



Точечный контроль сотрудников и расследование инцидентов по горячим следам

InfoWatch Person Monitor – это модуль InfoWatch Traffic Monitor для индивидуального наблюдения за сотрудниками и расследования инцидентов «по горячим следам».



Компонента
DLP-системы InfoWatch



Инструмент локального
расследования инцидентов



Мониторинг сотрудников
«под подозрением»

InfoWatch Person Monitor предназначен для контроля небольших групп пользователей (проектных групп, отделов) либо индивидуального мониторинга конкретных персон компании «под подозрением».

Решаемые задачи:

- Выявление инсайдеров – мошенников, нелояльного персонала, сотрудников, находящихся в поиске работы
- Поиск возможностей для оптимизации ресурсов организации (незэффективное исполнение рабочих обязанностей)
- Раннее обнаружение рисков, в том числе связанных с социально-опасным поведением персонала (терроризм, торговля оружием, наркотиками и т.д.)
- Внутреннее локальное расследование нарушений и инцидентов



СЦЕНАРИИ ПРИМЕНЕНИЯ

1. Наблюдение за сотрудниками под подозрением в режиме реального времени

InfoWatch Person Monitor обладает функционалом, который позволяет настроить точечный контроль за сотрудниками «под подозрением» и выявить тех, кто работает на конкурентов, занимается саботажем, мошенничеством, нелегальной деятельностью на рабочем месте.



Контроль за рабочим местом сотрудника (аудио и видео-наблюдение, снимки экранов (скриншоты рабочего стола))



Контроль переписки в мессенджерах (Skype, Lync, Viber, ICQ, QIP, Miranda, MailRu-агент) и электронной почты (включая вложения): Exchange/IMAP/POP3/SMTP/NRPC



Контроль мобильных сотрудников:
• Разговоры
• SMS-сообщения
• GPS-трекинг



Контроль буфера обмена (текст, картинки, файлы)



Контроль печати



Кейлоггер (перехват вводимого текста)



Контроль поисковых запросов сотрудников в различных поисковых системах



Операции с файлами на flash-накопителях с теневым копированием



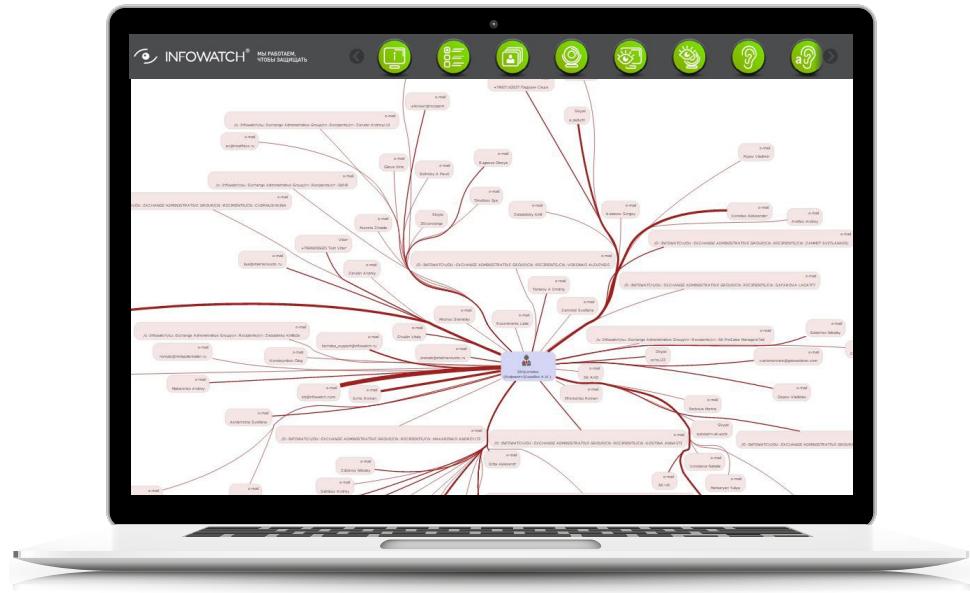
Мониторинг посещаемых сайтов



Граф связей (визуализация взаимосвязей и контактов сотрудника «под подозрением»)

В консоли задаются средние показатели по каждому контролируемому параметру, и любое отклонение от них фиксируется как аномальное и нетипичное поведение сотрудника. Отчеты по нетипичному поведению персонала помогают офицеру безопасности и руководителю видеть картину в компании целиком.

Интеллектуальная система распознавания состояния сотрудника за рабочим местом с высокой точностью определяет, кто входит в систему в каждый конкретный момент времени (контроль несанкционированного доступа к компьютеру).





2. Анализ рабочей активности персонала

Возможности InfoWatch Person Monitor помогают руководителю находить резервы для повышения производительности персонала и возможности оптимизации кадровых ресурсов.



Log in / Log off в системе



Мониторинг посещаемых сайтов



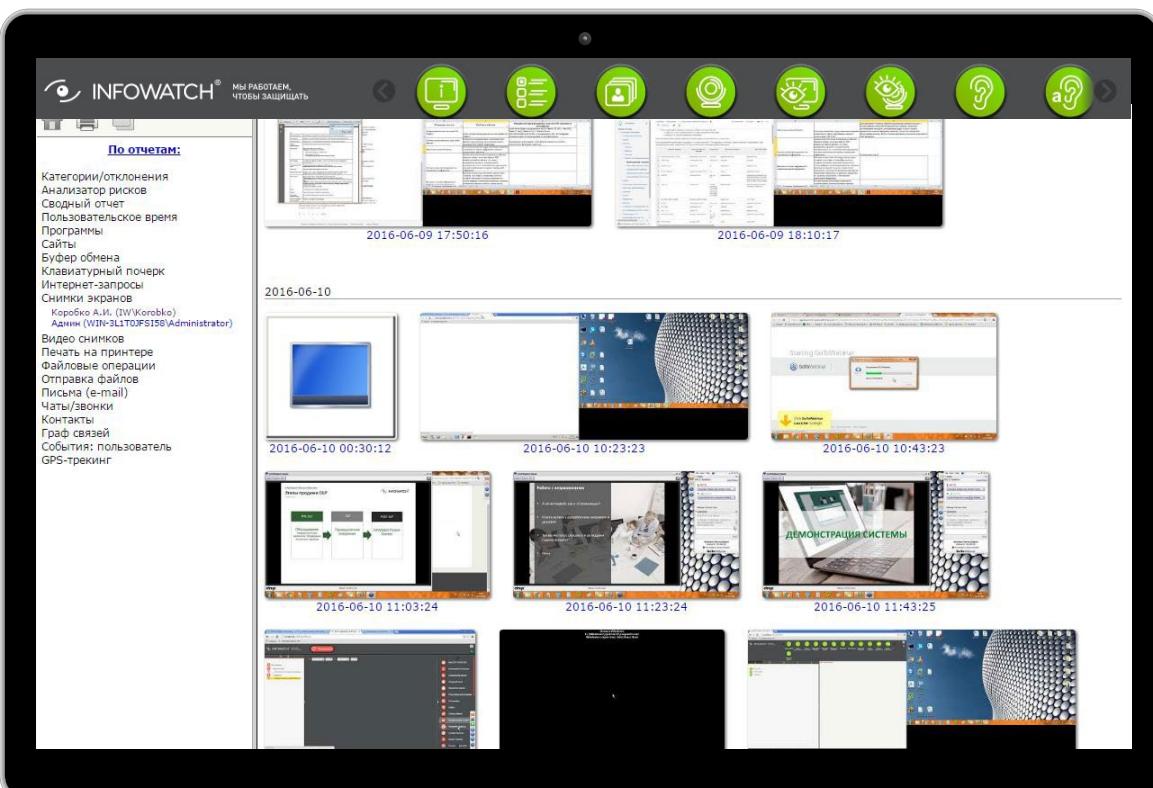
Прогулы, опоздания на работу



Машинное время: сколько времени был включен компьютер сотрудника



Мониторинг запускаемых приложений.
Активная работа в приложениях





3. Быстрое локальное расследование инцидентов

Любой инцидент и нарушение можно расследовать оперативно «по горячим следам» благодаря оперативным сводкам и возможностям онлайн-наблюдения.

InfoWatch Person Monitor генерирует отчеты по различным срезам данных:

- **Анализатор рисков и производительности** – настраиваемый на основе профилей и словарей отчет по эффективной, неэффективной работе сотрудника либо социально-опасному поведению
- **Отчет по категориям и отклонениям** – сводный отчет, показывающий статистику в разрезе используемых ресурсов, приложений и отклонений от средних значений по сотрудникам
- **Машинное время** – отчет о времени работы компьютеров
- **Пользовательское время** – активность сотрудников за день; прогулы, опоздания на работу, популярные программы и сайты
- **Граф связей** – визуальное представление списка контактов сотрудника, с которыми он общался по переписке e-mail, Skype и в чатах
- **Запуск программ** – в каких программах и сколько времени активно работал сотрудник
- **Мониторинг сайтов** – отчет по сайтам, на которые заходил сотрудник
- **Вводимый текст (кейлоггер)** – возможность перехвата вводимого текста
- **Буфер обмена** – текст, файлы и картинки в буфере обмена
- **Файловые операции** – отчет по операциям с данными: копирование, удаление, перенос файлов; доступ к теневым копиям
- **Контроль печати** – отчет по распечатанным сотрудником файлам с расчетом стоимости в зависимости от установленного тарифа
- **Подозрительные события** – отчет по событиям, которые настраиваются самостоятельно (запуск программ, сайтов, ввод текста с учетом алгоритма неточного сравнения слов и т.д.)
- **Поиск информации по сотруднику** – возможность поиска в сформированном отчете с учетом алгоритма неточного сравнения слов

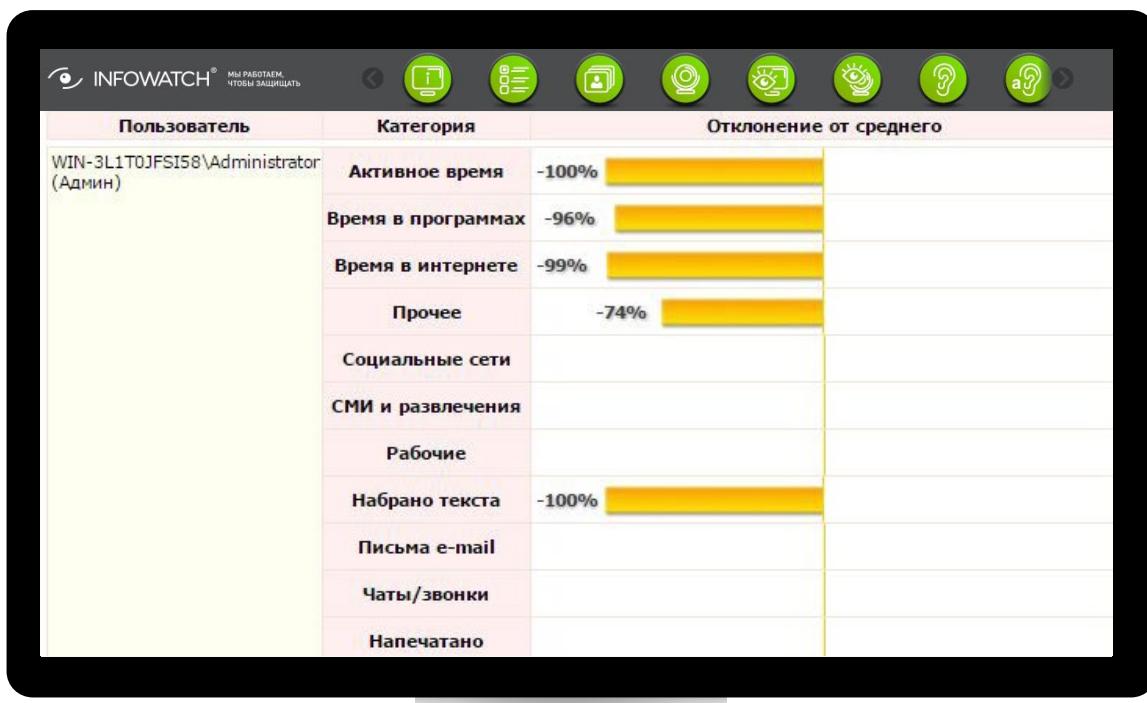
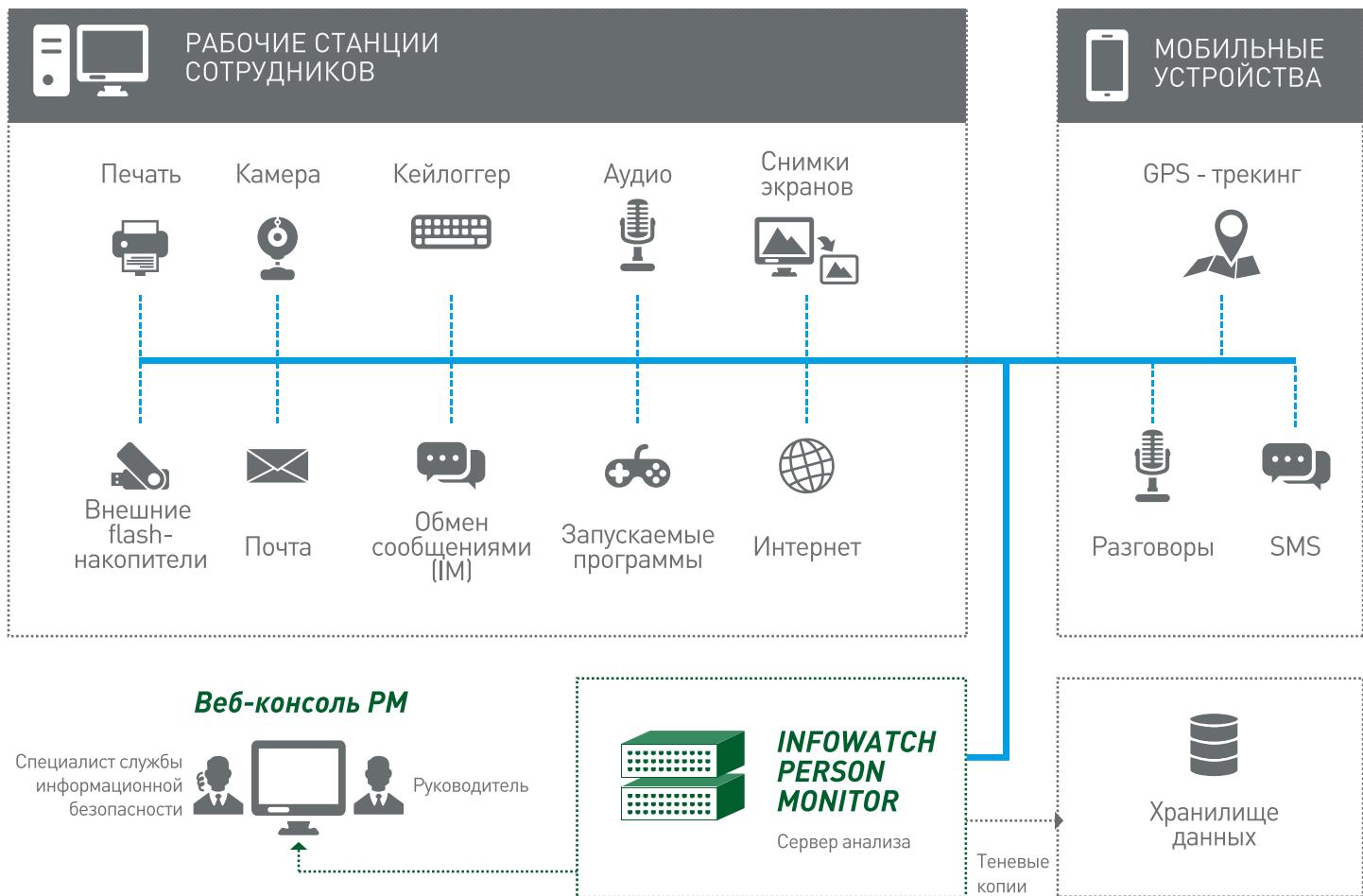




Схема работы модуля

InfoWatch Person Monitor представляет собой клиент-серверную архитектуру с поддержкой MySQL и Microsoft SQL Server. Модуль контролирует активность сотрудников на рабочих станциях и мобильных устройствах на базе Android. Все события и инциденты сохраняются

в базу для проведения расследований. Веб-консоль позволяет офицеру безопасности и руководителю следить за обстановкой в режиме реального времени и своевременно принимать решения в отношении нарушителей.



Дополнительная техническая информация

Поддержка нескольких серверов

InfoWatch Person Monitor может работать в режиме нескольких серверов и одной центральной базы данных

Терминальный сервер

Вся обработка данных ведется на сервере, поэтому не возникает никаких сложностей при работе модуля в терминальных сессиях

Уведомления об инцидентах

Оповещения о подозрительных событиях в трее и окне браузера со звуком. Возможность получения SMS и e-mail уведомлений

Поддержка IPv6

Работа как в IPv4, так и в IPv6 сетях

Поддержка нескольких доменов

Возможность синхронизировать данные одновременно с несколькими доменами компании

Скрытое и открытое наблюдение

Можно установить клиента на удаленные машины в скрытом от сотрудника режиме



Преимущества InfoWatch Person Monitor



Быстрое локальное расследование инцидентов

Все необходимые инструменты для проведения расследований «по горячим следам».



Предотвращение инцидентов на ранних стадиях

Благодаря контролю аномального и нетипичного поведения персонала и возможности индивидуального мониторинга сотрудников «под подозрением». Оперативное выявление рисков, исходящих от сотрудников организации.



Выявление инсайдеров и злоумышленников

Добавляйте сотрудников «под подозрением» в группы риска и ведите более плотный контроль их поведения.



Управление продуктивностью и рабочей активностью персонала

Контроль эффективности использования рабочего времени, выявление резервов для роста производительности сотрудников.



Удобные и разнообразные отчеты

Выбирайте любой срез данных, создавайте отчеты и принимайте решения.



Мониторинг в режиме реального времени

Веб-консоль с оперативными сводками и отчетами доступна из любой точки мира.



INFOWATCH®

+7 (495) 22-900-22

sales@infowatch.ru

www.infowatch.ru