INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Решения InfoWatch для контроля информационных потоков

Сучкова Елена
Директор по работе со стратегическими клиентами

Группа компаний InfoWatch

О компании

INFOWATCH®

Компания основана
в 2003 году, выросла
из внутреннего проекта
«Лаборатории Касперского»

Партнерская сеть в России,
СНГ и дальнем зарубежье

Продуктовый фокус:
решения для защиты
корпоративной информации

Обширная экспертиза и опыт
реализации проектов любой
сложности в государственном
секторе, ТЭК, финансовой,
телекоммуникационной
и других отраслях экономики

Лидер российского рынка
защиты данных от утечки

Инновационные продукты

InfoWatch Holding

2004 2010 2010 2011 2012

Матрица угроз

INFOWATCH®

Внутренние угрозы	Внешние угрозы
Случайные	
• Халатность • Разгильдяйство • Использование ресурсов в развлекательных целях • Ошибки • Некорректная работа информационных систем • Компьютерные сбои	• Массовые вирусы • Рекламный/AD-Фишинг • Перехват трафика • Утечка информации через контрагентов • Сбой работы провайдера
Намеренные	
• Саботаж • Сговор • Воровство • Мошенничество • Утечка информации • Запуск негатива изнутри • Клевета	• DDoS-атаки • Фишинг • Социальная инженерия • Таргетированные атаки • Запуск негатива извне • Мошенничество

Наши клиенты

INFOWATCH®

Банки и финансы

СБЕРБАНК Всегда рядом
Райффайзен БАНК
Связь Банк
ВТБ
HOME CREDIT BANK
Банк Москвы
Белгазпромбанк

Государственный сектор

- Федеральная Таможенная Служба
- Министерство Финансов Российской Федерации
- Федеральная налоговая служба
- Министерство обороны Российской Федерации
- Правительство Тульской области
- МЧС России

Фармацевтика

STADA CIS
акрихин Люди заботятся о Людях

Энергетика

РУСЭНЕРГО РЕСУРС
РОССЕТИ
РусГидро
e·on
ТВЭЛ
РУСЭНЕРГОСБЫТ

Нефтегазовый сектор

НОВАТЭК
СлавНефть
Газпром ВНИИГАЗ
TATNEFT
СНГ
ЛУКОЙЛ НЕФТЯНАЯ КОМПАНИЯ

Транспорт и логистика

РОСЖЕЛДОР ПРОЕКТ
НОВОРОССИЙСКИЙ МОРСКОЙ ТОРГОВЫЙ ПОРТ
РЖД Российские железные дороги

Промышленность

ОБЪЕДИНЕННАЯ ДВИГАТЕЛЕСТРОИТЕЛЬНАЯ КОРПОРАЦИЯ
ОБОРОНПРОМ
ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО МАГНИТОГОРСКИЙ МЕТАЛЛУРГИЧЕСКИЙ КОМБИНАТ
Московский вертолетный завод им. М.Л. Миля

Страхование

ВСК СТРАХОВОЙ ДОМ
СОГАЗ СТРАХОВАЯ ГРУППА

Торговля

МИР КНИГИ .RU
МАГНИТ
magnum cash & carry
KUPIVIP.RU

Телекоммуникации

Билайн
МТС

Эдвард Сноуден - типичный инсайдер

INFOWATCH®

- Работал системным администратором
- Не вызывал подозрений у работодателя
- Использовал для выноса данных общедоступные программы
- В АНБ США не использовались средства для контроля трафика

скачал около **1,7 млн** файлов
из внутреннего wiki-каталога АНБ

Законодательство в сфере утечек данных

Основные законы:

- 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Указ Президента №188 «Об утверждении перечня сведений конфиденциального характера»
- 152-ФЗ «О персональных данных»
- 98-ФЗ «О коммерческой тайне»

Ст. 272 УК РФ: неправомерный доступ к информации (н-р, копирование информации, охраняемой законом)- срок **до 2 лет**

Ст. 183 УК РФ: разглашение или использование сведений, составляющих коммерческую тайну, повлекшее тяжкие последствия, - срок **до 7 лет**

Основные требования и рекомендации регуляторов:

- Приказ ФСТЭК №21 (ПДн)
- Приказ ФСТЭК №17 (государственные информационные системы)
- СТО БР ИББС (банки)
- 382-П (НПС)
- PCI DSS (платежные системы)

Ст. 183 УК РФ: разглашение или использование сведений, составляющих коммерческую тайну, причинившее крупный ущерб, - срок **от 3-5 лет**

Прочие рекомендации:

ISO 27001/ISO 27002 (ГОСТ 27001/ГОСТ 17799)

Защита от утечек и внутренних угроз InfoWatch Traffic Monitor Enterprise

InfoWatch Traffic Monitor Enterprise

INFOWATCH®

Внутренние случайные
- Халатность
- Разгильдяйство
- Использование ресурсов в развлекательных целях

Внутренние намеренные
- Саботаж
- Сговор
- Воровство
- Мошенничество
- Утечка информации
- Запуск негатива изнутри
- Клевета

Примеры утечки данных

INFOWATCH®

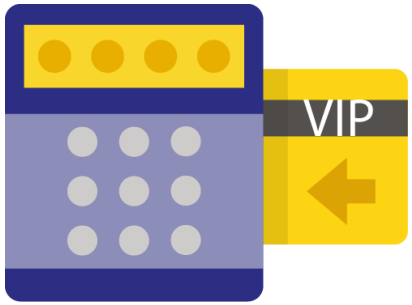
Ретейлер

База данных сотрудников (KPI, ЗП, премии)

Соцсети

Увеличение ЗП 169 сотрудникам. Ущерб: 15,5 млн руб./год

Сотрудник банка



Данные счетов VIP-клиентов с пин-кодами

Украдено 3,5 млн руб.

Известные меры защиты

INFOWATCH®

Организационные меры
Режим коммерческой тайны, регламенты, разграничение прав и т.д.

1. Нужны технические средства для контроля

Блокировка каналов передачи
USB, Интернет, внешняя почта

1. Вызывает негатив
2. Пользователи ищут пути обхода
3. Требует работы с исключениями

Слежка за персоналом
Видеонаблюдение, СКУД, программы-снифферы, Radmin и т.д.

1. Требует больших человеческих ресурсов
2. Низкая эффективность

Не достаточно

Комплексный подход к защите данных

INFOWATCH®

Наш подход к защите от утечек информации

Pre DLP

Аудит ИБ

Классификация данных

Внедрение режима коммерческой тайны

DLP

Установка и настройка ПО

Техническое сопровождение

Запуск мониторинга

Post DLP

Проведение расследований

Сопровождение внутренних расследований

Обеспечение хранения всех инцидентов

InfoWatch Traffic Monitor Enterprise

INFOWATCH®

Каналы мониторинга информационных потоков организации

Почта	SMTP, IMAP4, POP3, MAPI, Lotus Domino
Интернет-ресурсы	Блоги, соцсети, ЖЖ, форумы: HTTP, HTTPS, FTP, FTPS
Съемные носители	и другие устройства
Мессенджеры	ICQ, Skype, Gtalk, Mail.ru Agent, Lync, XMPP, MMP
Хранилища	Сетевые папки, локальные диски рабочих станций
Голос	Голосовой трафик
Печать	Локальные, сетевые принтеры
Моб. устройства	Камера, почта, интернет-трафик, сообщения

Технологии анализа данных

INFOWATCH®

Лингвистический анализ	Базы контентной фильтрации	Оптическое распознавание символов (OCR)	Цифровые отпечатки
Детектор паспортов	Детектор выгрузок из баз данных	Детектор заполненных форм	Детектор печатей

Гибридный анализ на основе комплекса технологий

Классификация данных

INFOWATCH®

До

После

Мы поймаем чёрную кошку в тёмной комнате

Стадии внедрения системы DLP

INFOWATCH®

Pre DLP

DLP

Post DLP

- Выявление сговоров и злоумышленников, лиц, занимающихся шпионажем
- Сбор цифровых доказательств
- Выявление аномальной активности
- Хранение всех инцидентов
- Обеспечение юридической значимости собранных доказательств

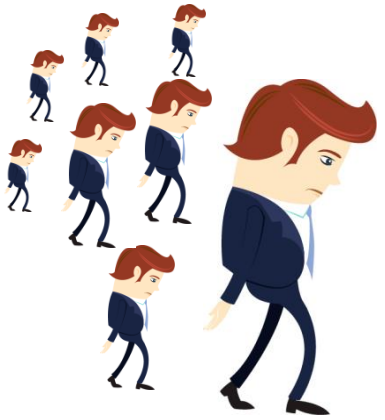
Успешный кейс

INFOWATCH®

Предотвращение утечек

Банк

Перехват баз данных клиентов



За квартал были пойманы 92 сотрудника

Traffic Monitor

1. выявил факт воровства
2. предотвратил ущерб **$420 млн**

Успешный кейс

Использование ресурсов компании

Сырьевая компания

Найдено письмо о сговоре между бухгалтером и главным технологом

Завышение себестоимости

Traffic Monitor

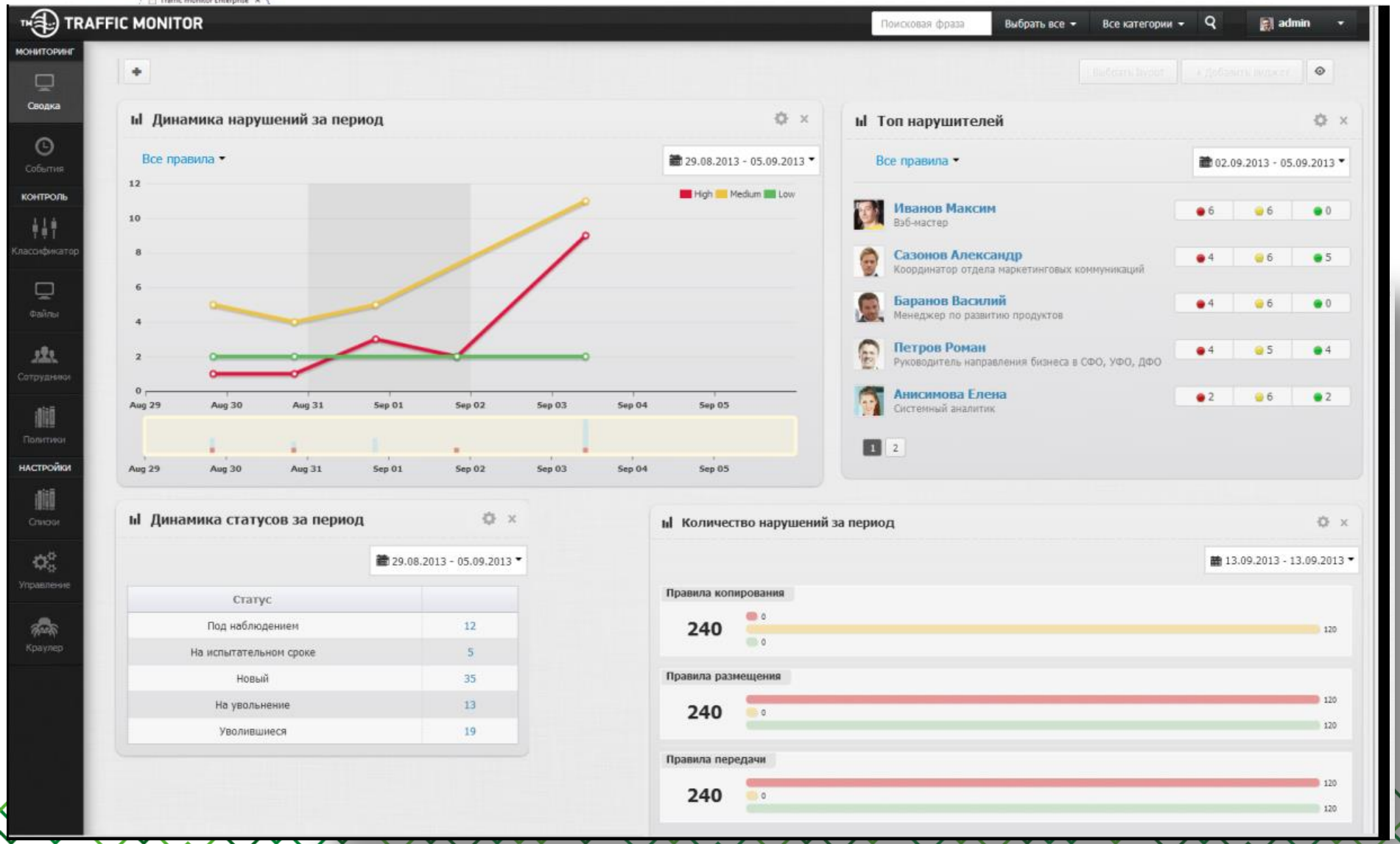
1. выявил сговор
2. предотвратил ущерб на **11 млн руб.**

InfoWatch Traffic Monitor Enterprise

- Лидер российского рынка
- Более 300 крупных клиентов
- 11 лет на рынке
- Широкая партнерская сеть
- Продажи в 16 странах мира

Web-интерфейс

INFOWATCH®



Устранение нелегитимного хранения данных – Crawlrer

- **Контроль расположения файлов на:**
  - сетевых хранилищах
  - SharePoint
  - рабочих станциях

Вовлечение бизнеса

Участие бизнес-подразделений в управлении безопасностью:

- Самостоятельное создание политик ИБ
- Чувствительность к изменениям бизнес-процессов
- Чувствительность к изменениям в документообороте
- Политики доступны всем и просты в создании


HR-служба


Юридический департамент


Топ-менеджмент


Отдел продаж


Финансовый отдел


IT-служба

Преимущества InfoWatch Traffic Monitor

- модульность и гибкая схема интеграции в IT-инфраструктуру
  - архитектура Решения позволяет гибко интегрироваться в существующую инфраструктуру организации
  - модульная архитектура Решения позволяет поэтапно расширять функциональность без необходимости переустановки системы
- **высокая производительность и отказоустойчивость**
  - **единственное Решение, которое рассчитано на крупные организации с большими объемами анализируемого трафика и территориально-распределенной структурой**
  - может работать на 1000 рабочих станций и выше (ограничения в производительности задаются только ИТ-инфраструктурой заказчика)
  - обладает встроенными средствами кластеризации и балансировки нагрузки

INFOWATCH®

InfoWatch KRIBRUM
как мы слушаем Интернет

Онлайн-сервис мониторинга и анализа социальных медиа

INFOWATCH®

Клиенты – в Интернете

62% **населения страны пользуется интернетом (Минкомсвязь России, 2015)**

90% **из них пользуются социальными медиа (TNS Web-Index, 2014)**

- Массовость – миллионы авторов
- Лавинообразное распространение
- Интерактивность
- Подверженность влиянию
- Слабая контролируемость

Формирование и проявление общественного мнения

- Пропаганда, обсуждения
- Информационные вбросы и атаки
- Отношение населения к явлениям, объектам, персонам

Угрозы безопасности и признаки правонарушений

- Экстремизм, наркотики
- Угрозы экономической и информационной безопасности
- Нарушения авторского права

INFOWATCH®

Факторы разрушения репутации

Отрицательные отзывы клиентов

- Клиенты чаще делятся негативом, чем положительным опытом – чем популярнее бренд, тем больше его ругают
- Люди доверяют отзывам и обзорам больше, чем рекламе и PR
- Отсутствие реакции на жалобу усугубляет неудовлетворенность

Информационные атаки и «черный» PR конкурентов

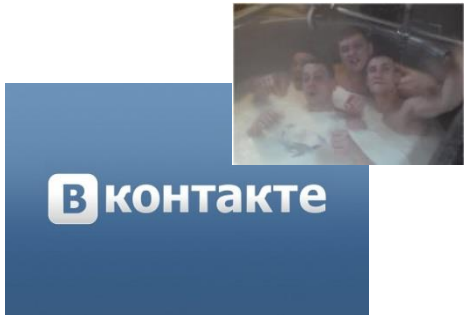
Неподобающее поведение сотрудников

- Разглашение конфиденциальной информации
- Жалобы на работу, коллег, начальника

INFOWATCH®

Факторы разрушения репутации

Сотрудники Омского сырного завода



Публикация фотографии неуважительного отношения к потребителям

Пострадала репутация всей отрасли, завод закрыли

ПОЧТА РОССИИ

«Почта России» - рекордсмен по количеству жалоб в 2013 год

Из всех жалоб на операторов связи 90% - на «Почту России»

Грозил штраф в 15 млн рублей*
Ухудшение репутации
Отток клиентов

Известия

INFOWATCH®

Использование сервиса

Облачный сервис с периодической оплатой (подписка)

Ценообразование строится на:

- количестве объектов мониторинга
- необходимости аналитических отчетов (работа экспертов)
- основе запросов дополнительных услуг

Нет ограничений по:

- количеству рабочих мест
- количеству ключевых слов поиска
- количеству собираемых упоминаний
- объему хранимых данных

INFOWATCH®

Для маркетинга и бизнес-подразделений

- Маркетинговые исследования
- Управление продуктом и сервисами
- Эффективность маркетинговых коммуникаций и PR
- Управление лояльностью
- Онлайн-поддержка
- Анализ качества работы с клиентами
- Конкурентный анализ

INFOWATCH®

KRIBRUM
для службы безопасности

- Детектирование появления в открытых источниках информации ограниченного доступа
- Оперативное выявление неправомерного/некорректного поведения сотрудников в Интернете
- Мониторинг информационных вбросов, «черного» PR
- Определение первоисточников
- Пики и динамика распространения
- Активные площадки и авторы

INFOWATCH®

KRIBRUM
для руководства

- Как клиенты воспринимают компанию в целом, ее отдельные продукты и уровень обслуживания
- Что делают конкуренты, как относятся к этому клиенты
- Что происходит в сфере PR, где и как обсуждаются другие VIP-персоны отрасли и т.д.
- Полная непредвзятая информация, не искаженная докладчиками
- Наглядная аналитика, в любое время доступная в интернет-браузере

Успешный кейс

Кейс: - крупный оператор связи

Цель: сохранение лояльности абонентов через развитие поддержки и коммуникаций с клиентами в соцмедиа

Собрано за 15 месяцев:

- более 2 300 000 сообщений, почти 1 000 000 оригинальных
- среди них 850 000 только по МТС, почти 350 000 оригинальных
- профили 803 000 авторов сообщений по телеком-тематике

Использование системы:

Несколько сотен ответов на отзывы и вопросы онлайн ежедневно

Результат:

Клиент удовлетворен качеством сбора и анализа данных.
InfoWatch KRIBRUM интегрирован с контакт-центром компании

Успешный кейс

INFOWATCH®

Кейс: XXXбанк

Цель: повышение удовлетворенности клиентов через изучение их потребностей и развитие коммуникаций в соцмедиа

Сбор информации о Сбербанке и основных конкурентах:

- 1500 - 2000 сообщений в день
- 50 000 - 60 000 в месяц

Использование системы:

- Исследование отзывов клиентов на различные темы:
  - удовлетворенность клиентским сервисом в офисах
  - потребности клиентов в регионах
  - пожелания к банковским продуктам и др.
- Прямые коммуникации с клиентами и поддержка онлайн

Результат: Развитие практик управления лояльностью
Вовлечение регионов
Интеграция с другими ИТ-системами

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Спасибо за внимание!

InfoWatch

www.infowatch.ru
+7 495 22 900 22

Сучкова Елена
Директор по работе со стратегическими клиентами