

ПРЕИМУЩЕСТВА

1

Существенное повышение эффективности использования DLP-системы в организации благодаря:

- контролю «серой» зоны информационных потоков (то, что остается за скобками политик безопасности)
- мгновенной обработке больших объемов данных (за секунды обрабатываются 10 млн событий)
- анализу информационных потоков с помощью наглядных визуализаций и графиков

2

Наглядное и прозрачное представление результатов работы службы ИБ благодаря гибкой отчетности:

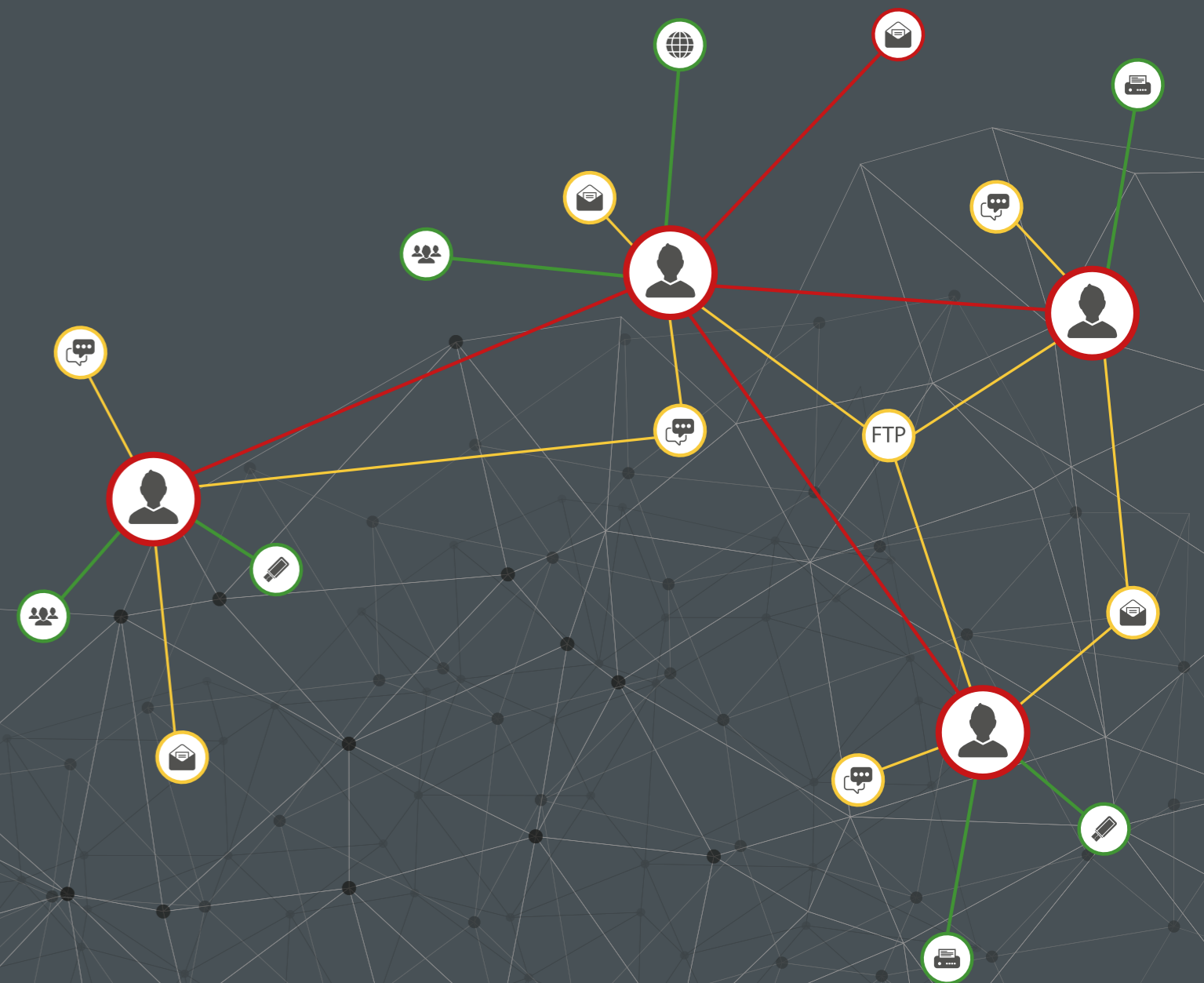
- отчетность отражает любой срез данных по любым метрикам (люди, политики, даты и др.)
- отчетность служит достаточным основанием для принятия управленческих решений
- возможность строить специфические отчеты по инцидентам



INFOWATCH VISION



INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ



 INFOWATCH® МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Бизнес-центр «Верейская плаза»

121357, Москва, ул. Верейская,
д.29, стр.134

www.infowatch.ru

+7 (495) 22-900-22
+7 (499) 37-251-74
sales@infowatch.ru



InfoWatch Vision – инструмент визуальной аналитики информационных потоков в режиме реального времени. Первая версия продукта разработана непосредственно для работы с **InfoWatch Traffic Monitor** и расширяет его возможности в рамках анализа подозрительных активностей сотрудников и проведения расследований.

НОВЫЕ ВОЗМОЖНОСТИ

1. Выявление подозрительной активности и связей сотрудников, которые остаются вне поля зрения политик DLP:

- Построение карты внешних коммуникаций
- Выявление общения между несвязанными отделами
- Обозначение неформального круга общения сотрудников
- Выявление нестандартных схем движения конфиденциальных данных

2. Мгновенный доступ к деталям любой подозрительной активности

3. Гибкая отчетность в режиме реального времени для любого среза данных

КЛЮЧЕВОЙ ФУНКЦИОНАЛ



Интерактивный граф связей

Граф используется офицером безопасности для визуального анализа связи сотрудников и внешних контактов. Граф можно строить сразу для нескольких сотрудников или целого отдела. Граф мгновенно перестраивается в зависимости от выбранных параметров: сотрудники, временные периоды, политики, пересылаемые файлы, объекты защиты и пр. Узлы и связи на графе кликабельны – можно провалиться в события любой связи.



Досье по сотруднику или внешнему контакту

Досье используется офицером безопасности для контроля конкретных сотрудников и полного анализа их активности в компании. Досье на внешний контакт позволяет оценить, с кем из компании он связан, какие политики назначены, какие файлы он получил и отправил. Досье на внешний контакт формируется автоматически без участия офицера безопасности.



Динамическая сводка безопасности по всей компании или по отделам

Сводка используется офицером безопасности для ежедневного мониторинга информационных потоков компании, а также для проведения расследования при отсутствии прямых входящих данных (инцидент, дата, сотрудник и т.д.).

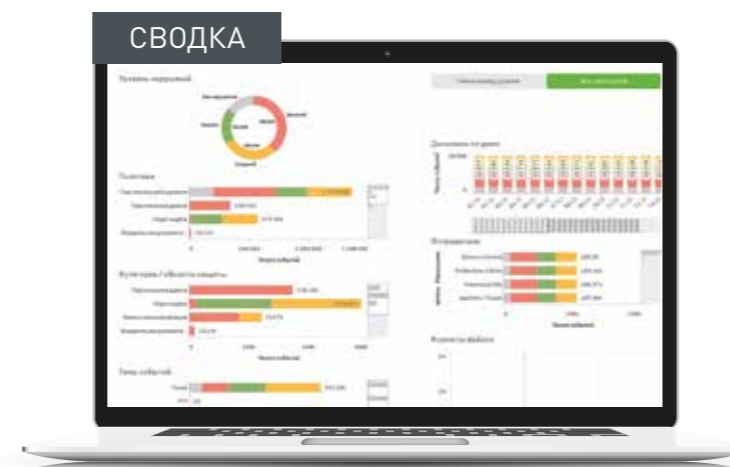


Конструктор для построения специфических отчетов

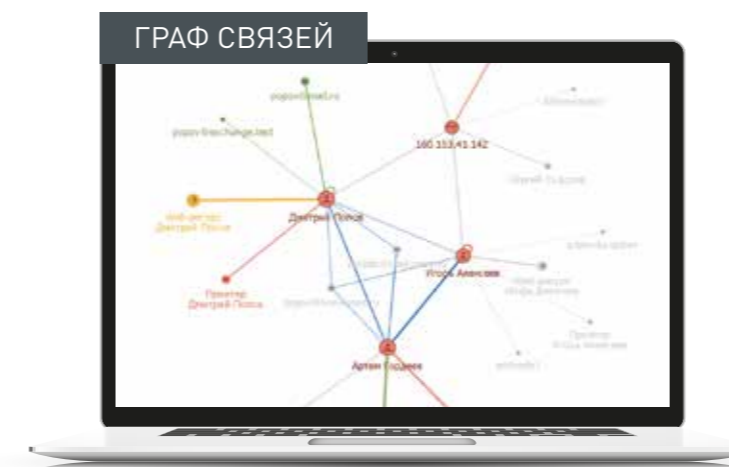
Конструктор позволяет формировать отчеты по инцидентам информационной безопасности, представлять специфические разрезы статистики и графики в одном окне, добавлять комментарии, изображения и выгружать результаты в формате PDF и PPT.

СТРУКТУРА INFOWATCH VISION

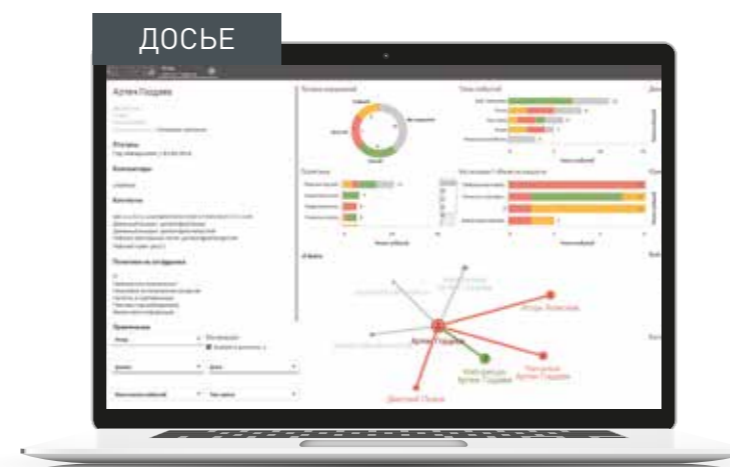
InfoWatch Vision состоит из 4 интерактивных листов:



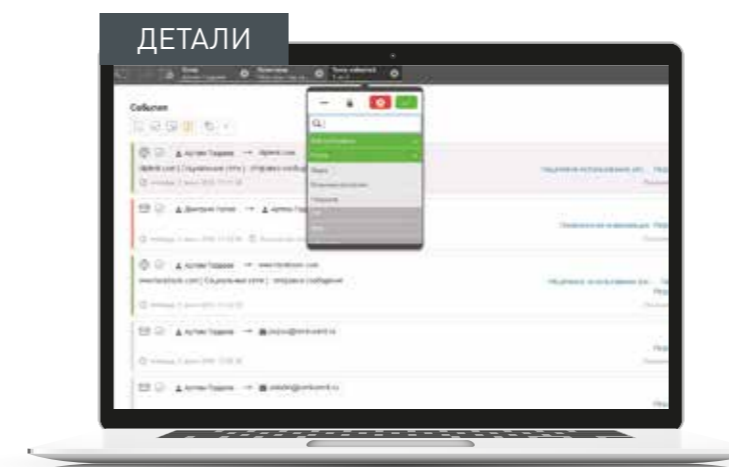
Сводка позволяет заглянуть внутрь информационных потоков, выявить нестандартные активности сотрудников и движение чувствительной информации



Граф связей позволяет визуально проанализировать связи сотрудников, внешних контактов и перемещение информации на USB-накопители, принтеры, веб-ресурсы



Досье консолидирует информацию по сотрудникам компании и внешним контактам (политики, граф связей, категории объектов защиты и т.д.)



Детали позволяют провалиться в конкретное событие, просмотреть текст письма или сообщения, выгрузить вложение и список событий по выборке

КАК ЭТО РАБОТАЕТ?

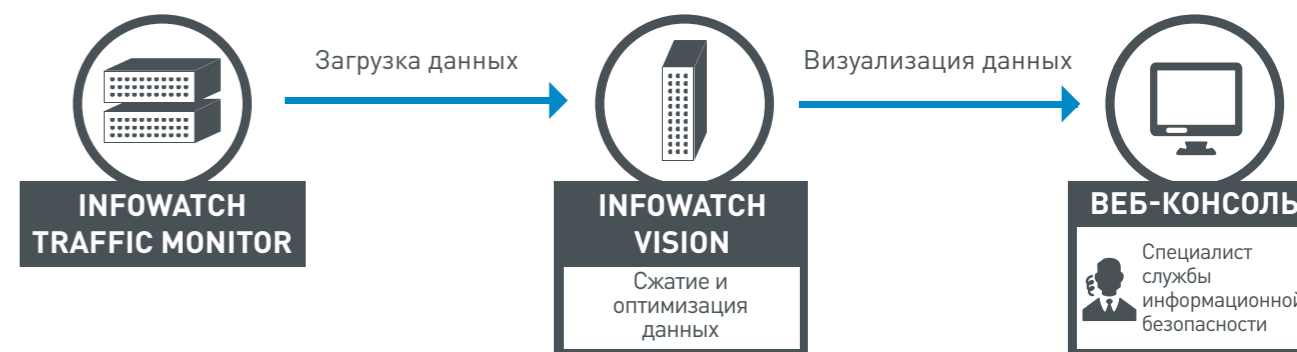
Все интерактивные листы связаны между собой и всегда отражают единый срез данных:



1. Листы Сводка, Граф связей и Досье используются для формирования выборки данных. Выборки создаются с помощью фильтров и кликабельных графиков

2. Лист Детали используется для просмотра списка событий по сформированной выборке и детальной информации по ним

АРХИТЕКТУРА



При установке InfoWatch Vision происходит автоматическая загрузка всей информации из базы данных InfoWatch Traffic Monitor. В дальнейшем обновленная информация загружается по расписанию либо вручную

Загруженная информация постоянно находится в оперативной памяти InfoWatch Vision. Поэтому любой срез информации всегда доступен по клику мыши

Ежедневная работа с событиями и проведение расследований осуществляется в веб-консоли InfoWatch Vision. Веб-консоль InfoWatch Traffic Monitor используется только для конфигурирования системы и корректировки политик