INFOWATCH®

МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

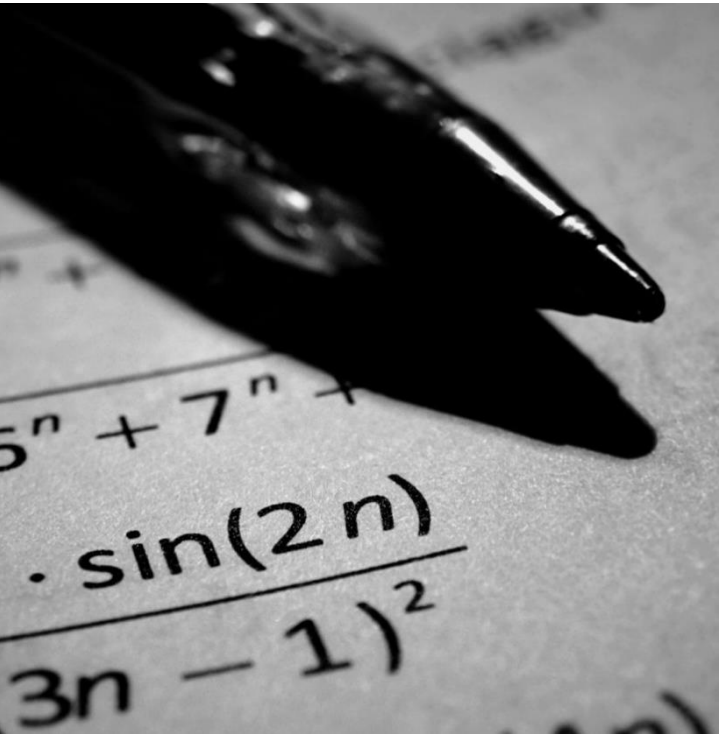
Защита от внутренних угроз

Никита Зайчиков
менеджер технической
поддержки продаж

Москва, 2018

УТЕЧКИ ДАННЫХ

Пример. Космический форум



ОПИСАНИЕ СИТУАЦИИ:

Инженер на предприятии ОПК хотел посоветоваться, как правильно посчитать уравнение и спросил помощи на **интернет форуме**, выложив **фактические данные** по разрабатываемому **изделию**

Результат:

Мониторинг чувствительной информации

Контроль за внешними сетями

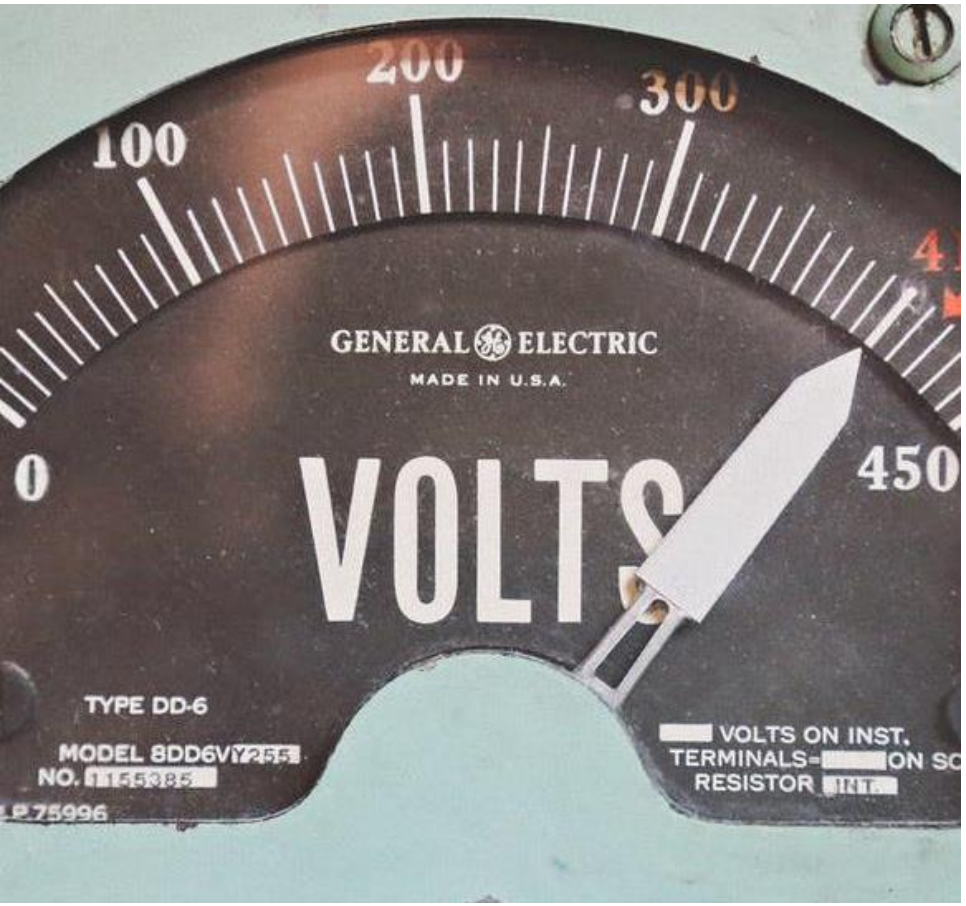
Пример. Перемещение грузов

ОПИСАНИЕ СИТУАЦИИ:

Сотрудник дочерней компании в **транспортном** холдинге по запросу отправлял выписки из **БД** о **перемещении товаров**.
Утечки были поставлена **на поток** и производились для разных «заказчиков»

Результат:
Мониторинг защищенной БД

Риски утечек данных



Регуляторные

Сертификаты и лицензии

Финансовые

- Усиление конкурентов
- Затраты на расследование

Операционные

Нарушение бизнес-процессов

Репутационные

Потеря доверия клиентов

Методы парирования угроз

Правовые

- Доказательная база

Организационные

- Аудит процессов
- Аудит информации
- Обучение сотрудников

Технические

- Управление доступом
- Контроль трафика
- Аудит действий пользователя

ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ

Основные проблемы

INFOWATCH®

Большой объем данных

Сложность ручной обработки нарушений и «серой» зоны

Расследование

Инцидентов требует разнообразного инструментария офицера безопасности

Сложная структура

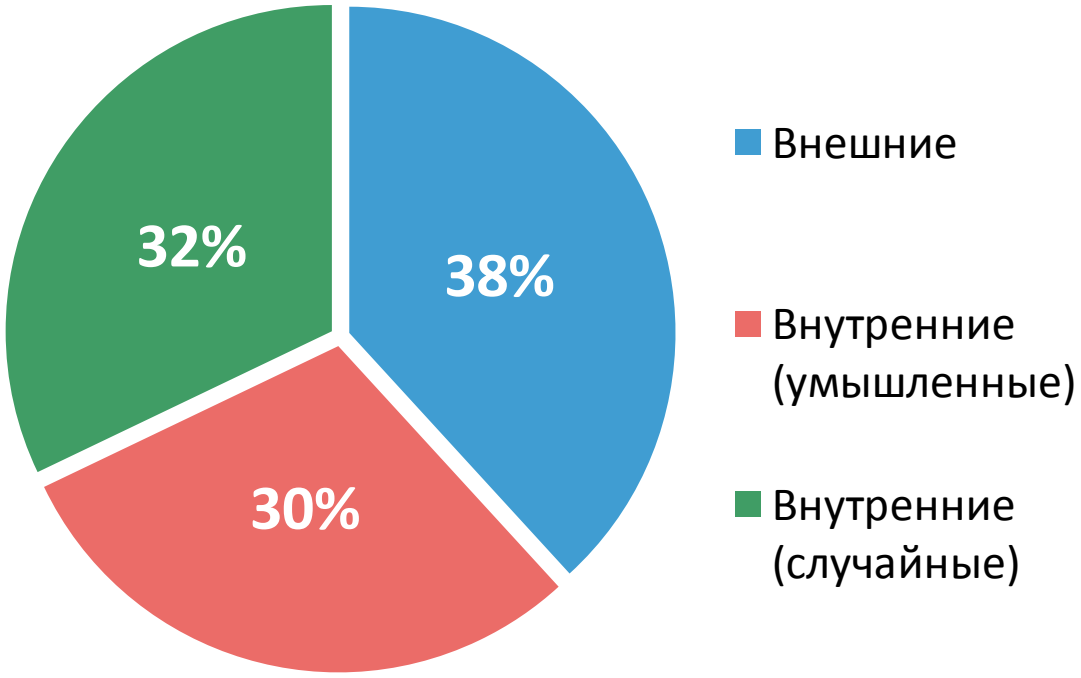
Данные слабо структурированы, что осложняет их защиту стандартными средствами

Требования регуляторов

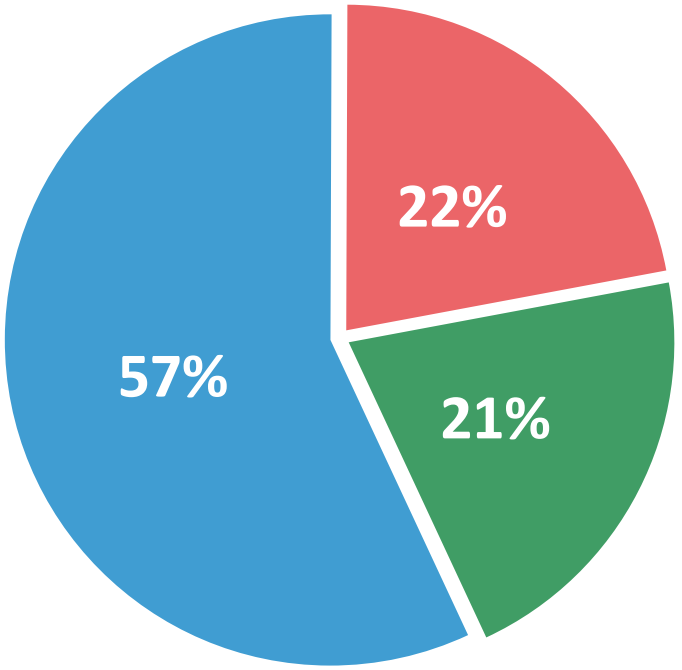
Требования и рекомендации по информационной безопасности, сбор доказательной базы

Источники утечек

По данным InfoWatch*



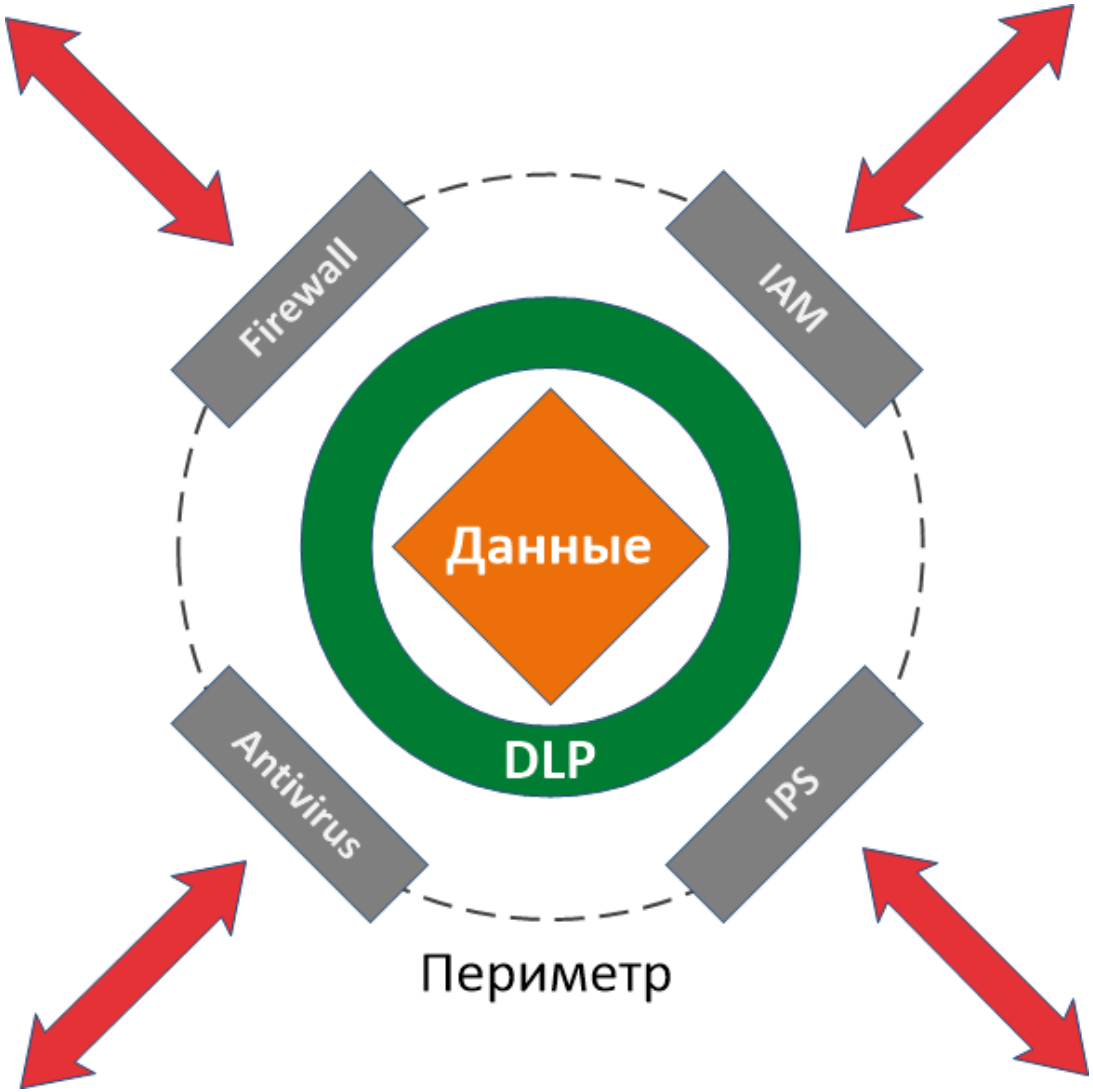
По данным Intel Security**



* **Глобальное исследование утечек конфиденциальной информации в 2016 году** *(Аналитический центр InfoWatch, 2017)*

** **Grand Theft Data.** Data exfiltration study: Actors, tactics, and detection *(Intel Security, 2015)*

Инструменты ИБ



Firewall и IPS

доступ и закрытие каналов

IAM

доступ к местам хранения данных

Antivirus

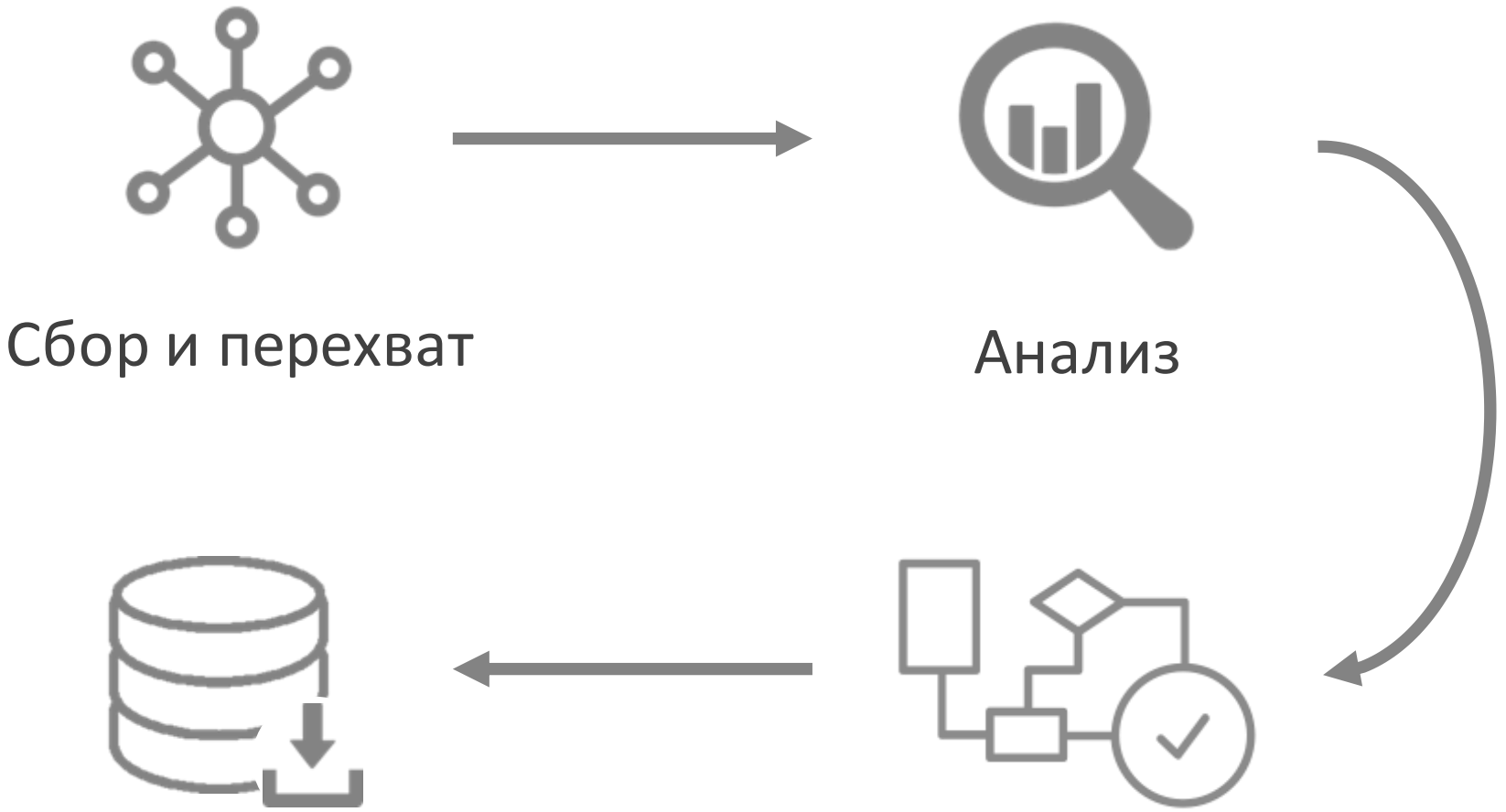
проникновение вредоносного ПО

DLP

анализ и мониторинг данных

INFOWATCH TRAFFIC MONITOR

Логика работы

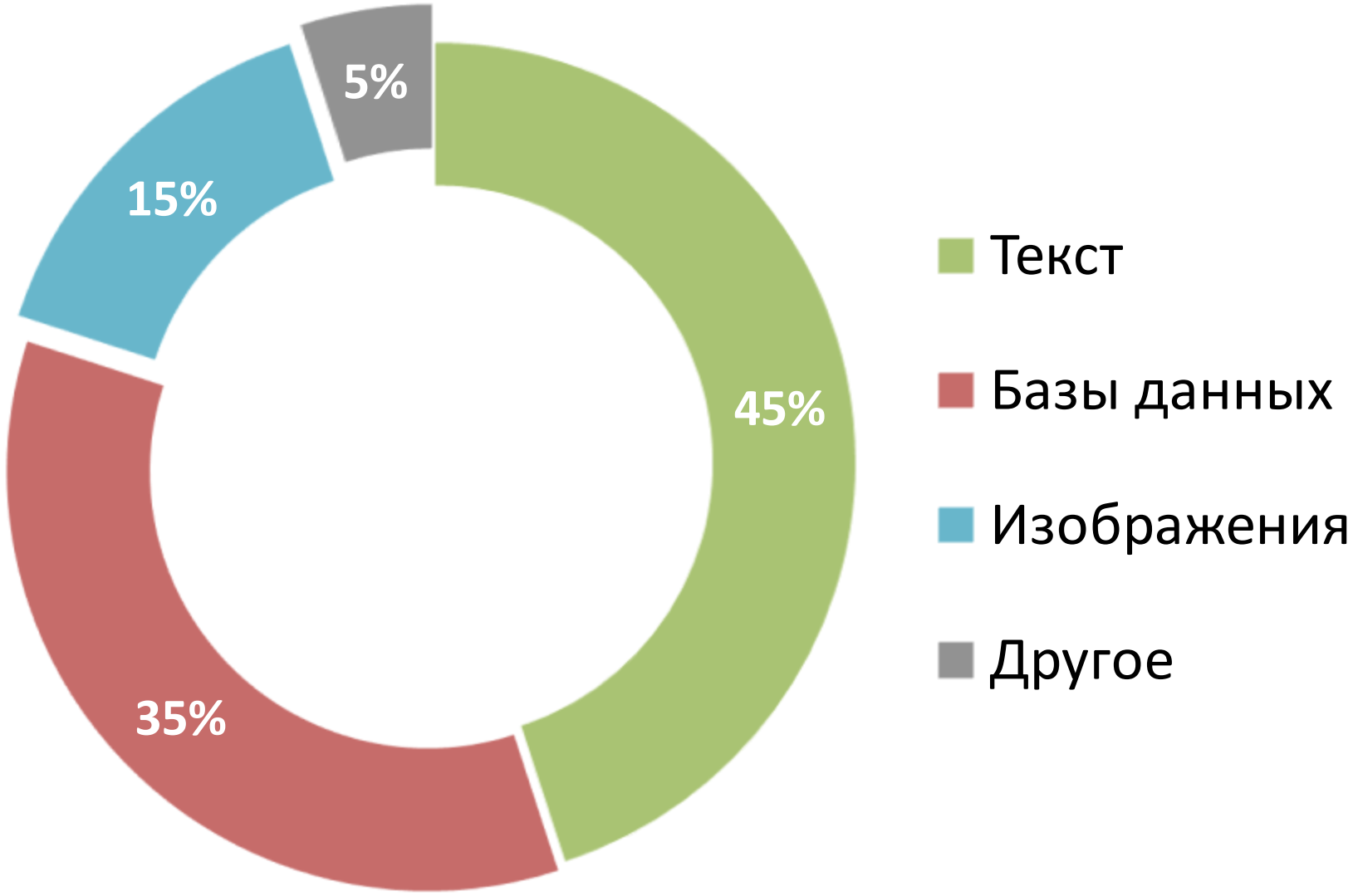


Контролируемые каналы

- Электронная почта
- Интернет
- Внешние устройсва
- Мессенджеры
- Хранилища данных
- Печать
- Мобильные устройства

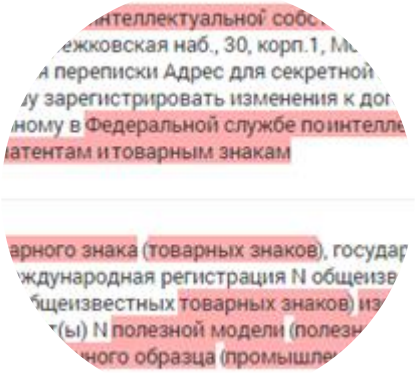
Каналы, по которым может вестись блокировка

Утечки данных по типам



*** Grand Theft Data.** Data exfiltration study: Actors, tactics, and detection *(Intel Security, 2015)*

Технологии анализа: Текст



Лингвистический анализ

Цифровые отпечатки

Текстовые объекты

Бланки и формы

Технологии: Базы данных

Детектирование БД

- Выгрузки до 5 млн. записей
- Гибкие правила детектирования
- Работа с различными форматами

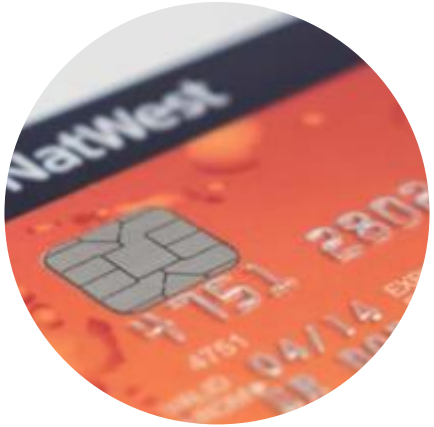
Примеры

- Клиентские базы
- Финансовая информация
- Персональные данные

Технологии: Изображения

Графические объекты

Детектор паспортов



Банковские карты

Печати

Комбинирование технологий: объекты защиты

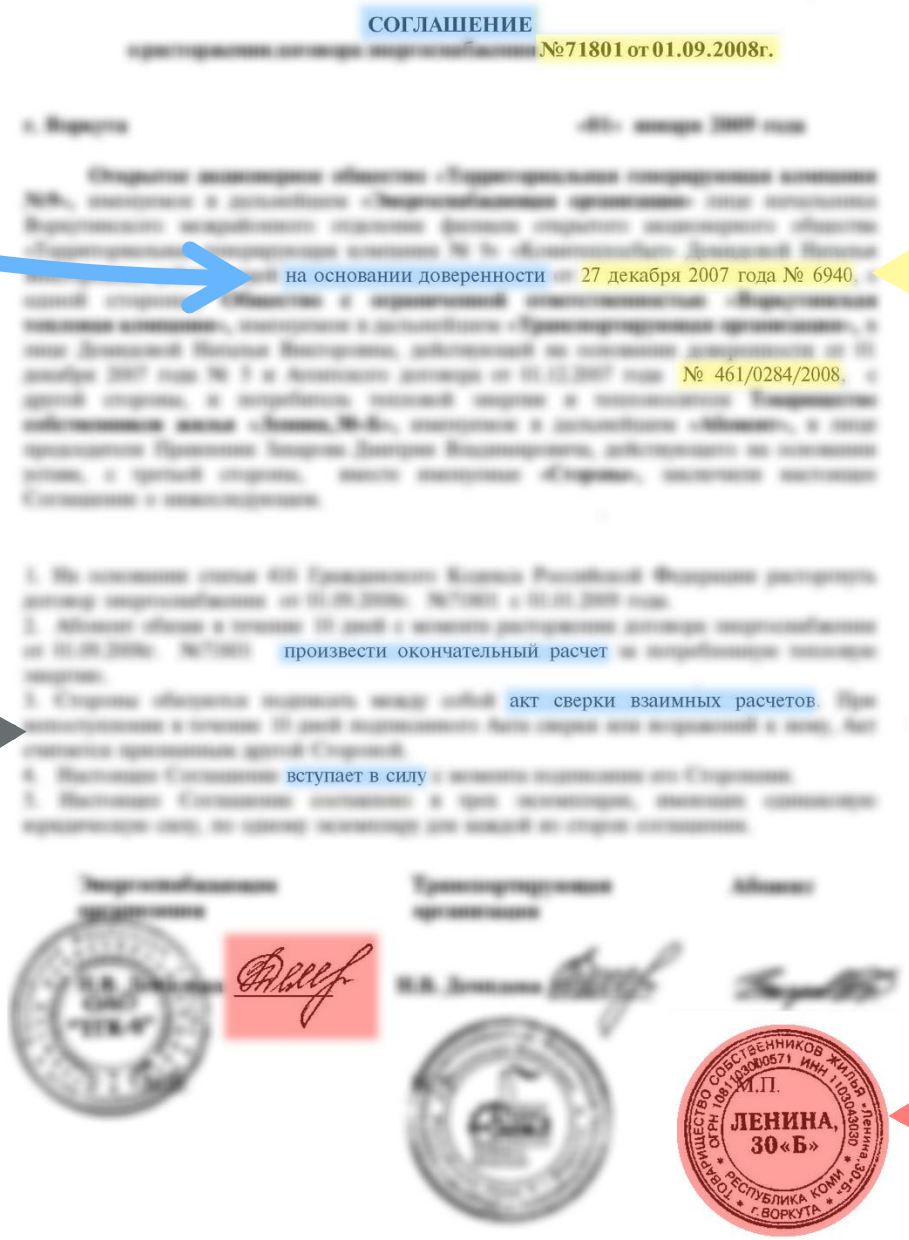
Лингвистический анализ

Текстовые объекты

Цифровой отпечаток

Шаблон договора

Печать и факсимиле



INFOWATCH VISION

Визуальная аналитика

Выявление скрытых связей

Фильтрация в реальном времени

Аудит и адаптация политик

Лицензии и сертификаты

АРПП «Отечественный Софт»

Аккредитация ЦБ РФ

Сертификат ФСТЭК России СВТ-5

Обеспечивает соответствие требованиям регуляторов

Комплексная защита информации

Некоторые клиенты

INFOWATCH®

Банки и финансы

СБЕРБАНК Всегда рядом
Райффайзен БАНК
Связь Банк
Банк Кольцо Урала
HOME CREDIT BANK
Банк Москвы
Белгазпромбанк

Энергетика

РУСЭНЕРГО РЕСУРС
ЭЛЕКТРОГЕНЕРАЦИЯ ИНТЕР РАО КАШИРСКАЯ ГРЭС
e.on
ТВЭЛ
РУСЭНЕРГОСБЫТ

Промышленность

ОБЪЕДИНЕННАЯ ДВИГАТЕЛЕСТРОИТЕЛЬНАЯ КОРПОРАЦИЯ
ОБОРОНПРОМ
lira
Московский вертолетный завод им. М.Л. Миля

Государственный сектор

Федеральная Таможенная Служба
Министерство обороны Российской Федерации
Федеральная налоговая служба
Фонд Социального Страхования
Правительство Тульской области

Страхование

ВСК СТРАХОВОЙ ДОМ
СОГАЗ СТРАХОВАЯ ГРУППА

Нефтегазовый сектор

Газпром автоматизация
СлавНефть
Газпром Вниигаз
Транснефть
СНГ
ЛУКОЙЛ НЕФТЯНАЯ КОМПАНИЯ

Торговля

МИР КНИГИ .RU
МАГНИТ
magnum cash & carry
KUPIVIP.RU
FIX price
Дикси

Фармацевтика

STADA CIS
акрихин Люди заботятся о Людях
НИАРМЕДИК

Транспорт и логистика

РОСЖЕЛДОР ПРОЕКТ
Газпром авиа
SPSR express

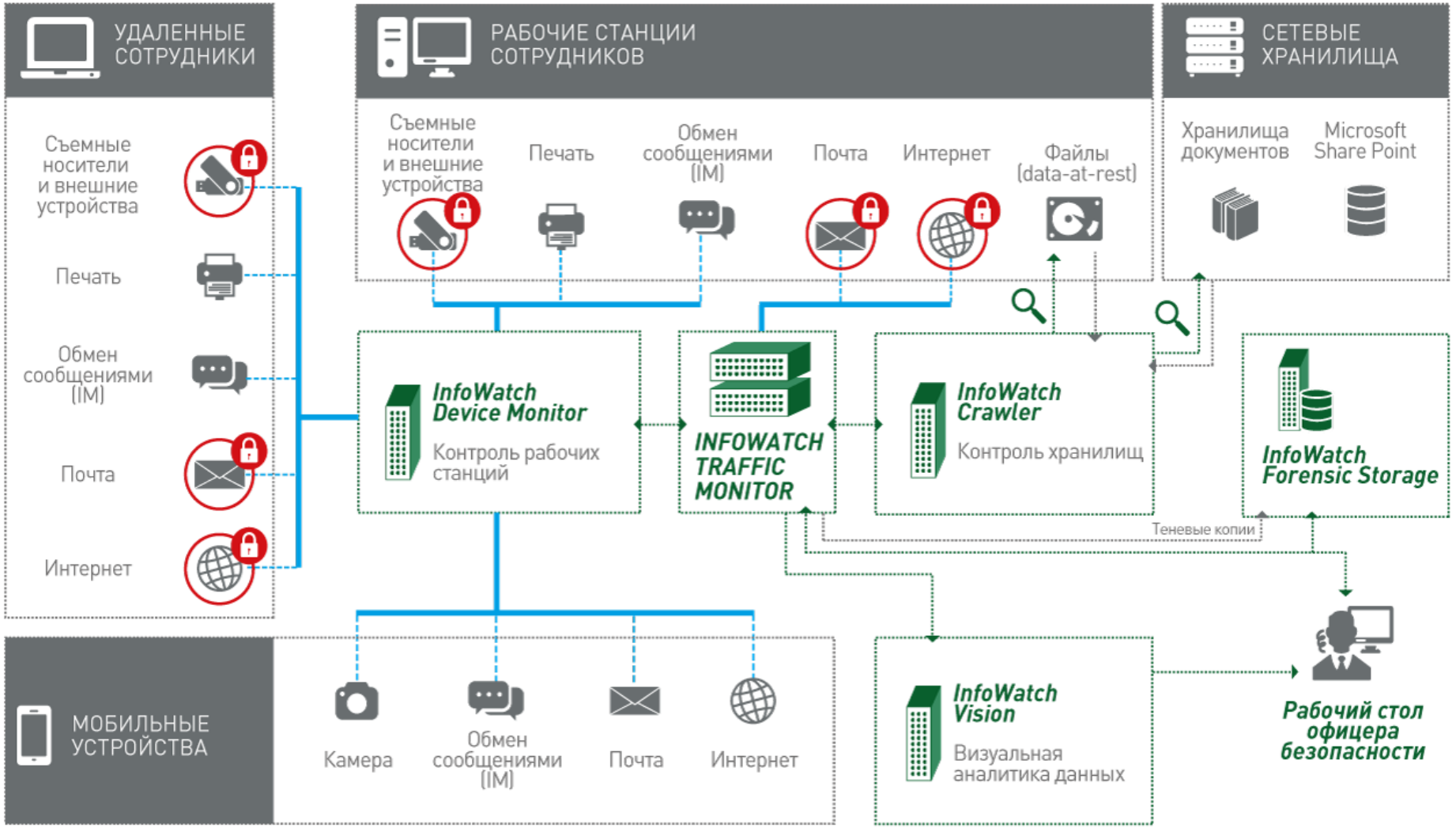
Телекоммуникации

МегаФон Точикистон
МТС
ВГТРК
Билайн

Благодарю за внимание!

Ваши вопросы?

Архитектура решения



Блокировка непосредственно на агенте