

# Практический опыт и этапы развёртывания DLP системы Infowatch

Квитко Виталий  
Инженер сервисной группы  
[vkvitko@polikom.ru](mailto:vkvitko@polikom.ru)

- 1. Подготовительный**
- 2. Внедрение**
- 3. Тестирование**
- 4. Подведение Итогов**

# Подготовительный этап

1. Заполнение опросного листа
2. Подписание юридических договоров
3. Согласование старта и времени проведения пилота
4. Определение мощностей для развёртывания
5. Продолжительность этапа от 2х до 5 дней



# Этап внедрения

1. Подготовка серверов
2. Развёртывание систем
3. Интеграция в инфраструктуру заказчика
4. Распространение клиентов на рабочие станции
5. Продолжительность этапа от 1 до 3х дней



# Тестирование

1. Проверка корректности работы системы
2. Инструктаж по работе с системой
3. Ответы на возникающие вопросы
4. Тестирование самого продукта
5. Продолжительность этапа от 3х до 8 недель



# Подведение Итогов

1. Подведение итогов
2. Привлечение аналитика из компании InfoWatch для составления отчёта (при необходимости)
3. Вывод всех систем из инфраструктуры заказчика
4. Продолжительность этапа от 3х до 8 недель



# Аппаратные и программные требования

## Traffic Monitor

- от 16 CPU
- от 16Гб (норм 32Гб)
- HDD от 700 Gb
- 2 LAN
- без операционной системы

## Device Monitor

- от 2 CPU
- от 4Гб RAM
- HDD от 200Гб
- Windows Server 2008 R2 (или выше)
- включить в домен
- MS SQL Express 2008 (или выше)
- Рабочие станции Windows XP SP3 или выше

## Endpoint Security

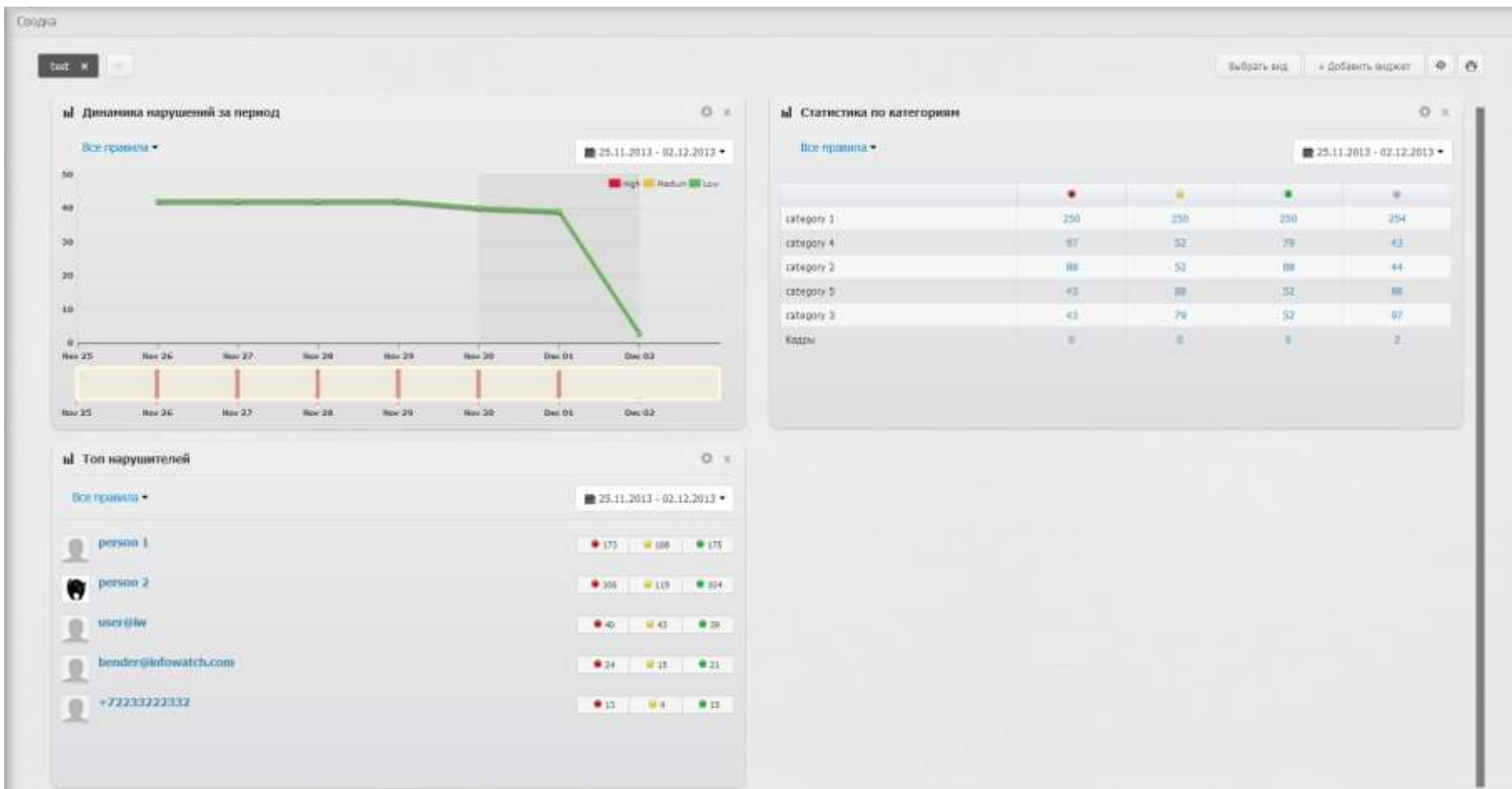
- от 2 CPU
- от 6Гб RAM
- HDD от 200Гб
- Windows Server 2008 R2 (или выше)
- включить в домен
- MS SQL Express 2008 (или выше)
- Рабочие станции Windows XP SP3 или выше

# Интерфейс Traffic Monitor





# Интерфейс Traffic Monitor



# Интерфейс Device Monitor

The screenshot shows the 'Infowatch Device Monitor Management Console' interface. The window title is 'infowatch Device Monitor Management Console - superuser@localhost - Панель меню'. The interface is divided into several sections:

- Панель навигации (Navigation Panel):** Located on the left side, it contains a 'Политики' (Policies) section with a tree view showing 'Политика на устройства (0)' and 'Политика теневого копирования'. Below this are sections for 'Группы сотрудников', 'Группы рабочих станций', 'Белые списки', 'Категории сигнатур', 'Приложения', 'Журнал', 'Задачи', and 'События'.
- Панель меню (Main Menu):** Located at the top, it includes 'Главное меню' (Main Menu) and 'Панель правила' (Policy Panel).
- Панель правила (Policy Panel):** A table listing various security rules and their actions. The table has columns for 'Наименование' (Name), 'Операция' (Operation), and 'Период дейст...' (Action Period).
- Панель Подробно (Detailed Panel):** Located below the main table, it provides a detailed view of a selected rule, showing its 'Наименование', 'Политика', 'Перехватчик', 'Операция', 'Период действия', 'Исключить из перловата', and 'Использовать маску файла'.
- Панель Изменения (Changes Panel):** A section for managing rule changes, currently empty.
- Панель Статуса (Status Panel):** A section for monitoring the status of the system, showing a 'Журнал консоли' (Console Log) with timestamps and messages.

Наименование	Операция	Период дейст...
Теневое копирование документов	Копирование в файл на съемном устройстве	всегда
Теневое копирование печати	Копирование в файл на съемном устройстве	всегда
Контроль МФР	МФР: Использование разрешено	всегда
Контроль МФУ	МФУ: Использование разрешено	всегда
Контроль Skype	Skype: Использование разрешено	всегда
Контроль FTP	FTP: Использование разрешено	всегда
Контроль почты	Mail: Разрешить отправку и получение почты	всегда
Контроль HTTPS	HTTPS: Использование разрешено	всегда

Правило	Наименование	Политика	Перехватчик	Операция	Период действия	Исключить из перловата	Использовать маску файла
Теневое копирование документов	Политика теневого копирования	File Monitor	Копирование в файл на съемном устройстве	всегда	Нет	Нет	*

Журнал консоли

- 12:31:44 Приложение запущено.
- 12:31:54 Подключение к серверу «localhost»...
- 12:31:58 Соединение с сервером «localhost» успешно установлено.
- 12:31:58 Произошло событие.

# Интерфейс Endpoint Protection

Управление правами » Контроль

Структура службы каталогов

Поиск:

Перейти к синхронизации

Политики по умолчанию

Избранное

Имя	КД	АУ	ШУ	ШП	КП	УП	Администр...	E-Mail	Соглашени...	Комментарии
Administrator	✓	✓	✓	✓	✓	✓	Пользователь	Administrator@iwtest.local		
Claudia Smith	✓	✓	✓	✓	✓	✓	Пользователь	csmith@iwtest.local		
DiscoverySearchMailbox (D9198A05-46A6-415F-80AD-7E093346B852)	✓	✓	✓	✓	✓	✓	Пользователь	DiscoverySearchMailbox (D9198A...		
FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042	✓	✓	✓	✓	✓	✓	Пользователь	FederatedEmail.4c1f4d8b-8179-4...		

Контроль | Аудит | Фильтры | Шифрование | Контроль приложений | Green IT | Безопасное удаление

Устройства и порты | Облачные хранилища | Настройки пользователя | Мобильные устройства | Журнал

Сохранить | ⚠ Запретить все | Устройства | Порты | Профиль: Online | Сводная информация

Тип устройства	Права доступа	Расписание	Временный доступ	Наследование
<b>Накопители</b>				
CD / DVD	нет доступа			
Floppy Disk	полный доступ			
Внешние накопители	только чтение			
Несъемные диски	полный доступ			
Сетевые каталоги	полный доступ			
Терминальные диски	по расписанию			
<b>Устройства</b>				
Звуковые, видео и игров...	полный доступ			
Локальные принтеры	полный доступ			

# Выполненные пилотные проекты за 2015 год

1. Строительная компания (более 1000 клиентов)
2. Судостроительный завод (более 300 клиентов)
3. Представительские услуги, ГУП (более 200 клиентов)
4. Пассажирские перевозки, ГУП (более 2000 клиентов)
5. Естественный монополист, ГУП
6. Один из крупных банков Санкт-Петербурга (более 200 клиентов)
7. Научно-производственная компания (радиоэлектроника) (более 600 клиентов)

# Спасибо за внимание!

**Виталий Квитко**

тел: + 7 (812) 325 84 00

e-mail: [vkvitko@polikom.ru](mailto:vkvitko@polikom.ru)

**ПОЛИКОМ ПРФ**

*Просто работаем*