INFOWATCH®

# ЗАЩИТА ОТ УТЕЧЕК ДАННЫХ И КИБЕРБЕЗОПАСНОСТЬ КИИ

**Что выбрать в условиях кадрового голода в ИБ?**

**Виталий гущин**
**Infowatch**

# 80%

**ГОСОРГАНИЗАЦИЙ, СИСТЕМООБРАЗУЮЩИХ КОМПАНИЙ И СУБЪЕКТОВ КИИ НЕ ХВАТАЕТ ИБ-СПЕЦИАЛИСТОВ**

Минцифры РФ

# Средства ИБ вынуждены совершенствоваться

INFOWATCH®

**×2**

## БОЛЬШЕ СРЕДНИЙ ОБЪЁМ УТЕЧКИ

*Данные ЭАЦ InfoWatch*

**98%**

## УТЕЧЕК — УМЫШЛЕННЫЕ

*Данные ЭАЦ InfoWatch*

**Объём утечек растёт. Они умышленные, а значит — более изощрённые**

# Средства ИБ совершенствуются — собирают всё больше данных

INFOWATCH®

**2 000 000**

**СОБЫТИЙ В ДЕНЬ**

регистрирует InfoWatch Traffic Monitor у нашего клиента

**5%**

**ИНЦИДЕНТОВ**

= 100 000 событий. Если не все данные под политиками ИБ, попыток утечки может быть ещё больше

**Вручную всё обработать невозможно. Как сфокусироваться на важном?**

# Защищать 100% данных становится дороже — стоимость и эксплуатация


## Для глубокой и непрерывной аналитики приходится

— Использовать всё больше средств ИБ

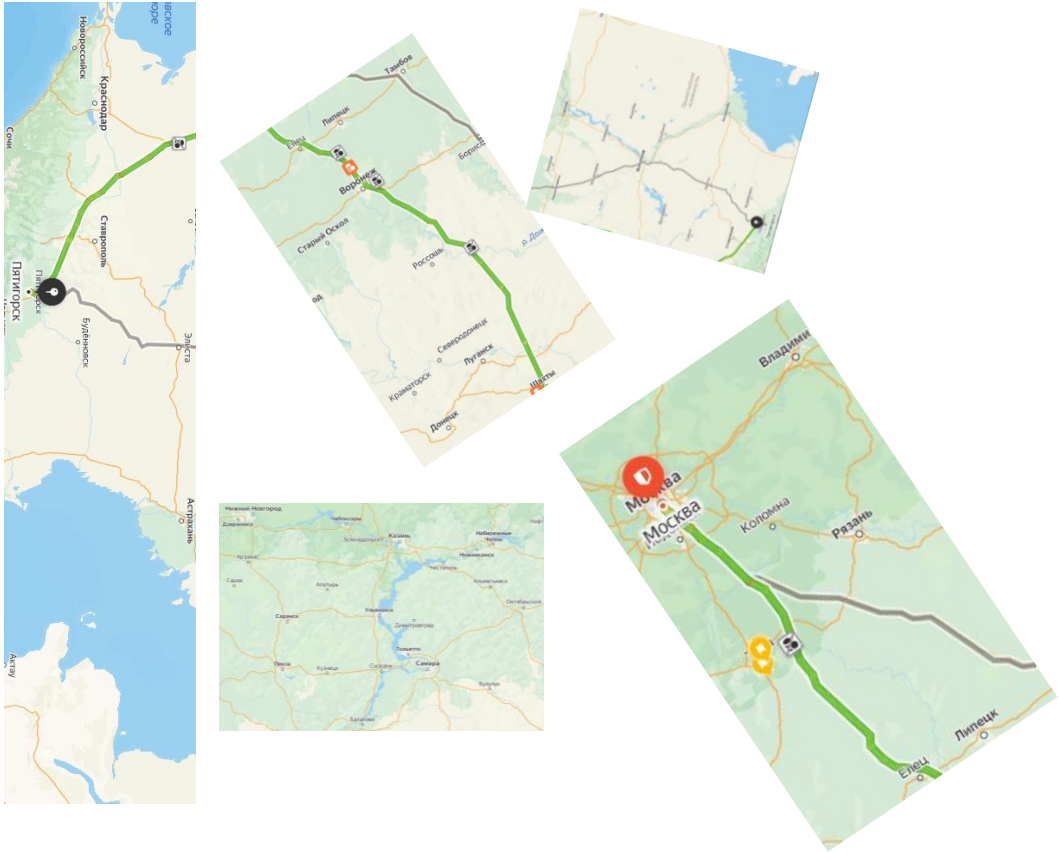
— Сопоставлять данные из нескольких средств ИБ

— Расширять департамент ИБ

— Делать выводы на основе разных данных, обеспечивать совместную работу и оформлять кросс-отчёты

**А сопоставлять вручную = терять непрерывность и регулярность защиты**

# Другие инструменты ИБ на рынке




— **DLP без всех необходимых возможностей**

Нет возможностей — нет проблем
с переключением внимания

— **Возможности есть, единой консоли нет**

Сложно переключаться и сохранять контекст
расследования

— **Единая консоль есть, единого фильтра нет**

Сохранять контекст мешает механизм
получения данных — через статичные отчёты

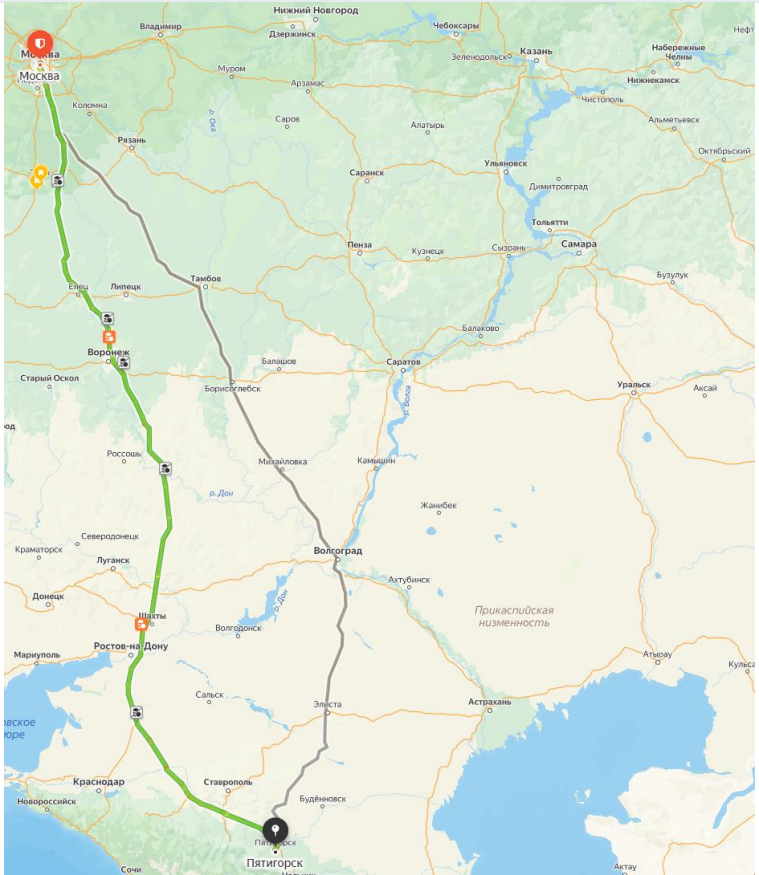
— **Набор рабочих панелей ограничен**

Специалист ИБ тратит лишнее время
на ежедневный мониторинг и контроль

— **Результаты расследований в стороннем ПО**

В MS Word, Excel или облачных блокнотах

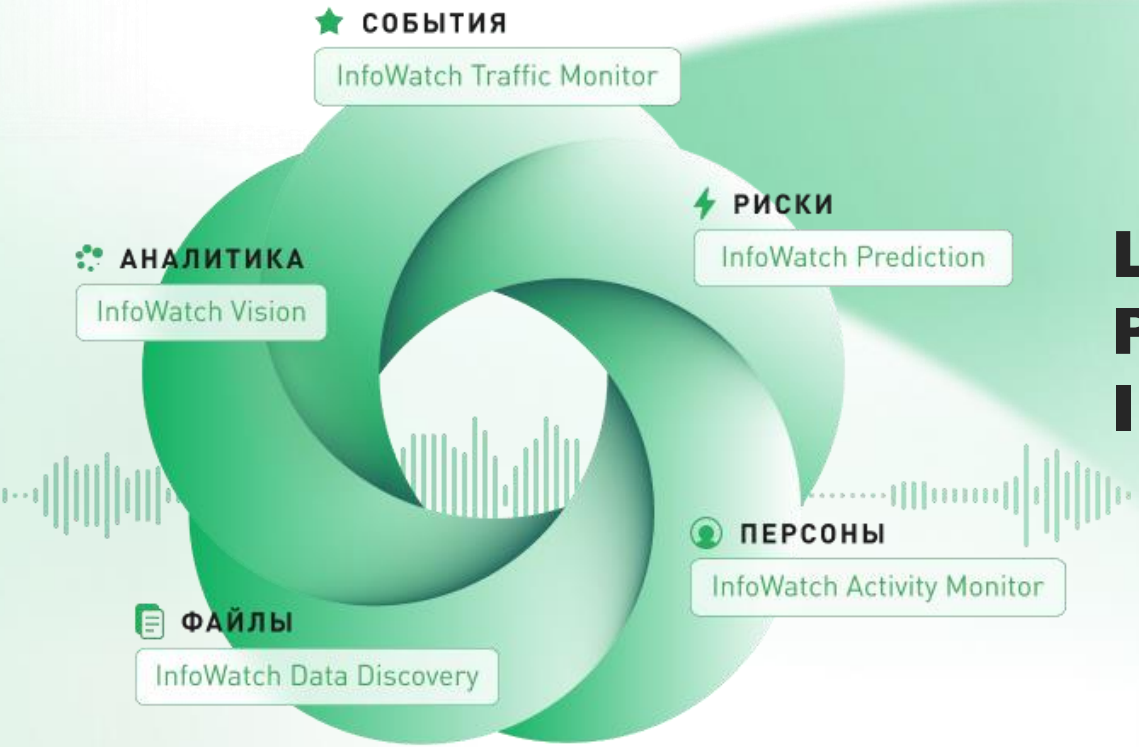
# Как в 3 раза сократить время от первого подозрения до принятия решения?




- **Нормализовать и сопоставить данные** — в едином информационном пространстве
- **Единая консоль** — быстро переключаться между средствами ИБ
- **Единый фильтр и интерактивный интерфейс** — быстро переключаться между срезами данных, сохранять контекст и фокус на важных деталях
- **Настраиваемые рабочие панели** — нужное количество под каждую роль
- **Встроенный блокнот расследований** — оформление отчёта без переключения на стороннее ПО

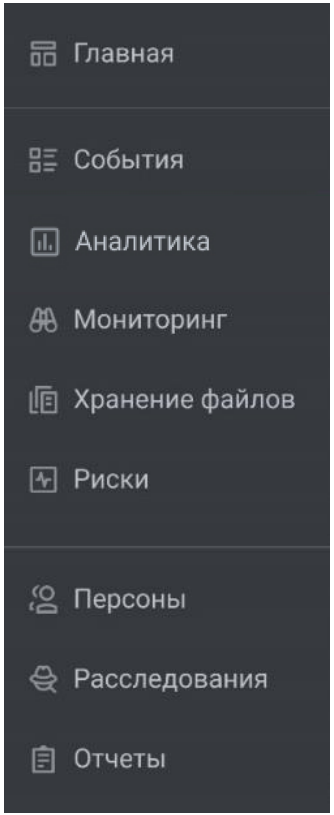
# Расследования и мониторинг выходят на новый уровень!

INFOWATCH®




## ЦЕНТР РАССЛЕДОВАНИЙ INFOWATCH

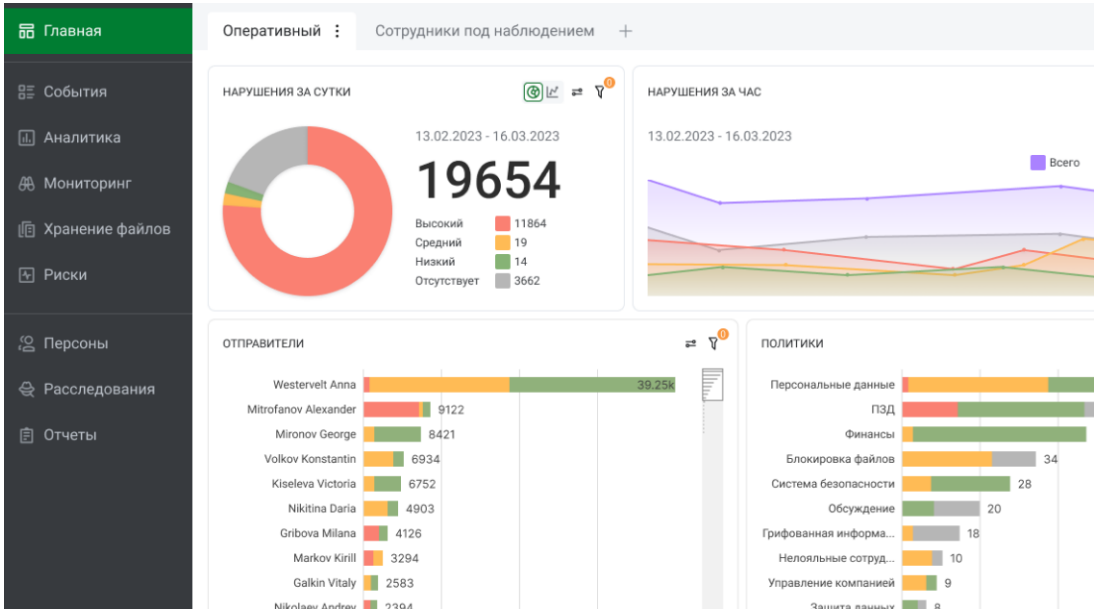
# Пример расследования в едином информационном пространстве

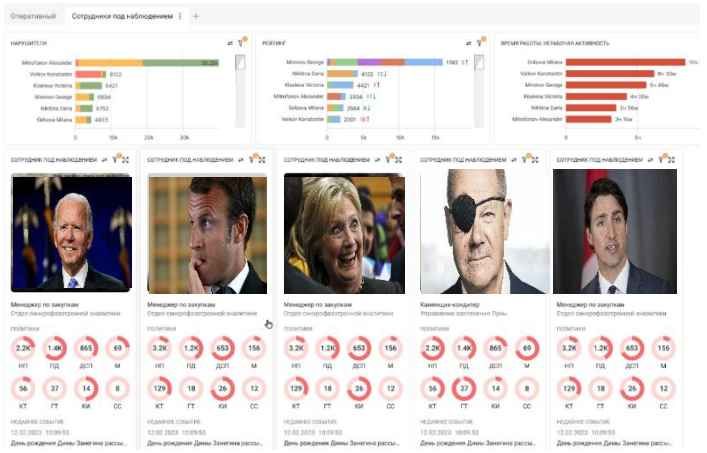



1. На виджете «**Отправители**» специалист ИБ увидел нарушителя и начал по нему расследование
2. Перешёл в **события,** добавил нужные в расследование
3. Посмотрел все связи подозреваемого и нашёл подельников на **графе связей**
4. Изучил **хронологию** — что сотрудник делал до, во время и после нарушения
5. Провёл аудит — какая ценная информация хранится на ПК сотрудника и в его «облаке»
6. Посмотрел, в какие **группы риска** входит подозреваемый
7. Изучил **досье**
8. Оформил **расследование**

# Настраиваемые рабочие панели

## Искать самые критичные инциденты или сконцентрироваться на персонах под особым контролем



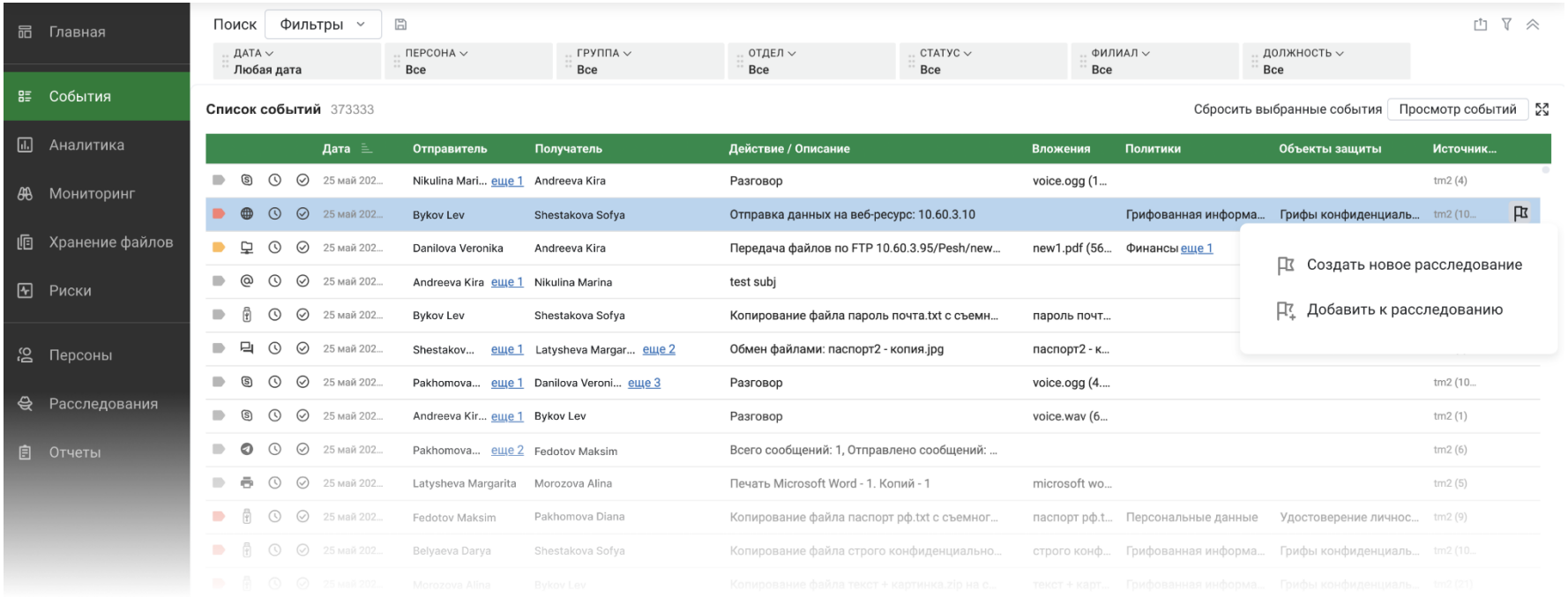



— 38 виджетов на выбор

— Можно настроить положение, порядок и размер

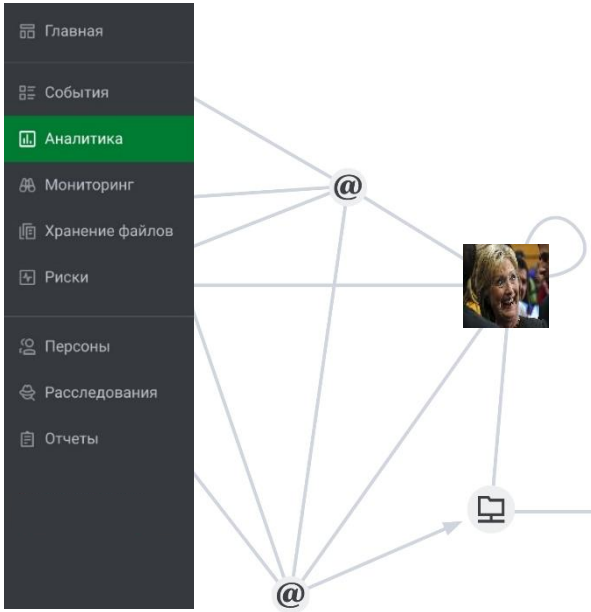
# Лента событий DLP

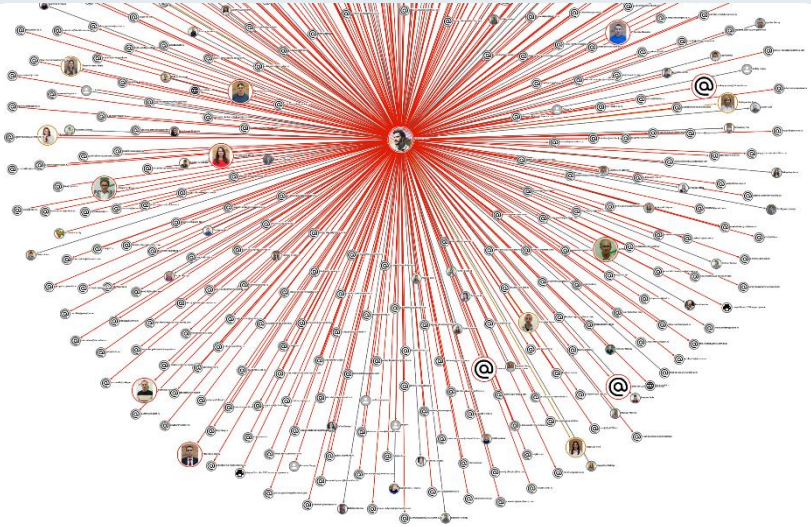
## С детализацией, фильтрацией и возможностью добавить события в новое или открытое расследование



# Интерактивный граф связей

**Найти всех соучастников, выявить неявные связи и пути перемещения документов**

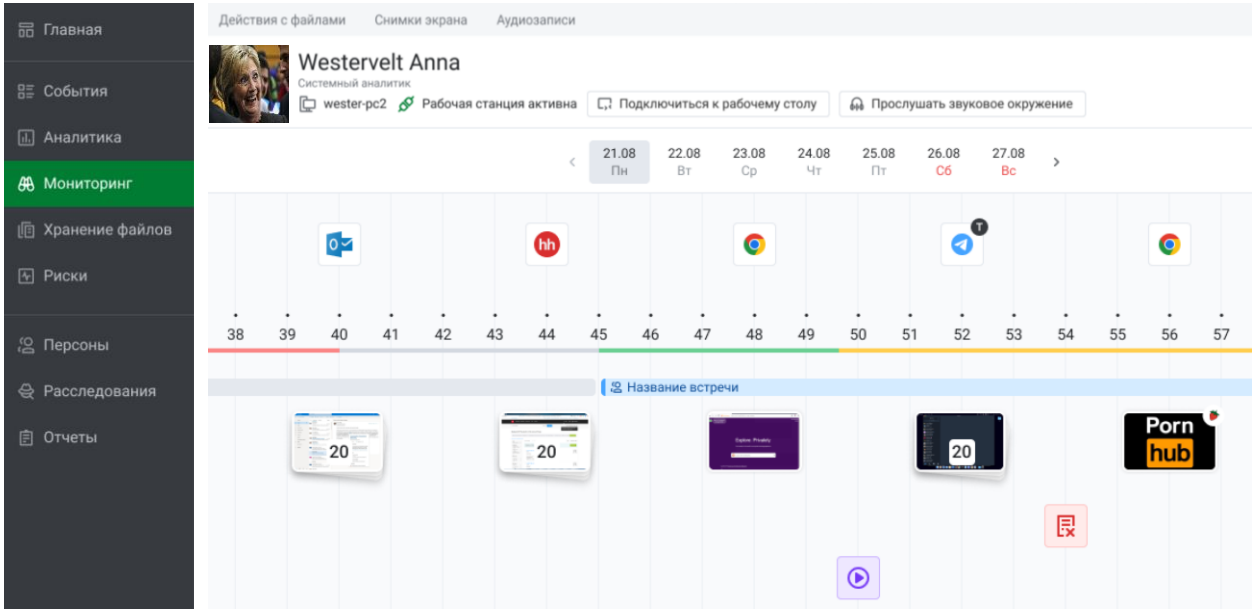


- Отображает одновременно до 50 000 узлов
- Динамически перестраивается при применении фильтров
- Данные для фильтрации можно выбрать прямо на графе

# Интерактивный таймлайн действий

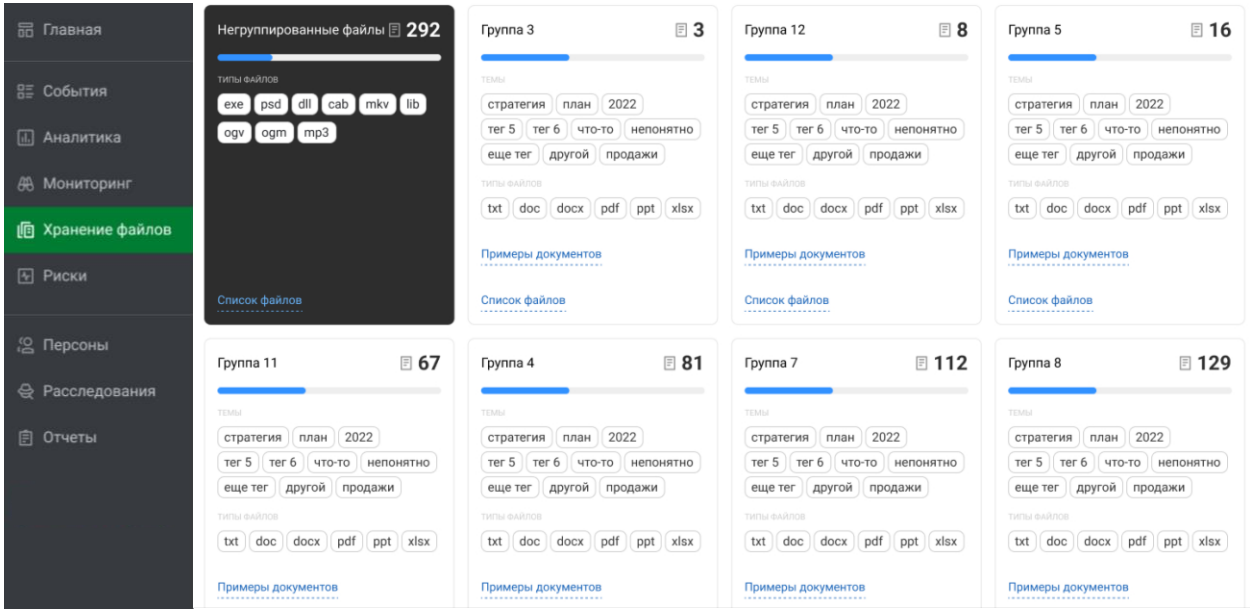
**Восстановить полную картину действий сотрудника до, во время и после инцидента**




- Проходы по СКУД, входы и выходы из учётной записи, введённый с клавиатуры текст, поисковые запросы и открытые сайты, работа файлами и приложениями, снимки экрана, аудиозаписи и их расшифровка
- Визуализирует картину рабочего дня и позволяет восстановить контекст
- По клику на элементы таймлайна доступны детали всех событий

# DCAP и категоризация 100% документов

## Аудит хранения и прав доступа, исправление проблем



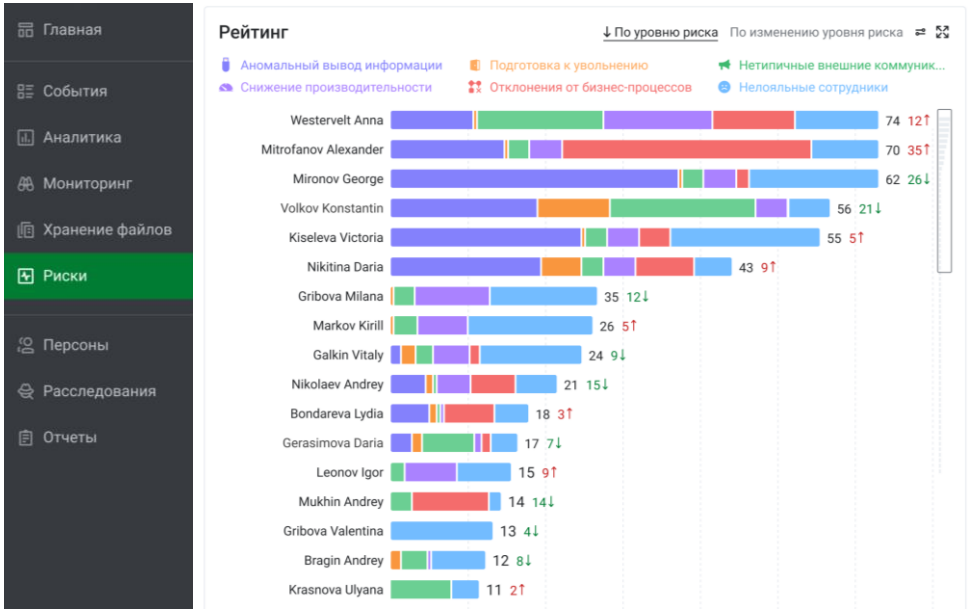

## Технологии искусственного интеллекта

— Поиск новых незащищённых активов и автоматизированная донастройка DLP

— Мгновенный поиск всех документов, аналогичных по смыслу, но не по структуре, и всех черновиков

# Поведенческая аналитика (модуль PREDICTION*)

## Автоматический анализ, корреляция и оценка рисков в поведении сотрудников




## Машинное обучение — вручную невозможно!

— Анализ по сотням тысяч событий ежедневно, раз в час, по 230+ параметрам — количественным, аномальностям, регулярности, нерабочему времени, трендам

— 20 паттернов поведения, 6 групп риска

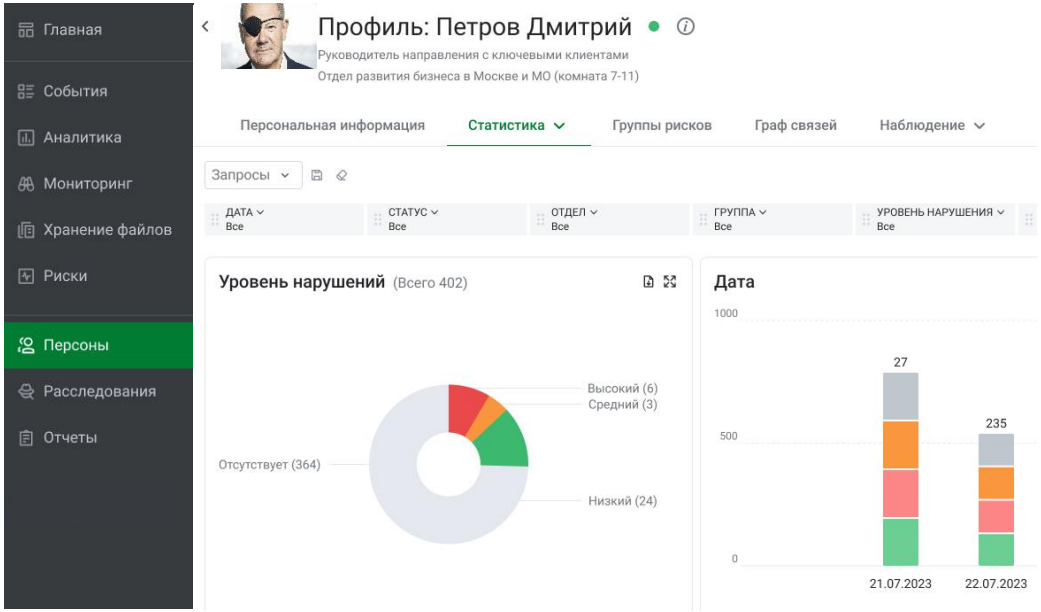
— Подозрительное поведение — признак подготовки или скрыто протекающего нарушения

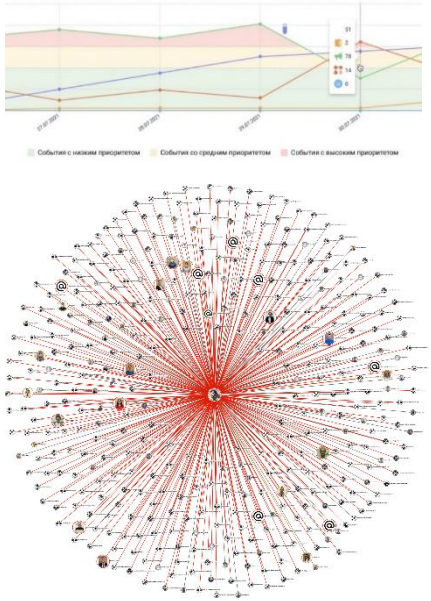
— Сотрудники по группам риска — кого стоит проверить в первую очередь

*В связи с новыми поправками в Налоговом кодексе РФ* для заказчиков InfoWatch при постановке на баланс основных средств и нематериальных активов, относящихся к сфере ИИ, суммы начисляемой амортизации увеличиваются в 1,5 раза.
Пример расчёта: ПО за 100 руб. можно отнести на затраты в размере 150 руб. и получить чистой экономии по налогу на прибыль 50*20% = 10 руб.

# Единое досье сотрудников

## Исчерпывающая информация по персоне

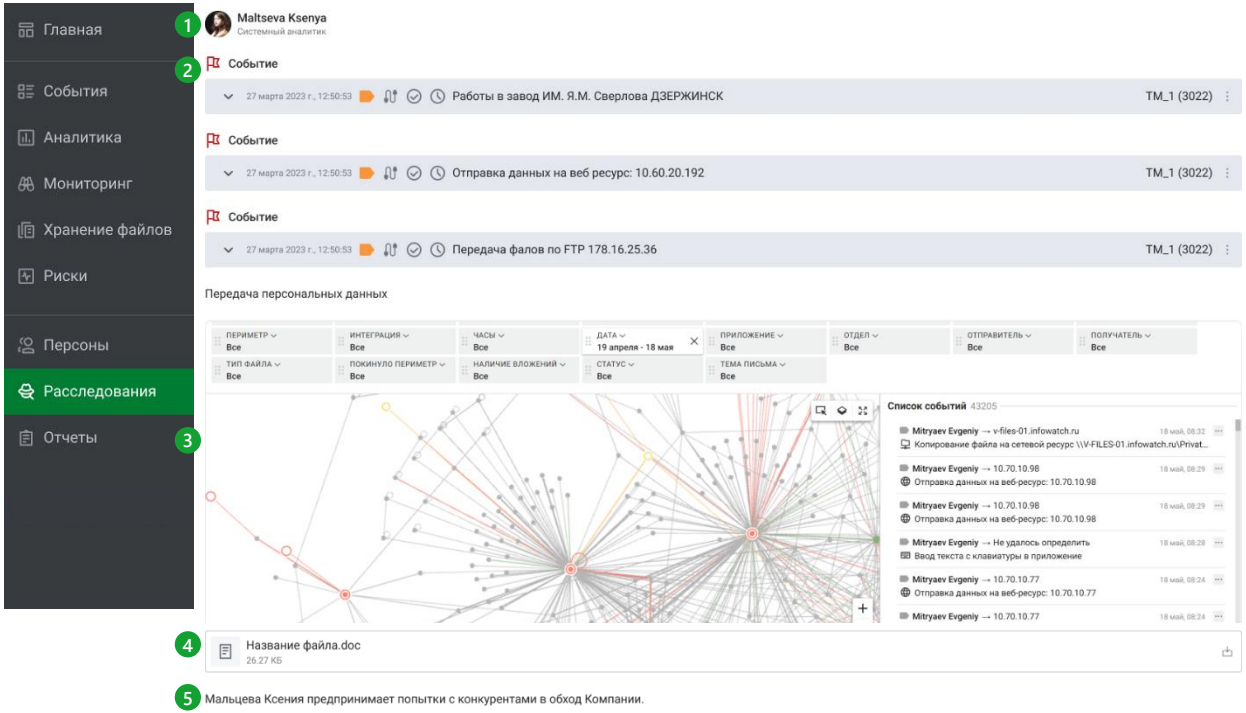


Персональная информация, нарушения, риски, карта коммуникаций, аудиозаписи с микрофона ПК, снимки и видео экрана

# Редактор расследований

## Обобщить, представить в соответствии с методологией или формой отчётности

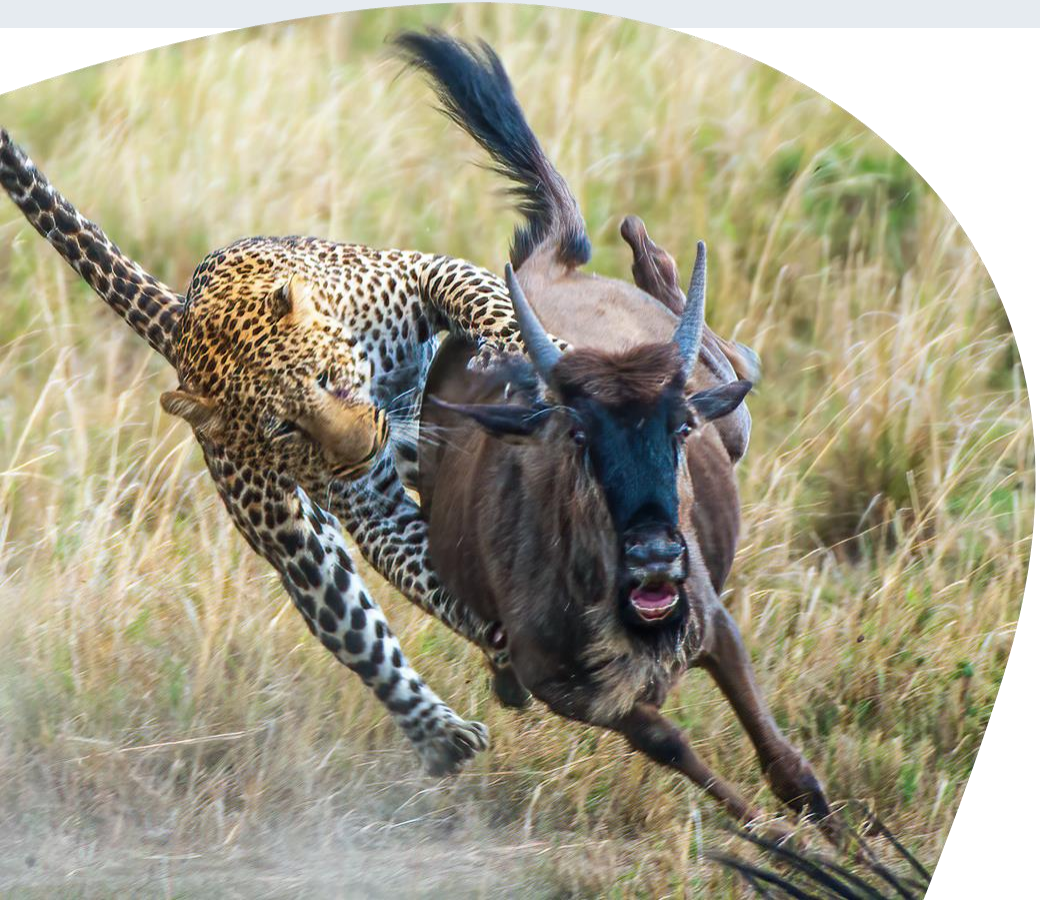



**Формирование результатов расследования в виде документа без перехода в сторонние приложения**

1. Добавить досье персон — объекта расследования и связанных лиц
2. Добавить события DLP-системы из Vision
3. Добавить изображения — скриншоты ПК, фото, сканы документов, скриншоты графа связей и диаграммы виджетов
4. Приложить любые файлы
5. Написать пояснения

# Центр расследований в 3 раза сокращает время от первого подозрения до принятия решения

INFOWATCH®



- Максимум релевантных данных под рукой
- Удобное визуальное представление
- Интерактивные инструменты выборок, сопоставления и поиска взаимосвязей
- Гибкость работы с данными и единый контекст
- Готовая аналитика для смежных подразделений

# Центр расследований InfoWatch

## Единая консоль DLP: События. Персоны. Файлы. Риски. Аналитика

INFOWATCH® ARMA

# Кибербезопасность промышленных предприятий с InfoWatch ARMA

# ИБ на промышленном предприятии

## Ключевые вызовы

| | |
|---|---|
| 1 | Дефицит экспертов ИБ по защите АСУ ТП |
| 2 | Персонал АСУ ТП не обучен ИБ |
| 3 | Нужна документация, чтобы не допустить повторный инцидент |
| 4 | Слишком много разрозненных систем |
| 5 | Специалисту ИБ приходится вручную реагировать на большое количество однотипных инцидентов |
| 6 | Ускоренное импортозамещение |

# Концепция InfoWatch ARMA для ИБ АСУ ТП

**Комплексная система**
Все продуты интегрированы между собой — выгоднее и легче внедрение

**Выполнение до 90% технических требований**
ФСТЭК России (Приказ №239)

**Эшелонированная защита**
МЭ, IDS / IPS, VPN, DPI, Proxy

**DPI промышленных протоколов**
Фильтрация до уровня команд

**Автоматизация реагирования**
в условиях нехватки кадров

**Создание замкнутой программной среды**

# 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

# Некоторые клиенты

INFOWATCH®


Министерство обороны РФ


Центральное таможенное управление

Федеральная налоговая служба


Министерство энергетики РФ


Министерство сельского хозяйства РФ
























INFOWATCH®

# ХОТИТЕ ПОПРОБОВАТЬ НАШИ ТЕХНОЛОГИИ В ДЕЛЕ?

# ПРОВЕДЁМ ПИЛОТ БЕСПЛАТНО!

Виталий Гущин • Infowatch

Менеджер по работе с клиентами и партнерами на территории ЮФО и СКФО

/InfoWatch

/InfoWatchOut

infowatch.ru