



# ЗАЩИТА ОТ УТЕЧЕК ДАННЫХ И КИБЕРБЕЗОПАСНОСТЬ КИИ

Что выбрать в условиях  
кадрового голода в ИБ?



Виталий гушин  
Infowatch

# 80%

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



**×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



**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

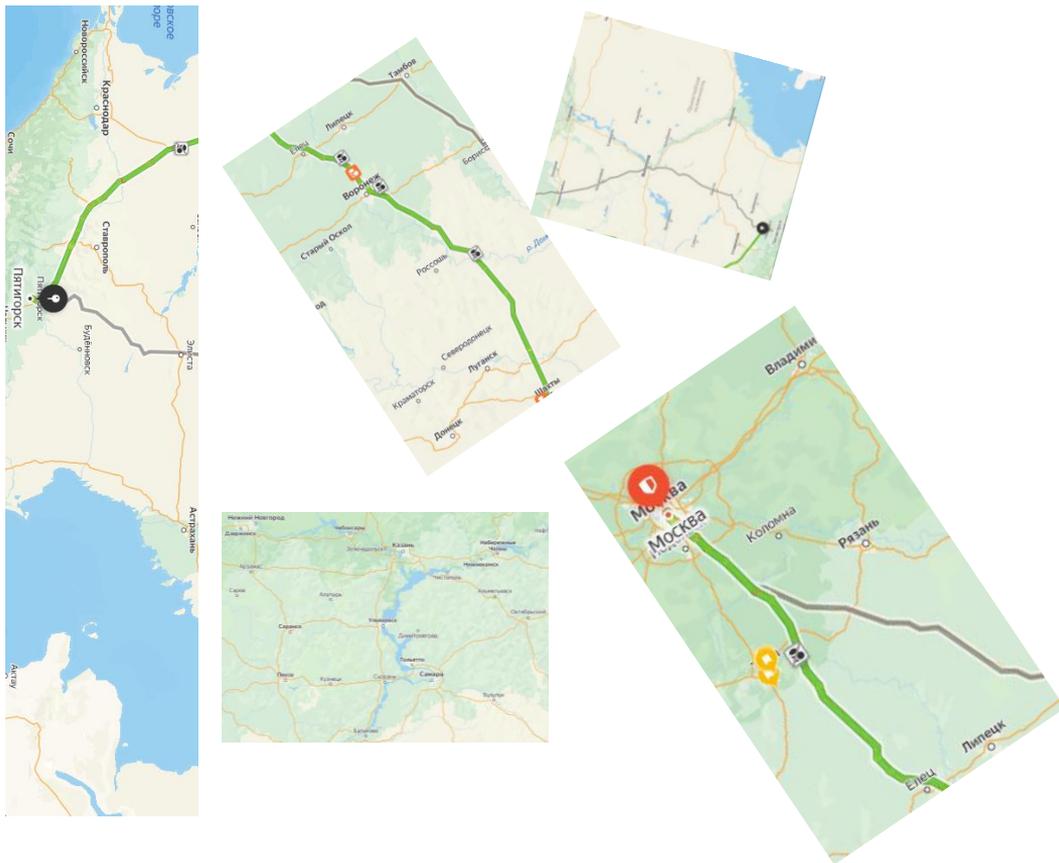


## Для глубокой и непрерывной аналитики приходится

- 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

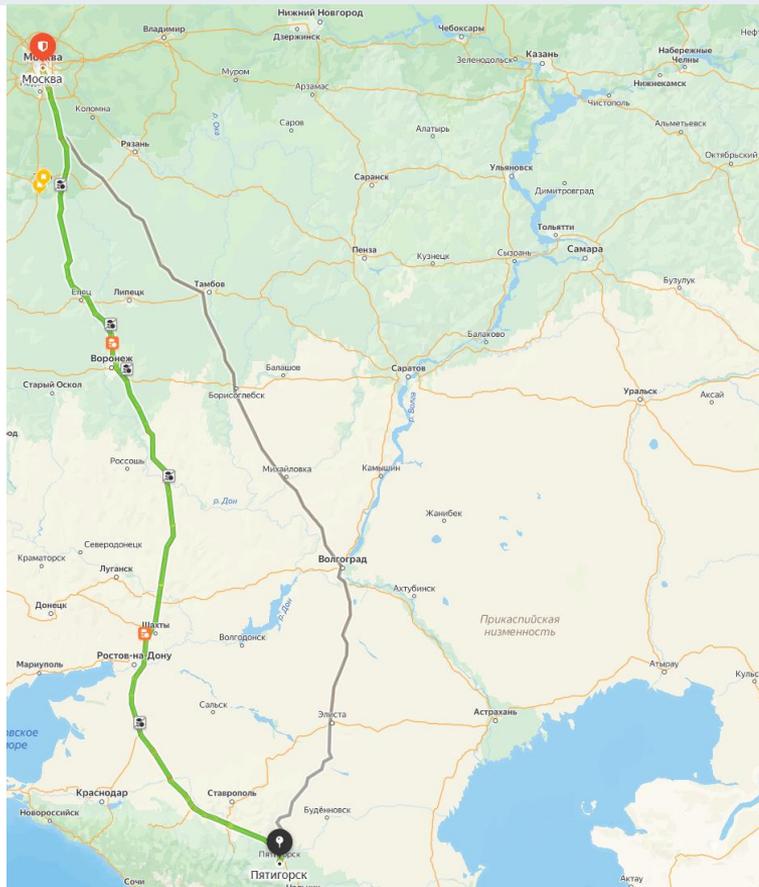
А сопоставлять вручную = терять непрерывность и регулярность защиты

# 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!

★ СОБЫТИЯ

InfoWatch Traffic Monitor

⚡ РИСКИ

InfoWatch Prediction

🔍 АНАЛИТИКА

InfoWatch Vision

👤 ПЕРСОНЫ

InfoWatch Activity Monitor

📁 ФАЙЛЫ

InfoWatch Data Discovery

# ЦЕНТР РАССЛЕДОВАНИЙ INFOWATCH

# Пример расследования в едином информационном пространстве

Главная

События

Аналитика

Мониторинг

Хранение файлов

Риски

Персоны

Расследования

Отчеты

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»

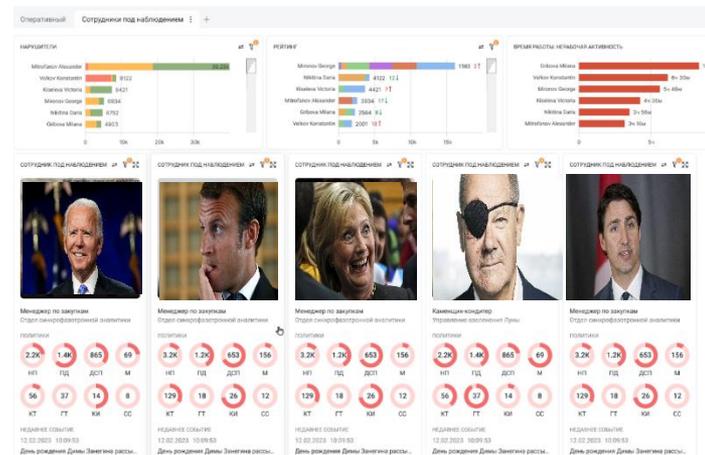
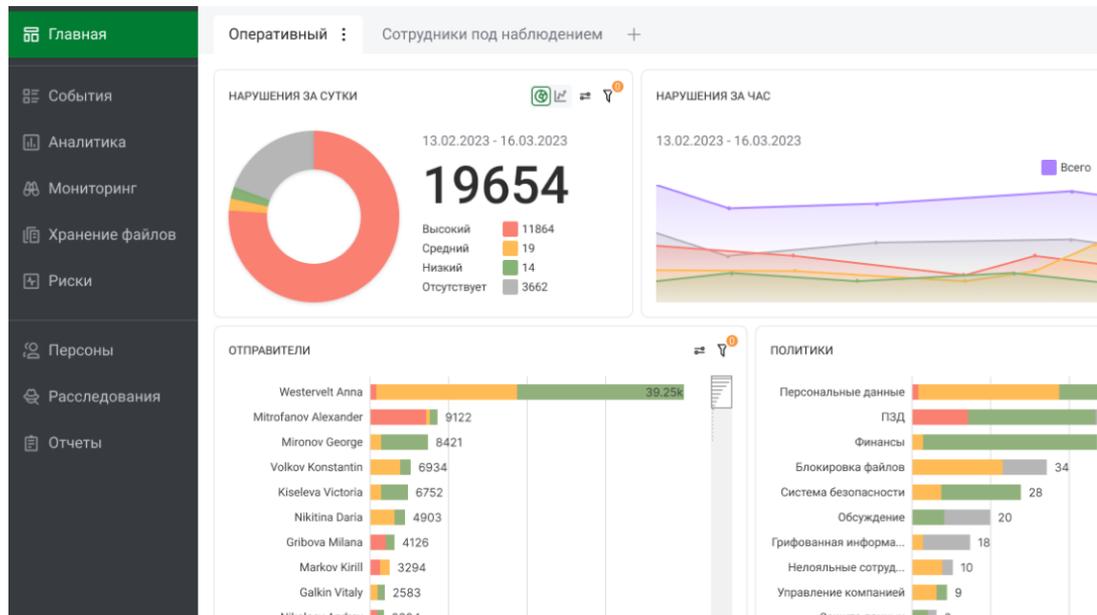
6 Посмотрел, в какие **группы риска** входит подозреваемый

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



Главная

События

Аналитика

Мониторинг

Хранение файлов

Риски

Персоны

Расследования

Отчеты

Поиск

ДАТА ▾ Любая дата

ПЕРСОНА ▾ Все

ГРУППА ▾ Все

ОТДЕЛ ▾ Все

СТАТУС ▾ Все

ФИЛИАЛ ▾ Все

ДОЛЖНОСТЬ ▾ Все

Сбросить выбранные события

Просмотр событий

Список событий 373333

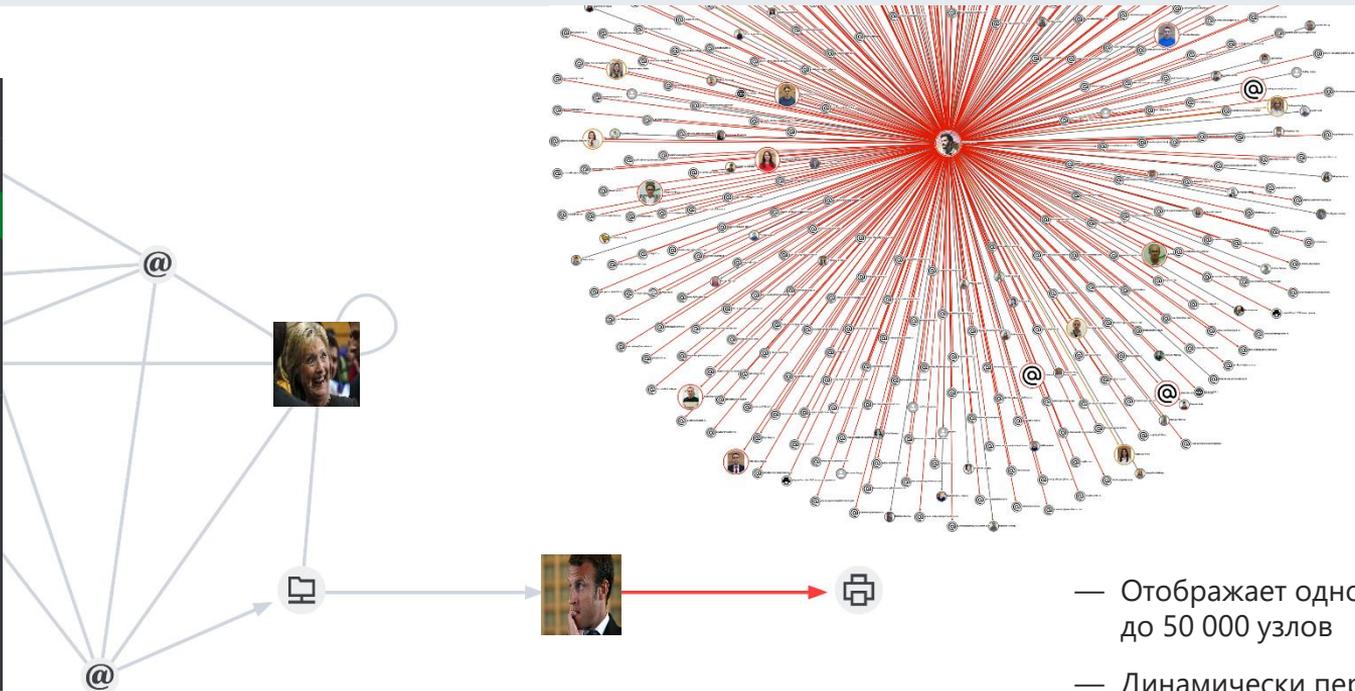
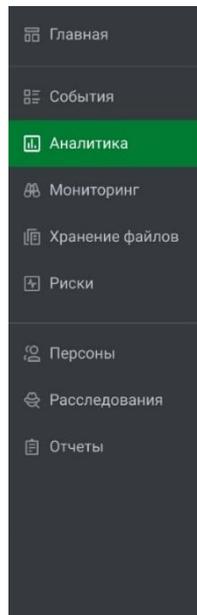
Дата	Отправитель	Получатель	Действие / Описание	Вложения	Политики	Объекты защиты	Источник...
25 май 202...	Nikulina Mari... <a href="#">еще 1</a>	Andreeva Kira	Разговор	voice.ogg (1...			tm2 (4)
25 май 202...	Bykov Lev	Shestakova Sofya	Отправка данных на веб-ресурс: 10.60.3.10		Грифованная информа...	Грифы конфиденциаль...	tm2 (10...
25 май 202...	Daniilova Veronika	Andreeva Kira	Передача файлов по FTP 10.60.3.95/Pesh/new...	new1.pdf (56...	Финансы <a href="#">еще 1</a>		
25 май 202...	Andreeva Kira <a href="#">еще 1</a>	Nikulina Marina	test subj				
25 май 202...	Bykov Lev	Shestakova Sofya	Копирование файла пароль почта.txt с съемн...	пароль почт...			
25 май 202...	Shestakov... <a href="#">еще 1</a>	Latysheva Margar... <a href="#">еще 2</a>	Обмен файлами: паспорт2 - копия.jpg	паспорт2 - к...			
25 май 202...	Pakhomova... <a href="#">еще 1</a>	Daniilova Veroni... <a href="#">еще 3</a>	Разговор	voice.ogg (4...			tm2 (10...
25 май 202...	Andreeva Kir... <a href="#">еще 1</a>	Bykov Lev	Разговор	voice.wav (6...			tm2 (1)
25 май 202...	Pakhomova... <a href="#">еще 2</a>	Fedotov Maksim	Всего сообщений: 1, Отправлено сообщений: ...				tm2 (6)
25 май 202...	Latysheva Margarita	Morozova Alina	Печать Microsoft Word - 1. Копий - 1	microsoft wo...			tm2 (5)
25 май 202...	Fedotov Maksim	Pakhomova Diana	Копирование файла паспорт рф.txt с съемног...	паспорт рф.t...	Персональные данные	Удостоверение личнос...	tm2 (9)
25 май 202...	Belyaeva Darya	Shestakova Sofya	Копирование файла строго конфиденциально...	строго конф...	Грифованная информа...	Грифы конфиденциаль...	tm2 (10...
25 май 202...	Morozova Alina	Bykov Lev	Копирование файла текст + картинка.zip на с...	текст + карт...	Грифованная информа...	Грифы конфиденциаль...	tm2 (21)

Создать новое расследование

Добавить к расследованию

# Интерактивный граф связей

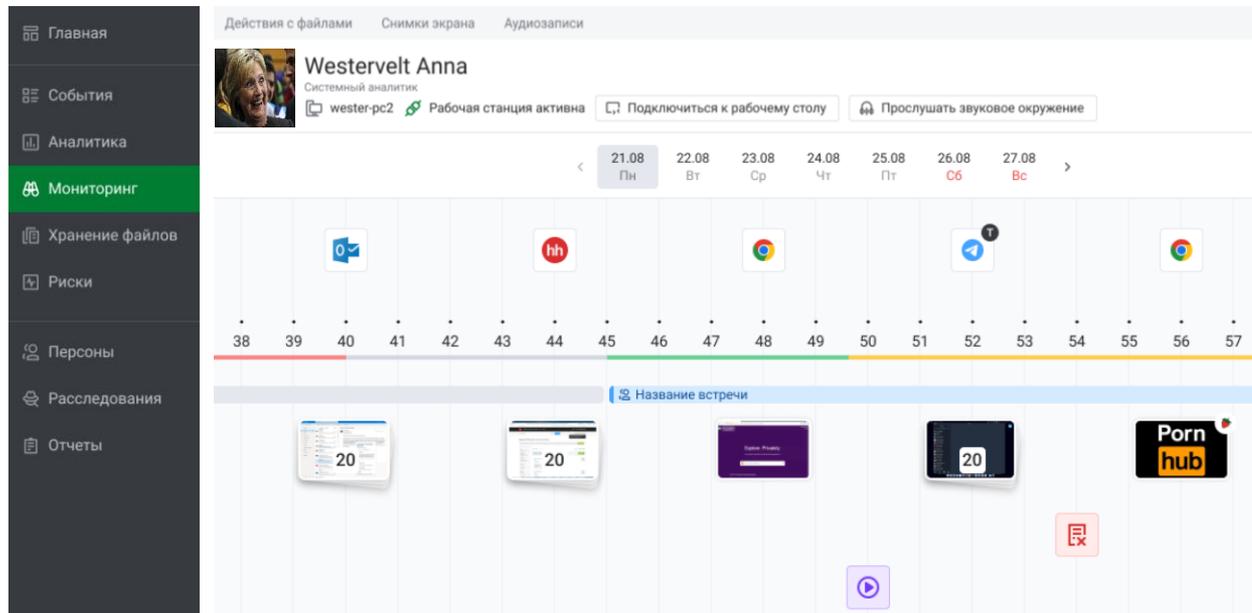
Найти всех соучастников, выявить неявные связи и пути перемещения документов



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

# Интерактивный таймлайн действий

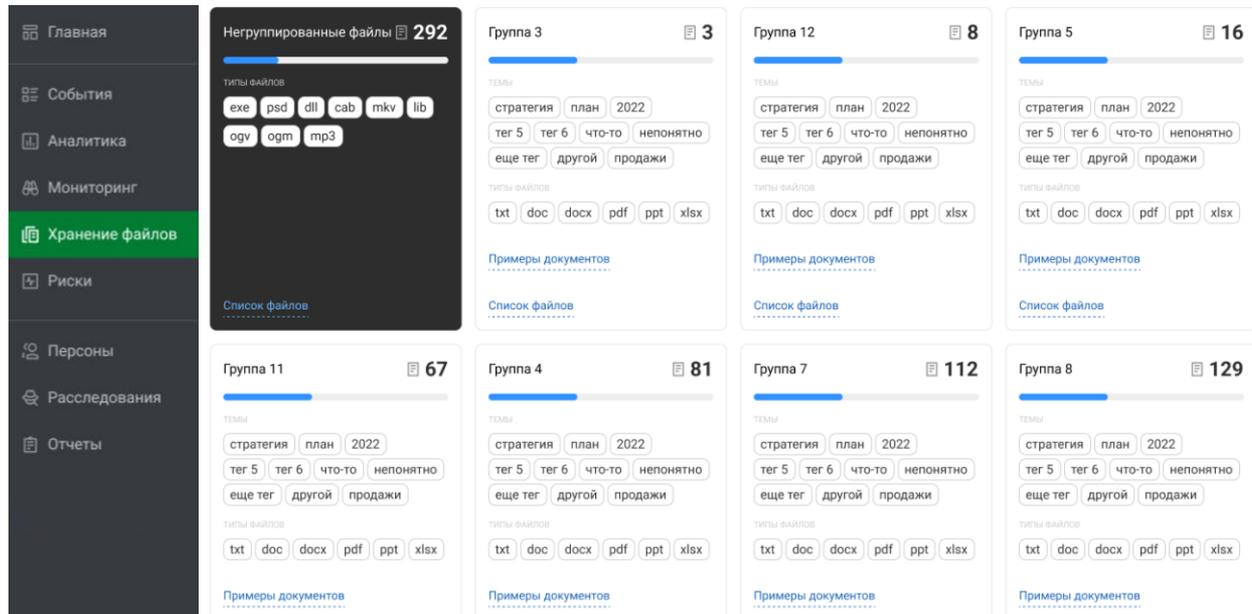
Восстановить полную картину действий сотрудника до, во время и после инцидента



- 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



Главная

События

Аналитика

Мониторинг

**Хранение файлов**

Риски

Персоны

Расследования

Отчеты

Негруппированные файлы 292

типы файлов

exe psd dll cab mkv lib

ogv ogm mp3

Список файлов

Группа 3 3

темы

стратегия план 2022

тег 5 тег 6 что-то непонятно

еще тег другой продажи

типы файлов

txt doc docx pdf ppt xlsx

Примеры документов

Список файлов

Группа 12 8

темы

стратегия план 2022

тег 5 тег 6 что-то непонятно

еще тег другой продажи

типы файлов

txt doc docx pdf ppt xlsx

Примеры документов

Список файлов

Группа 5 16

темы

стратегия план 2022

тег 5 тег 6 что-то непонятно

еще тег другой продажи

типы файлов

txt doc docx pdf ppt xlsx

Примеры документов

Список файлов

Группа 11 67

темы

стратегия план 2022

тег 5 тег 6 что-то непонятно

еще тег другой продажи

типы файлов

txt doc docx pdf ppt xlsx

Примеры документов

Группа 4 81

темы

стратегия план 2022

тег 5 тег 6 что-то непонятно

еще тег другой продажи

типы файлов

txt doc docx pdf ppt xlsx

Примеры документов

Группа 7 112

темы

стратегия план 2022

тег 5 тег 6 что-то непонятно

еще тег другой продажи

типы файлов

txt doc docx pdf ppt xlsx

Примеры документов

Группа 8 129

темы

стратегия план 2022

тег 5 тег 6 что-то непонятно

еще тег другой продажи

типы файлов

txt doc docx pdf ppt xlsx

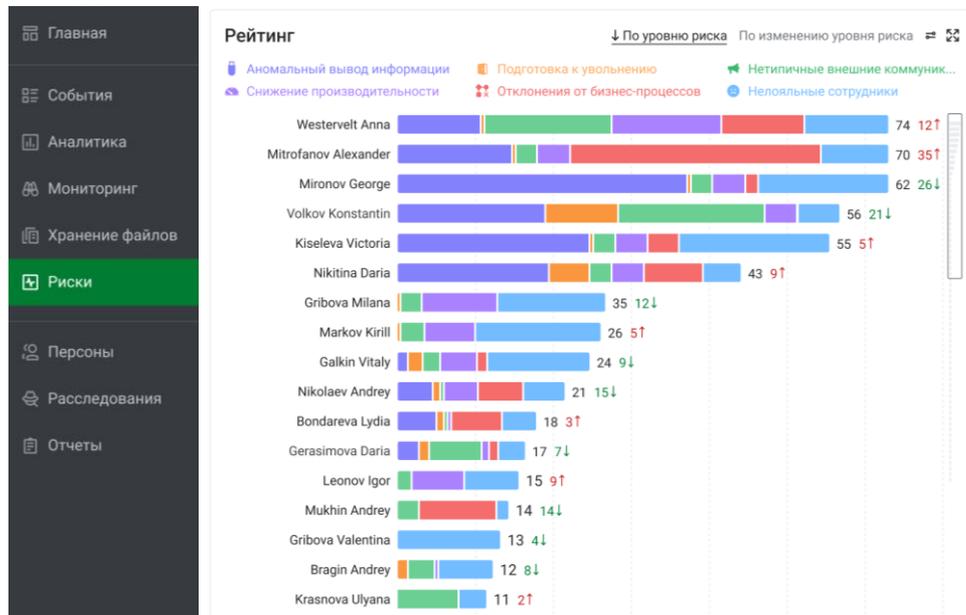
Примеры документов

## Технологии искусственного интеллекта

- Поиск новых незащищённых активов и автоматизированная донстройка 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  $50 \cdot 20\% = 10$  руб.

# Единое досье сотрудников

Исчерпывающая информация по персоне

Главная  
События  
Аналитика  
Мониторинг  
Хранение файлов  
Риски  
**Персоны**  
Расследования  
Отчеты

Профиль: Петров Дмитрий ● ⓘ  
Руководитель направления с ключевыми клиентами  
Отдел развития бизнеса в Москве и МО (комната 7-11)

Персональная информация    **Статистика**    Группы рисков    Граф связей    Наблюдение

Запросы

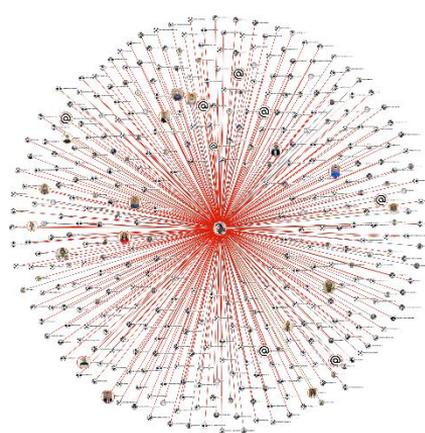
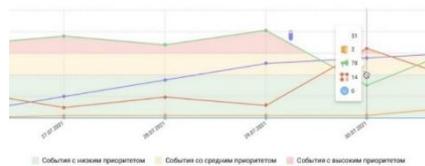
ДАТА: Все    СТАТУС: Все    ОТДЕЛ: Все    ГРУППА: Все    УРОВЕНЬ НАРУШЕНИЯ: Все

**Уровень нарушений** (Всего 402)

Уровень нарушения	Количество
Высокий	6
Средний	3
Низкий	24
Отсутствует	364

**Дата**

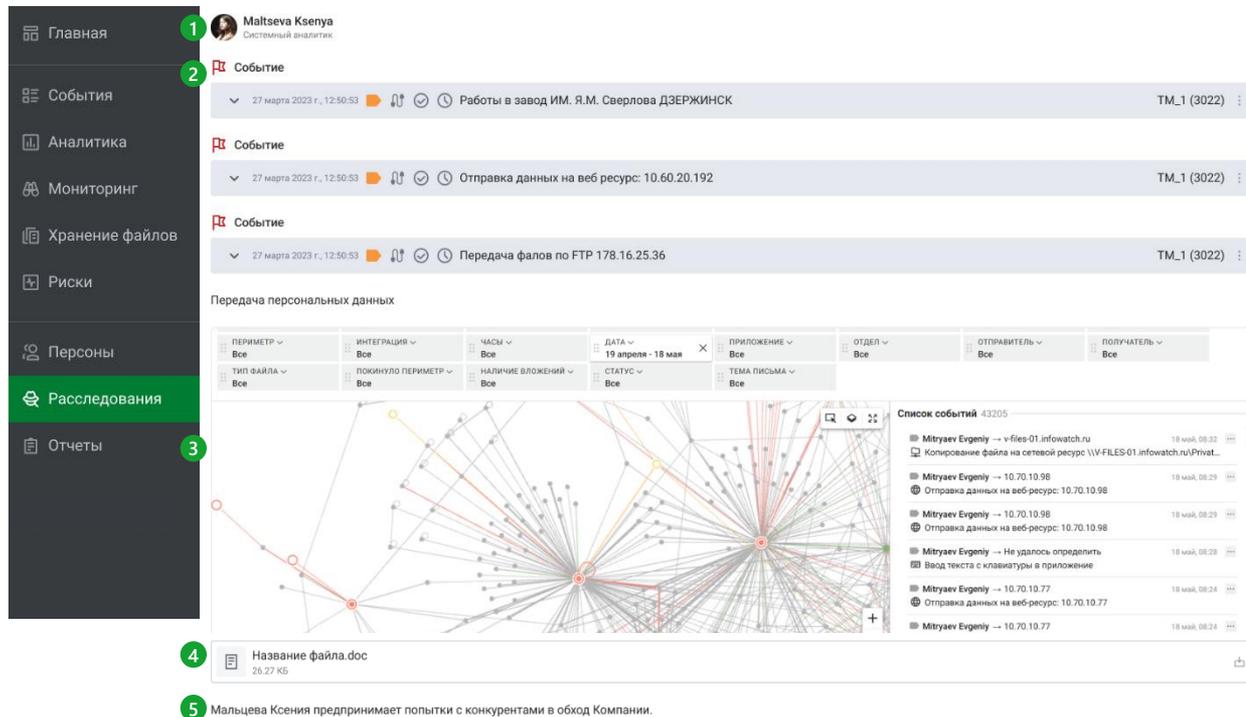
Дата	Высокий	Средний	Низкий	Итого
21.07.2023	1	1	25	27
22.07.2023	1	1	23	25



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



1 Maltseva Ksenya  
Системный аналитик

2 Событие

27 марта 2023 г., 12:50:53 Работы в завод ИМ. Я.М. Сверлова ДЗЕРЖИНСК TM\_1 (3022)

Событие

27 марта 2023 г., 12:50:53 Отправка данных на веб ресурс: 10.60.20.192 TM\_1 (3022)

Событие

27 марта 2023 г., 12:50:53 Передача фалов по FTP 178.16.25.36 TM\_1 (3022)

Передача персональных данных

ПЕРИМЕТР	ИНТЕГРАЦИЯ	ЧАСЫ	ДАТА	ПРИЛОЖЕНИЕ	ОТДЕЛ	ОТПРАВИТЕЛЬ	ПОЛУЧАТЕЛЬ
Все	Все	Все	19 апреля - 18 мая	Все	Все	Все	Все
ТИП ФАЙЛА	ПОКИНУЛО ПЕРИМЕТР	НАЛИЧИЕ ВЛОЖЕНИЙ	СТАТУС	ТЕМА ПИСЬМА			
Все	Все	Все	Все	Все			

Список событий 43205

- Mityaev Evgeniy → v-files-01.infowatch.ru 18 мая, 08:32
- Копирование файла на сетевой ресурс \\V-FILES-01.infowatch.ru\Privat...
- Mityaev Evgeniy → 10.70.10.98 18 мая, 08:29
- Отправка данных на веб-ресурс: 10.70.10.98
- Mityaev Evgeniy → 10.70.10.98 18 мая, 08:29
- Отправка данных на веб-ресурс: 10.70.10.98
- Mityaev Evgeniy → Не удалось определить Вид текста с клавиатуры в приложение 18 мая, 08:28
- Mityaev Evgeniy → 10.70.10.77 18 мая, 08:24
- Отправка данных на веб-ресурс: 10.70.10.77
- Mityaev Evgeniy → 10.70.10.77 18 мая, 08:24

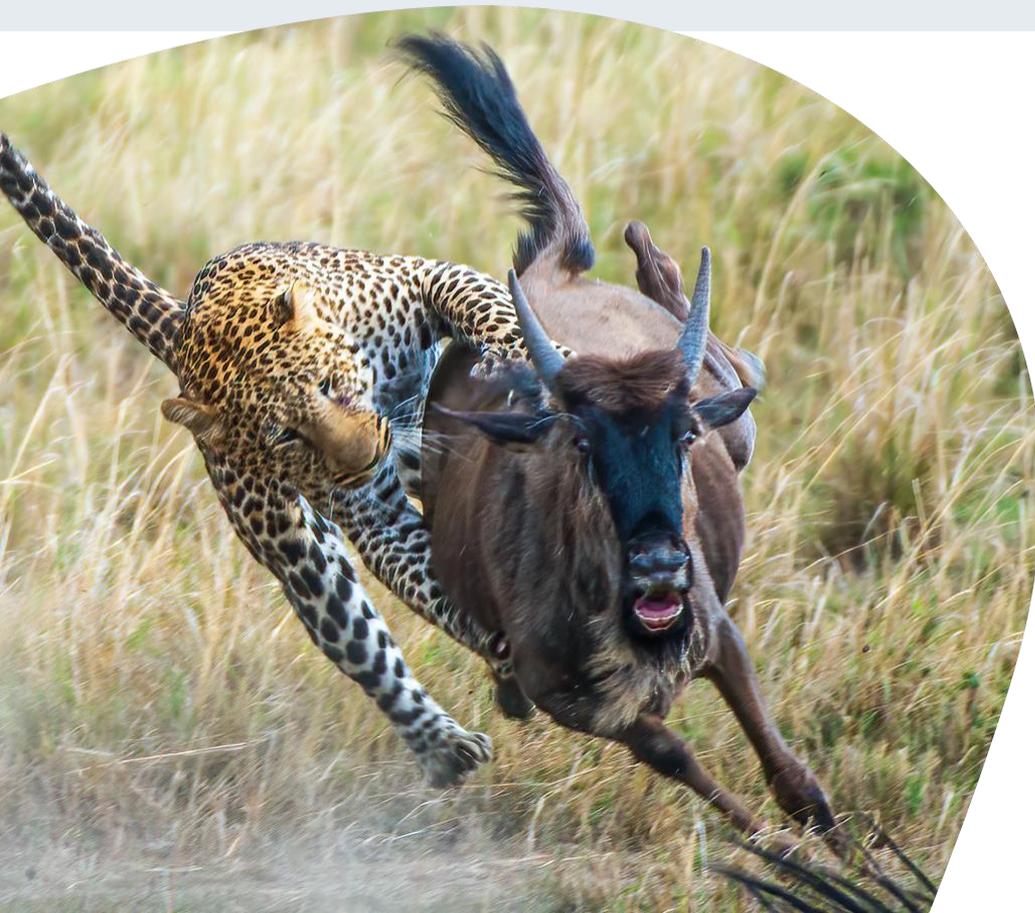
4 Название файла.doc  
26,27 KB

5 Мальцева Ксения предпринимает попытки с конкурентами в обход Компании.

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



Максимум релевантных данных под рукой



Удобное визуальное представление



Интерактивные инструменты выборки, 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



# 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 продукты 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

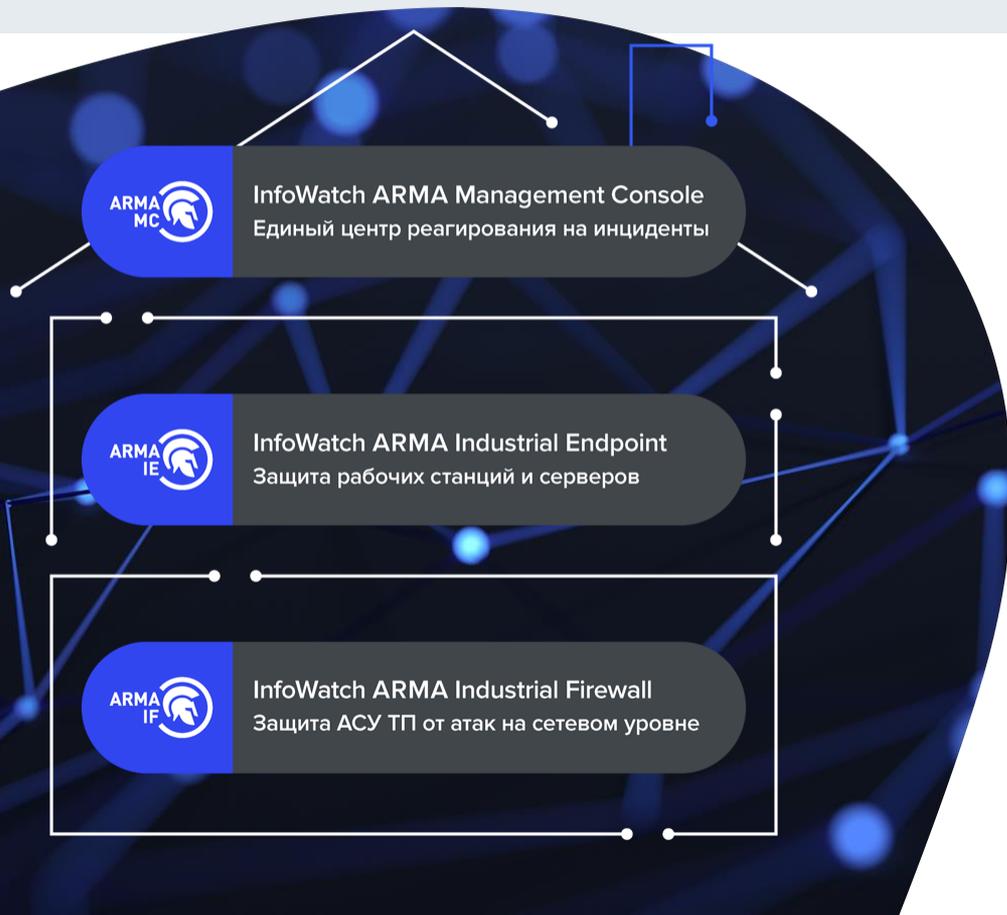
Фильтрация до уровня команд

## 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



Министерство  
обороны РФ



Центральное  
таможенное  
управление



Федеральная  
налоговая  
служба



Министерство  
энергетики  
РФ



Министерство  
сельского  
хозяйства РФ



Банк России

**Альфа Банк**



**ГАЗПРОМБАНК**



**СОВКОМБАНК**

**banki.ru**



РУССКИЙ СТАНДАРТ  
БАНК



**АЛЬФА  
СТРАХОВАНИЕ**



МОСКОВСКАЯ  
БИРЖА

Яков  
и Партнёры



**ВЕРТОЛЕТЫ  
РОССИИ**



**ТРАНСНЕФТЬ**



**РОСНЕФТЬ**



**ГАЗПРОМ  
ДОБЫЧА**



**РОСАТОМ**



**МОСВОДОКАНАЛ**



**Внуково**



**ТТК.ТрансТелеКом**

**ТАСС**

*Maraven*

**CG CAPITAL GROUP**





**ХОТИТЕ ПОПРОБОВАТЬ  
НАШИ ТЕХНОЛОГИИ  
В ДЕЛЕ?**

**ПРОВЕДЁМ  
ПИЛОТ  
БЕСПЛАТНО!**



**Виталий Гуцин · Infowatch**

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



**/InfoWatch**

**infowatch.ru**



**/InfoWatchOut**