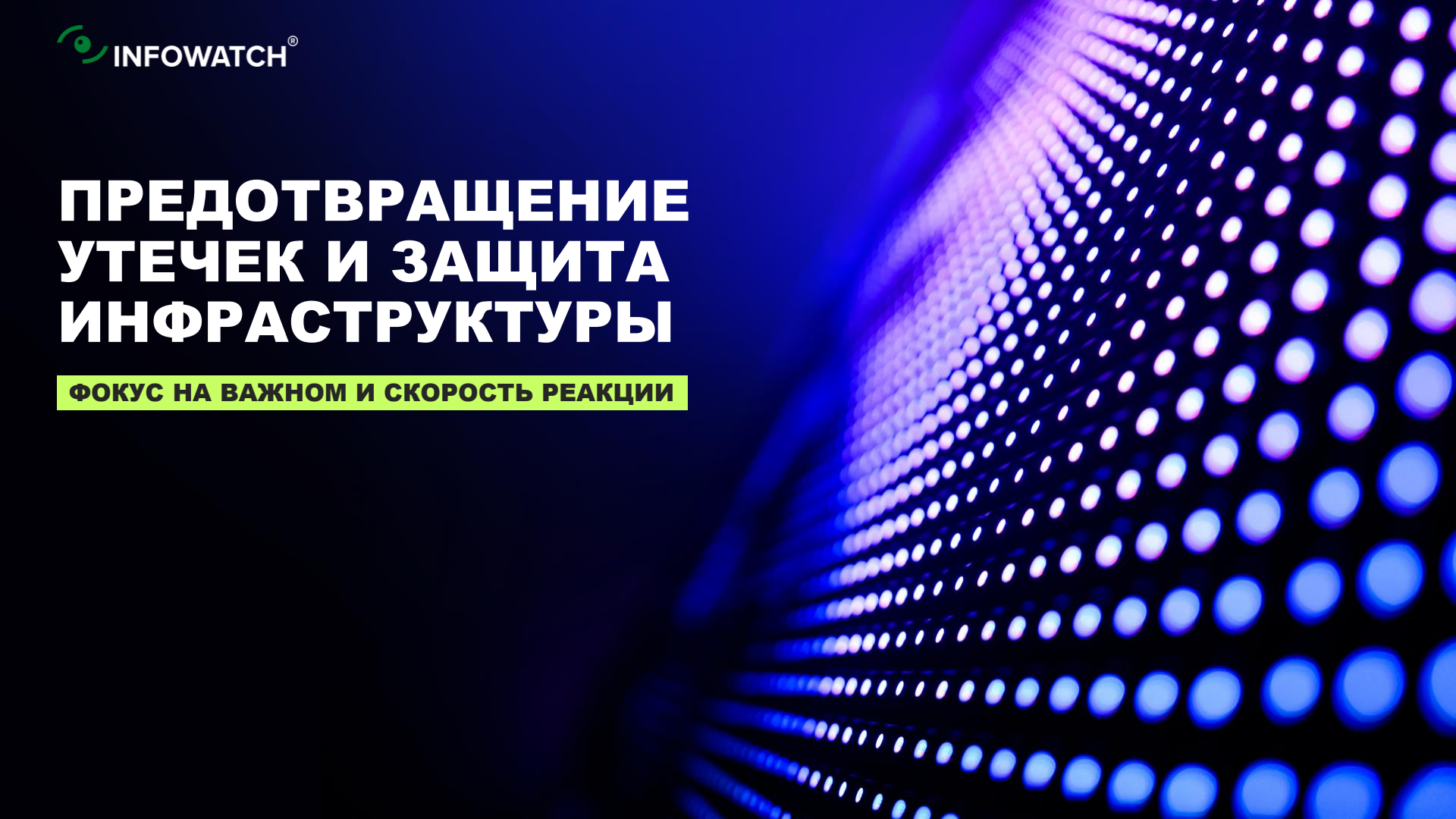
INFOWATCH®

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК И ЗАЩИТА ИНФРАСТРУКТУРЫ

ФОКУС НА ВАЖНОМ И СКОРОСТЬ РЕАКЦИИ



Что важно в расследовании инцидентов ИБ: мнения наших клиентов

INFOWATCH®

0 **Вовремя выявить нарушение**

1 **Расследование должно быть быстрым**

Чем дольше идёт расследование, тем меньшую ценность представляют его результаты

2 **Расследование может быть долгим и обстоятельным**

Но чем быстрее сбор значимых обстоятельств, тем расследование полнее = качественнее

3 **Нужно быть на шаг впереди нарушителя**

— Выявлять подготовку нарушений
— Выявлять скрыто протекающие нарушения
— Выявлять предпосылки

Сократить время на сбор значимых обстоятельств и восстановить полную картину

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

DLP-система нового поколения — целый комплекс возможностей

INFOWATCH®

DLP

Предотвращение утечек

МОНИТОРИНГ ДЕЙСТВИЙ СОТРУДНИКОВ

Доказательная база и наблюдение

DCAP

Аудит хранения и прав доступа

BI-АНАЛИТИКА

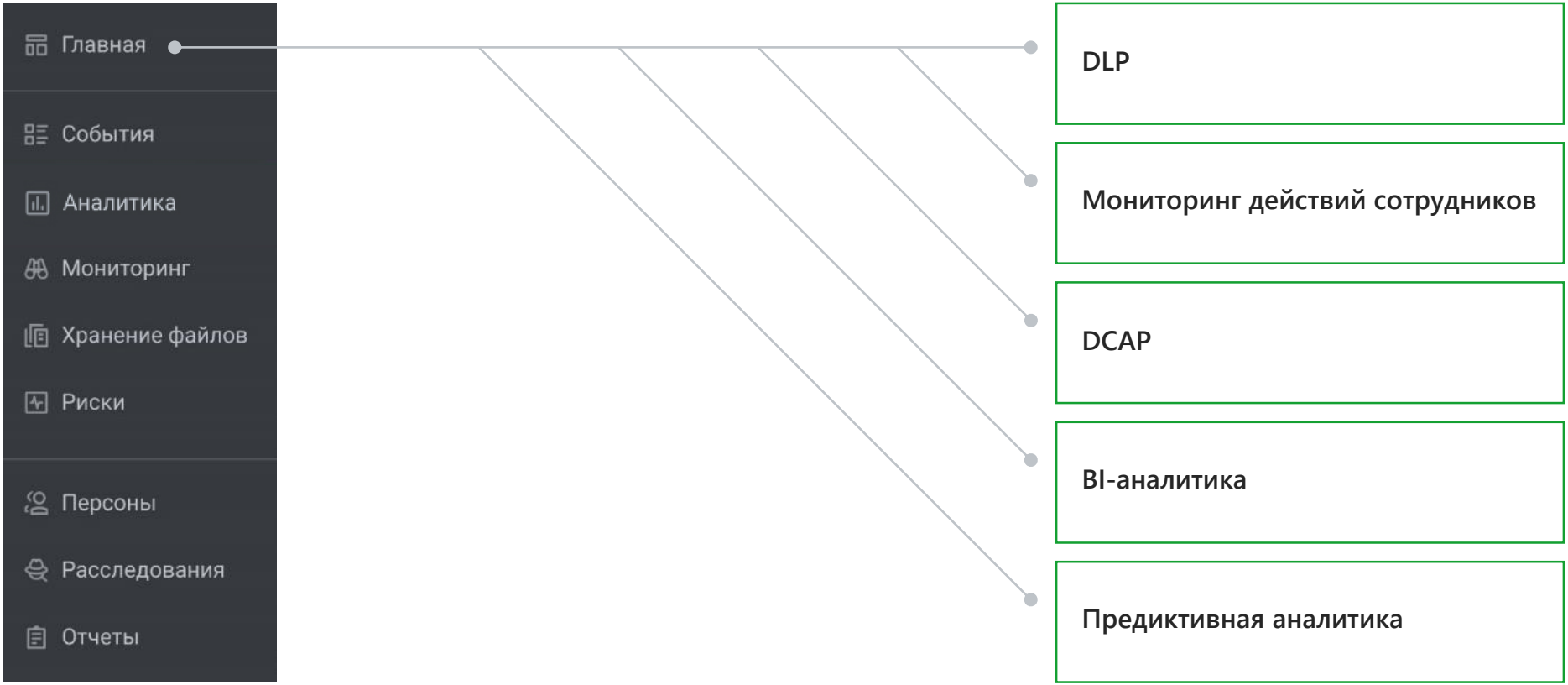
Ежедневный мониторинг
и быстрые расследования

ПРЕДИКТИВНАЯ АНАЛИТИКА

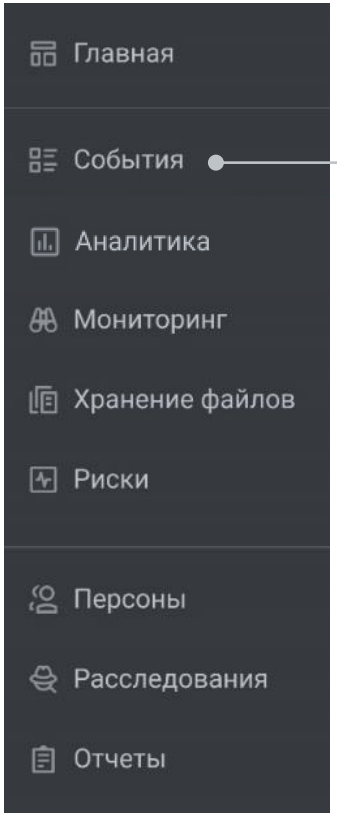
На кого обратить внимание
для превентивного реагирования

Как сохранить фокус и действовать быстро?

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

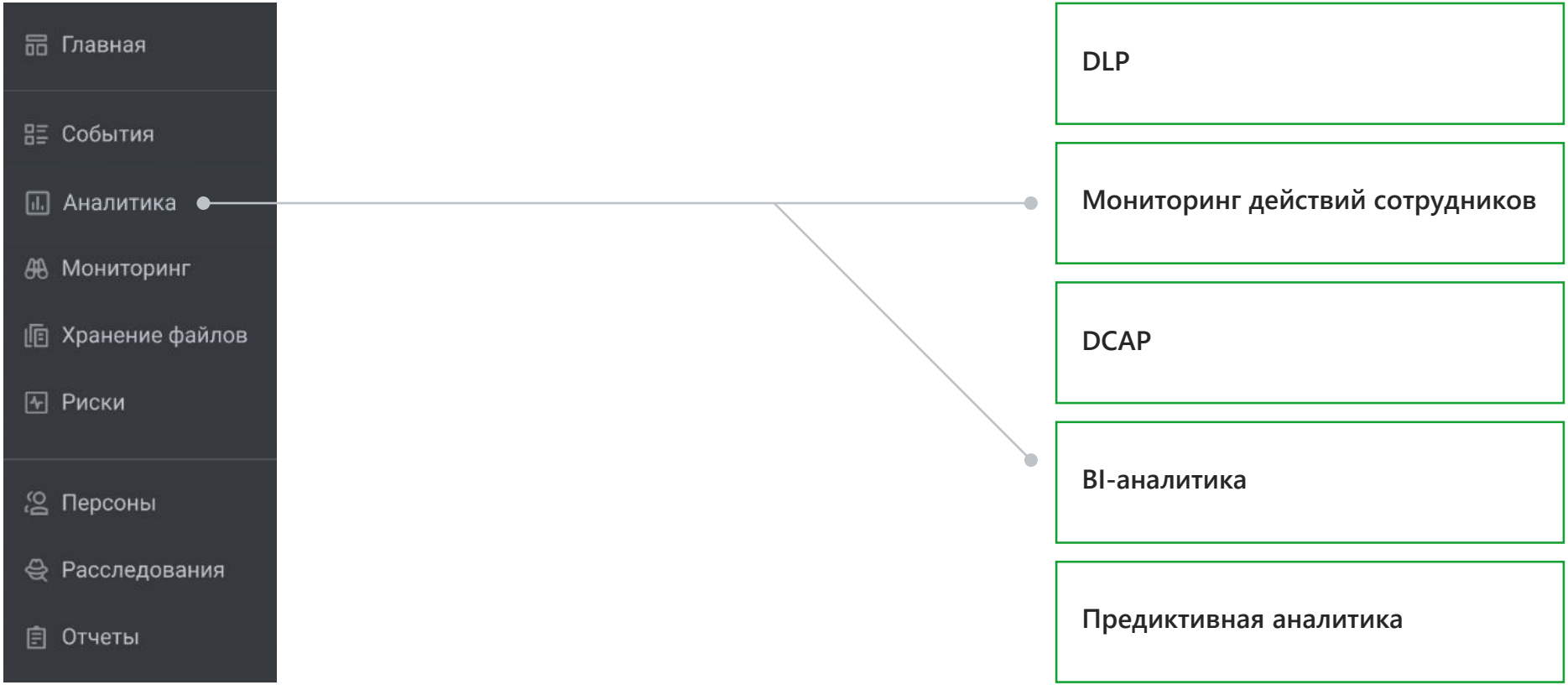


Единая консоль DLP
События. Персоны. Файлы. Риски. Аналитика

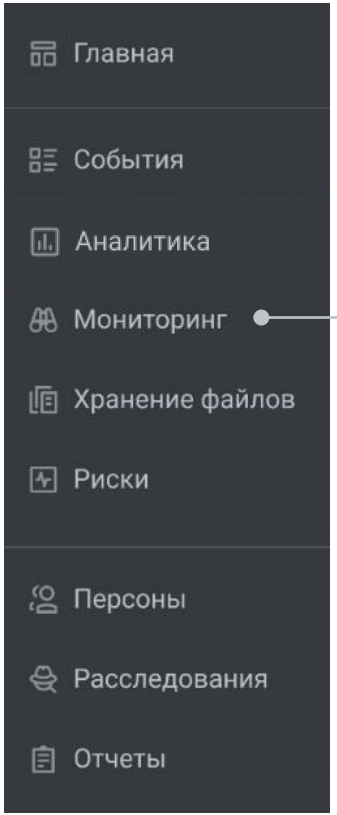


- DLP
- Мониторинг действий сотрудников
- DCAP
- BI-аналитика
- Предиктивная аналитика

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

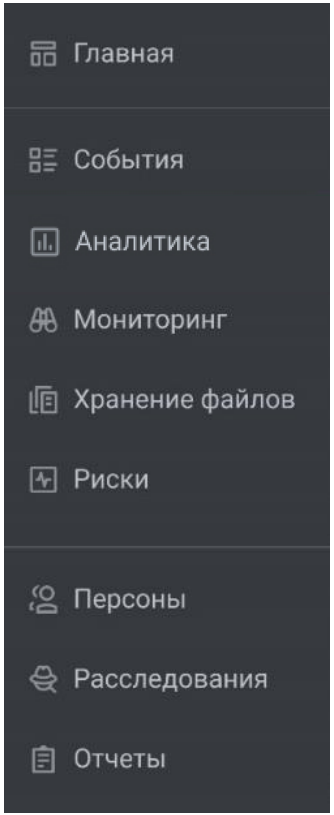


Единая консоль DLP
События. Персоны. Файлы. Риски. Аналитика



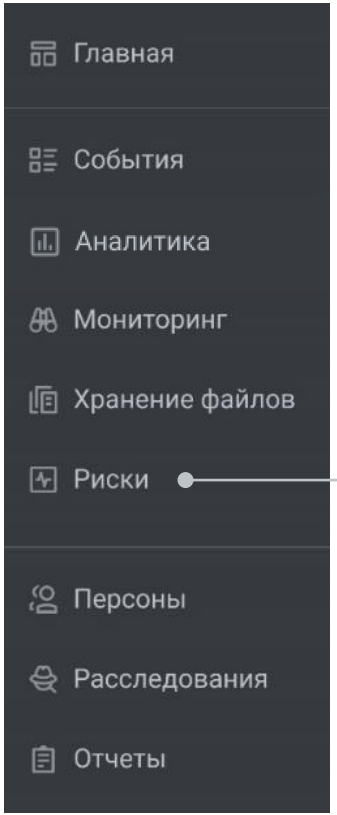
- DLP
- Мониторинг действий сотрудников
- DCAP
- BI-аналитика
- Предиктивная аналитика

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



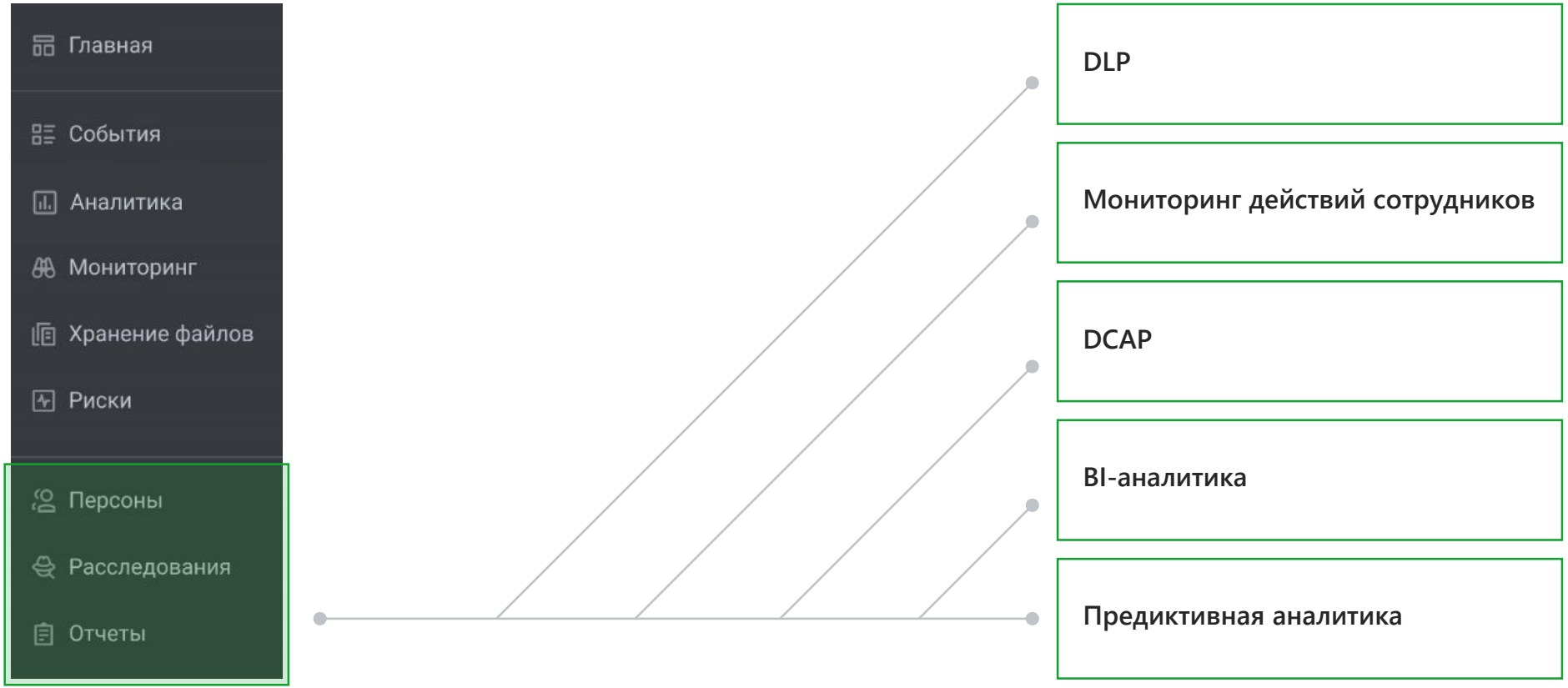
- DLP
- Мониторинг действий сотрудников
- DCAP
- BI-аналитика
- Предиктивная аналитика

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



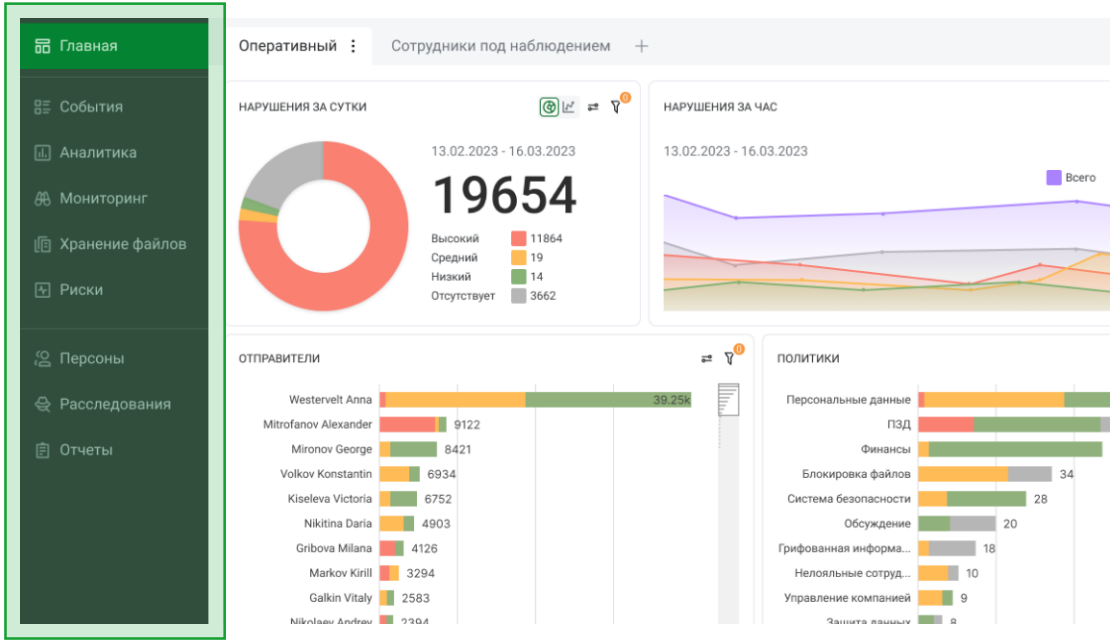
- DLP
- Мониторинг действий сотрудников
- DCAP
- BI-аналитика
- Предиктивная аналитика

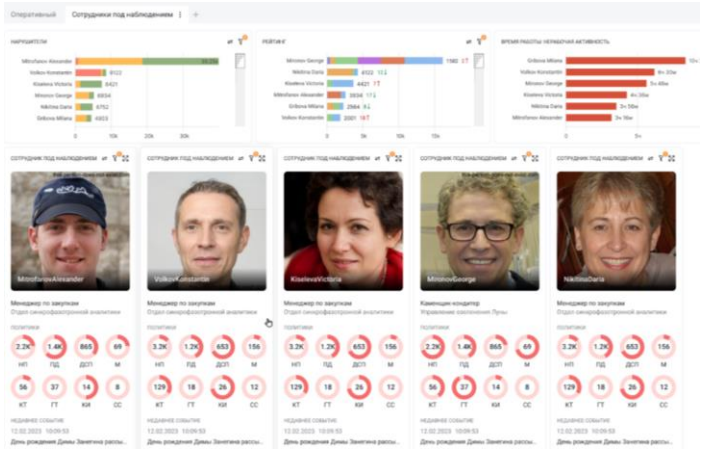
Единая консоль DLP
События. Персоны. Файлы. Риски. Аналитика



Настраиваемые рабочие панели

Искать самые критичные инциденты или сконцентрироваться на персонах под особым контролем



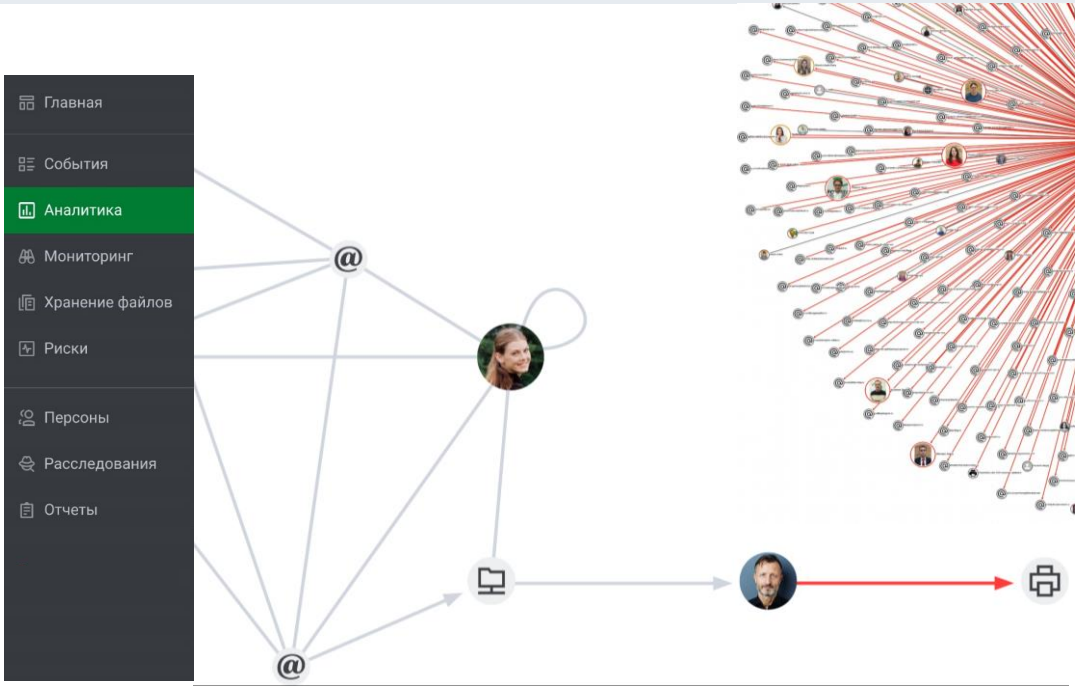


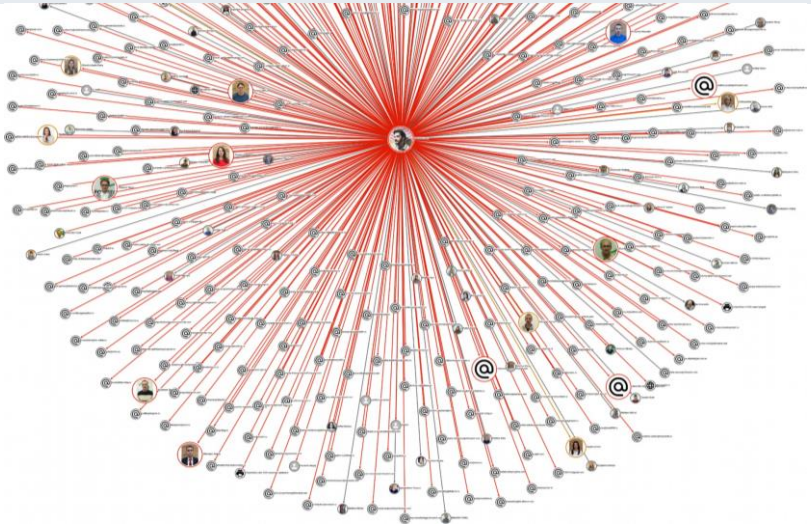
— 38 виджетов на выбор

— Можно настроить положение, порядок и размер

Интерактивный граф связей

Найти всех соучастников, выявить неявные связи и пути перемещения документов





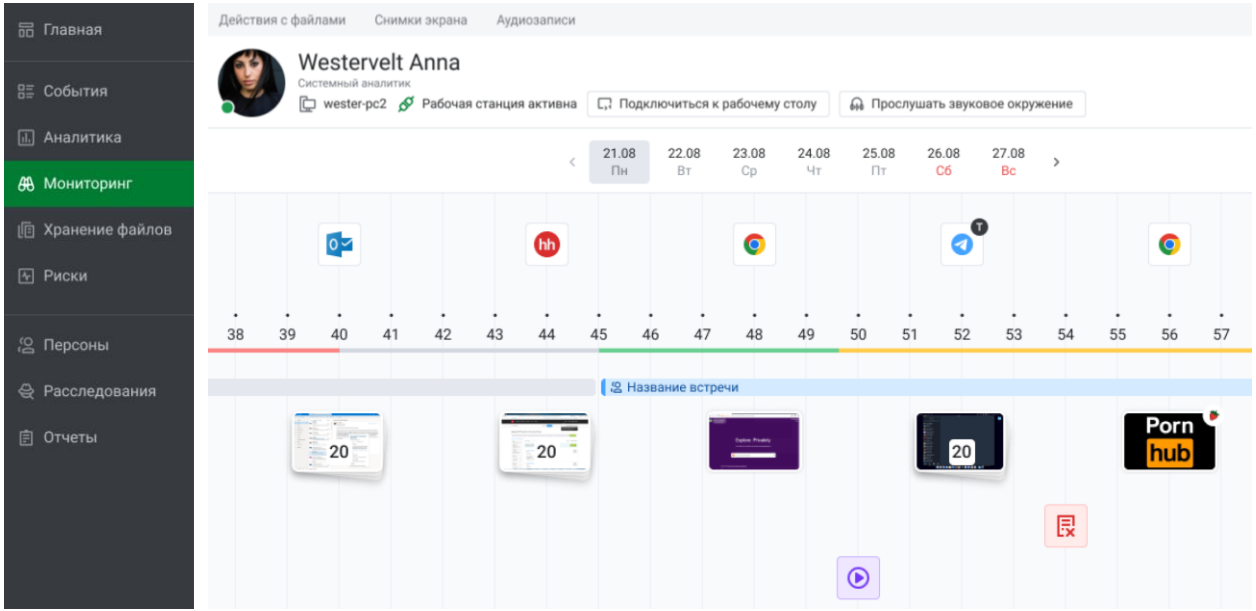
— Отображает одновременно до 50 000 узлов

— Динамически перестраивается при применении фильтров

— Данные для фильтрации можно выбрать прямо на графе

Интерактивный таймлайн действий

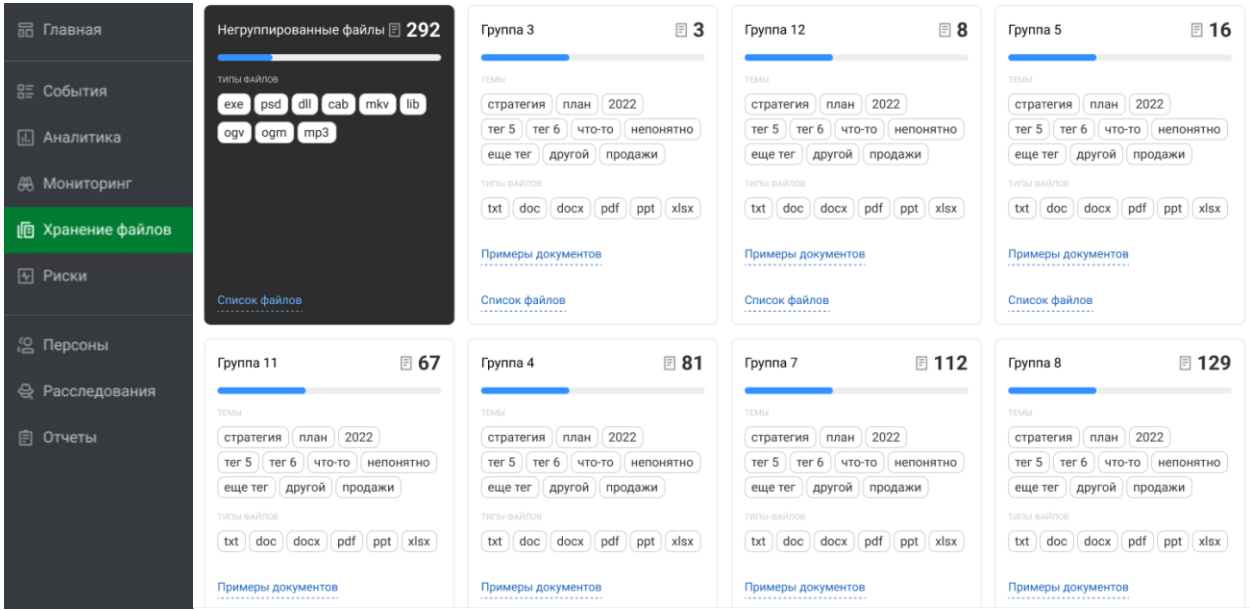
Восстановить полную картину — что делал сотрудник до, во время и после инцидента



- 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



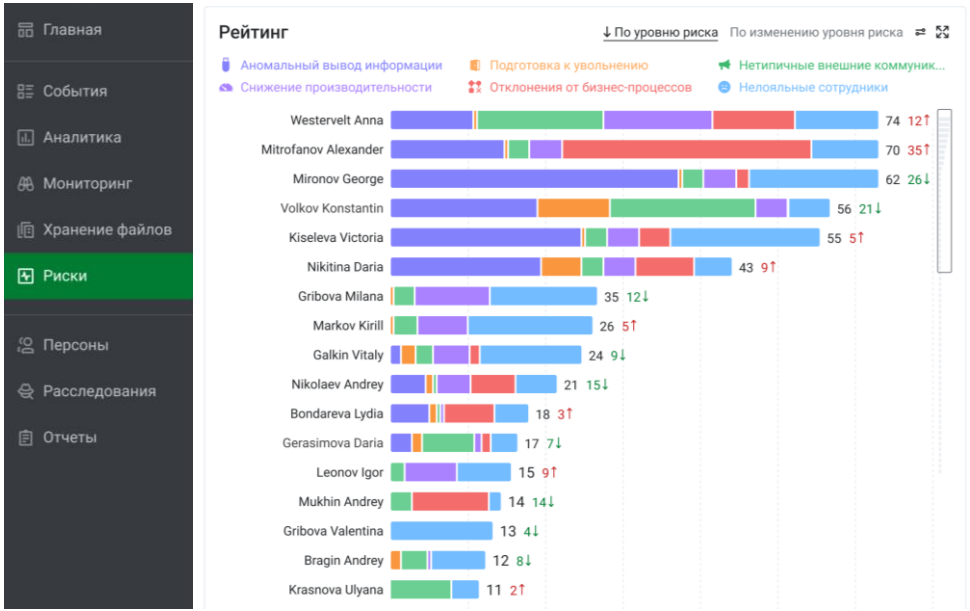
Технологии искусственного интеллекта

— Поиск новых незащищённых активов и автоматизированная донастройка DLP

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

Поведенческая аналитика

Автоматический анализ, корреляция и оценка рисков в поведении всех сотрудников



Машинное обучение — вручную невозможно!

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

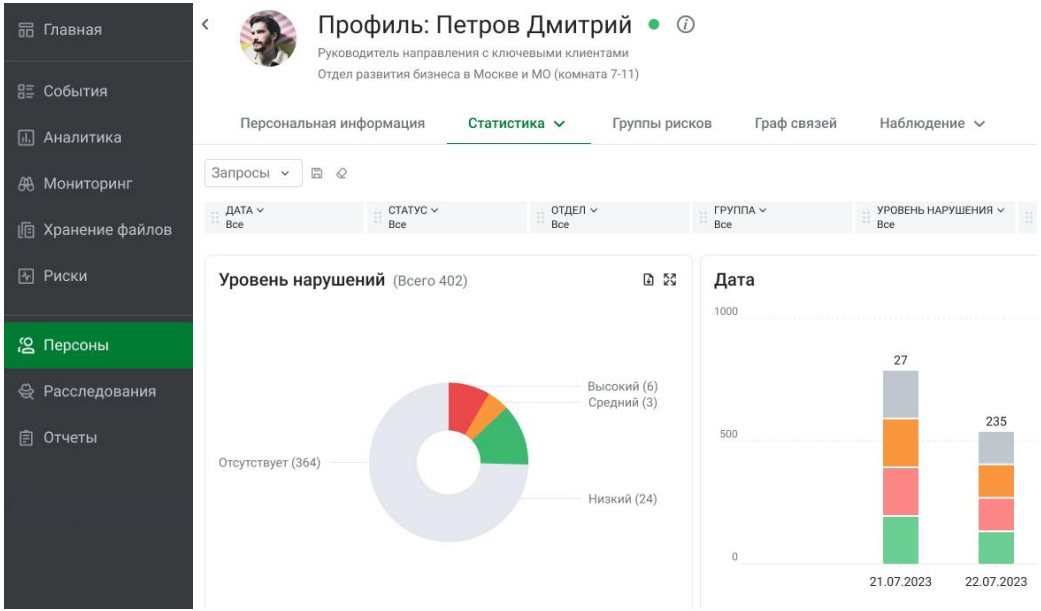
— 20 паттернов поведения, 6 групп риска

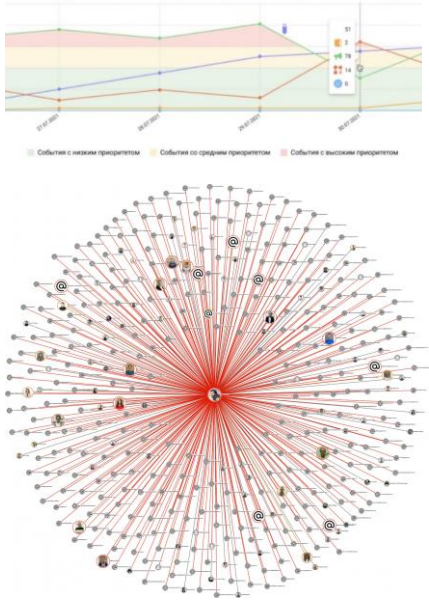
— Подозрительное поведение — признак подготовки или скрыто протекающего нарушения

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

Единое досье сотрудников

Исчерпывающая информация по персоне

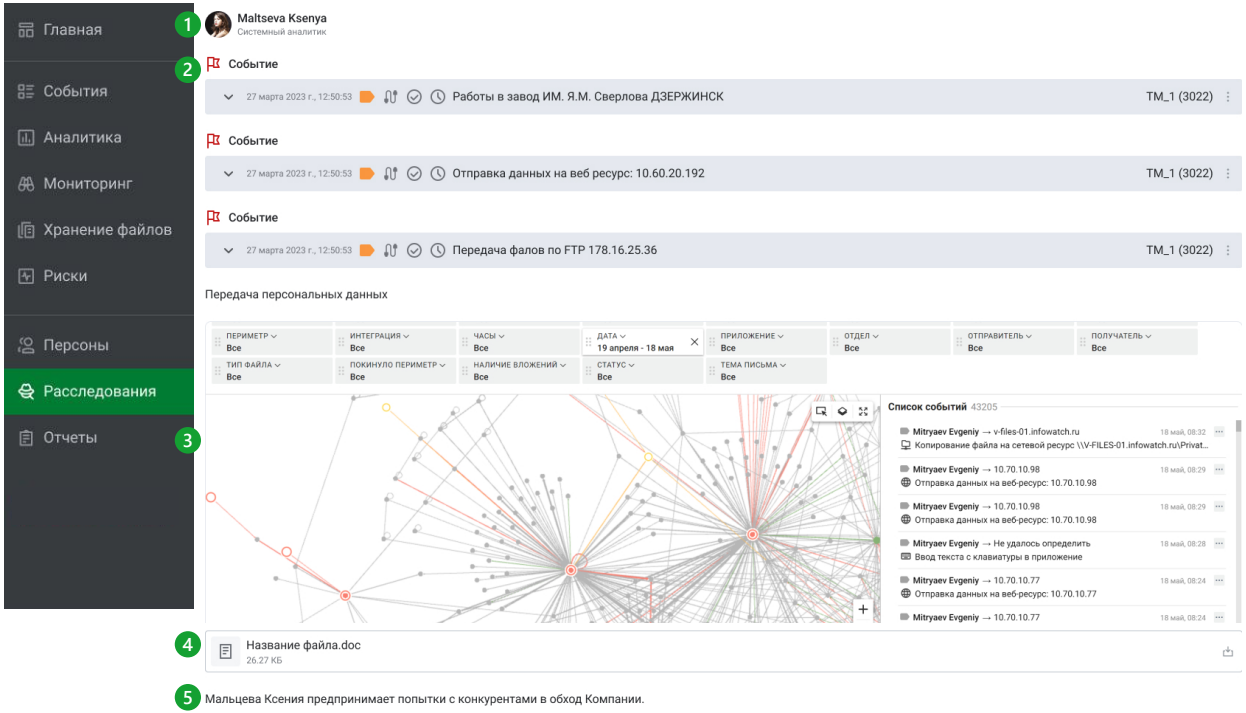




Персональная информация, нарушения, риски, карта коммуникаций, аудиозаписи с микрофона ПК, снимки и видео экрана

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

КЕЙС

Выявление факта промышленного шпионажа

INFOWATCH®

Горнодобывающее предприятие перешло государству после ухода иностранной компании

Часть сотрудников высылала отчёты бывшему руководству

1	**Главная+ Риски**	Специалист ИБ получил уведомление о сотрудниках в группе риска «Нетипичные внешние коммуникации»
2	**Главная+ События**	Специалист ИБ поставил сотрудников на контроль, ужесточил политики безопасности и вовремя заметил нарушения — пересылку конфиденциальных материалов
3	**Аналитика**	На графе связей по интенсивности коммуникаций выявлена организованная группа нарушителей
4	**Мониторинг**	Специалист ИБ собрал доказательную базу — как готовился и протекал слив информации

КЕЙС Выявление сговора с поставщиком услуг

У руководителя отдела доход не соответствовал расходу. Обнаружился его сговор с подрядчиком		**Банк нёс финансовые потери от неэффективных закупок**
1	**Мониторинг**	Сотрудник интересовался и приценивался к люксовым авто и ЖК, которые не смог бы позволить на одну зарплату
2	**Главная+ События+ Аналитика**	В переписке WhatsApp сработали БКФ «Мошенничество», «Угроза ИБ» и «Родственные связи». Сотрудник взят на контроль. Выявлена переписка с родственником, который работал в компании-подрядчике. Обсуждалась мошенническая схема
3	**Мониторинг+ Досье**	Скриншоты переписки, аудиозапись переговоров в онлайн-конференции легли в доказательную базу

КЕЙС Выявление «слива» базы поставщиков конкуренту

INFOWATCH®

Сотрудник готовился слить базу поставщиков конкурентам

Конкурент хотел предложить поставщику лучшие условия, чтобы выкупать весь объём. Компания могла потерять ключевой проект

1	**Хранение файлов**	При автоматическом аудите файлов на ПК сотрудника обнаружена информация о ключевых поставщиках и ценах закупки. В личной беседе сотрудник сказал, что информация попала на его компьютер по ошибке
2	**Мониторинг**	Специалист ИБ проверил действия сотрудника за ПК. Обнаружил, что сотрудник искал способ обойти DLP и какую ответственность он может понести
3	**Расследования**	Специалист ИБ добавил все события, файлы с ПК сотрудника, снимки экрана в Расследование. Добавил необходимые пояснения и свои выводы. И выгрузил отчёт для руководства для принятия срочных мер

Центр расследований InfoWatch

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

INFOWATCH®

Стабильная работа под нагрузкой в крупных организациях-клиентах InfoWatch

2 000 000
событий в день

100 000
событий в секунду — скорость BI-аналитики

100 000 000
записей ПДн в секунду — скорость технологии защиты базы клиентов

×20
раз быстрее поиск неизвестных ранее информационных активов

×3–4
раза быстрее расследования инцидентов

70%
инцидентов можно предотвратить на стадии подготовки

×3
раза меньше специалистов ИБ нужно для контроля 100% данных*

**по отзывам клиентов InfoWatch, >1000 сотрудников*

Консалтинг и внедрение

INFOWATCH ACADEMY

- **Использование лучших практик при внедрении и настройке**

  Даёт эффективную защиту уже на старте

- **Проверенная методология**

  Позволяет использовать возможности решения на 100%

- **Формирование юридической базы**

  Для легитимного применения систем DLP и Employee Monitoring

- **Измеримые показатели**

  Позволяют оценить качество функционирования процессов обеспечения информационной безопасности

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

InfoWatch ARMA NGFW

Закрывает бреши в защите ИТ-сетей после ухода иностранных вендоров

ПАК российского производства, отечественное ПО

Защита корпоративной сети

— Система обнаружения вторжений (СОВ)

— Application Control

— URL-фильтрация

— VPN (IPsec / OpenVPN / OpenVPN-ГОС)

— Защита от SSL-инспекций

— SSO

— Интеграция с DLP-системой InfoWatch Traffic Monitor

Некоторые клиенты

INFOWATCH®


Министерство обороны РФ


Центральное таможенное управление

Федеральная налоговая служба


Министерство энергетики РФ


Министерство сельского хозяйства РФ

InfoWatch в цифрах и фактах

20
лет на рынке информационной безопасности

30%
ежегодный рост инвестиций в разработку, 2020–2023

500+
сотрудников в компании

28
патентов на технологии

4000
клиентов из 12 отраслей в 26 странах

135+
аналитических отчётов в год

100+
технологических партнёров

5000+
обученных специалистов ИБ

Аккредитация ЦБ РФ

Рекомендовано АРПП «Отечественный софт»

Инновация года в ИБ, 2022
CNews FORUM Кейсы

Премия за продукт, 2022
ТБ Форум

Лучшее ИБ-решение, 2021
TAdviser

DLP Market Guide
Первое российское DLP-решение, вошедшее в Gartner Magic Quadrant и удерживающее признание более 10 лет