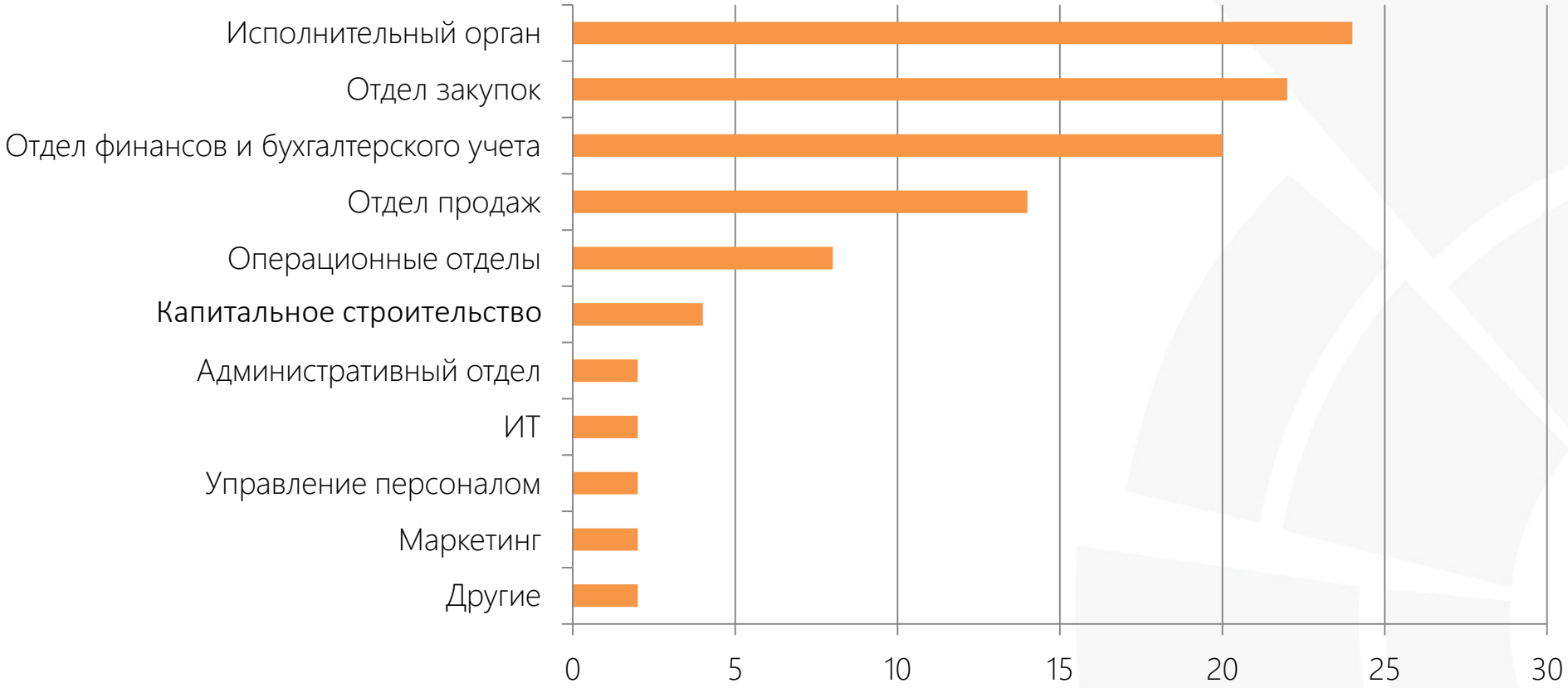
10% не нарушают никогда

80% нарушают в зависимости от обстоятельств

10% нарушают всегда

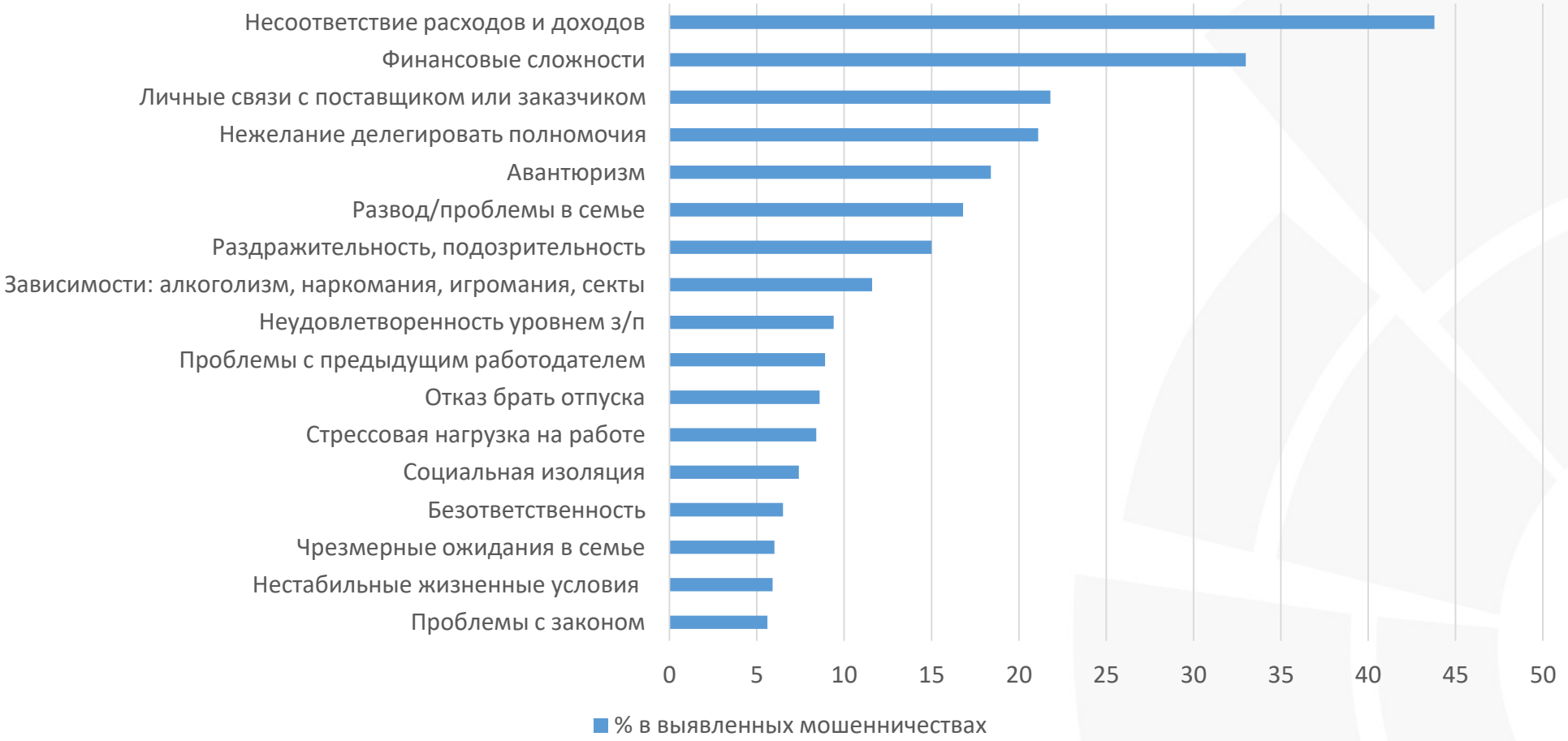
Группы риска

Рейтинг рисковых подразделений

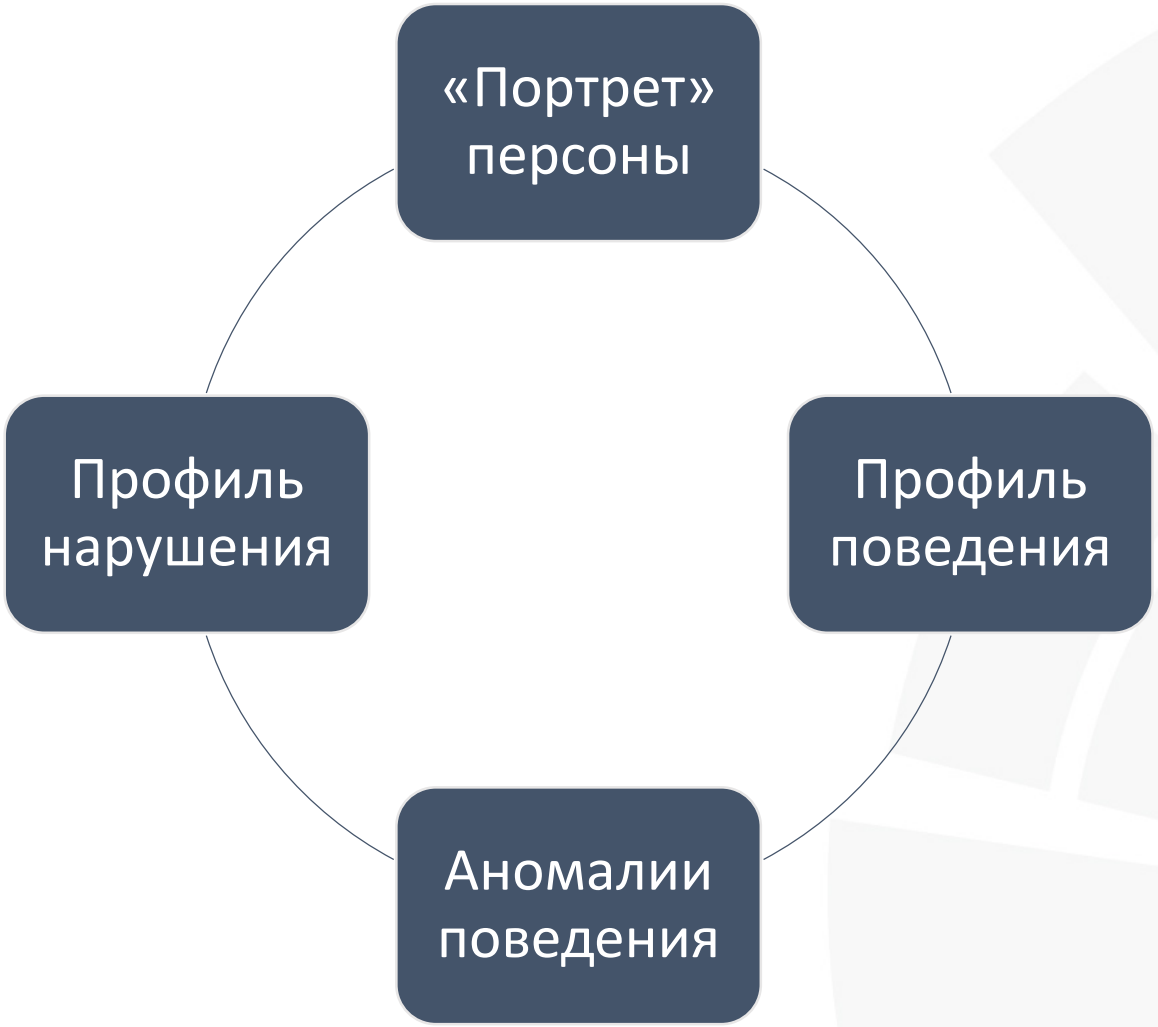


Группы риска

Поведенческие красные флажки



Анализ поведения пользователей

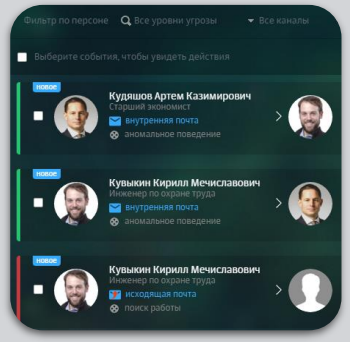


Портрет персоны

Портрет персоны. Досье

Информация

- Данные из внутренних систем
- Данные из внешних систем
- Заметки и приложенные файлы

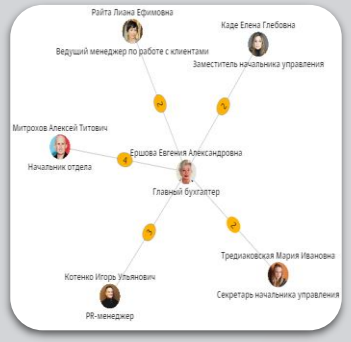


Нарушения

- Уровень доверия
- События и инциденты

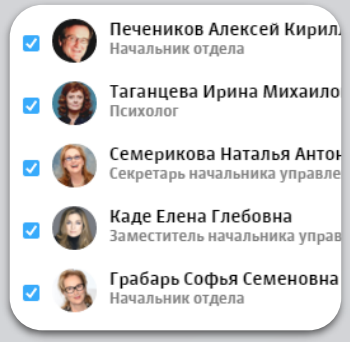
Коммуникации

- Карта коммуникаций по каналам
- Файлы, полученные и отправленные



Связи

- Внешние и внутренние контакты, домены
- Граф связей



Аномалии

- Контроль изменения уровня доверия
- Нехарактерные контакты

Портрет персоны

Рабочая станция:
Используемые приложения
Хранящиеся инф. активы
Создаваемые инф. активы
Считываемые/записываемые файлы
Файлы, копируемые на внешние носители и с внешних носителей

Мессенджеры:
Активность в мессенджерах
Передача инф. активов через мессенджеры

Интернет и внешние ресурсы:
Запросы в интернет
Посещаемые сетевые ресурсы
Входящий и исходящий трафик
Скачиваемые файлы
Публикации на внешних ресурсах
Считываемые/записываемых файлы «облачных» хранилищ

Активность в течение рабочего времени

Электронная почта:
Внутренняя переписка
Прием/получение внутренних писем
Внутреннее перемещение инф. активов
Внешняя переписка
Прием/получение внешних писем
Отправка вовне инф. активов
Получение извне инф. активов

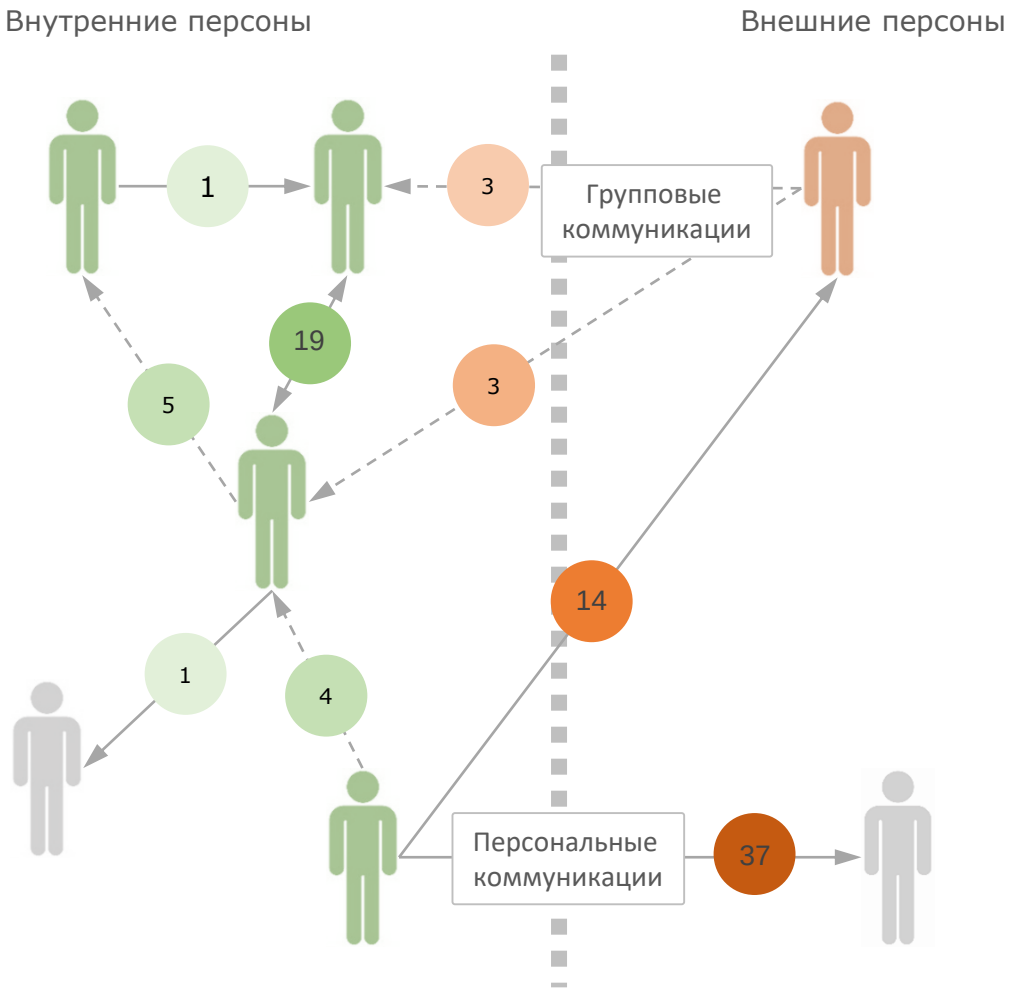
Внутренние информационные ресурсы:
Активность использования внутренних хранилищ
Считываемые/записываемые инф. активы
Публикации на внутренних ресурсах

Использование периферийных устройств:
Активность печати и использования МФУ
Отправка на печать и сканирование инф. активов

Профиль поведения персоны

Профиль контактов | Профиль трафика

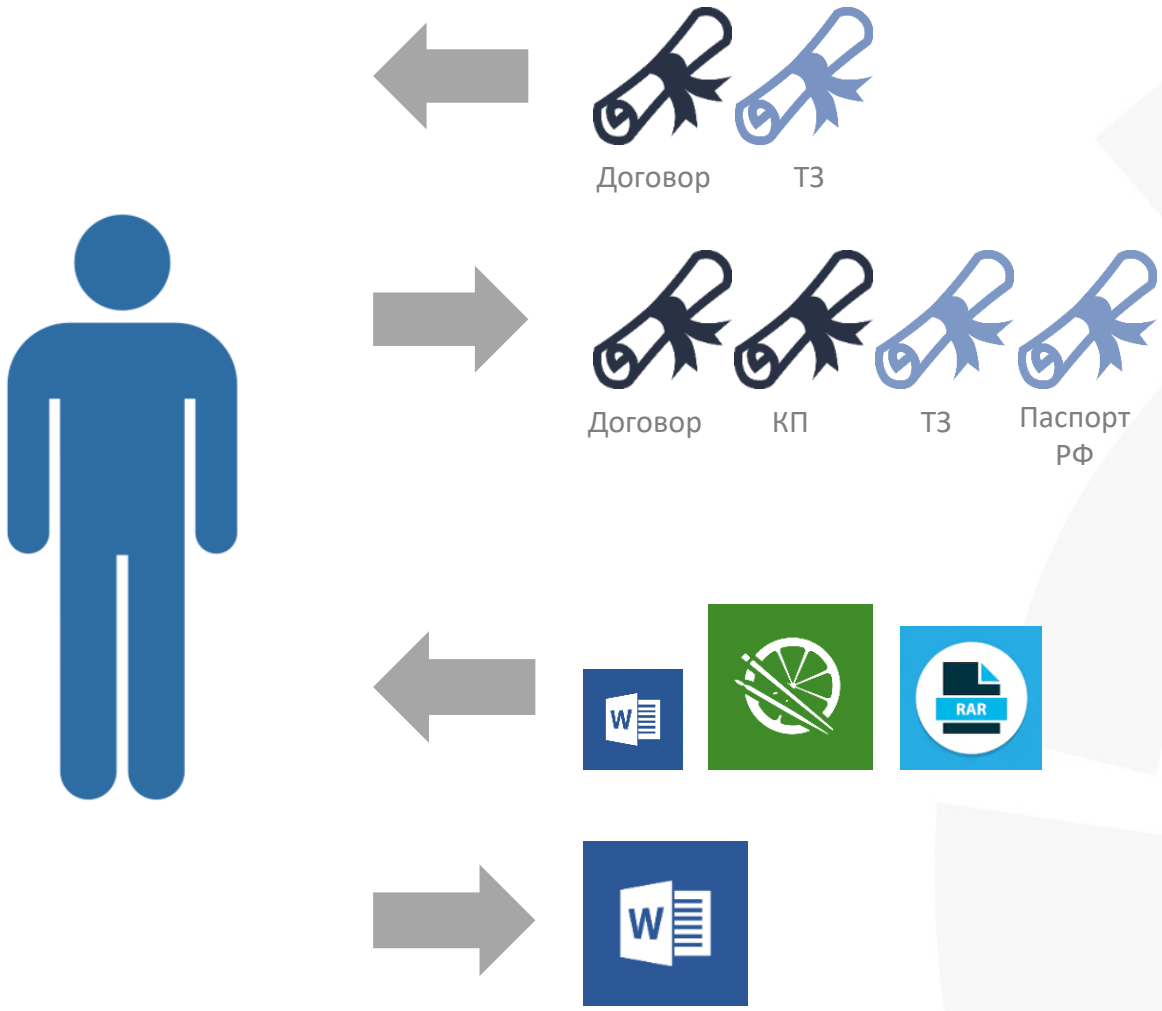
Основные свойства контактов



Круг общения по группам

Группы общения | Персональные связи | Опосредованные связи

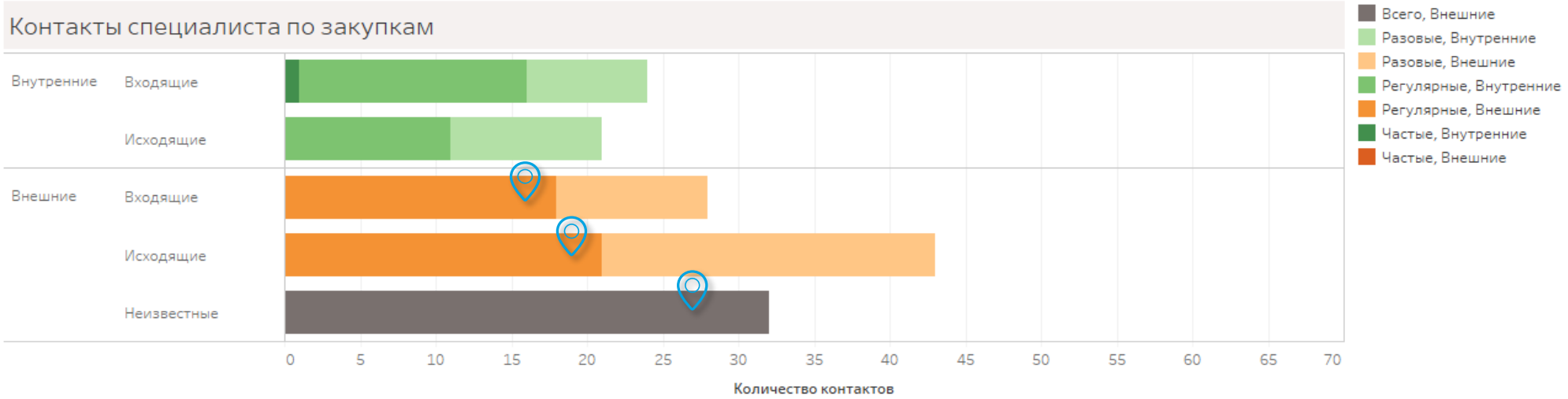
Отношение к информационным активам



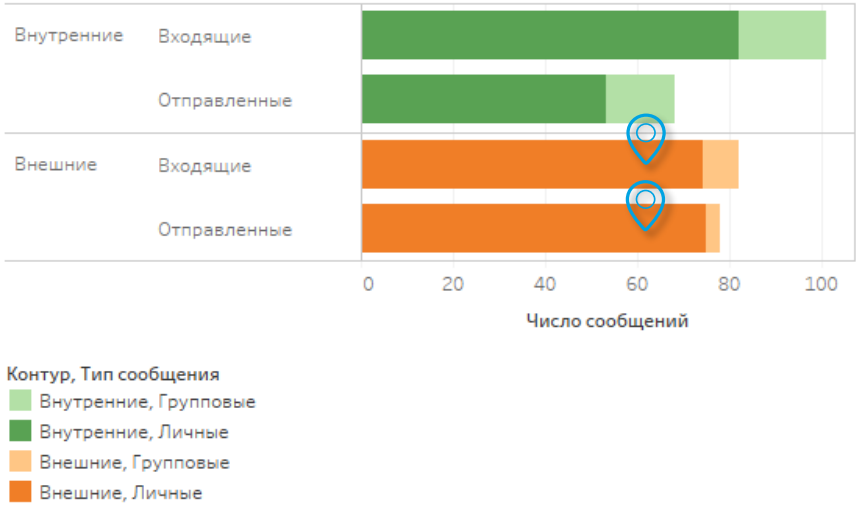
RTK-SOLAR

Профилирование по почтовому трафику

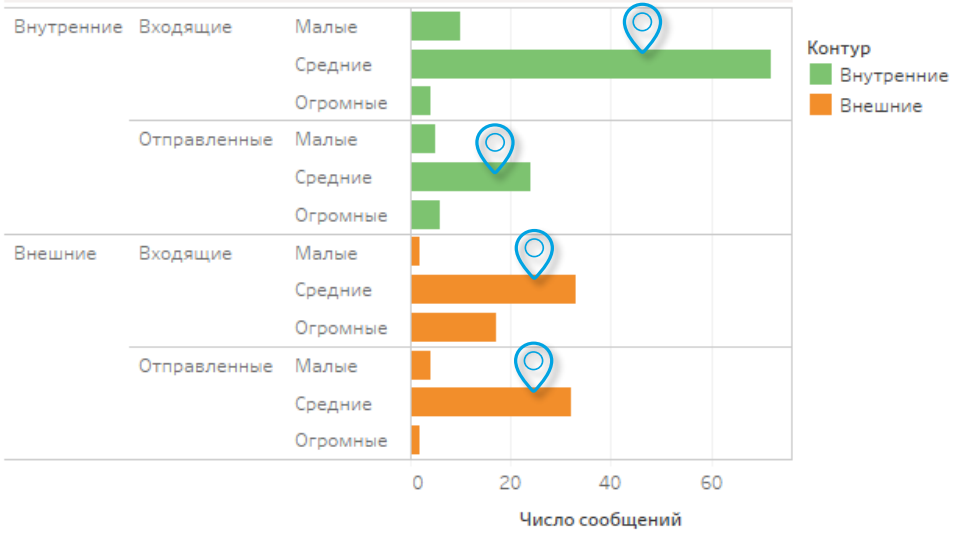
Контакты специалиста по закупкам



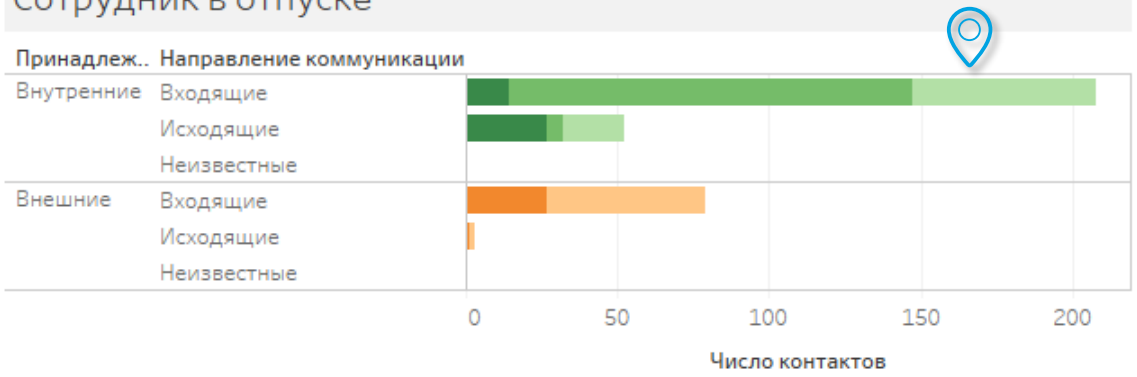
Сообщения специалиста по закупкам



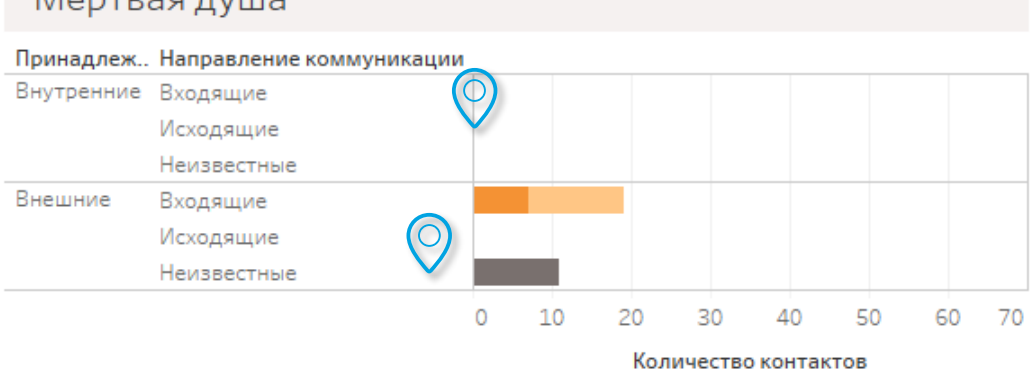
Трафик специалиста по закупкам



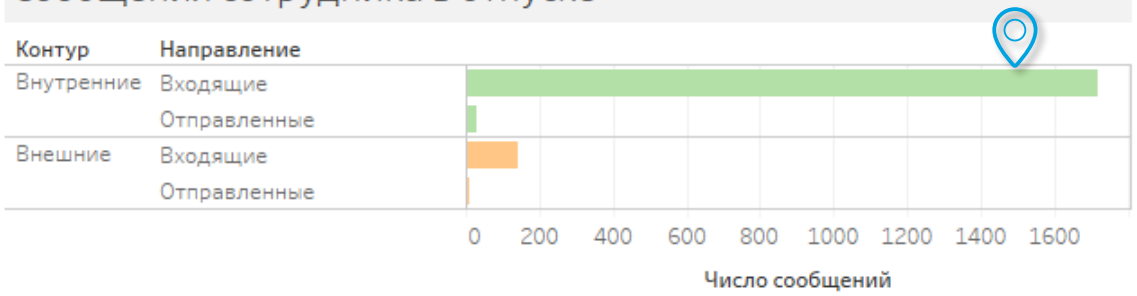
Сотрудник в отпуске



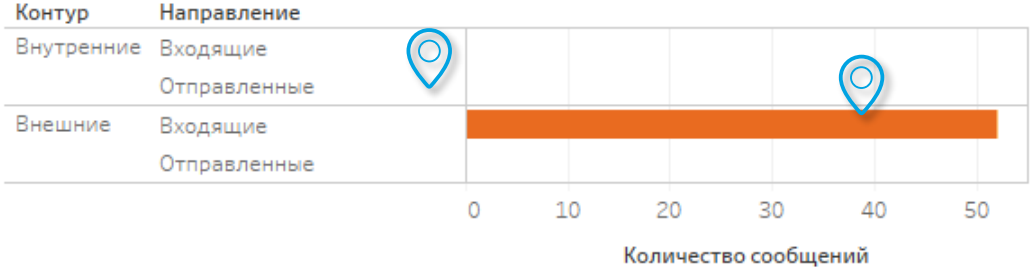
”Мертвая душа”

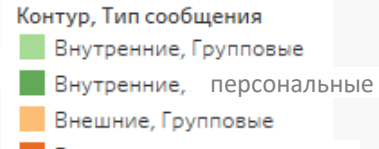


Сообщения сотрудника в отпуске

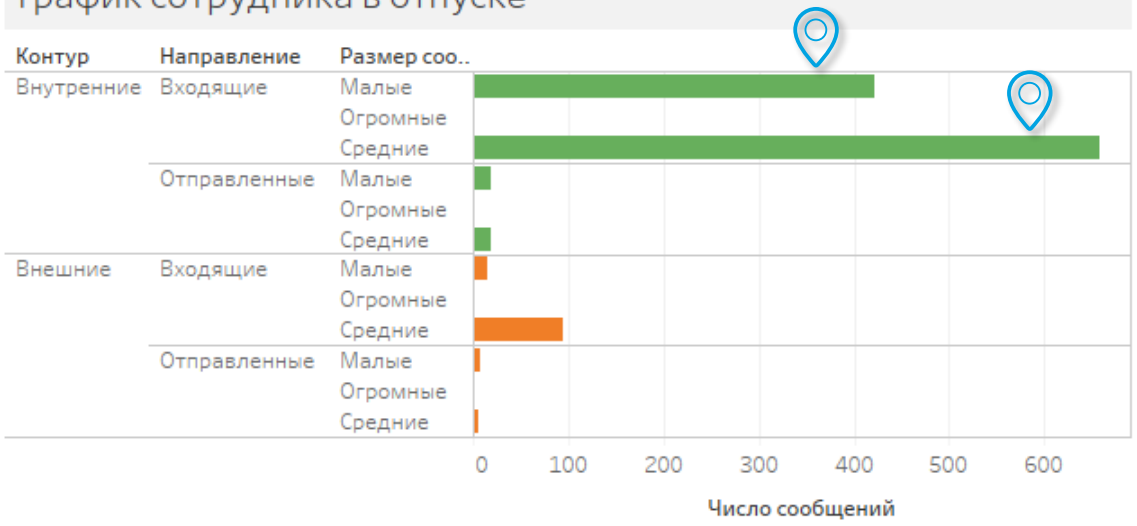


Сообщения ”мертвой души”

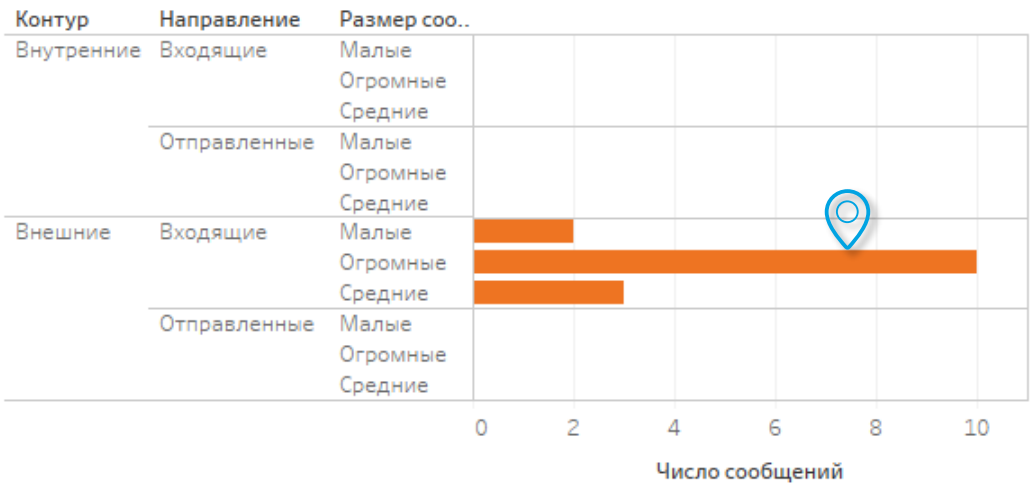


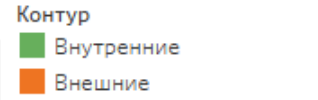


Трафик сотрудника в отпуске



Трафик ”мертвой души”

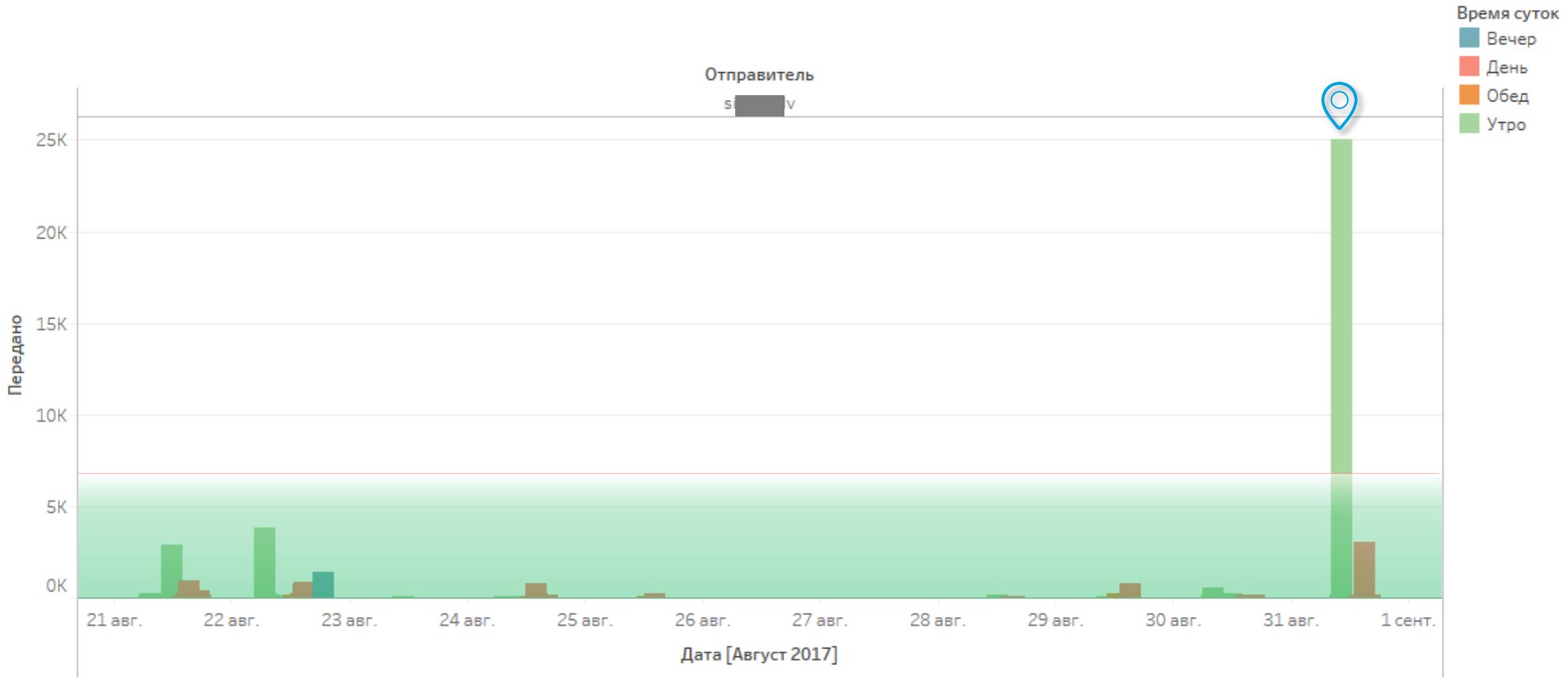




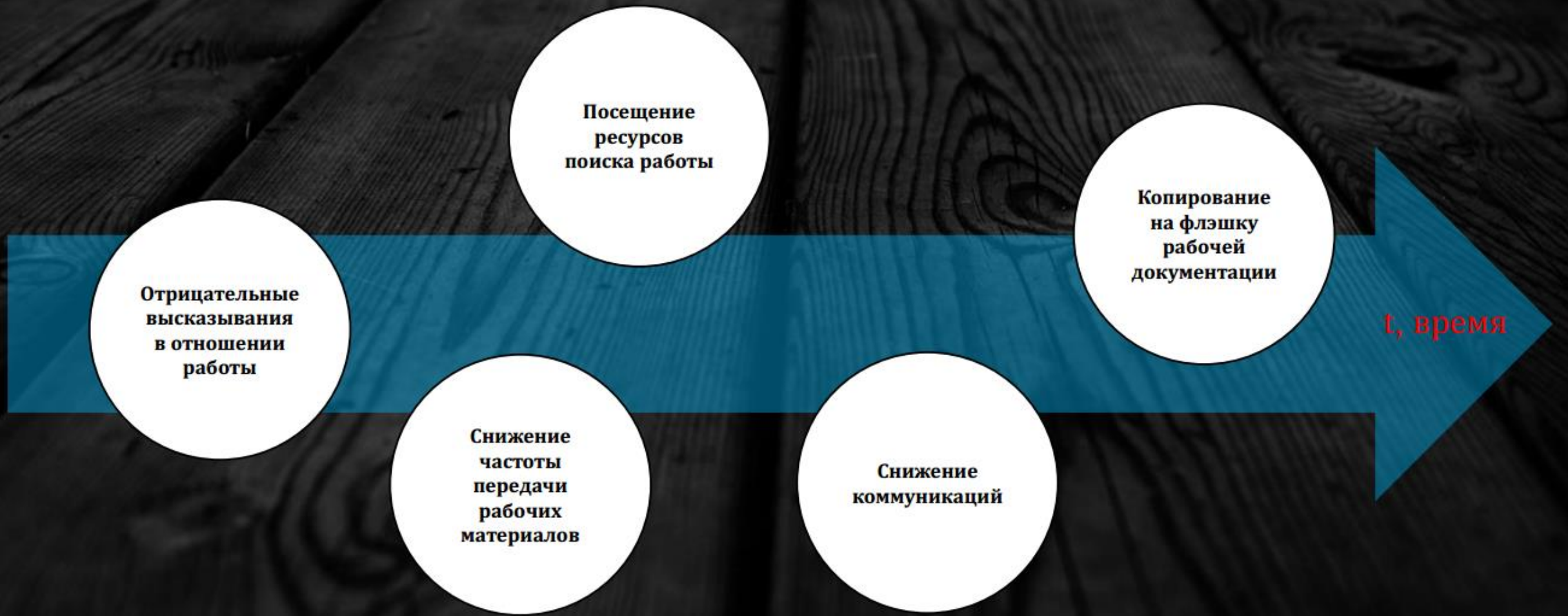
Аномалии поведения

kill chain

Аномалии трафика



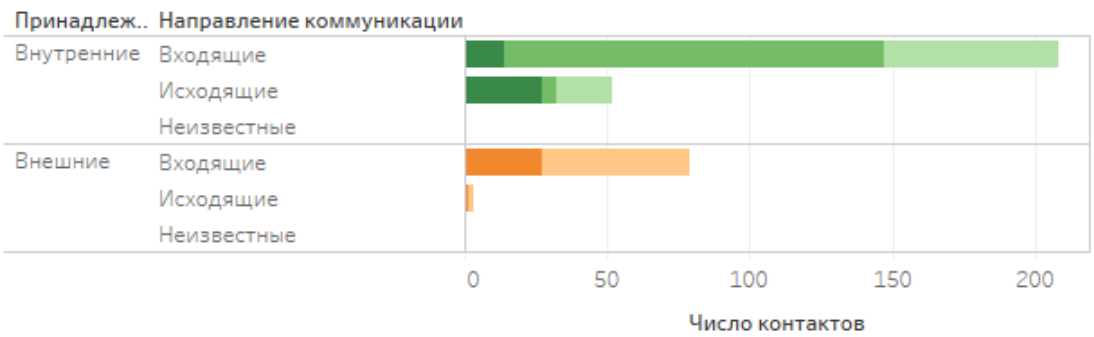
Case-ориентированные паттерны



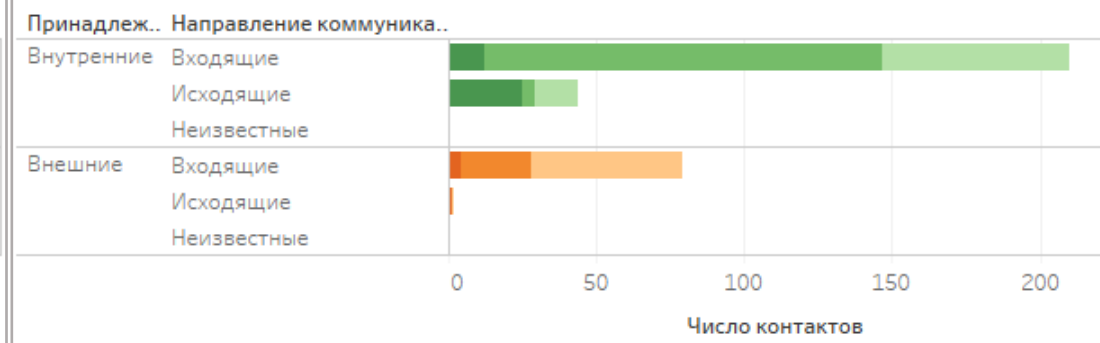
Профиль поведения

Поиск похожих

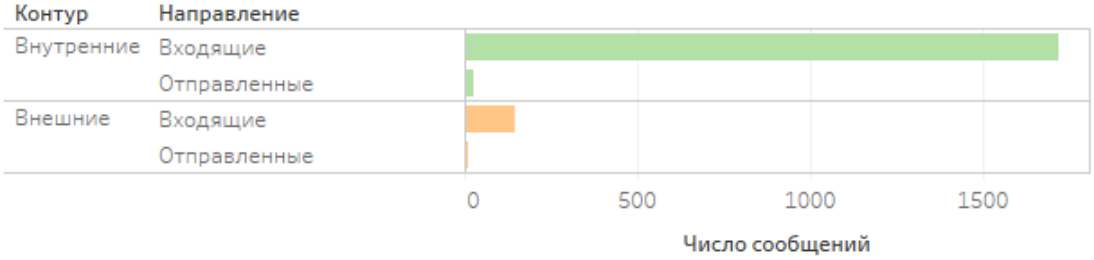
Сотрудник в отпуске



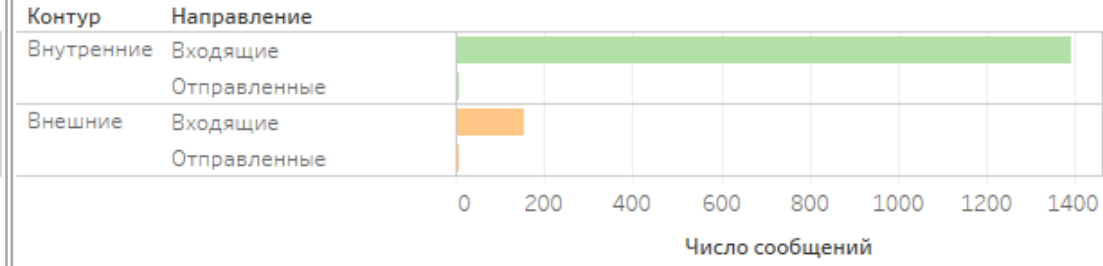
Сотрудник в отпуске 2

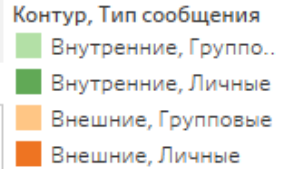


Сообщения сотрудника в отпуске

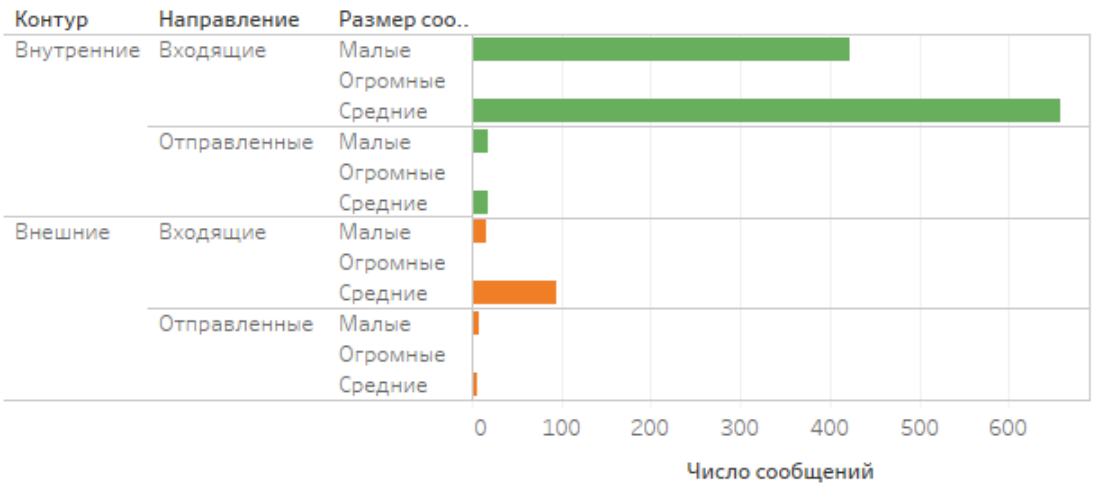


Сообщения сотрудника в отпуске 2

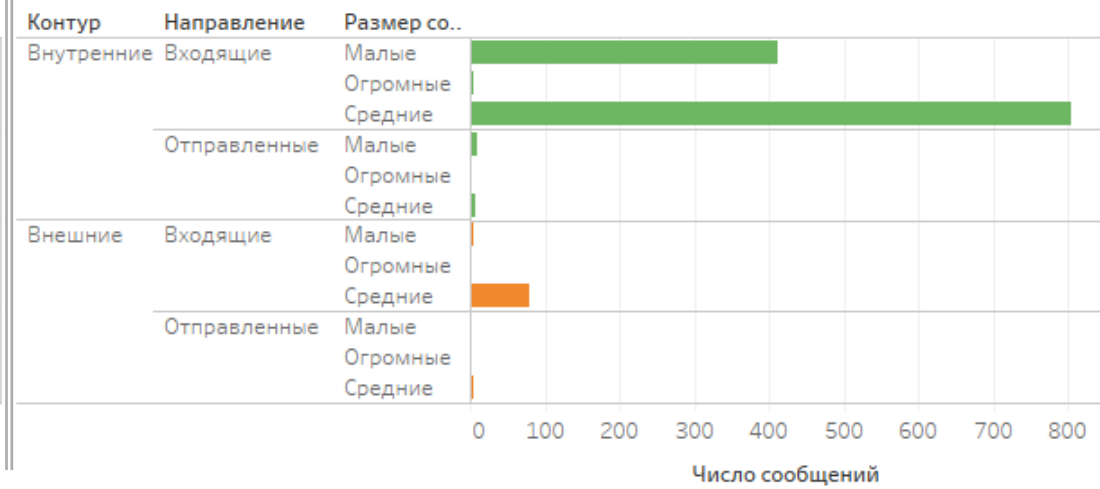


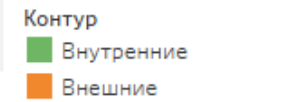


Трафик сотрудника в отпуске



Трафик сотрудника 2

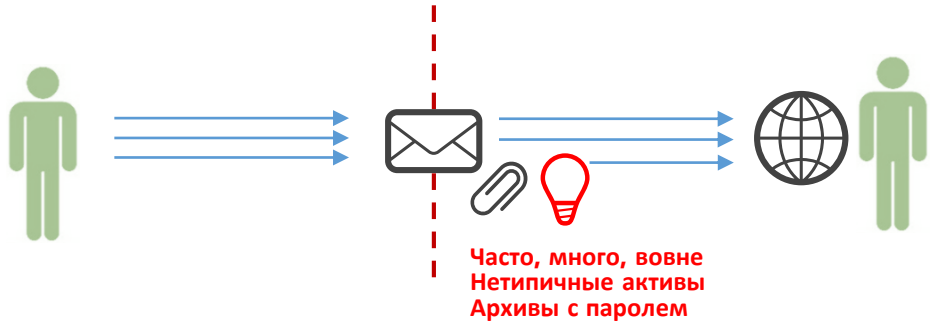




Кейсы

Кейс #1

Отправка сотрудником перед увольнением внутренней конфиденциальной информации компании на внешний личный адрес электронной почты

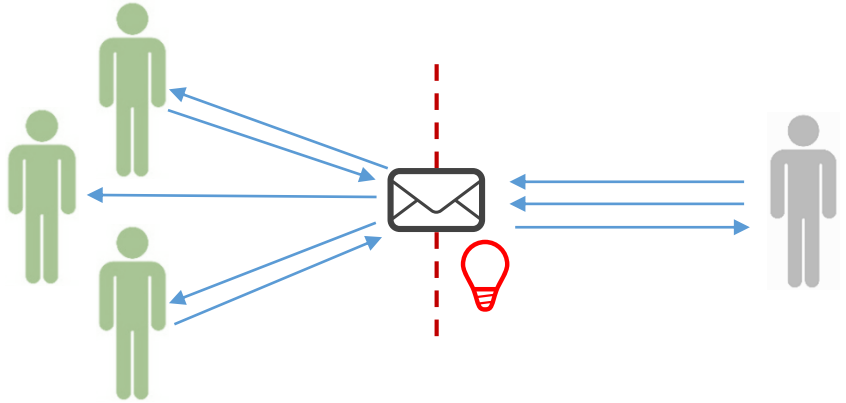


Детектирование

- Появление исходящих сообщений на неизвестный внешний адрес
- Заметное увеличение размеров и количества файлов, отправляемых вовне
- Нетипичные для профиля сотрудника форматы передаваемых вовне файлов
- Наличие среди передаваемых файлов архивов, в том числе защищённых паролем

Кейс #2

Коллективная «вербовка» внешним HR-агентом сразу нескольких сотрудников компании

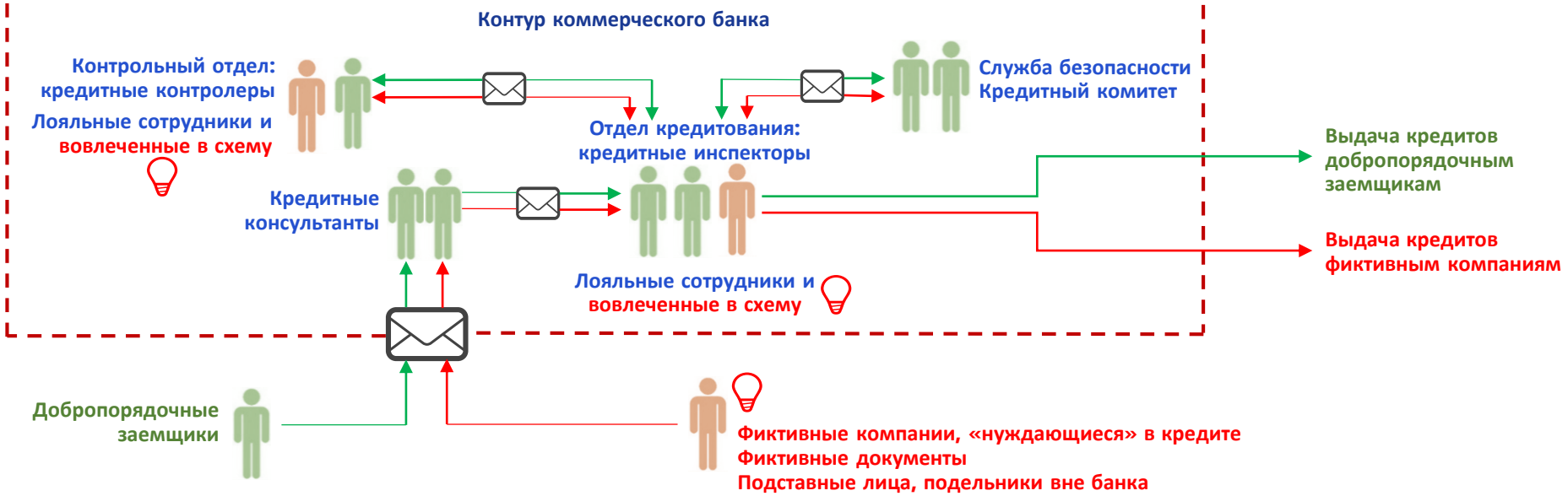


Детектирование

- Появление у нескольких персон, не входящих в общий круг общения, почтового адреса, с которого одному сотруднику поступают внешние почтовые сообщения и с другими ведётся взаимная переписка
- Обнаружение внешнего почтового адреса, взаимодействующего с несколькими персонами – сотрудниками компании
- Определение (по профилю), что данные сотрудники компании не входят в общий круг общения

Кейс #3

Реализация мошеннической схемы по кредитованию фиктивных компаний



Детектирование

- Отклонение числа входящих и исходящих сообщений при оформлении легитимных кредитов от числа сообщений при оформлении фиктивных кредитов (для фиктивных меньше примерно на 25%)
- Отсутствие регламентных нарушений по фиктивным кредитам
- Шаблонный текст переписки
- Отсутствие связей между внутренними сотрудниками, вовлеченными в схему (анализ профиля)

Находите инсайдеров!

Галина Рябова
Руководитель направления Dozor
g.ryabova@solarsecurity.ru
+7 915 03 06 003