



GIS  
D A Y S

# Защита от утечек — фокус на важном и скорость реакции

Татьяна Ксюнина

Руководитель направления по развитию бизнеса на территории СЗФО

InfoWatch

# DLP-система нового поколения – это целый комплекс возможностей

## DLP

Предотвращение утечек

## Мониторинг действий сотрудников

Доказательная база и наблюдение

## DCAP

Аудит хранения и прав доступа

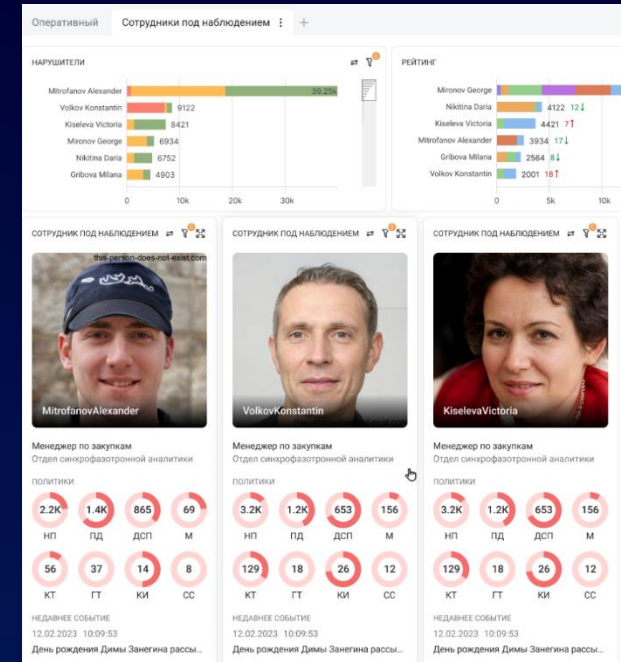
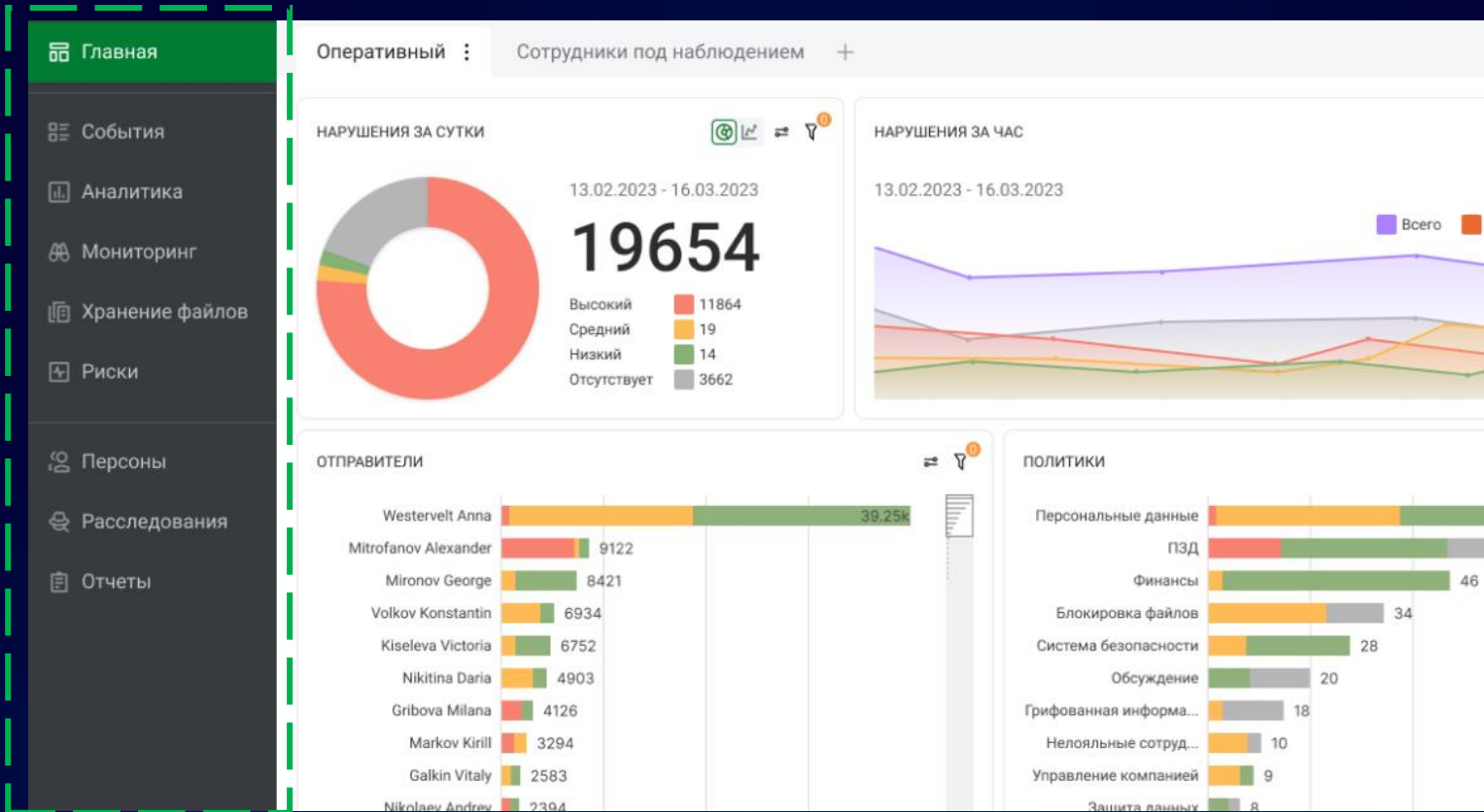
## BI аналитика

Ежедневный мониторинг и быстрые расследования

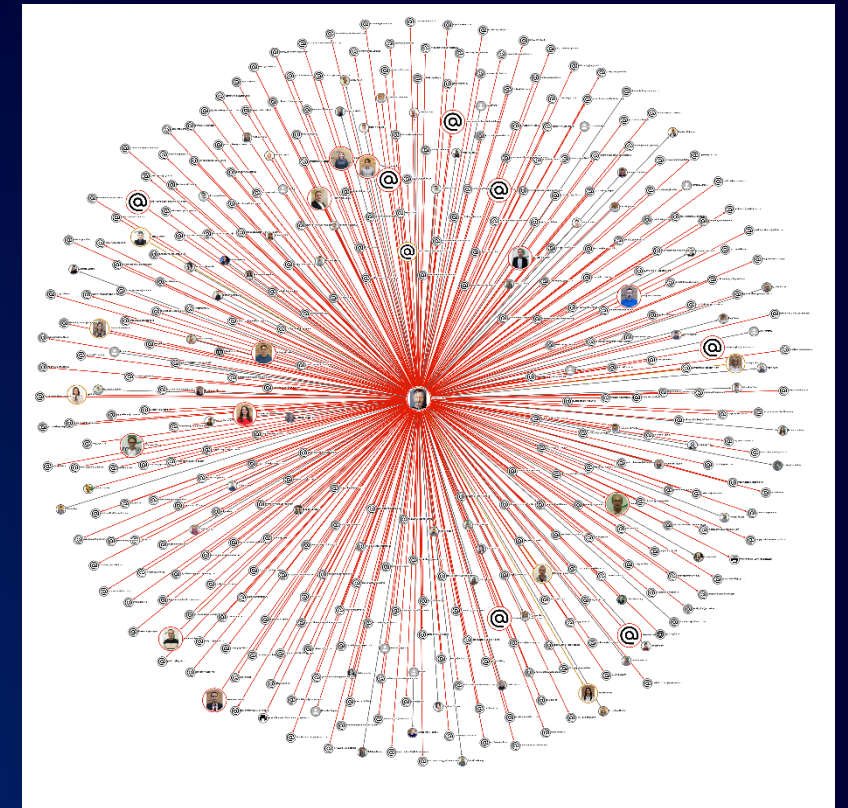
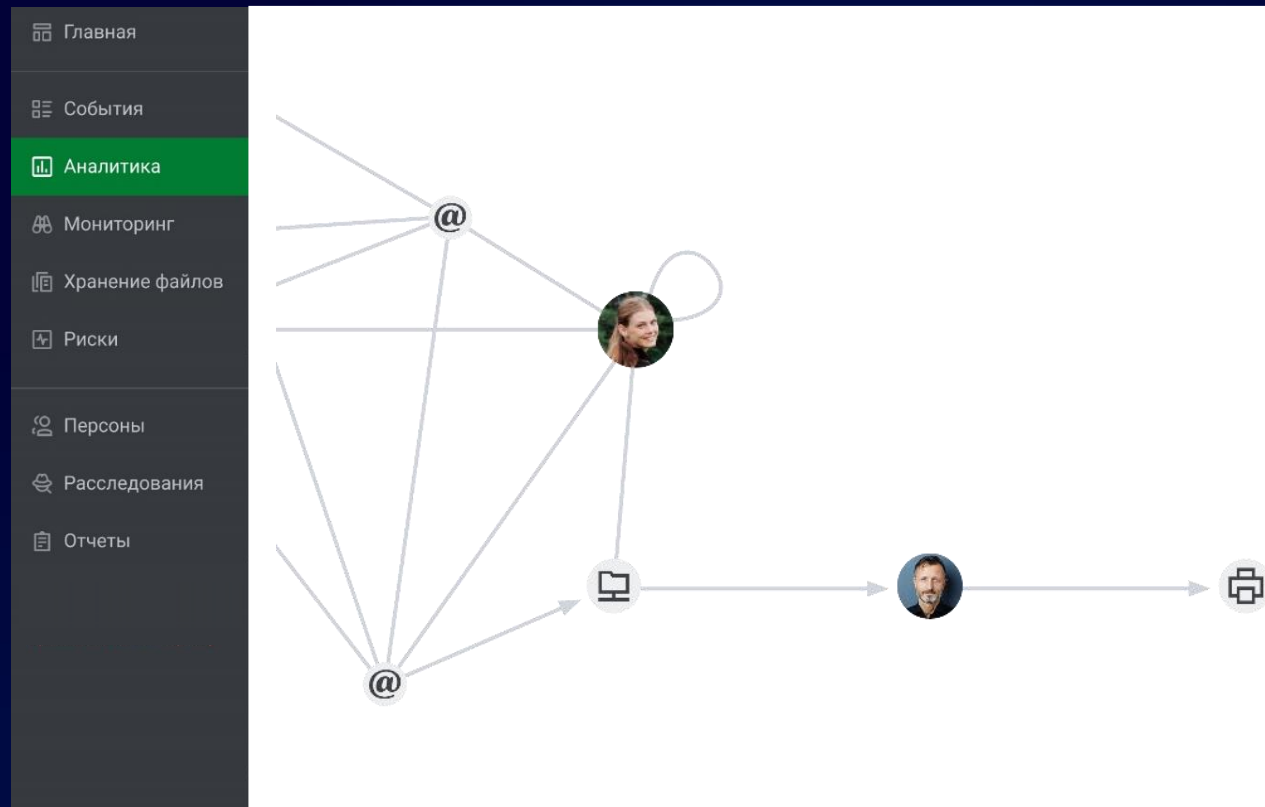
## Предиктивная аналитика

На кого обратить внимание для превентивного реагирования

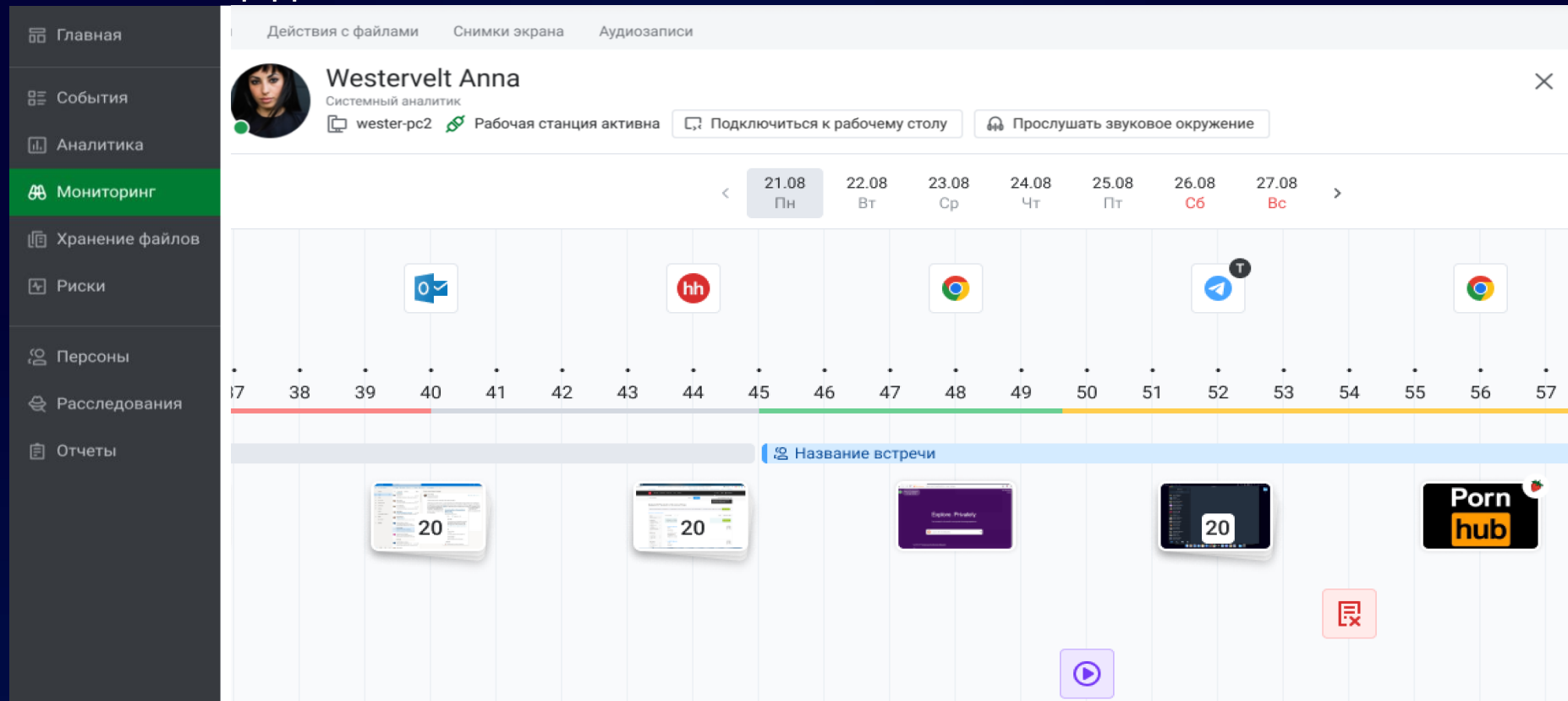




Чтобы найти всех соучастников, выявить неявные связи и пути перемещения документов



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



# DCAP и категоризация 100% документов

Аудит хранения и прав доступа, исправление проблем

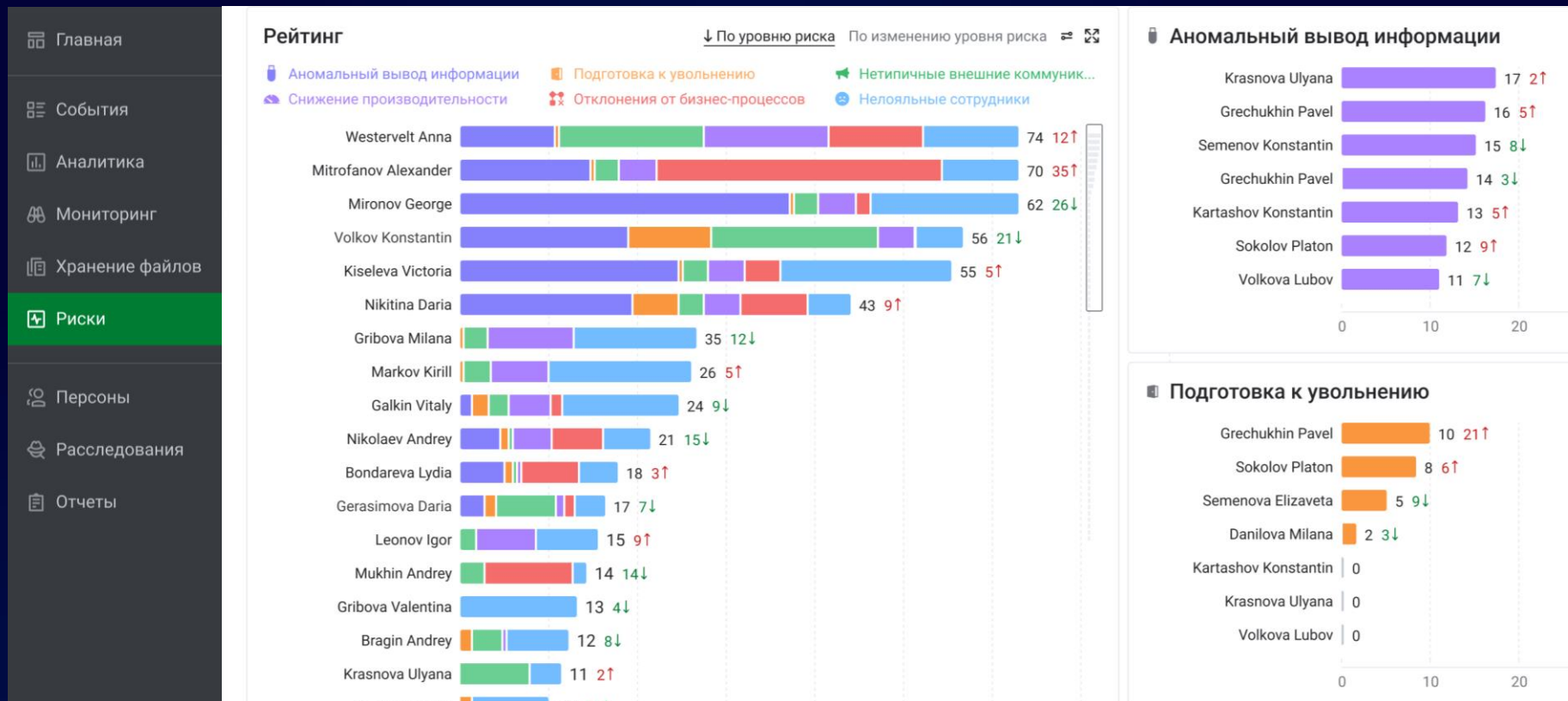
The screenshot displays the DCAP interface. On the left is a sidebar with navigation options: Главная, События, Аналитика, Мониторинг, **Хранение файлов** (highlighted), Риски, Персоны, Расследования, and Отчеты. The main area shows a dashboard with eight document group cards. The top-left card is for 'Негруппированные файлы' (292 files) and lists file types: exe, psd, dll, cab, mkv, lib, ogv, ogm, mp3. The other seven cards represent different groups (Группа 3, 4, 7, 8, 11, 12, 5) with varying file counts (3, 81, 112, 129, 67, 8, 16). Each group card includes a progress bar, a 'ТЕМЫ' section with tags like 'стратегия', 'план', '2022', 'тег 5', 'тег 6', 'что-то', 'непонятно', 'еще тег', 'другой', 'продажи', and a 'ТИПЫ ФАЙЛОВ' section with tags: txt, doc, docx, pdf, ppt, xlsx. Each card also has links for 'Примеры документов' and 'Список файлов'.

Поиск новых незащищенных активов и автоматизированная донастройка DLP

Технологии искусственного интеллекта

# Рейтинг сотрудников с подозрительным поведением – по группам риска

## Кого стоит проверить в первую очередь



Технологии  
искусственного  
интеллекта

# Единое досье сотрудников

Исчерпывающая информация по персоне: персональная, нарушения, риски, карта коммуникаций, аудиозаписи с микрофона ПК, снимки и видео экрана

**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

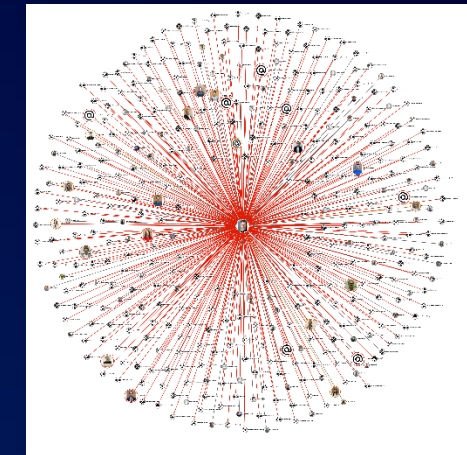
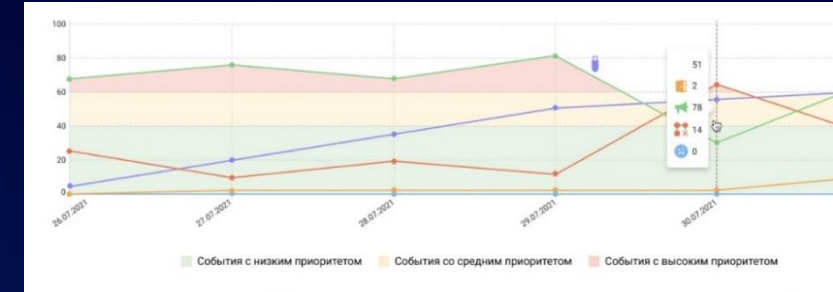
Дата: Все | Статус: Все | Отдел: Все | Группа: Все | Уровень нарушения: Все

**Уровень нарушений (Всего 402)**

Отсутствует	364
Низкий	24
Средний	3
Высокий	6

**Дата**

21.07.2023	27
22.07.2023	2





Обобщить, представить в соответствии с методологией или формой отчётности

**ID#1 Первое расследование**

**Romanov Andrey**  
Ведущий менеджер по продажам

**Событие**

13 июль 2018, 10:43:11 Работы в ЗАВОД ИМ. Я.М. СВЕРДЛОВА ДЗЕРЖИНСК

**Подозрение в коррупции**

**Событие**

12 июль 2018, 13:39:47 Отправка данных на веб-ресурс: 10.60.20.192

**Разглашение условий конкурса**

**Событие**

12 июль 2018, 13:34:34 Передача файлов по FTP 178.16.25.36

**Передача персональных данных**

Объекты защиты

Объект защиты	Количество
Коррупция	129
Гриф секретности	66
Документы коммерч...	46
Документы отделе вн...	34
Конкурсная документ...	6
Счета	4
Платёжные реквизиты	4
ВСУ	2

Статистика\_Романов\_A.jpg

Резюме\_Романов\_A...  
12.43 КБ

Романов Андрей предпринимает попытки договориться с конкурентами в обход Компании. Также замечена активность на

Внутри DLP, без перехода в сторонние приложения.

# Кейс. Выявление факта промышленного шпионажа

Горнодобывающая компания перешла под контроль государства 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 подразделения уровень дохода не соответствовал расходам. Он был в сговоре с поставщиком услуг



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. Предотвращение «слива» базы поставщиков конкуренту

Сотрудник готовился слить базу поставщиков конкурентам



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

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





GIS  
DAYS

СПАСИБО ЗА ВНИМАНИЕ



Tatiana.Ksyunina@infowatch.com  
www.infowatch.ru

 **INFOWATCH®**