INFOWATCH®

УСИЛИВАЕМ ЗАЩИТУ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

на примере новой версии Traffic Monitor

Владимир Дурнев

Менеджер по работе с клиентами и партнерами

InfoWatch Калининград

Группа компаний InfoWatch

INFOWATCH®

С 2003 года на рынке информационной безопасности

Сертификация на соответствие требованиям **ФСБ, ФСТЭК** и отраслевых стандартов

37 из 50-ти крупнейших компаний России используют решения InfoWatch

Технологическое лидерство, подтверждённое патентами

Представительства в **15-ти регионах** России и СНГ

3500 проектов из 20-ти отраслей в 20-ти странах

Решения InfoWatch

InfoWatch Traffic Monitor

Система защиты конфиденциальной информации нового поколения, которая с помощью технологий искусственного интеллекта предотвращает утечку конфиденциальной информации, в автоматизированном режиме актуализирует политики безопасности и помогает прогнозировать риски ИБ

- → Модуль для автоматизированной настройки политик безопасности. Оптимизация работы службы ИБ
- → Модуль для визуальной аналитики данных, собранных DLP-системой. Ускорение расследований
- → Для мониторинга персонала. Эффективность работы
- → Модуль для предиктивной аналитики данных DLP-системы. Управление рисками

InfoWatch ARMA

Эшелонированная защита промышленных предприятий

- → INFOWATCH ARMA INDUSTRIAL FIREWALL
- → INFOWATCH ARMA MANAGEMENT CONSOLE
- → INFOWATCH ARMA INDUSTRIAL ENDPOINT

INFOWATCH®

InfoWatch Traffic Monitor

DLP-система нового поколения

- → Высокая точность детектирования данных благодаря искусственному интеллекту
- → Продвинутые технологии контентного анализа
- → Автоматизация настроек политик безопасности
- → Универсальный перехватчик файлов
- → Интеграция с любыми системами благодаря открытому API

Какие данные мы защищаем

→ Защита конфиденциальных документов

Договор, бухгалтерская документация, налоговая декларация, исходный программный код

→ Защита персональных и других именованных данных

Данные сотрудников, клиентов, номенклатура, прайс-листы, паспортные данные, ИНН

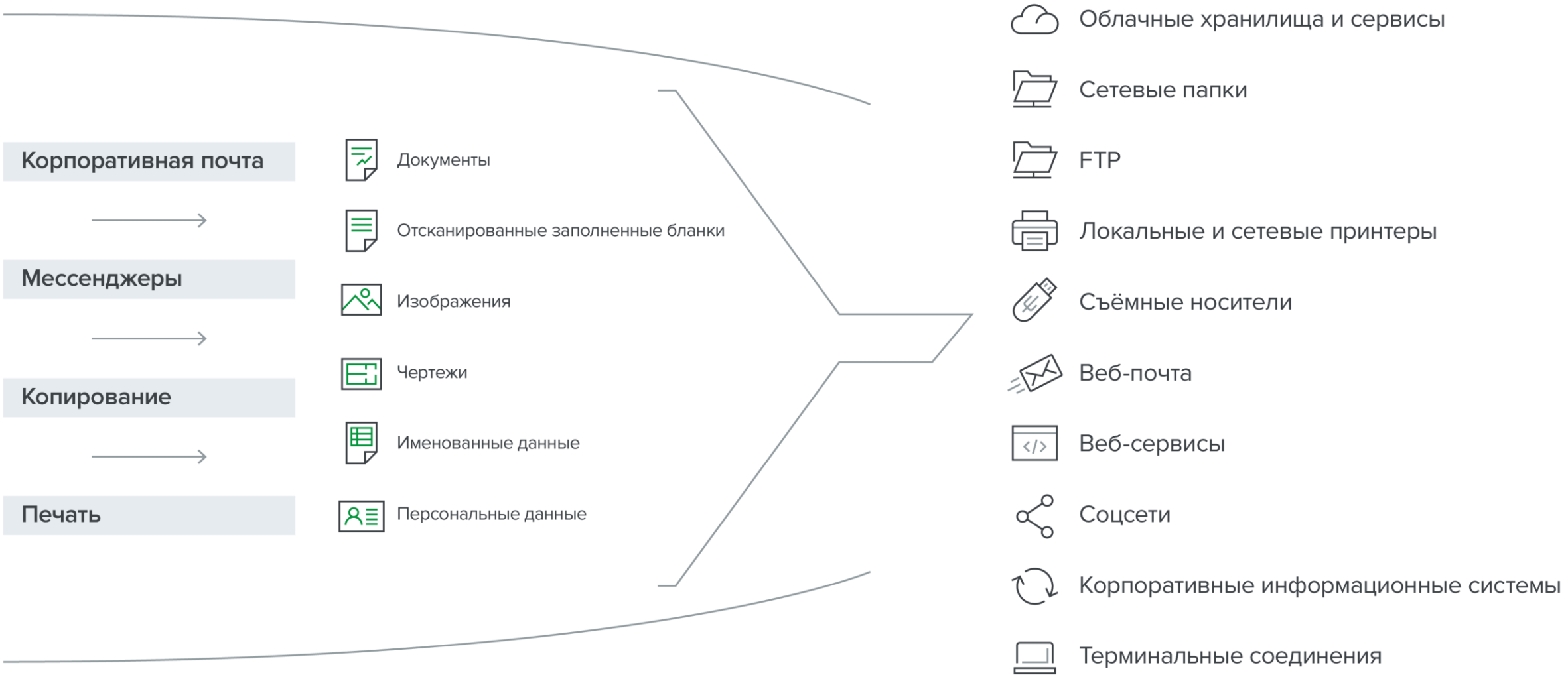
→ Защита графических данных

Сканы и фото документов, печати, анкеты, бланки, фотоматериалы, географические карты, схемы, сканы паспортов и банковских карт

→ Защита конфиденциальных чертежей

Проектной, конструкторской и технической документации

...по всем необходимым каналам коммуникаций и пунктам назначений



Универсальный перехватчик файлов

Чтобы контролировать передачу файлов через приложение, нужно, чтобы **DLP-вендор поддержал это приложение**

При изменении протокола приложения **перехват может отвалиться,** такое случается регулярно

Универсальный перехватчик файлов

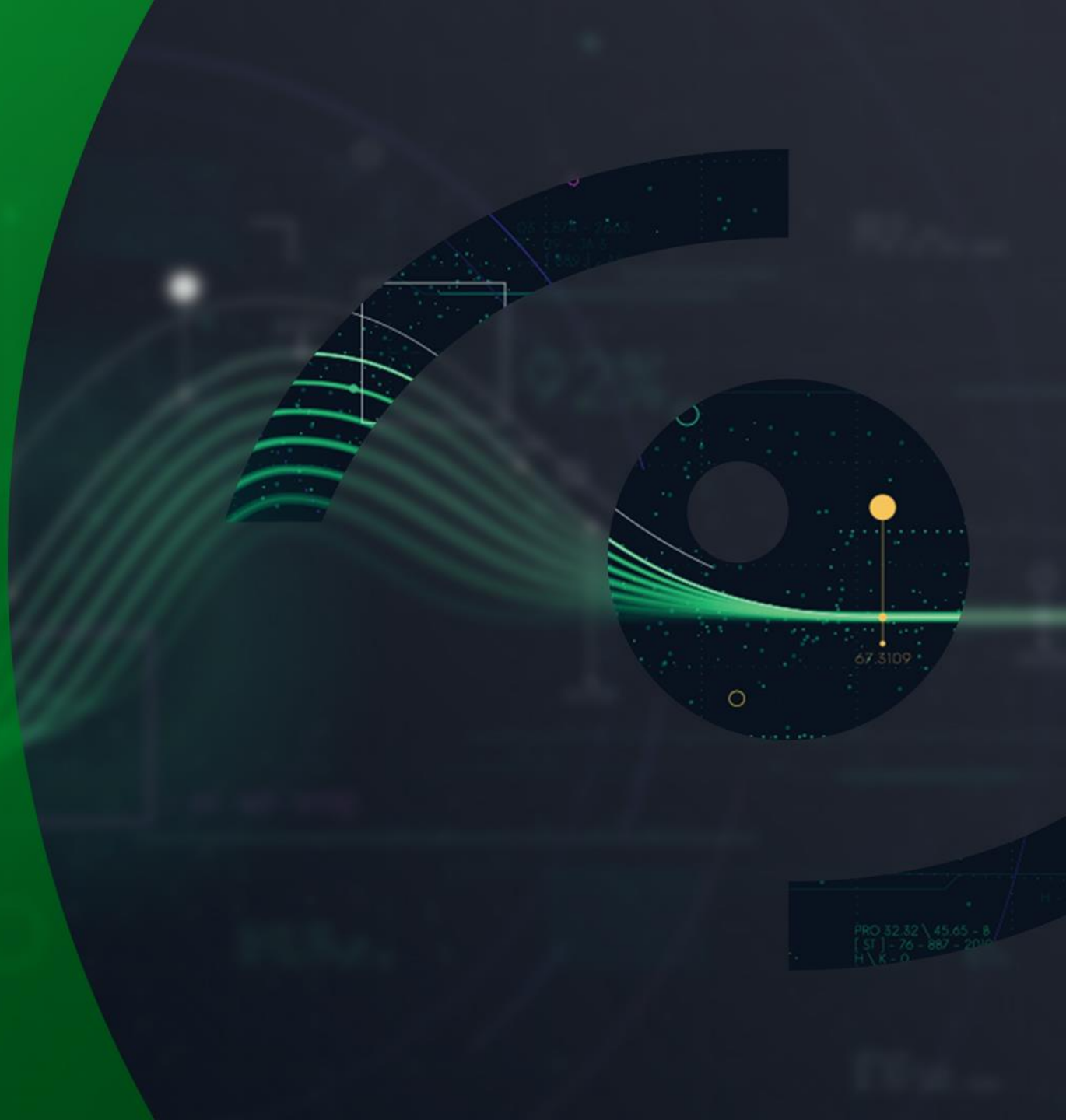
Не зависит:

- → От протокола приложения
- → От способа шифрования
- → От специфики передачи данных веб-сервиса (например, AWS, Google, MS Azure могут передавать файлы через WebSocket*)
- → Доработка под любое приложение за несколько часов

INFOWATCH®

НОВЫЙ МОДУЛЬ INFOWATCH DATA EXPLORER

Меняет традиционные практики работы с системой защиты конфиденциальной информации



Активный этап пилотирования

Обучение DLP-системы под каждого заказчика

→ **Эксперты InfoWatch помогут настроить DLP-систему** с учётом уникальных особенностей и специфики бизнес-задач заказчика

→ **Но что делать, если нет возможности пригласить экспертов?**

Использовать ИИ для классификации текста

Автоматизированная настройка политик безопасности

INFOWATCH®

→ **При внедрении.** Департаменту ИБ не всегда известно, как устроены бизнес-процессы, какая информация и как ходит в компании

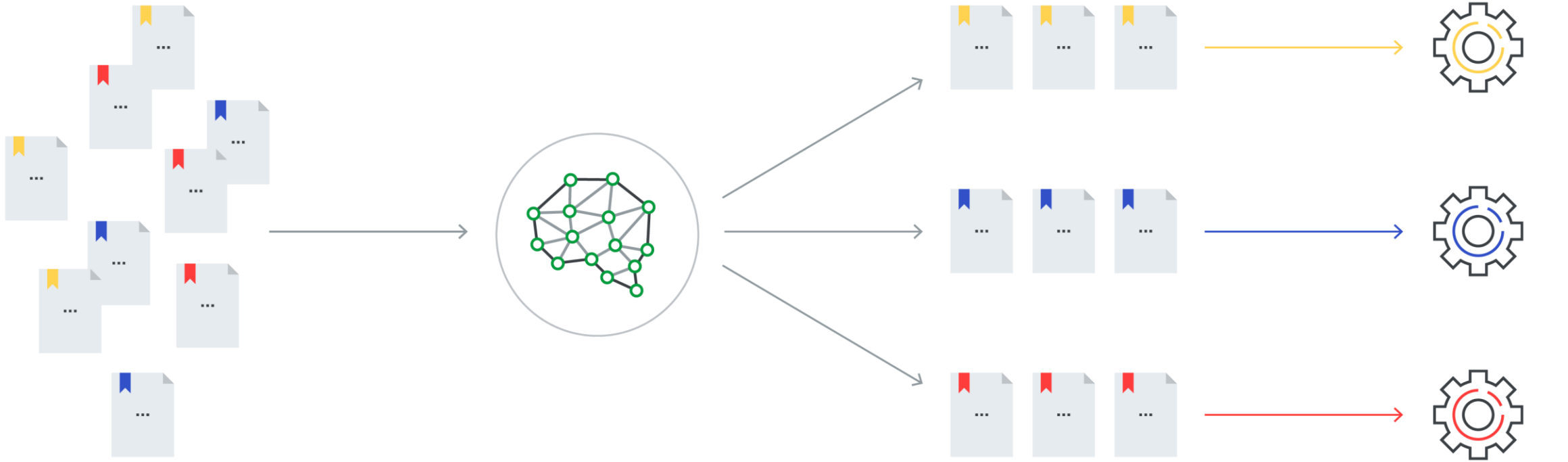
→ **В процессе эксплуатации.** Новые категории конфиденциальной информации появляются постоянно, количество данных увеличивается лавинообразно

- Исследование информационных потоков может занимать 2 недели
- Создание словаря для категории документов — 5–10 дней
- Наличие «слепой зоны» — удаётся контролировать до 30% документов

Как упростить настройку и обновление политик безопасности и делать это чаще, чем раз в полгода?

ИИ-технологии позволят быстро и безошибочно классифицировать документы и настраивать политики безопасности

Data Explorer — категоризация документов с помощью технологий ИИ



Неисследованный поток данных

ИИ категорирует ВСЕ документы компании за 1 день

Документы по категориям

Обучение DLP с помощью Автолингвиста

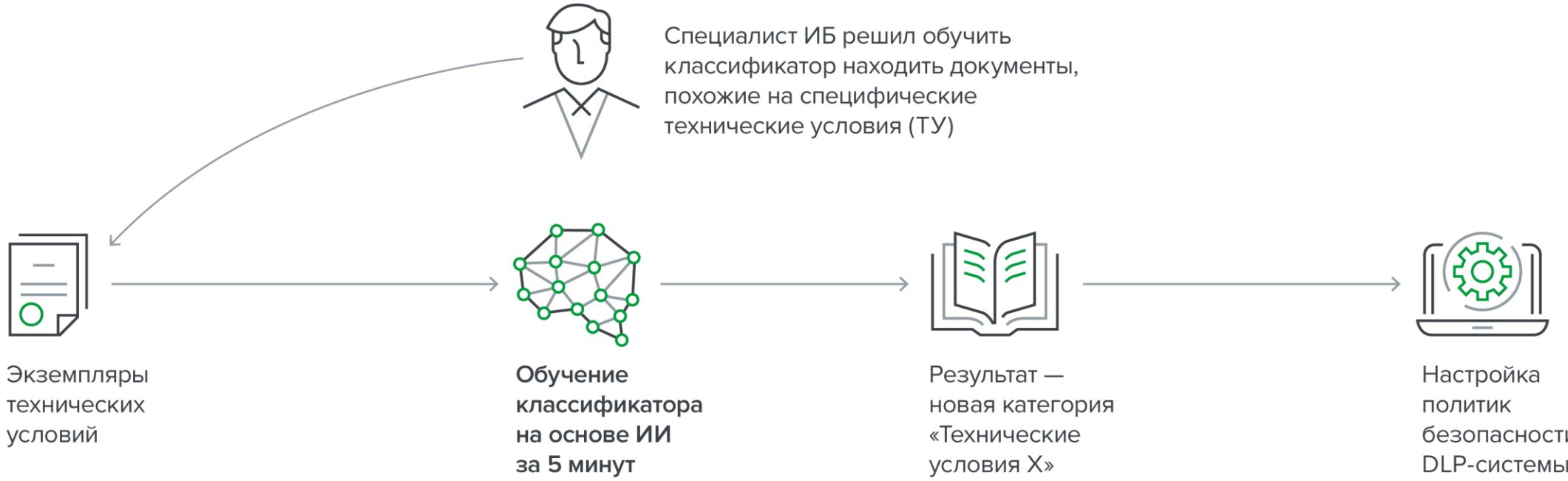
Автолингвист — автоматическое обучение DLP-системы новым категориям документов

INFOWATCH®

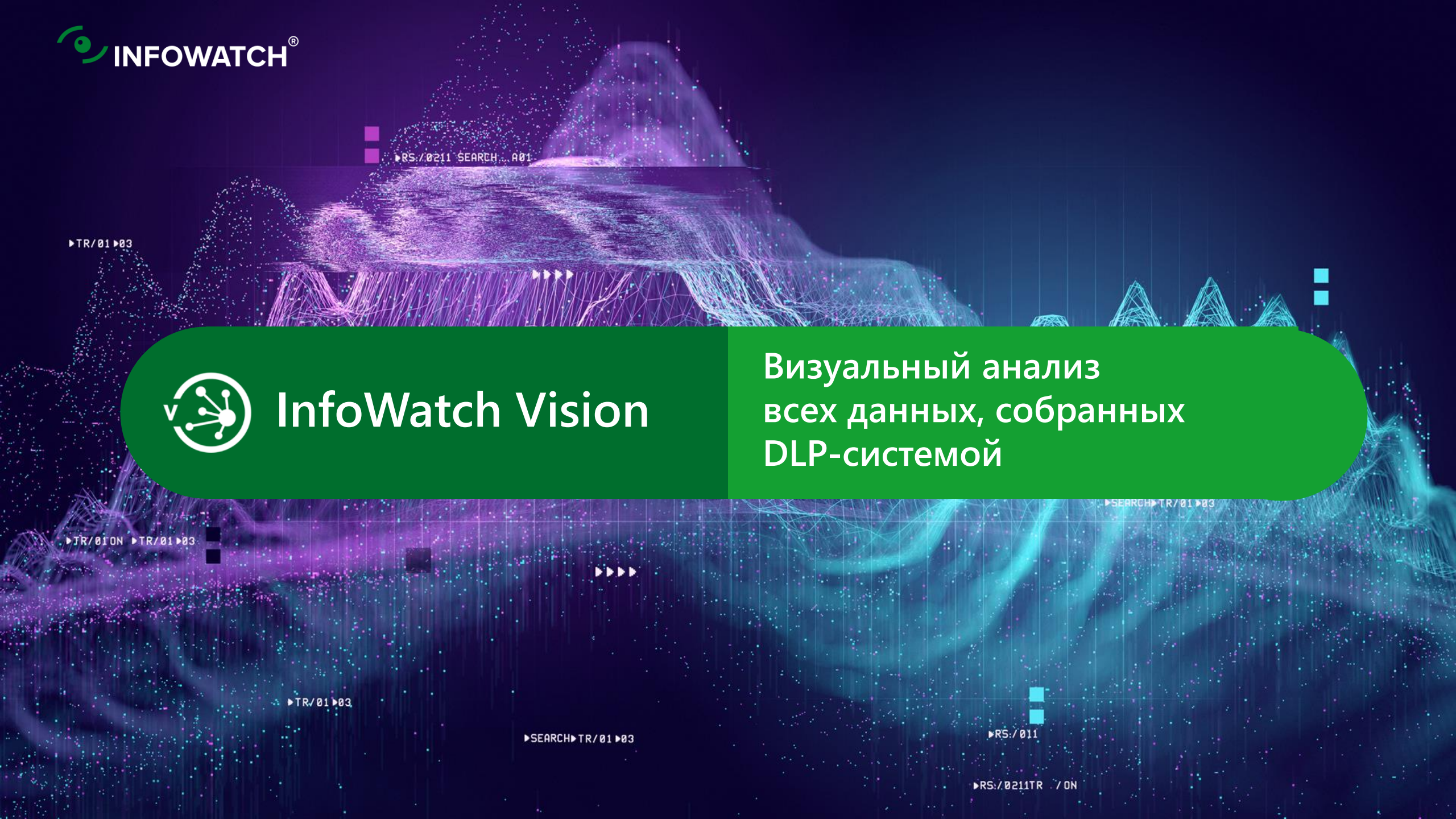
→ На документах заказчика

→ Без привлечения экспертов-лингвистов

→ ВСЕ документы за 1 час, а не 10 дней



Автоматизация настроек политик безопасности и ликвидация «серых зон»

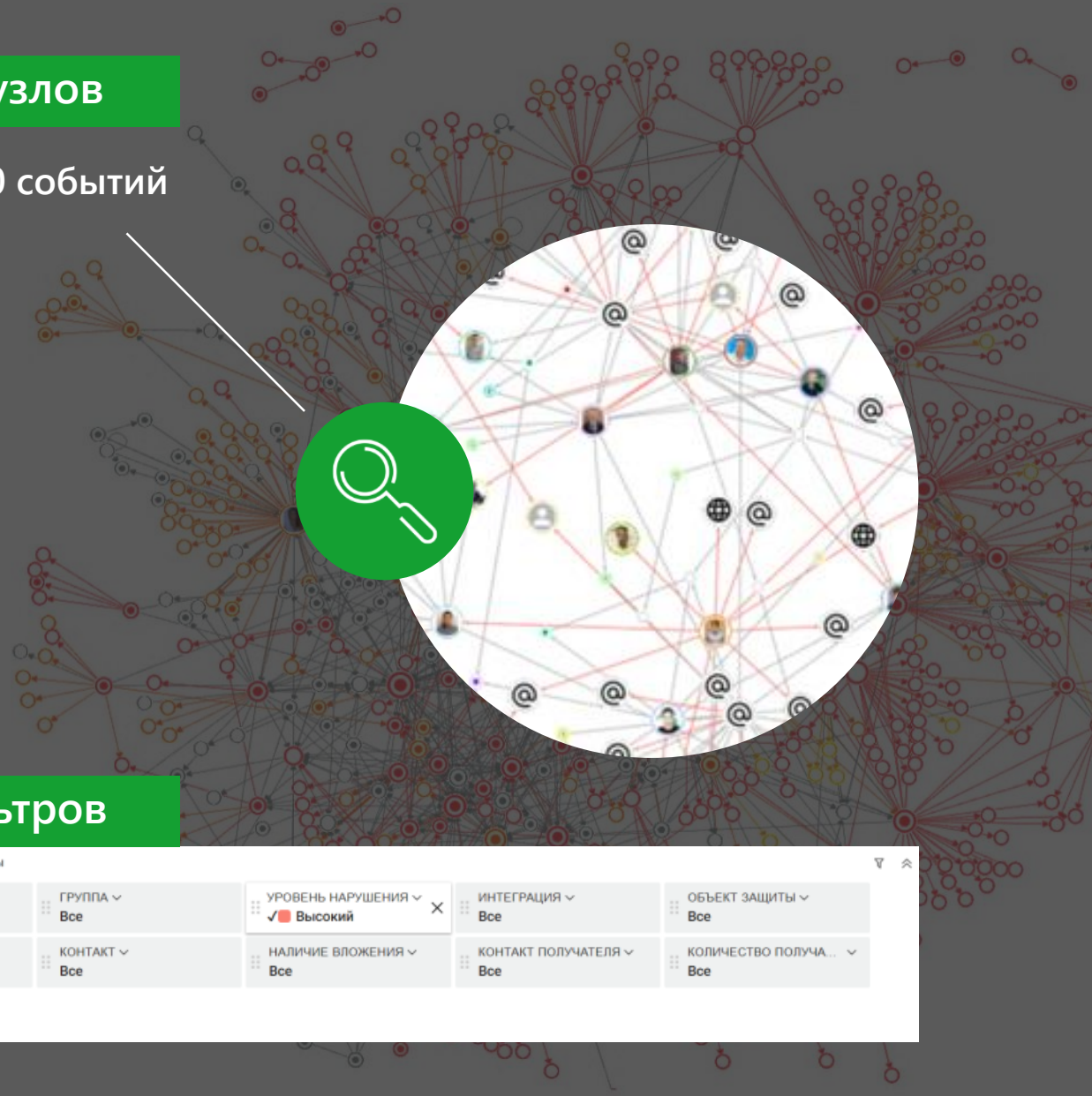

INFOWATCH®
InfoWatch Vision
Визуальный анализ
всех данных, собранных
DLP-системой

DLP видит реальную картину и в разных срезах

INFOWATCH®

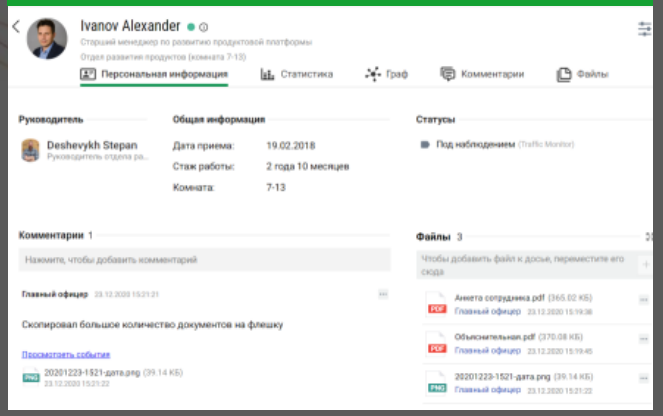
Граф связей 50K узлов

→ Анализ 100 000 000 событий в секунду



25 виджетов

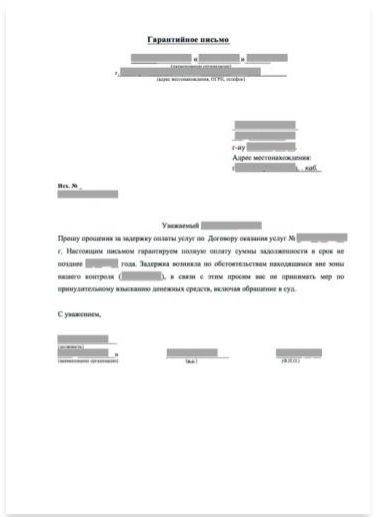
Цифровые досье

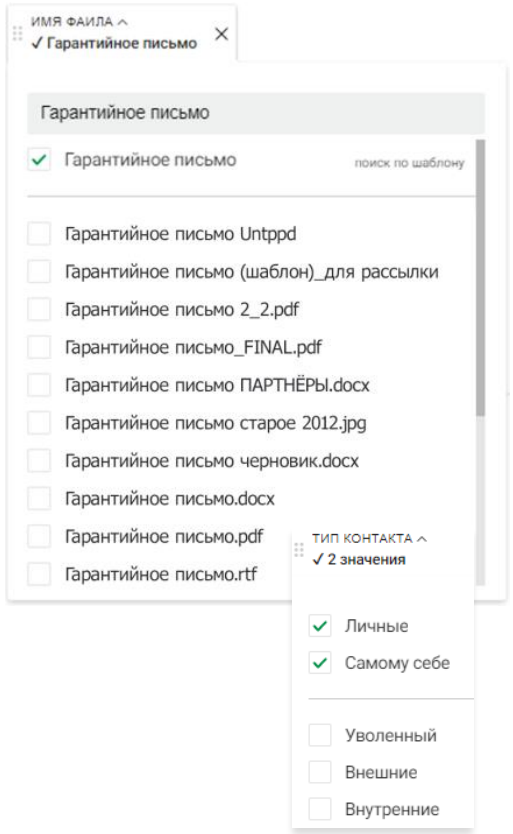


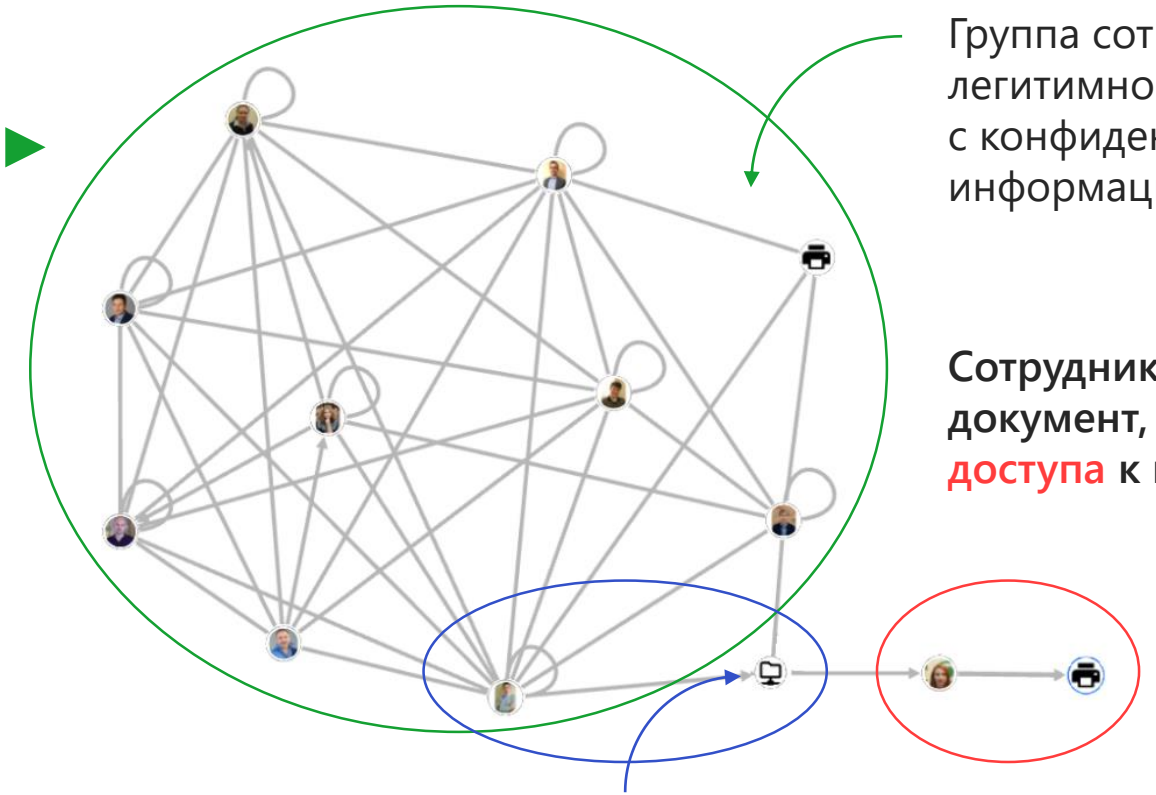
40 сквозных фильтров

Как провести расследование за 5 минут, а не за несколько часов?

1	В интернете обнаружено фото документа
2	Поиск по общей части в имени файла
3	Граф связей перемещения информации в компании







Группа сотрудников легитимно работает с конфиденциальной информацией

Сотрудник распечатал документ, хотя не имел доступа к информации

Выгрузка в сетевую папку

INFOWATCH®

InfoWatch Prediction — предиктивная аналитика данных DLP-системы

От рутинной работы с инцидентами — к прогнозированию и профилактике

- → Анализ поведения сотрудников **с помощью ИИ**
- → Построение **динамических моделей поведения** каждого сотрудника
- → Оценка рисков и **оповещение о самых опасных** тенденциях

Группы риска: как ищем отклонения

Поведение сотрудника анализируется с помощью технологий машинного обучения, чтобы показать:

Аномалии относительно привычного поведения сотрудника

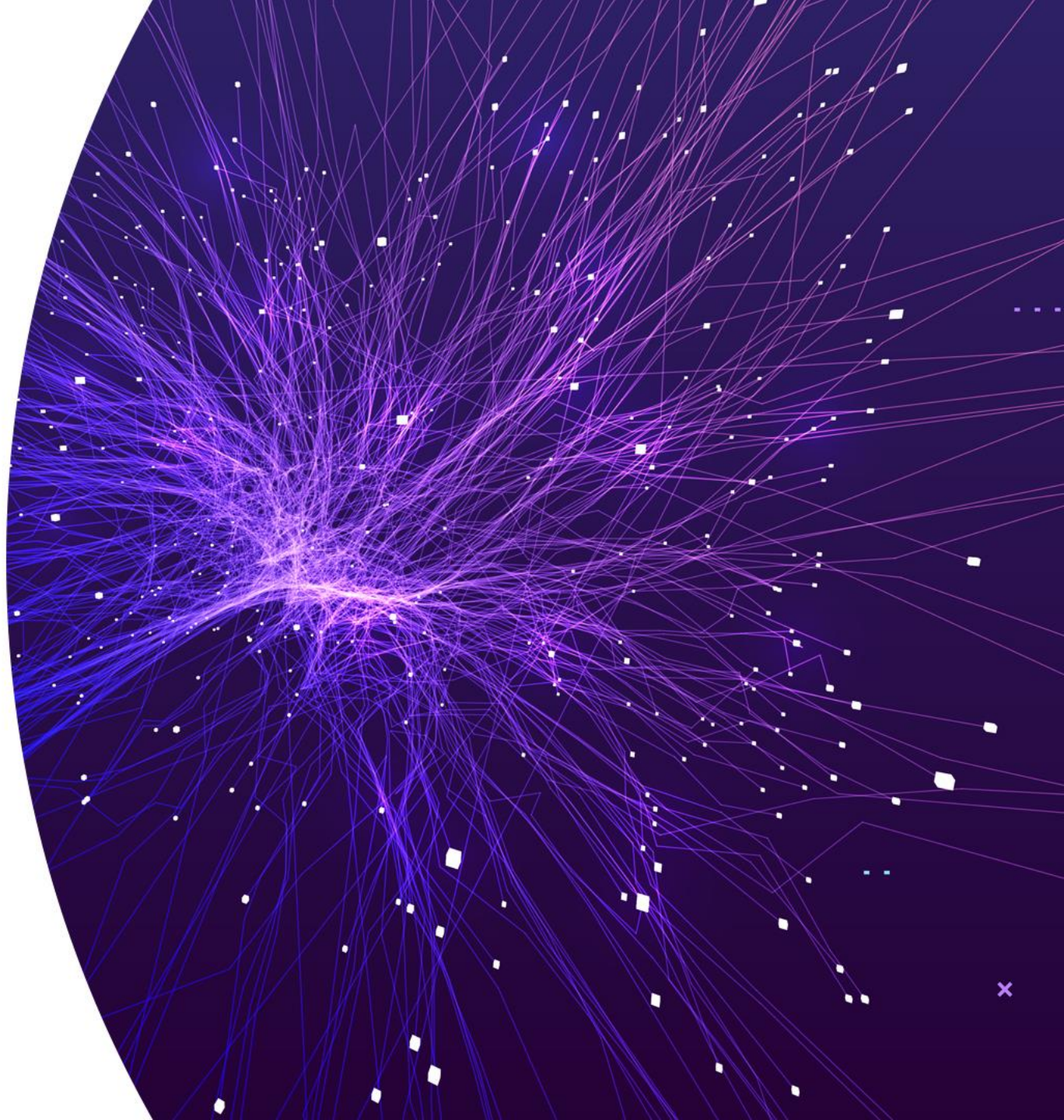
Например: сотрудник напечатал нетипично большой для него объём документов. Возможно, он использует корпоративные ресурсы в личных целях

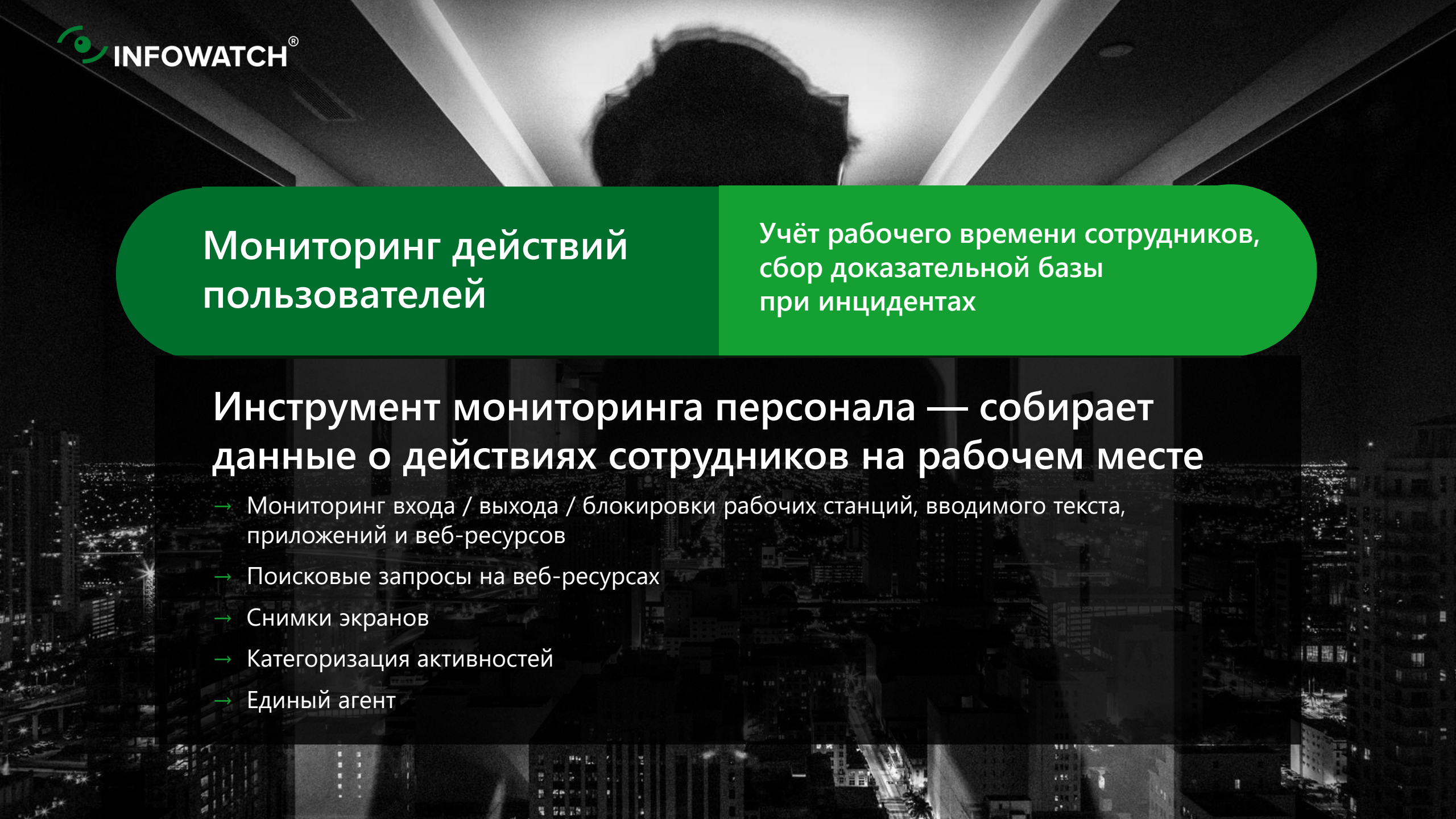
Цепочки связанных потенциально опасных действий

Например: сегодня сотрудник написал коллеге, что ему всё надоело, через неделю стал опаздывать на работу, потом отправил несколько файлов на личную почту и ещё пару сохранил на флешку. Похоже, сотрудник решил увольняться и уже начал понемногу выводить информацию

Prediction автоматически прогнозирует риски и уведомляет о самых значимых

- → **Анализ поведения сотрудников** с помощью машинного обучения
- → **Динамические модели** поведения каждого сотрудника, а не статичные шаблоны. Группы риска на основе индивидуального скоринга
- → **Оценка рисков и оповещение** о самых опасных трендах
- → **Только необходимые оповещения с заданной частотой!**





INFOWATCH®

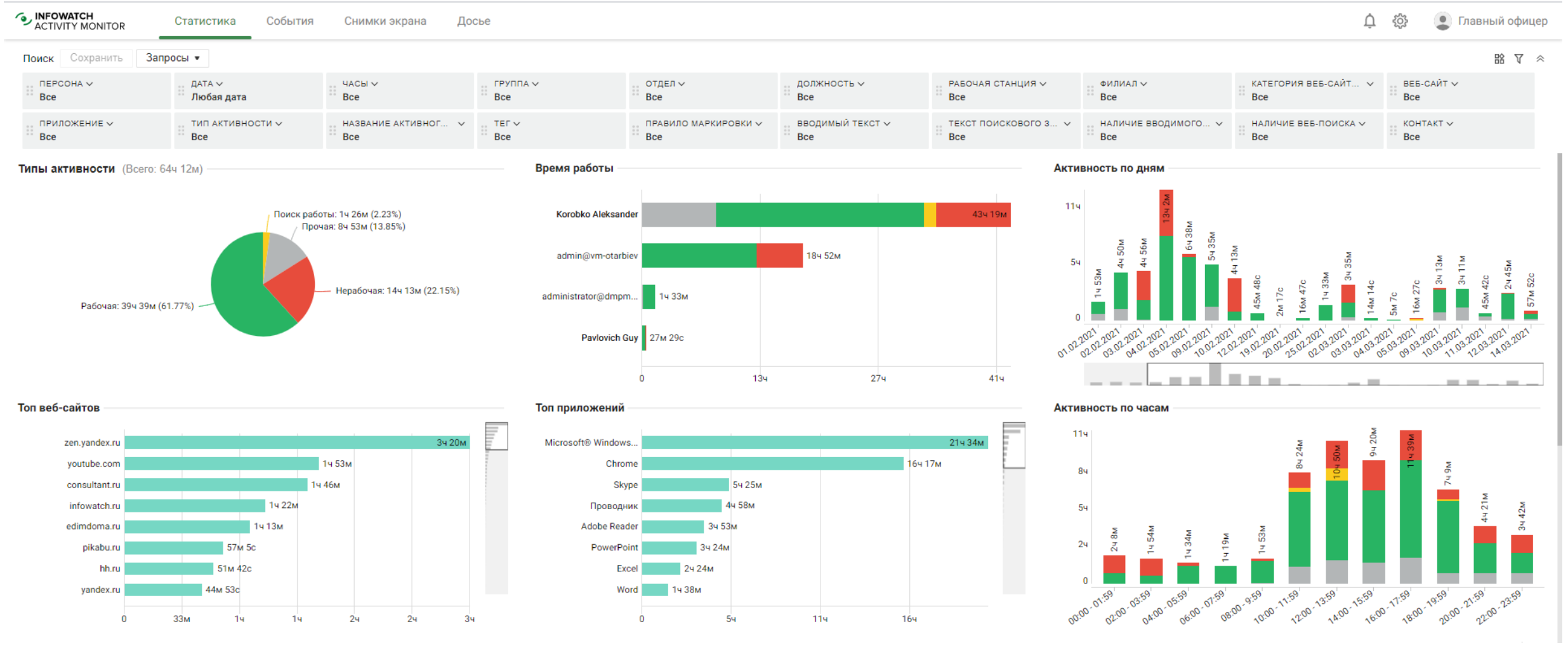
Мониторинг действий пользователей

Учёт рабочего времени сотрудников, сбор доказательной базы при инцидентах

Инструмент мониторинга персонала — собирает данные о действиях сотрудников на рабочем месте

- → Мониторинг входа / выхода / блокировки рабочих станций, вводимого текста, приложений и веб-ресурсов
- → Поисковые запросы на веб-ресурсах
- → Снимки экранов
- → Категоризация активностей
- → Единый агент

Единая консоль и быстрый анализ статистики



Сводная статистика по времени активности сотрудников,
топ приложений, топ сайтов, динамика по датам и времени

Новаторский подход InfoWatch к защите данных

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

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

Консалтинг

Процессы * система = эффективность

Чтобы данные были действительно защищены, а система помогала в расследовании инцидентов и отрабатывала на 100%, необходимо сначала навести порядок в процессах, а потом внедрять технологии.

Учитывая юридические тонкости.

Консалтинг от InfoWatch это:

- → Определение проблемных зон в процессах защиты
- → Обследование, анализ, разработка процессов категорирования и обращения с информацией
- → Разработка нормативных документов в области информационной безопасности
- → Выстраивание процессов ИБ

INFOWATCH®

ПОПРОБОВАТЬ ТЕХНОЛОГИИ В ДЕЛЕ?

ПРОВЕДЁМ ПИЛОТ БЕСПЛАТНО!

Больше полезной информации:

/InfoWatchOut

/InfoWatch

Владимир Дурнев

Vladimir.Durnev@infowatch.com

www.infowatch.ru