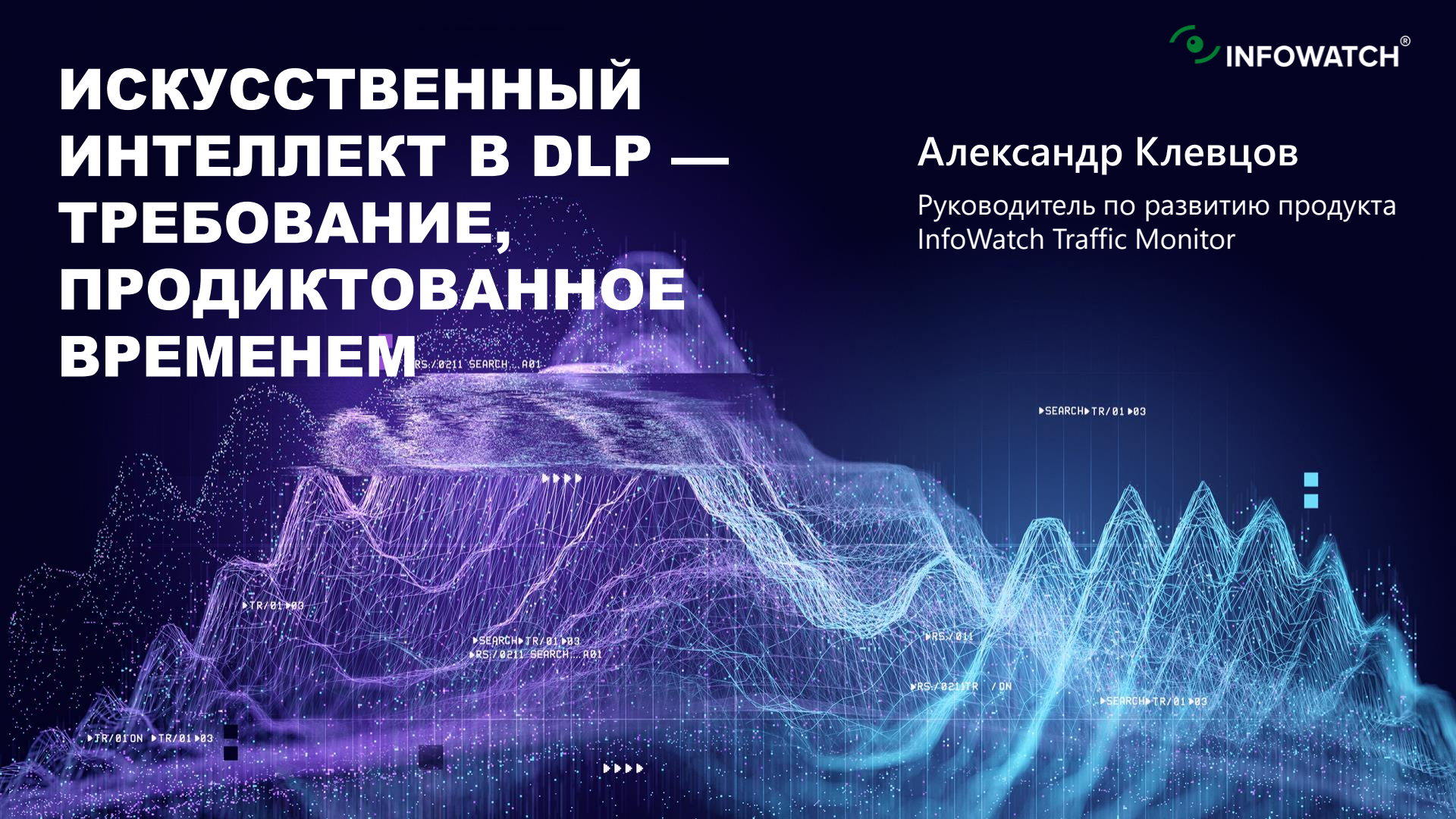
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В DLP — ТРЕБОВАНИЕ, ПРОДИКТОВАННОЕ ВРЕМЕНЕМ

Александр Клевцов

Руководитель по развитию продукта
InfoWatch Traffic Monitor



INFOWATCH®

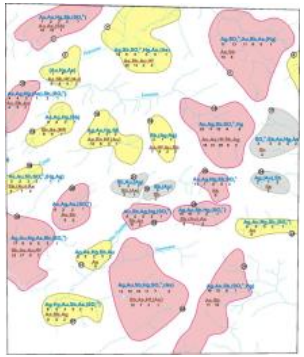
3 класса задач от наших заказчиков, где ИИ незаменим

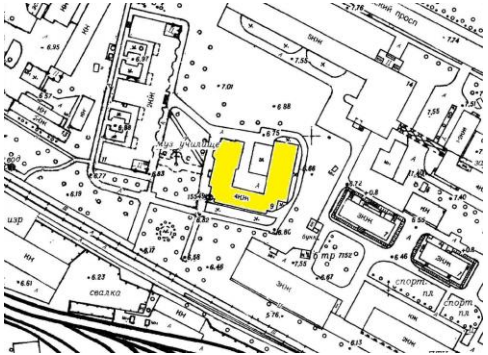
Защита конфиденциальной графики

Автоматическое обучение DLP новым категориям документов

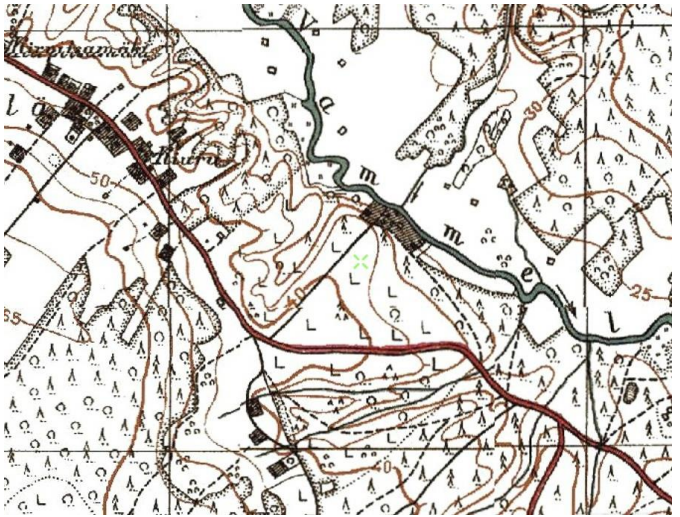
Прогнозирование рисков

Защита конфиденциальных изображений даже без текста





OCR не поможет!

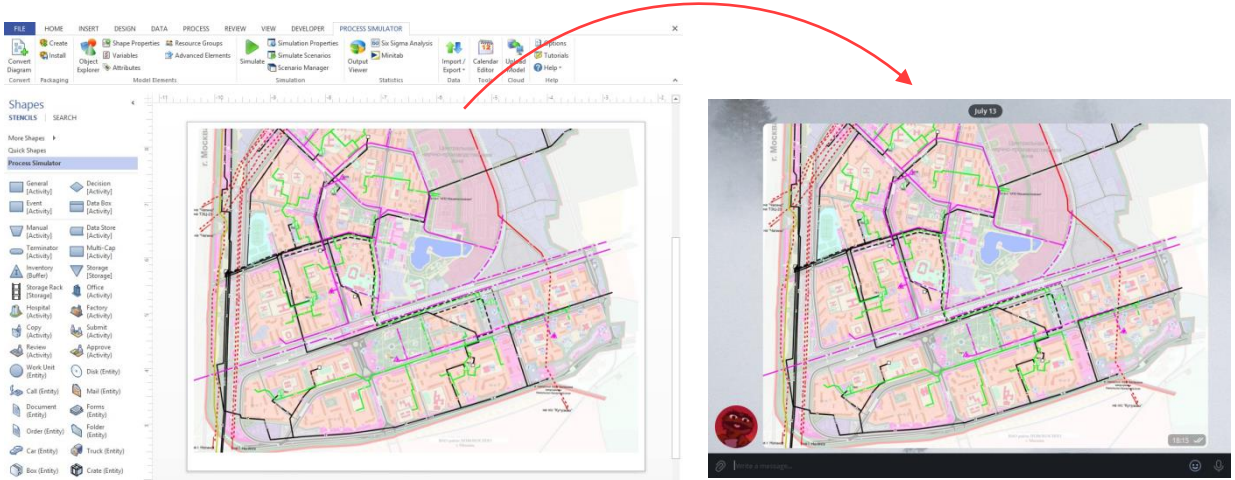


Защита сканов документов

OCR не поможет!

Защита изображений любого типа с помощью машинного зрения

Машинное зрение определяет что именно изображено на картинке

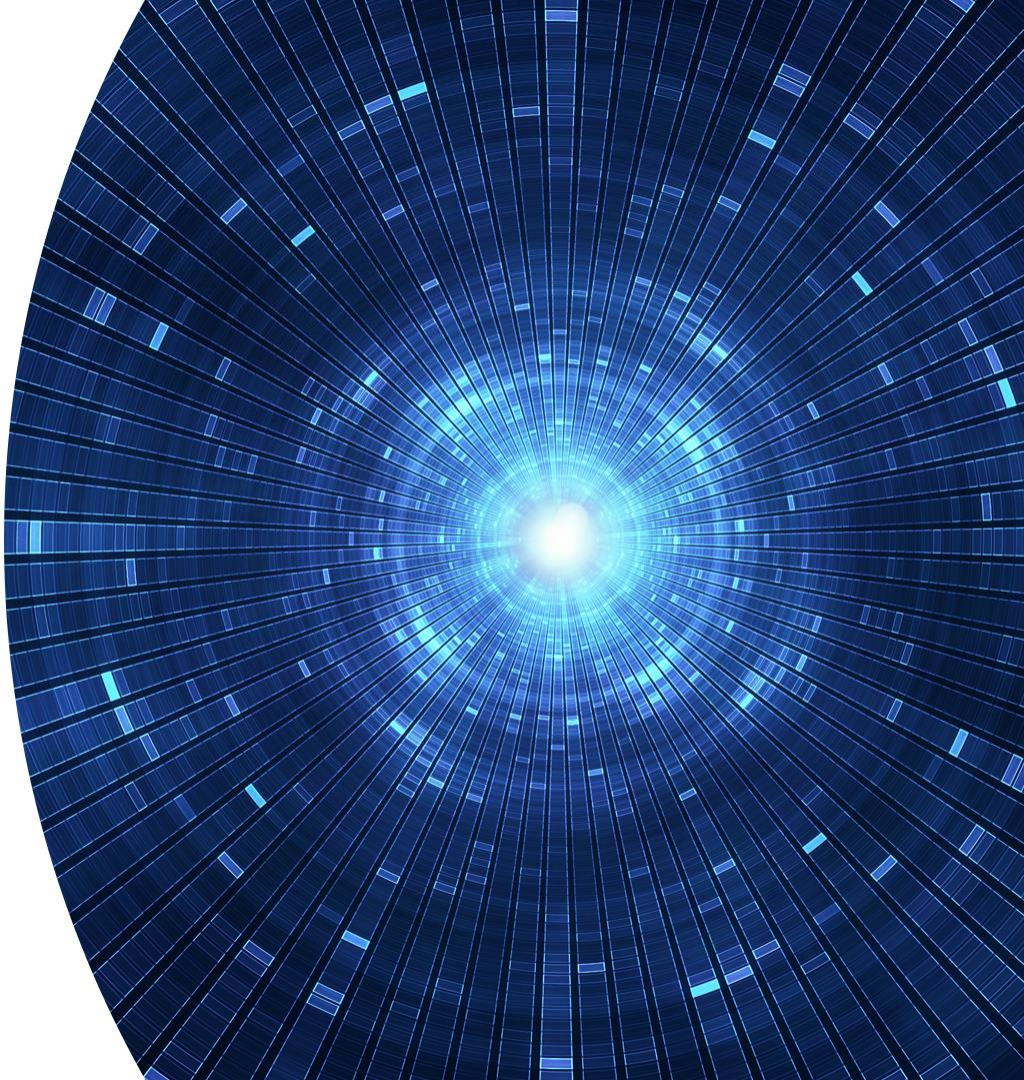


Самостоятельное обучение системы

На коллекции документов клиента с помощью технологий машинного обучения

Машинное зрение для защиты конфиденциальных изображений

- → Готовые категории – чертежи, сканы удостоверений, планы помещений итд
- → Скорость детектирования в 10 раз выше, чем при применении OCR
- → Определение лиц, гистограммный фильтр, нормализация, снижение шумов
- → Обучение DLP-системы новой категории изображений силами заказчика, без отправки коллекции на сторону



Обучение DLP-системы новым категориям конфиденциальных документов

INFOWATCH®

Нет возможности отправить на сторону конфиденциальные документы?
Нет возможности держать лингвистов в штате?

У многих наших клиентов до 20 словарей одновременно. И регулярно появляются новые категории документов

- → **289 категорий**
- → **Учитываем транслит, опечатки, литспик**
- → **42 языка, 20 — с полной морфологией**

- — 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
- — ...

Автоматическое обучение DLP-системы новым категориям документов

INFOWATCH®

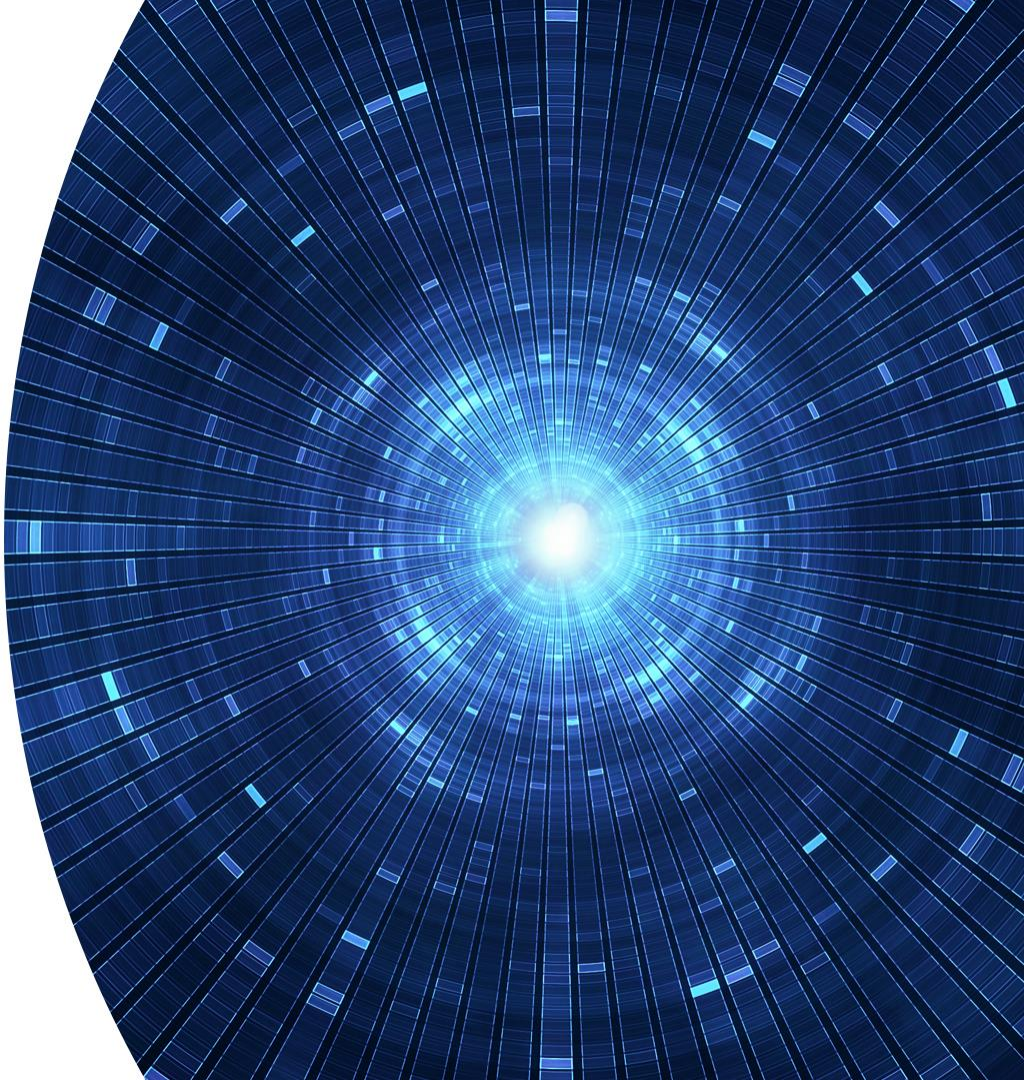
→ На документах заказчика

→ Без привлечения экспертов-лингвистов

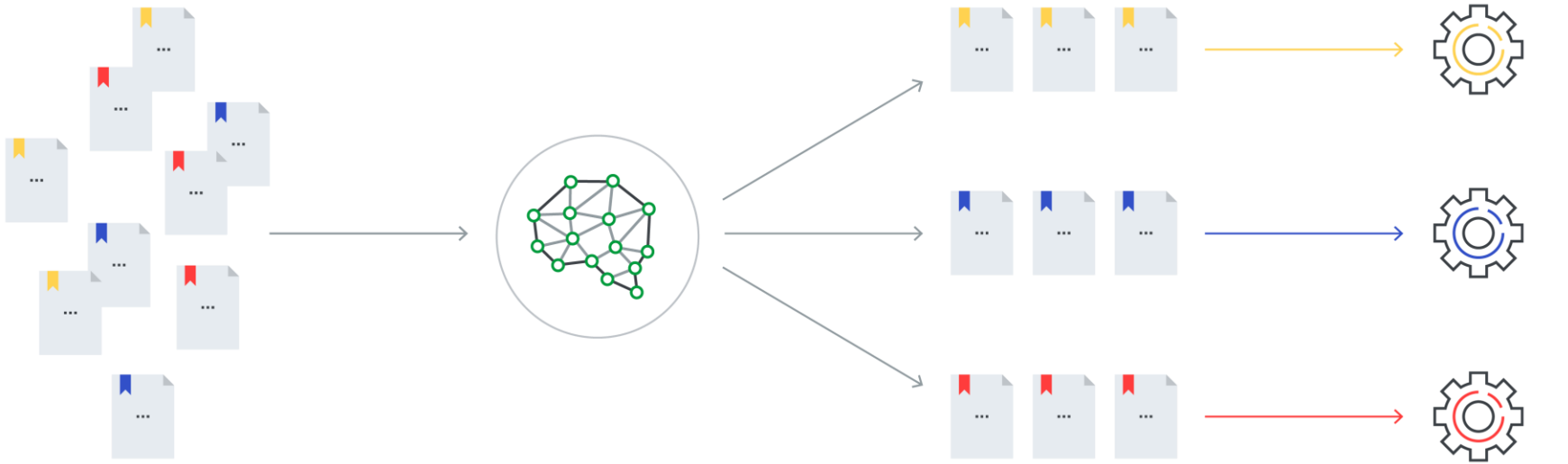
→ Пару минут и готово

Машинное зрение для защиты конфиденциальных изображений

- → Никаких профессиональных знаний
- → Никакой предварительной обработки
- → Документы разного типа, объема, и содержания
- → Обучение всего пару минут
- → Качество как у профессионального лингвиста



Автоматический поиск образцов документов



Неисследованный поток данных

ИИ категорирует ВСЕ документы компании за 1 день

Документы по категориям

Обучение DLP с помощью Автолингвиста

Автоматизированное обучение DLP-системы с помощью ИИ

- → Нахождение новых категорий документов, в условиях полной неизвестности
- → Профилактика ЛОС
- → Исследование серых зон

Предотвращение скрытых или готовящихся нарушений

У департамента ИБ не всегда есть ресурсы на мониторинг аномалий и подозрительных совокупностей событий

Мониторинг и реагирование на инциденты

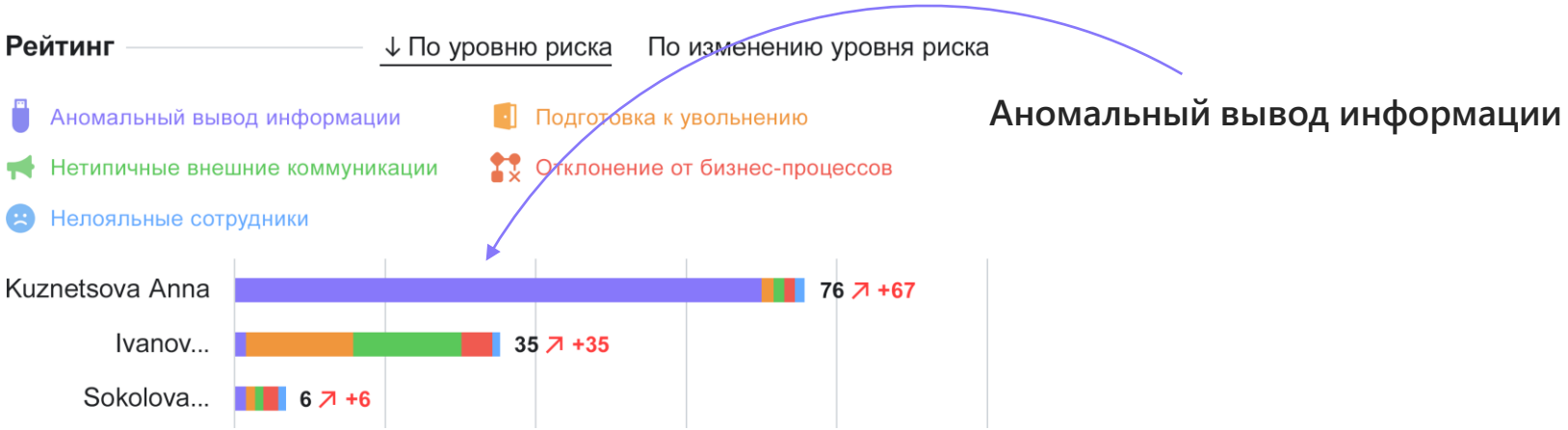
Активные меры по блокировке утечек

Прогнозирование и управление рисками

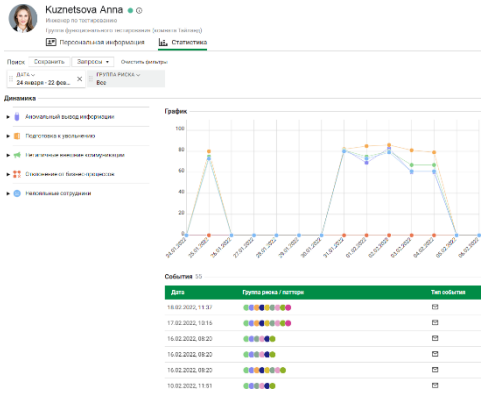
- Аномальный вывод информации
- Подготовка к увольнению
- Нетипичные внешние коммуникации
- Отклонение от бизнес-процессов
- Нелояльные сотрудники

Кейс. Массовый вывод информации

Специалист ИБ обнаружил на 1 месте в рейтинге Prediction инженера производственно-технического отдела



Кейс. Массовый вывод информации
Анализ досье Prediction



1 На протяжении недели, даже в выходные, массово копировал документы на внешний носитель — **800 документов** →

Проверка деталей событий

- **Сотрудник отправил:** технологические карты, акты, согласующие письма, паспорта качества, журналы продукции, личные документы под паролем — рекомендации по трейдингу, кредитные договоры
- **Под действие политик попало только 18 файлов из 800, остальные в «серой зоне»**

2 Самые массовые копирования, более 200 и 400 файлов, за границами рабочего дня — до 9:00 и после 18:00

Сотрудник поставлен на особый контроль. Ужесточена политика копирования на внешние носители. Файлы под паролем проверены на предмет утечки

Предиктивная аналитика на основе ИИ помогает управлять рисками и работать на опережение

- → Подсказывает, каких сотрудников необходимо проверить или поставить на особый контроль в первую очередь
- → Помогает понять, когда политики DLP нуждаются в подстройке
- → Предоставляет конкретные данные для принятия решений и снижает рутинную нагрузку на департамент ИБ

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®

УВИДИМСЯ В НАШЕМ ТЕЛЕГРАМ-КАНАЛЕ!

Свежий отчёт об утечках на подходе!

/InfoWatchOut

/InfoWatch

INFOWATCH

СПАСИБО ЗА ВНИМАНИЕ!

Александр Клевцов

Руководитель по развитию продукта
InfoWatch Traffic Monitor

/InfoWatchOut /InfoWatch