



# INFOWATCH

**Защита от внутренних угроз**

# 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

# Матрица «УГРОЗЫ=ПРОДУКТЫ»

## Внутренние - намеренные

- Саботаж
- Сговор
- Воровство
- Мошенничество
- Утечки информации
- Запуск негатива изнутри
- Клевета

## Внутренние - случайные

- Халатность
- Использование ресурсов в развлекательных целях
- Ошибки
- Некорректная работа информационных систем
- Компьютерные сбои

## Внешние - случайные

- Массовые вирусы
- Рекламный/AD-Фишинг
- Утечка информации через контрагентов
- Сбой работы провайдера

## Внешние намеренные

- DDoS-атаки
- Фишинг
- Социальная инженерия
- Таргетированные атаки
- Мошенничество



# InfoWatch Traffic Monitor

InfoWatch Traffic Monitor

## Решаемые задачи



*InfoWatch Traffic Monitor –  
автоматизированная система контроля  
информационных потоков организации  
для выявления утечек информации и  
других внутренних угроз*



Автоматическая классификация  
информационных потоков



Мониторинг и анализ данных

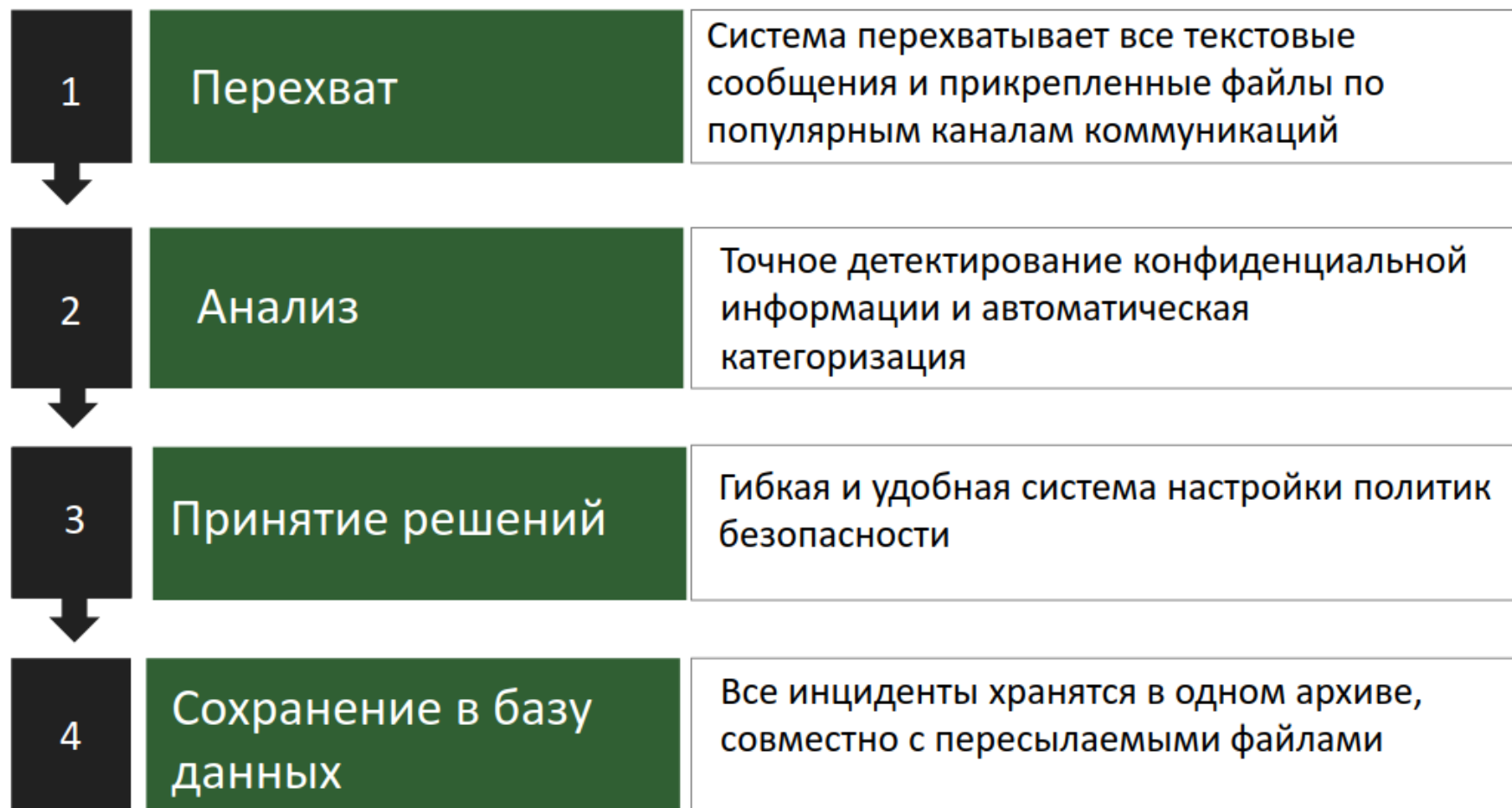


Предотвращение утечек  
конфиденциальных данных



Безопасное хранение данных для  
анализа и проведения  
расследований

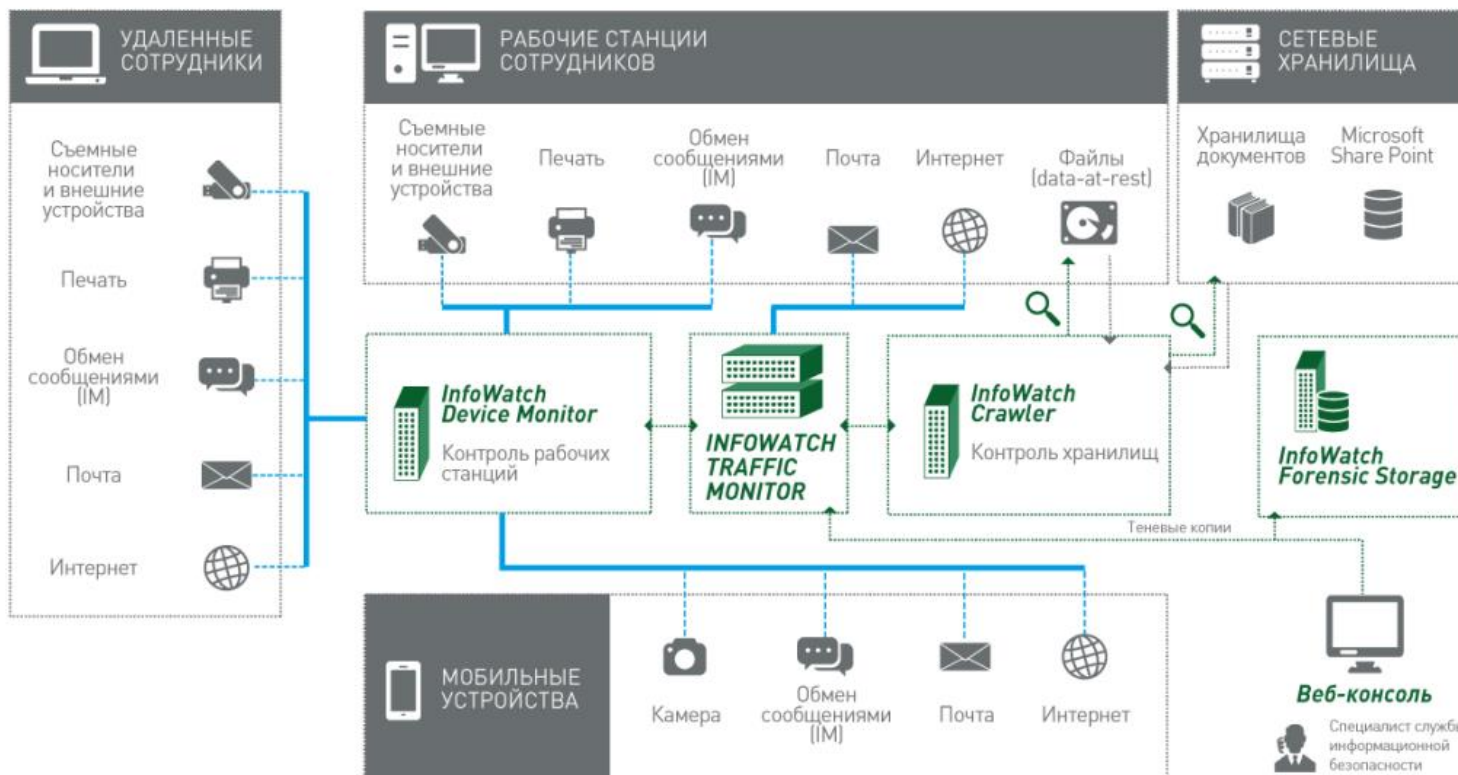
# Логика работы



# Схема работы модуля

InfoWatch Traffic Monitor

## Схема работы



# Контролируемые каналы

InfoWatch Traffic Monitor

**Контролируемые каналы: рабочие станции**



| РАБОЧИЕ СТАНЦИИ СОТРУДНИКОВ                                                                                                |                                                                                   |                                                                                                                                               |                                                                                                                     |                                                                                     |                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Съемные носители и внешние устройства                                                                                      | Печать                                                                            | Обмен сообщениями (IM)                                                                                                                        | Почта                                                                                                               | Интернет                                                                            | Файлы (data-at-rest)                                                                                                     |
|                                           |  |                                                              |                                  |  |                                       |
| <ul style="list-style-type: none"><li>• USB</li><li>• HDD</li><li>• FireWire</li><li>• Wi-Fi</li><li>• Bluetooth</li></ul> | <ul style="list-style-type: none"><li>• Локальные и сетевые принтеры</li></ul>    | <ul style="list-style-type: none"><li>• ICQ</li><li>• Skype</li><li>• Jabber</li><li>• Yahoo</li><li>• Lync</li><li>• Mail.ru Agent</li></ul> | <ul style="list-style-type: none"><li>• SMTP</li><li>• IMAP4</li><li>• POP3</li><li>• MAPI</li><li>• NRPC</li></ul> | <ul style="list-style-type: none"><li>• HTTP(s)</li><li>• FTP(s)</li></ul>          | <ul style="list-style-type: none"><li>• Сетевые хранилища</li><li>• Диски рабочих станций</li><li>• Sharepoint</li></ul> |

# InfoWatch Person Monitor

InfoWatch Person Monitor

## Возможности InfoWatch Person Monitor



Наблюдение за сотрудниками  
под подозрением в режиме  
реального времени

Анализ производительности  
сотрудников и всесторонняя  
визуализация результатов

Анализ аномального поведения  
персонала

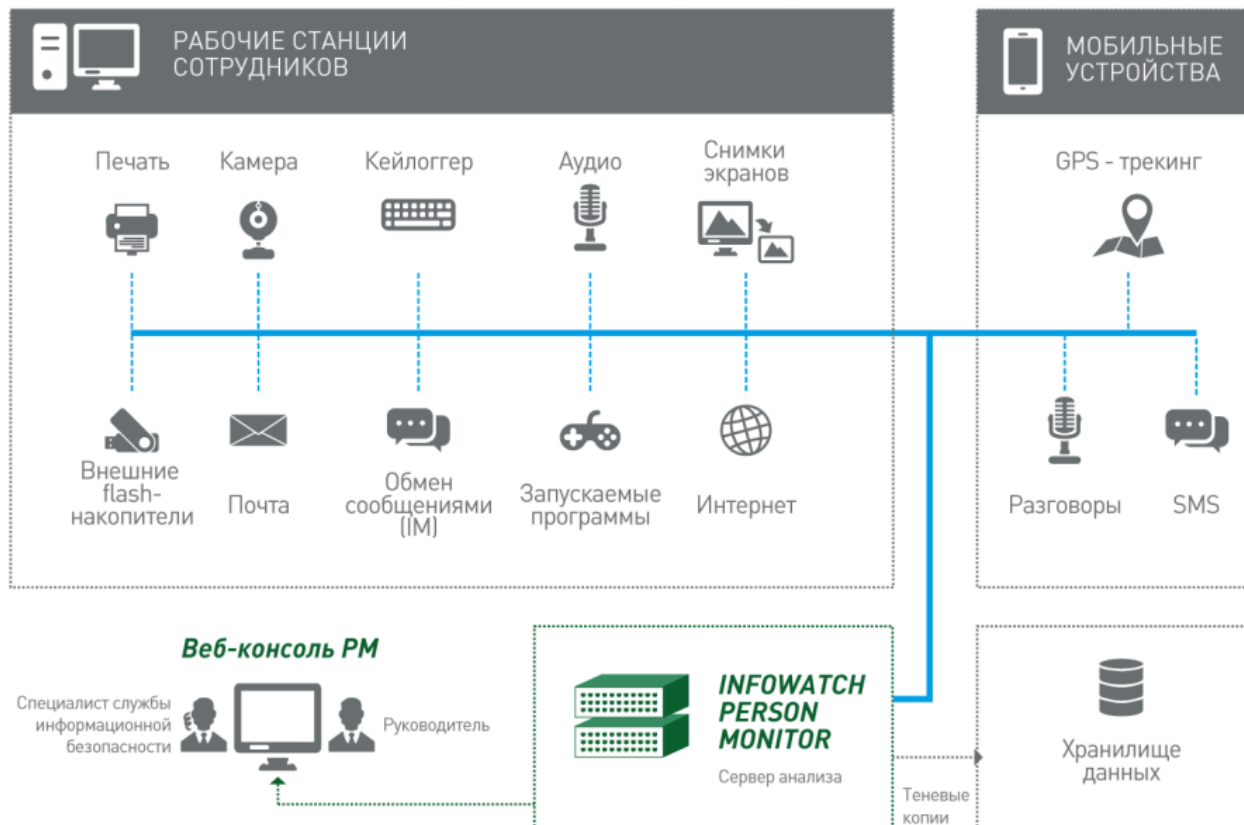
Расследование инцидентов и  
нарушений по «горячим следам»

Контроль мобильных  
сотрудников

# Схема работы модуля

InfoWatch Person Monitor

## Схема работы модуля



# Анализ поведения

InfoWatch Person Monitor

## Анализ аномального (нетипичного) поведения персонала



| **Клавиатурный почерк** – определение состояния сотрудника за рабочим местом

| **Операции с данными** (копирование, удаление, отправка) в браузерах, почтовых клиентах, мессенджерах и на внешних носителях

| **Контроль поисковых запросов** (Google, Yandex и т.д.)

| **Контроль буфера обмена**

| **Мониторинг посещаемых сайтов** (экстремизм, терроризм, наркотики, продажа оружия и прочее социально-опасное поведение)

| **Контроль количества копий установленного ПО, контроль изменений** в составе оборудования и ПО

# Анализ производительности

InfoWatch Person Monitor

## Анализатор производительности персонала



**Мониторинг сайтов:** активность сотрудника в сети Интернет за день, месяц и т.д.

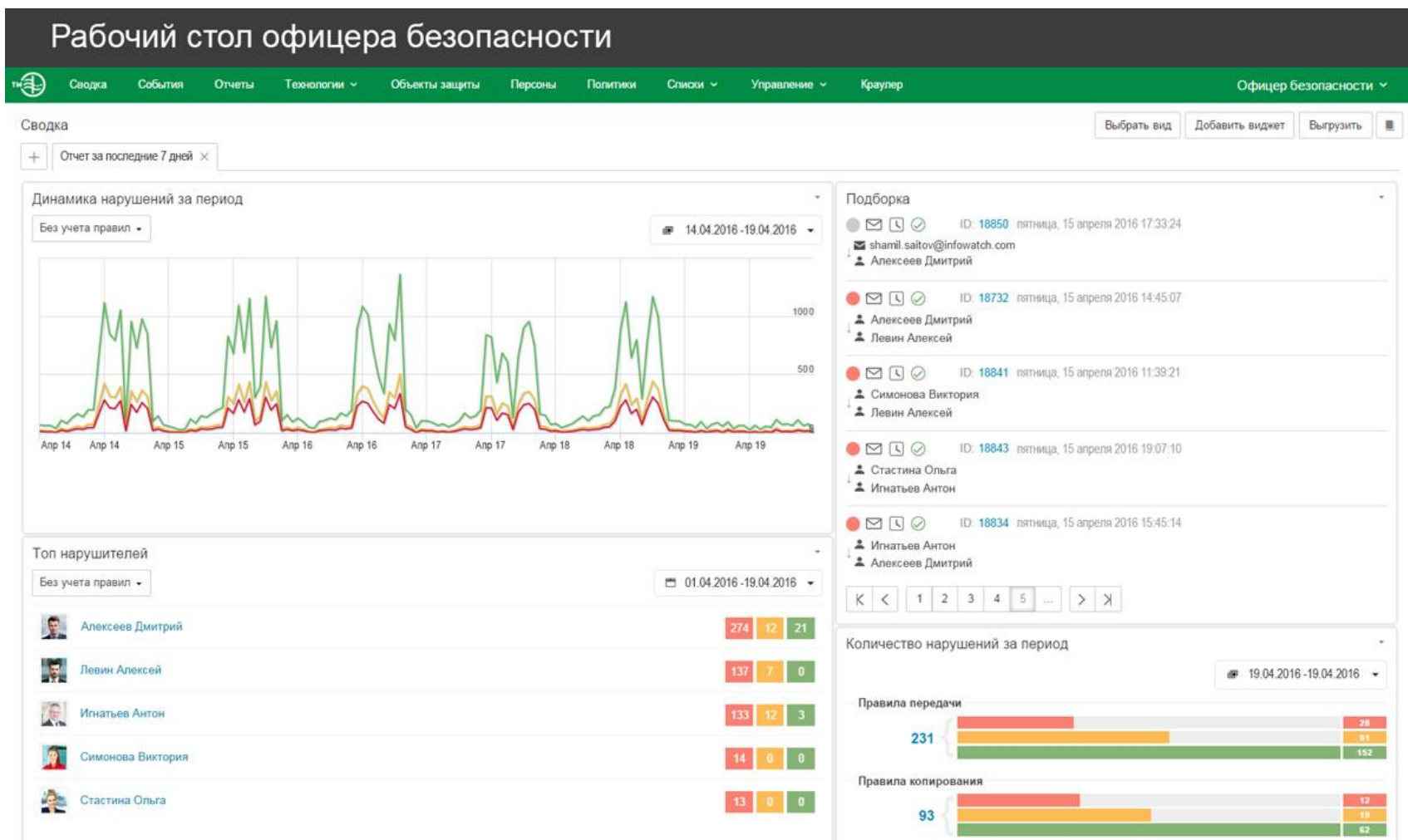
**Запускаемые программы:** какими программами и сколько времени пользовался сотрудник .

**Прогулы, опоздания на работу**

**Log in / Log off**

**Машинное время:** сколько времени был включен компьютер сотрудника

# Скриншот программы 1



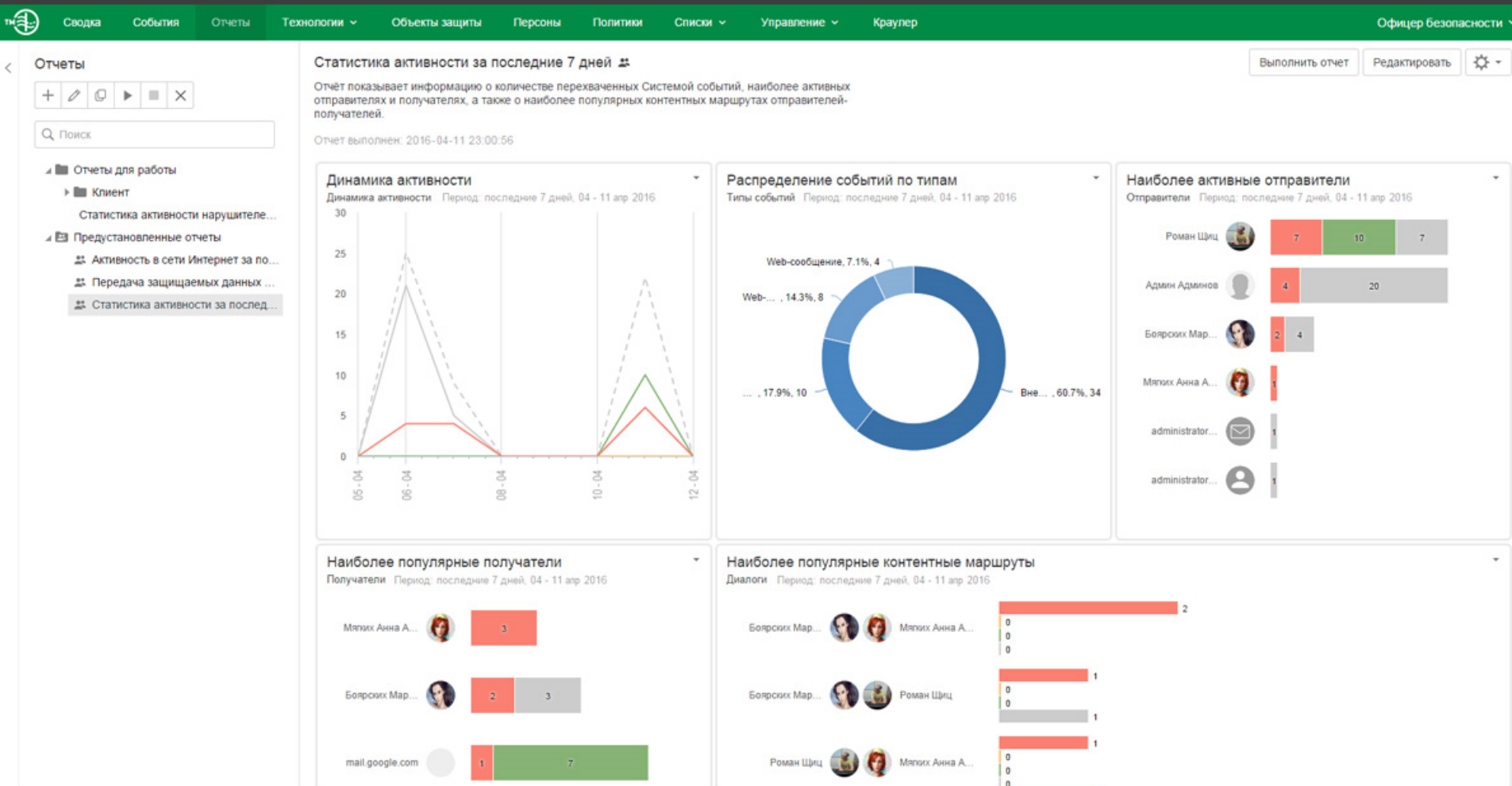
## Скриншот программы 2

The screenshot displays the QuadroSoft application interface. The top navigation bar is green and contains the following items: a logo, 'Сводка', 'События', 'Отчёты', 'Технологии', 'Объекты защиты', 'Ещё', and 'Username'. The main content area is divided into two panels. The left panel, titled 'Запросы', contains a search bar and a list of filters: 'События всех отделов', 'Печать отдела продаж', 'Нарушения за прошедший час', 'Необработанные нарушения', 'Запросы по областному фил...', 'Новая папка', 'Нарушение политик' (highlighted), 'Перехват ОЗ', 'Сливы', 'Фоточки в инстаграм', 'Запросы по Тверскому филла...', 'Перехват буфера обме...', and 'Выход больших файлов за...'. The right panel, titled 'Нарушение политик', displays a table of violations with columns for 'Отправители', 'Получатели', 'Политики', and 'Дата пер...'. The table contains 8 rows of data, each with a set of status icons on the left.

| Отправители          | Получатели        | Политики               | Дата пер...  |
|----------------------|-------------------|------------------------|--------------|
| Konstantin Konsta... | Ivan Konstantinov | Персональные данные    | 11.07.201... |
| Ivan Konstantinop... | Konstantin Petrov | Персональные данные    | 11.07.201... |
| username             | username_4 Ko...  | Обсуждение НИОКР вн... | 11.07.201... |
| Konstantin Konsta... | Ivan Konstantinov | Персональные данные    | 11.07.201... |
| Ivan Konstantinon... | Konstantin Petrov | Персональные данные    | 11.07.201... |
| Konstantin Konsta... | Ivan Konstantinov | Финансы                | 11.07.201... |
| Konstantin Konsta... | Ivan Konstantinov | Флуд                   | 11.07.201... |
| Konstantin Konsta... | Konstantin Konstv | Флуд                   | 11.07.201... |

# Скриншот программы 3

## Отчеты



# С чего начать?



## Задачи:

- Выполнение требований законодательства
- Поймать злодея, закрыть «дыру»
- Минимальное влияние на ИТ-инфраструктуру
- Качественный результат – отчет

## С чего можно начать?

- Пилотный проект
- Референсный визит
- Демонстрация
- Демонстрация



# Контакты



+375 (17) 241 77 66



info@quadrosoft.by



www.quadrosoft.by