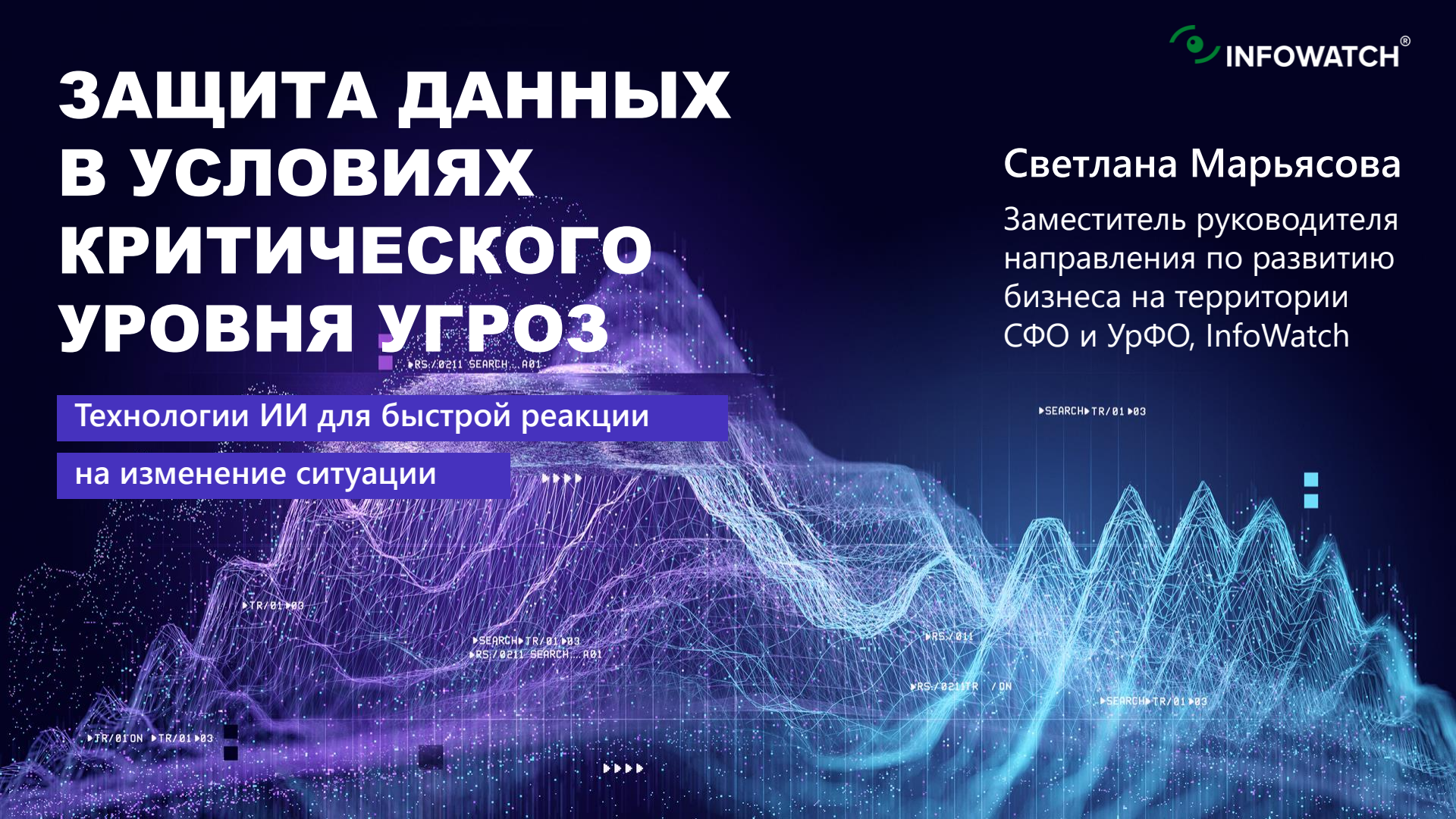
ЗАЩИТА ДАННЫХ В УСЛОВИЯХ КРИТИЧЕСКОГО УРОВНЯ УГРОЗ

Технологии ИИ для быстрой реакции на изменение ситуации

Светлана Марьясова

Заместитель руководителя направления по развитию бизнеса на территории СФО и УрФО, InfoWatch



Защита от внешних киберугроз — очень важно. А как же инсайдерские и комбинированные атаки?

1. **Инсайдерские атаки могут быть не менее чувствительными, чем внешние.** Вплоть до остановки бизнеса…

2. **Утечки становятся ухищрённее,** совершаются группами лиц, времени на расследования всё меньше

3. **У департамента ИБ не всегда есть ресурсы,** чтобы действовать на опережение и анализировать подозрительные события

Быстро реагировать на изменившуюся ситуацию

- → **За 1 день категорировать** все документы в организации и **за 1 час обучить** DLP-систему новой категории документов или изображений
- → **За 5 минут провести расследование** инцидента и обнаружить все связи подозреваемых
- → Предотвратить инцидент на **стадии подготовки** нарушения

С помощью ИИ и продвинутой аналитики DLP-системы от InfoWatch

Технологии ИИ и продвинутая аналитика от InfoWatch

InfoWatch Data Explorer и Автолингвист

Технологии ИИ. Найти ВСЕ типы документов, требующих защиты, и обучить DLP за 1 день

InfoWatch Employee Monitor

Сбор доказательной базы при инцидентах, учёт рабочего времени сотрудников

InfoWatch Vision

BI-система для DLP — быстрый поиск всех причастных к утечке и удобный ежедневный мониторинг инцидентов

InfoWatch Prediction

Технологии ИИ для автоматизации управления рисками — рейтинг сотрудников с подозрительным поведением

INFOWATCH®

InfoWatch Data Explorer и Автолингвист

На основе ИИ

Категоризация ВСЕХ документов и обучение DLP
за 1 день без привлечения специалистов со стороны

Классификация текстов «из коробки»: отраслевые и тематические словари

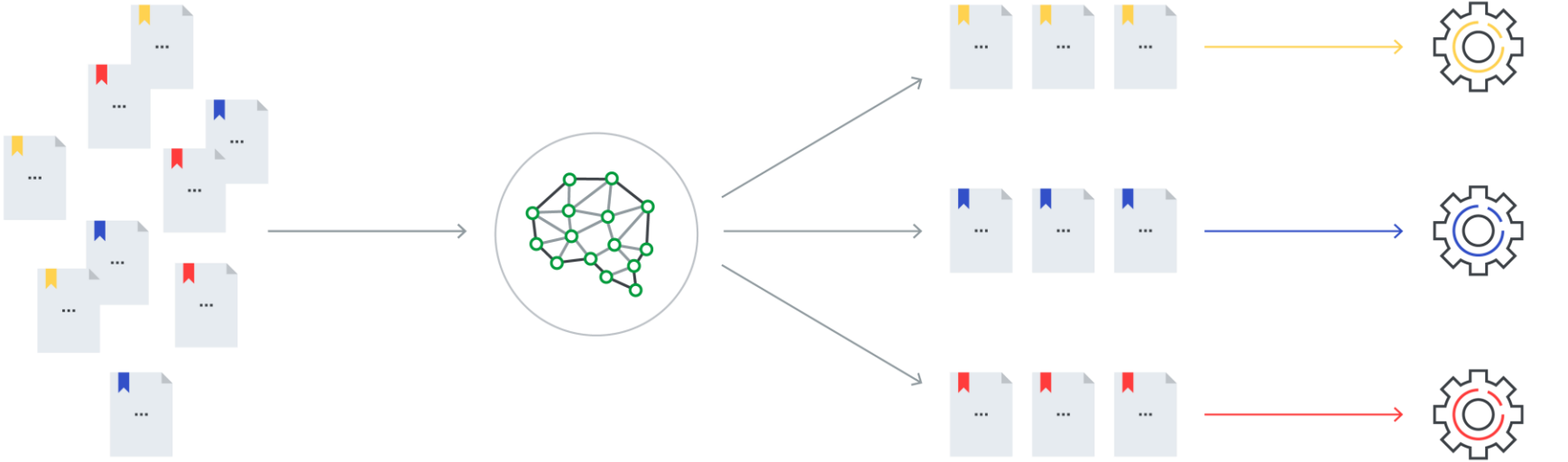
Для точного детектирования и снижения ложных срабатываний

- **Авиапромышленная**
- **Автопромышленная**
- **Агропромышленная**
- Атомная
- Банковская
- Геологическая
- **Госструктуры**
- **Гостайна**
- Железнодорожная
- **Инженерно-производственная**
- Ислам
- Исходный код
- Космическая
- Медицинская
- МФЦ
- Налоговая
- Нарушение законодательства
- **Нелояльные сотрудники**
- **Нефтегазовая**
- Нецензурная лексика
- Религиозная
- Страховая
- Строительная
- Судостроение
- Таможенная
- Телекоммуникационная
- Торговая
- **Транспортировка нефти**
- Фармакологическая
- Христианство
- Экстремизм
- **Энергетическая**
- ...

Учитываем специфику ваших терминов: доработка базы под каждого заказчика

289 категорий

Категоризация документов за 1 день



Неисследованный поток данных

ИИ категорирует ВСЕ документы компании за 1 день

Документы по категориям

Обучение DLP с помощью Автолингвиста

Автоматическое обучение DLP-системы новым категориям документов за 1 час

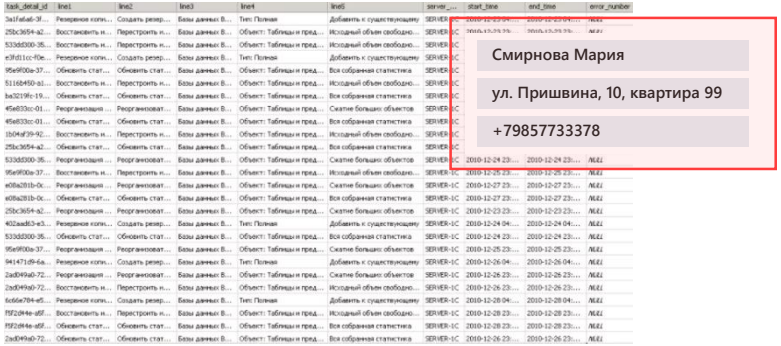
INFOWATCH®

→ На документах заказчика

→ Без привлечения экспертов-лингвистов

→ ВСЕ документы за 1 час, а не 10 дней

Защита персональных и любых именованных данных: детектор выгрузок баз данных



- → Контролируем **движение конкретных данных,** а не просто доступ к базе
- → Скорость — **100 000 000 записей** в секунду
- → Защищаем **актуальные** данные — динамическое обновление данных

ЗАПАТЕНТОВАНО

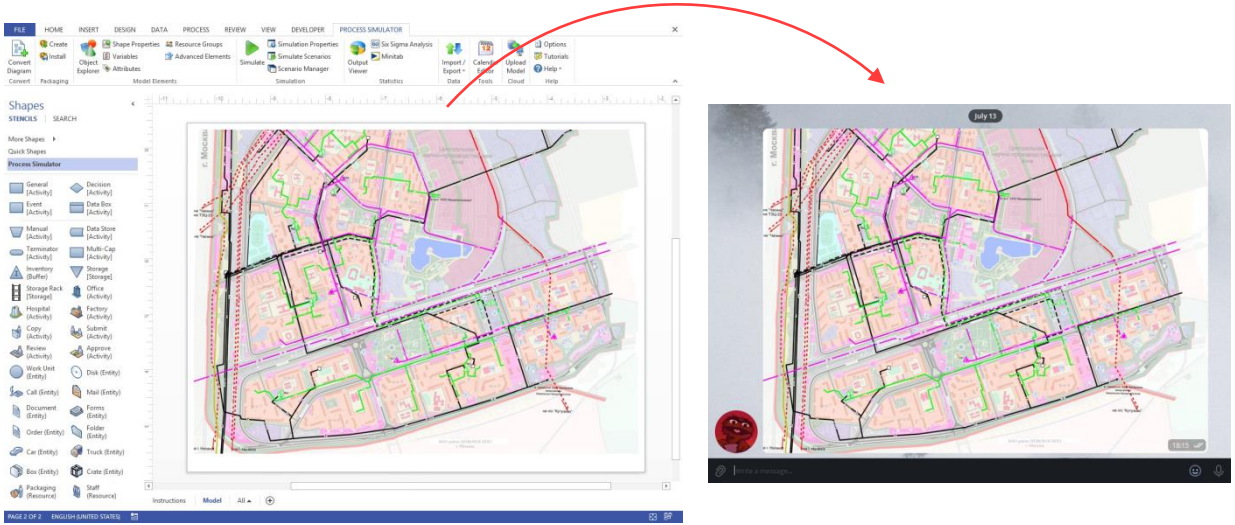
Особенности

Для каждой защищаемой сущности (ПДн, база клиентов, поставщиков, сотрудников) несколько критериев срабатывания — например, комбинации полей и порция переданных данных.

Это единственный способ контролировать ПДн или прайс-листы без шквала ложноположительных срабатываний

Защита изображений любого типа с помощью машинного зрения

Машинное зрение защищает конфиденциальные фото, сканы, картинки



Готовые категории

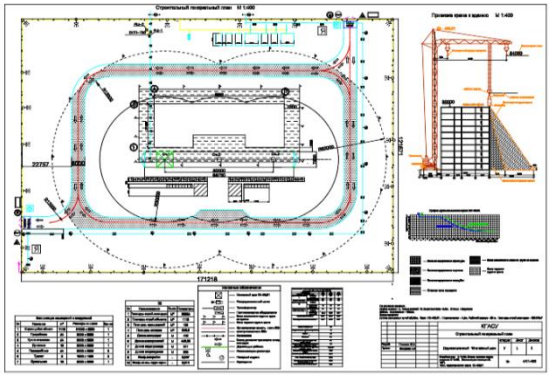
- → Паспорт гражданина РФ
- → Технические чертежи
- → Географические карты

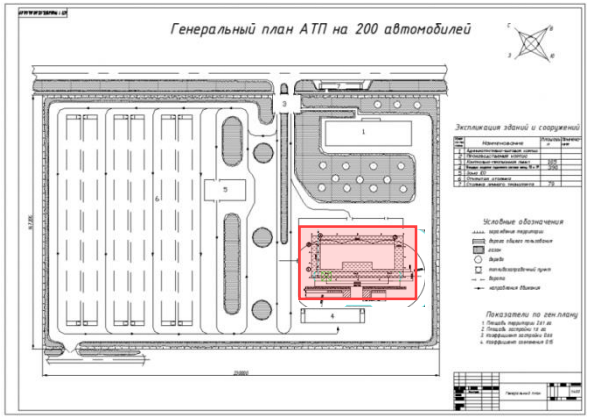
Самостоятельное обучение системы

На коллекции документов клиента с помощью технологий машинного обучения.

Защита изображений любого типа с помощью машинного зрения

Векторные цифровые отпечатки для защиты схем, чертежей, карт в CAD-формате



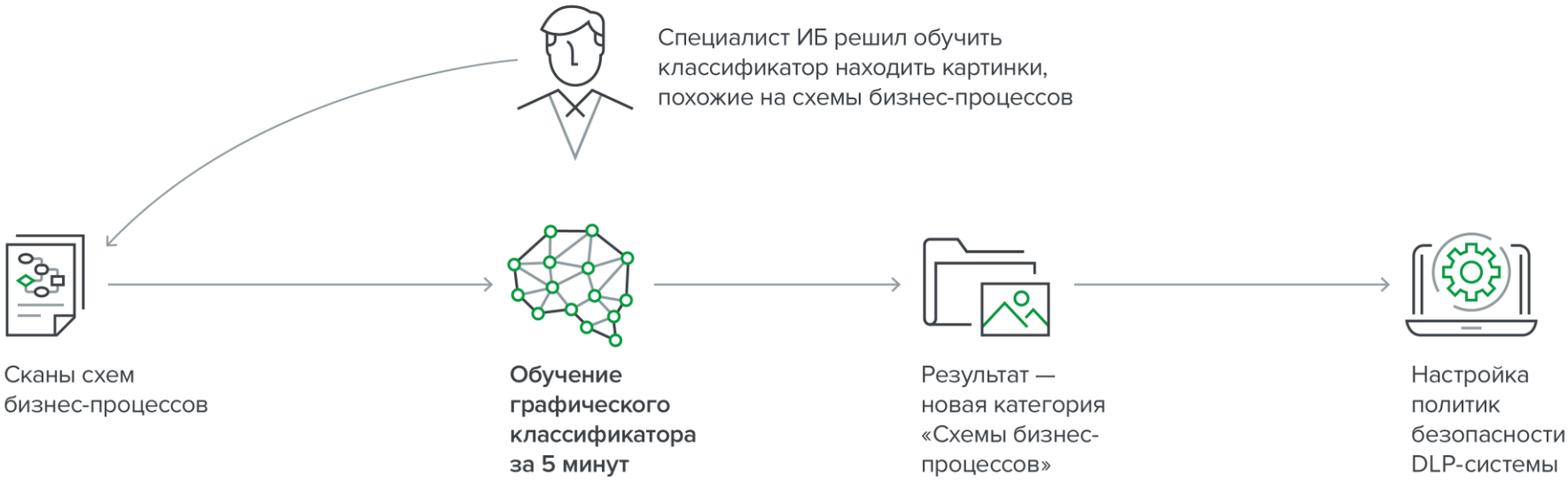


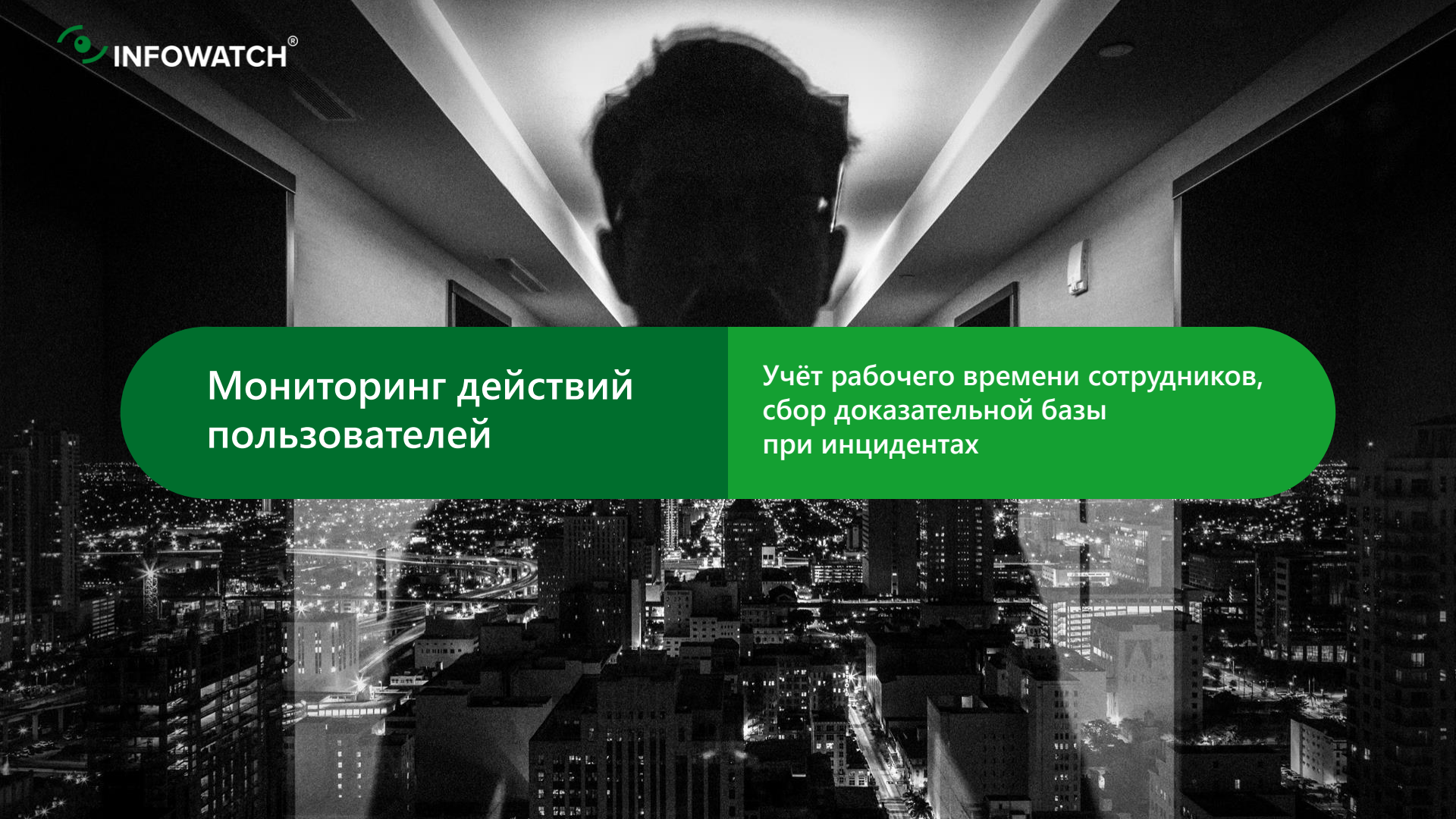
- → Анализируем чертёж как комплекс векторных составляющих
- → **Детектируем даже части конфиденциального чертежа** в пересылаемом файле + поворот, вставка в другой чертёж, изменение детализации

Автообучение графического классификатора новым категориям картинок

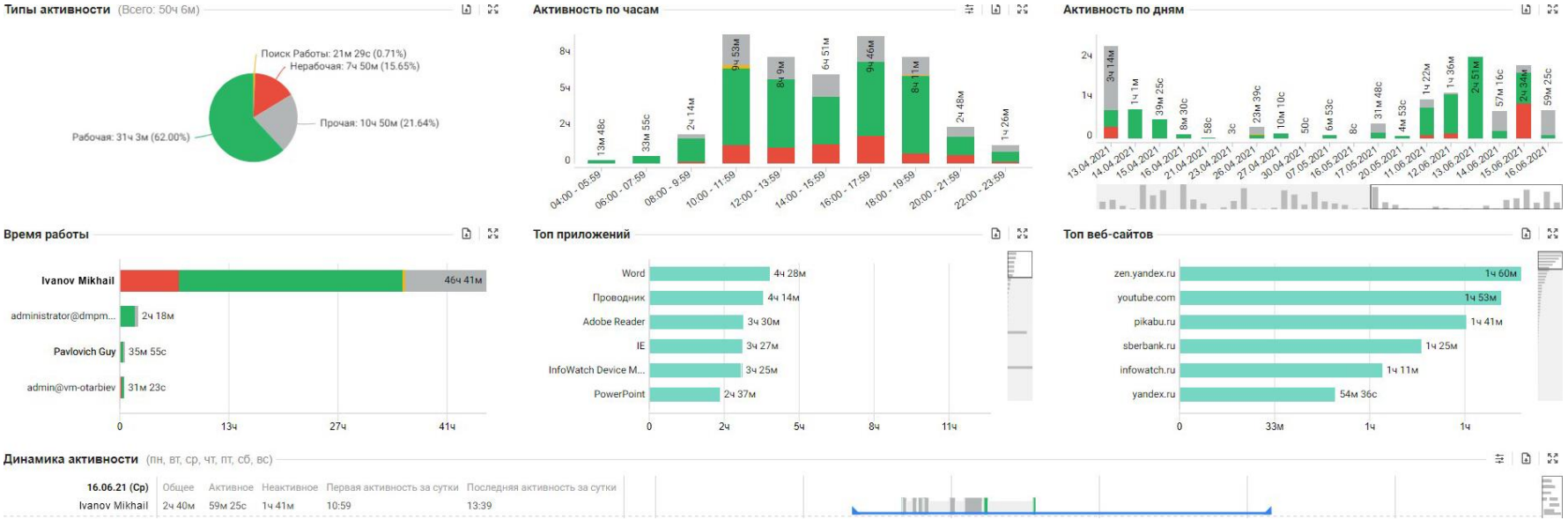
→ Обучение DLP-системы на любых картинках заказчика

→ Без привлечения экспертов InfoWatch




INFOWATCH®
Мониторинг действий пользователей
Учёт рабочего времени сотрудников, сбор доказательной базы при инцидентах

Employee Monitoring: чем заняты сотрудники?



Последовательная картина рабочего дня

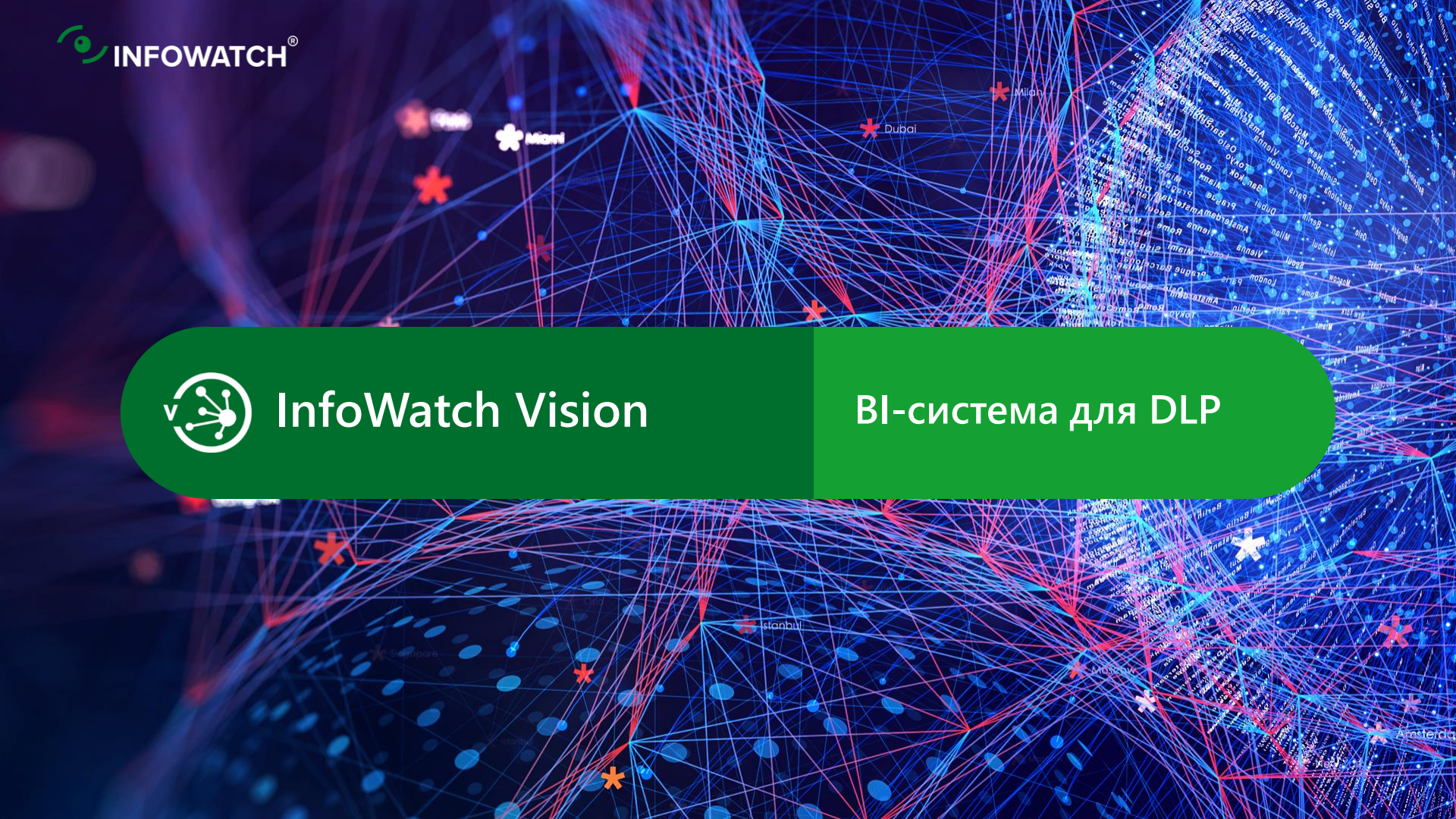
- → Когда сотрудник начал и закончил работать
- → Когда был на встречах (интеграция с MS Outlook)
- → Сколько из этого времени был за компьютером
- → Сколько из этого времени был активен (в т. ч. периоды бездействия, частые переключения...)

Статистика активности по всей компании, департаменту или сотруднику, например:

- → 60% — рабочая активность
- → 30% — нерабочая
- → 10% — требует разбора

Топ приложений и веб-ресурсов

- → Кем используются
- → Когда
- → Как долго


INFOWATCH®
InfoWatch Vision
BI-система для DLP

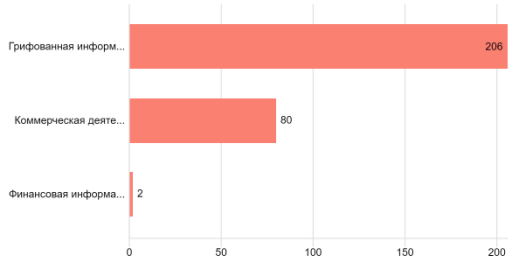
Что позволит сделать визуализация данных DLP?

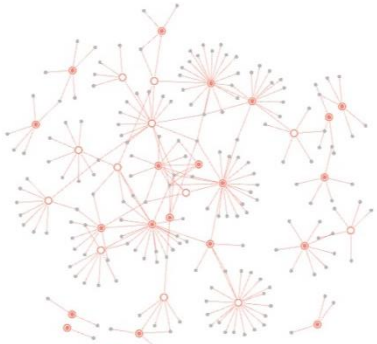
1. За утренним кофе **проанализировать** последние события в поисках инцидентов

2. За минуты найти **все связанные** с инцидентом события и увидеть **общую картину** на графе связей

3. Найти инциденты даже **в неразмеченных событиях** и понять, когда политики DLP пора обновить

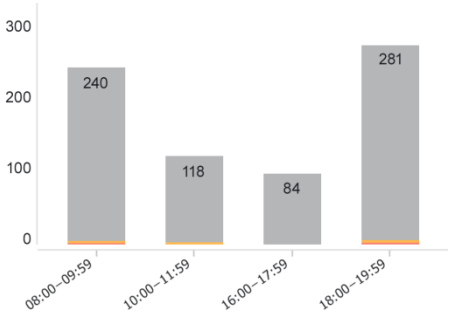
Ежедневно проверять оперативную обстановку на предмет нарушений и подозрительных всплесков

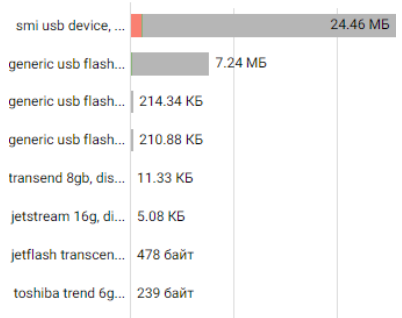




Мониторинг вывода грифованной информации за неделю

И путей её распространения





Активность в нерабочее время

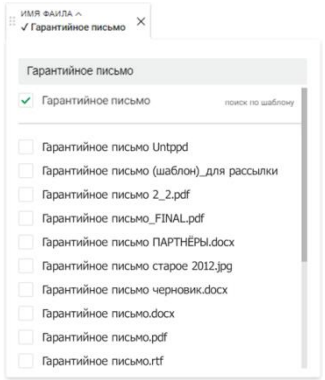
Накопление большого количества информации на флешке

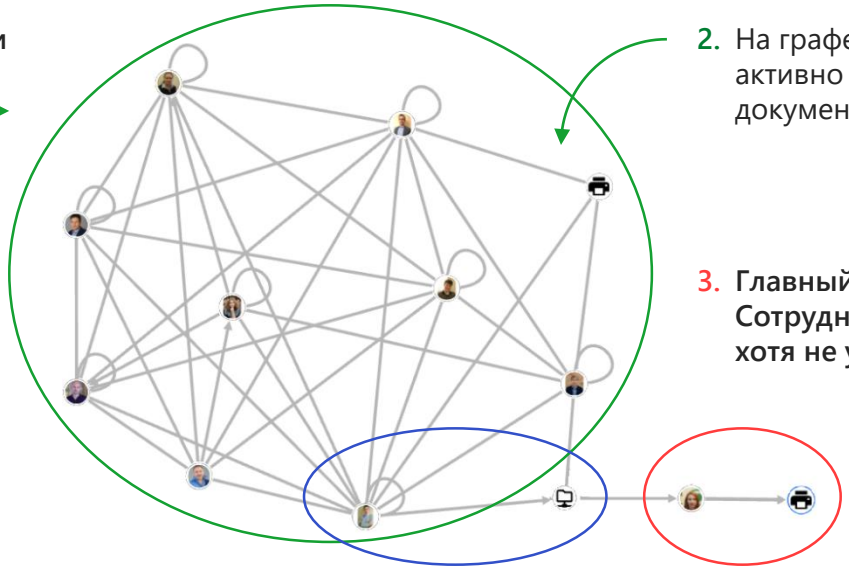
Выявить всех виновных в сливе фото конфиденциального документа за 5 минут

INFOWATCH®

В интернете обнаружено фото гарантийного письма
→ Есть 1 час до доклада руководству итогов расследования

1. **Поиск в Vision по общей части в имени файла** показал все копии документа





2. На графе видна группа сотрудников, активно **участвовавшая в разработке** документа

3. **Главный подозреваемый. Сотрудник распечатал документ, хотя не участвовал в обсуждении**

4. **Утечке поспособствовала выгрузка документа в сетевую папку для совместной работы**

INFOWATCH®

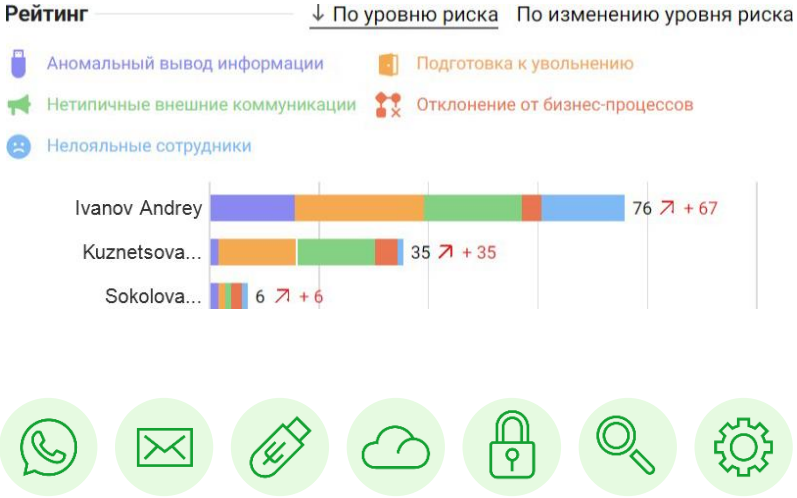
InfoWatch Prediction

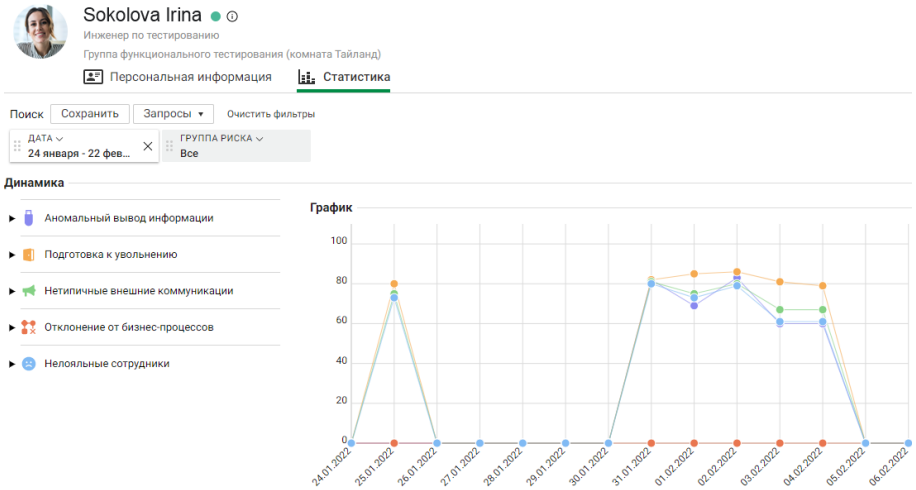
Автоматизация управления рисками

InfoWatch Prediction позволяет быстро понять, чьё поведение требует анализа в первую очередь

- → **Подсказываем, на что обратить внимание,** если событий очень много
- → **Подсказываем, где могут скрываться риски,** если не хватает опыта
- → **Помогаем разобрать «серую зону»,** когда ресурсов ИБ не хватает
- → **Помогаем автоматизировать рутину** и сконцентрироваться на важном

Автоматическое формирование рейтинга и досье для анализа динамики и сочетания аномалий

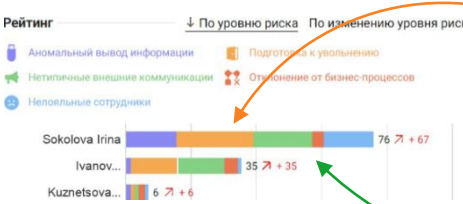




Конкретные данные для принятия решений, а не ещё одни данные для аналитики.
Обучение системы — 1 месяц!

Заметить подготовку к увольнению

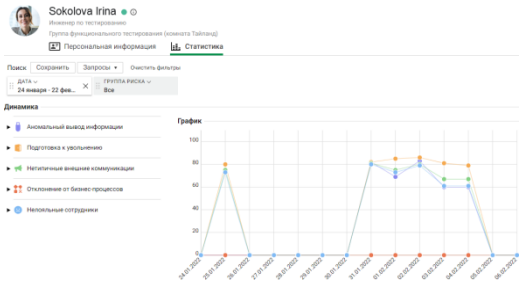
1 Специалист ИБ обнаружил **на 1 месте в рейтинге Prediction** сотрудника, попавшего сразу в две группы риска



Подготовка к увольнению

Нетипичные внешние коммуникации

2 **Анализ досье Prediction**



→ Несколько дней подряд — аномалия по посещению hh.ru. Заходил утром и в обед

→ Затем неделю аномалии по отправке писем с корпоративной почты на свою личную

→ Затем количество аномалий по посещению hh.ru возросло — несколько раз в день на несколько часов

Проверка деталей событий

Сотрудник отправил: логины и пароли коллег к корпоративным ресурсам, сайты компаний-конкурентов, замечания на монтаж оборудования, инструкции по проведению работ как портфолио. **Не подпадают под политики безопасности: события из «серой зоны»**

Проведена профилактическая беседа о недопустимости утечки конфиденциальной информации. Уведомлён отдел HR

Комплексное решение от InfoWatch

InfoWatch Employee Monitoring

InfoWatch Traffic Monitor

InfoWatch Vision

InfoWatch Prediction

Контроль действий и учёт рабочего времени сотрудников

DLP-система на основе ИИ: надёжная защита от утечек и контроль трафика

Визуальная аналитика данных — BI-система для DLP

Предиктивная аналитика данных DLP — с применением ИИ

Что случилось?

- → Защита от утечек
- → Контроль информационных потоков
- → Контроль действий сотрудников

Почему это случилось?

Оперативная обстановка, ускорение расследований и отчёты

Что может произойти?

Автоматизация оценки рисков и рейтинг подозрительных сотрудников

Данные для аналитики

Аналитика данных

TADVISER
Государство. Бизнес. ИТ

INFOWATCH®

INFOWATCH TRAFFIC MONITOR — ЛУЧШЕЕ ИБ-РЕШЕНИЕ 2021 ПО ВЕРСИИ TADVISER

За визуальную и предиктивную аналитику и расширение возможностей DLP-системы

Ускорение расследований в 3–4 раза

Не только блокировка, но и профилактика утечек

Данные для ЭБ, IT, HR...

INFOWATCH®

Международный
ТБ ФОРУМ
Технологии Безопасности

INFOWATCH TRAFFIC MONITOR — ПРЕМИЯ ЗА ПРОДУКТ НА ТБ-ФОРУМЕ 2022

За автоматизированное обучение новым категориям текстовых и графических документов с помощью ИИ

Обучение новой категории документов за 1 час

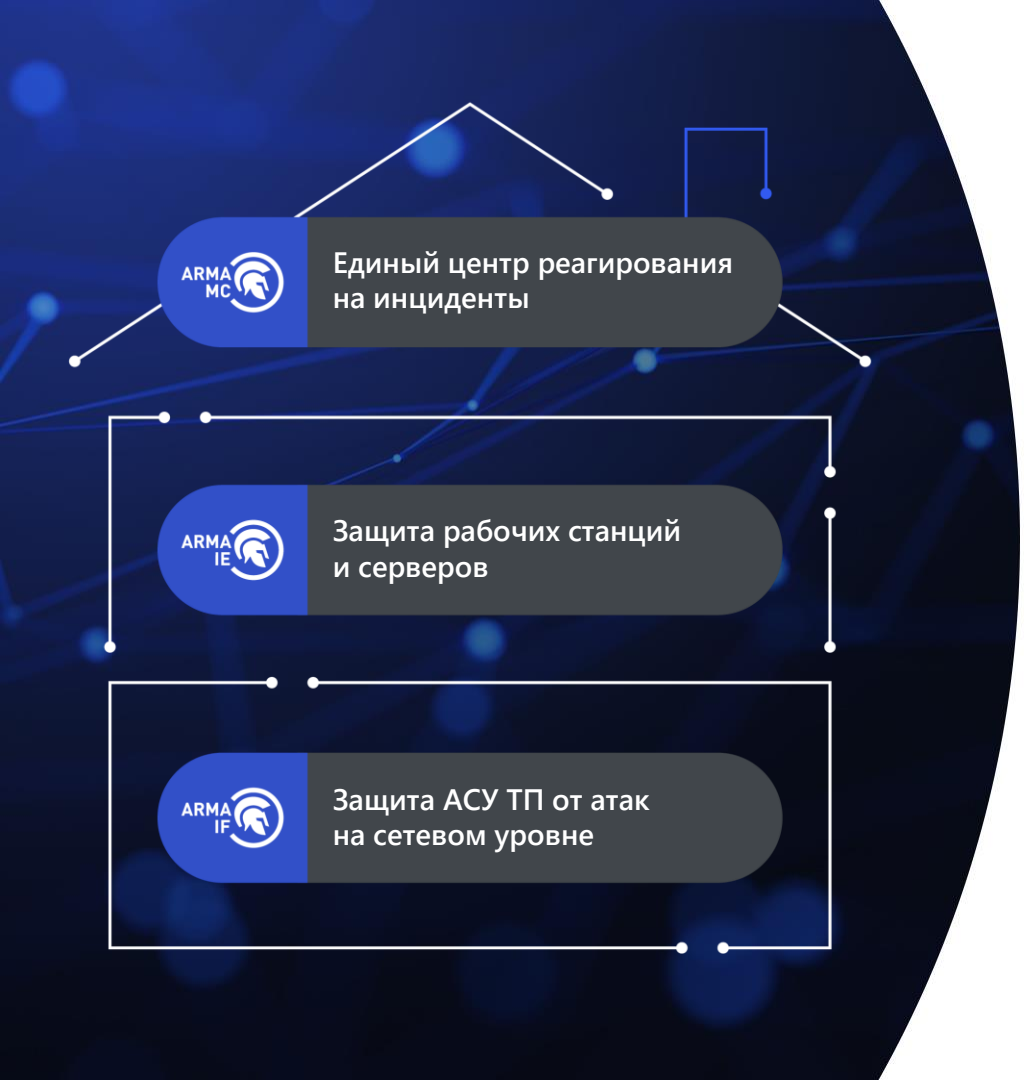
Силами заказчика без привлечения лингвистов

Без передачи документов на сторону

INFOWATCH®

InfoWatch ARMA

Защита АСУ ТП от кибератак



INFOWATCH®

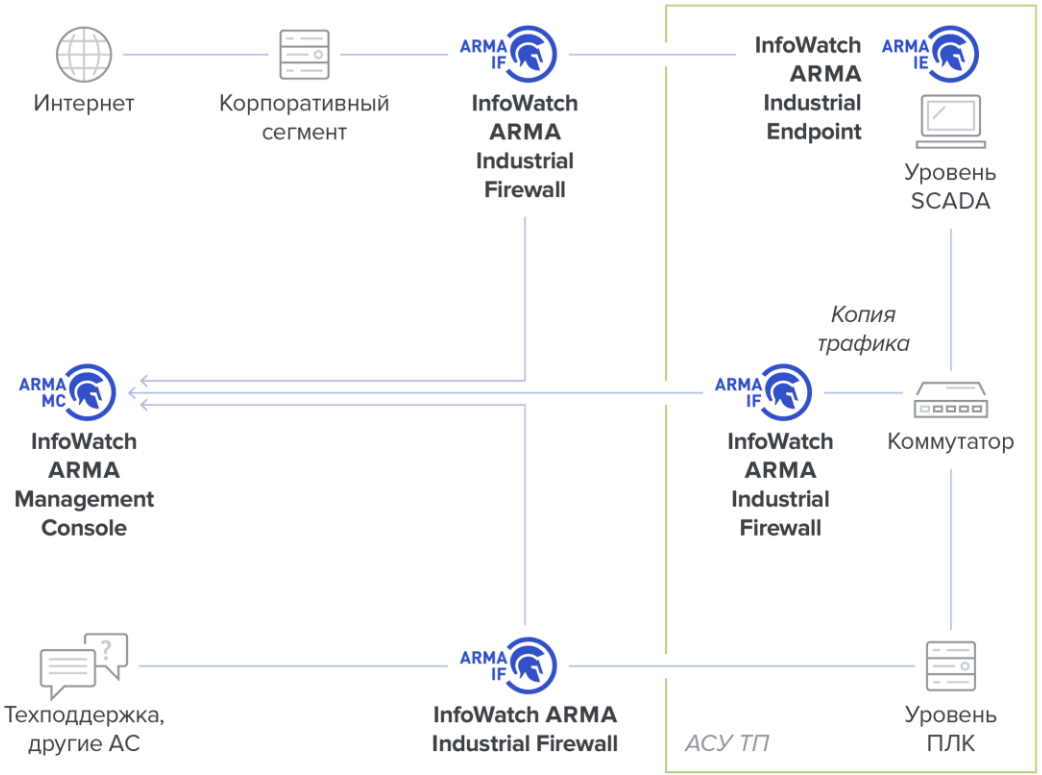
InfoWatch ARMA — комплексная система для обеспечения кибербезопасности АСУ ТП

→ Эшелонированная **защита с единым центром управления** системой защиты информации

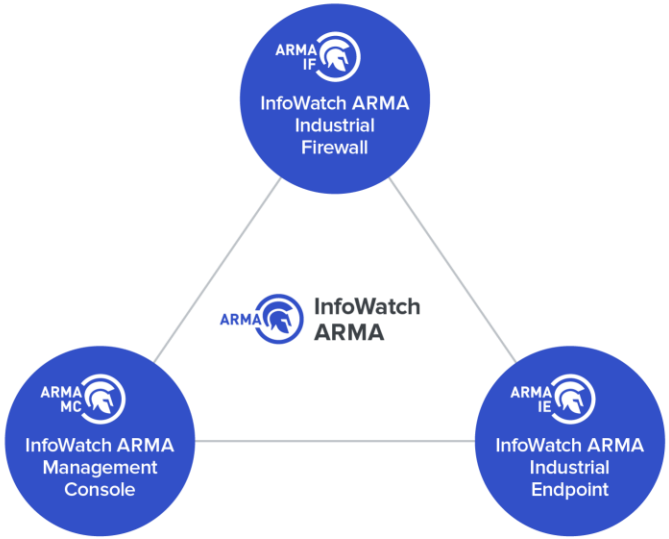
→ **Инструмент для выполнения до 90% технических требований** приказа ФСТЭК России № 239

→ **Снижение стоимости владения** и ресурсов на сопровождение системы

Комплексная система — выгоднее и легче внедрение



Все продукты интегрированы между собой: могут эксплуатироваться как самостоятельные продукты, так и в комплексе

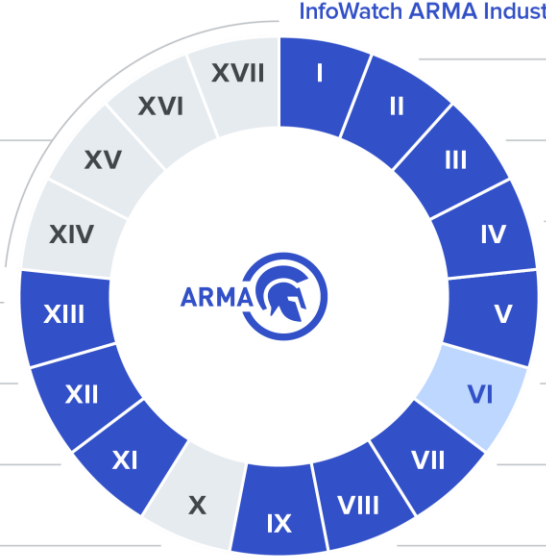


Инструменты защиты

Экспертиза	Продукты
Поиск уязвимостей для компонентов АСУ ТП	**InfoWatch ARMA Management Console** Варианты поставки: ПО и ПАК
Тестирование на проникновение	**InfoWatch ARMA Industrial Firewall** Варианты поставки: ПО и ПАК
Анализ событий ИБ по запросу Оценка того, является ли цепочка событий инцидентом	**InfoWatch ARMA Industrial Endpoint**

До 90% выполнения технических требований Приказа № 239 ФСТЭК России

INFOWATCH®



СОВ
InfoWatch ARMA Industrial Firewall

СОВ, МЭ
InfoWatch ARMA Industrial Firewall

Endpoint
InfoWatch ARMA Industrial Endpoint

Endpoint
InfoWatch ARMA Industrial Endpoint

СОВ, МЭ
InfoWatch ARMA Industrial Firewall

Антивирусная защита
Q2 2022

СОВ
InfoWatch ARMA Industrial Firewall

Endpoint, МЭ
InfoWatch ARMA Industrial Endpoint

МЭ
InfoWatch ARMA Industrial Firewall

Физическая безопасность

Endpoint, МЭ
InfoWatch ARMA Industrial Firewall / Industrial Endpoint

Средства управления инцидентами
InfoWatch ARMA Management Console

Endpoint
InfoWatch ARMA Industrial Endpoint

Организационные меры

Получите карту соответствия InfoWatch ARMA группам мер ФСТЭК России

Оставьте запрос на сайте
arma.infowatch.ru

INFOWATCH®

ПРОГРАММА ПОДДЕРЖКИ

во время повышенного риска кибератак и инсайдерских угроз

Срочные консультации по защите критических данных и инфраструктуры с возможностью использования СЗИ InfoWatch бесплатно — по итогам консультации

INFOWATCH

СПАСИБО ЗА ВНИМАНИЕ!

Светлана Марьясова

Заместитель руководителя направления по развитию бизнеса на территории СФО и УрФО, InfoWatch

/InfoWatchOut /InfoWatch