DLP как процесс.
Почему нет эффекта от средств контроля утечек информации и как изменить ситуацию?

Артём Пахомов

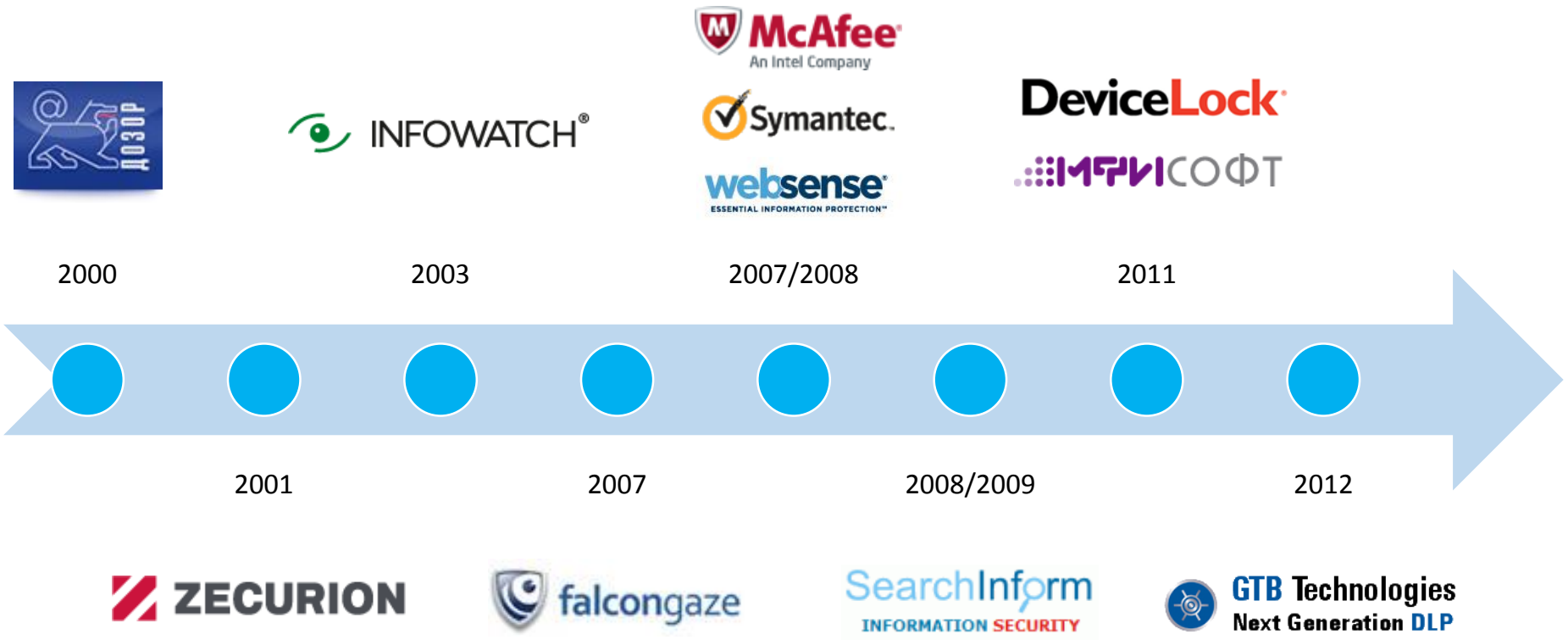
Архитектор по информационной безопасности

ЗАО НИП «Информзащита»

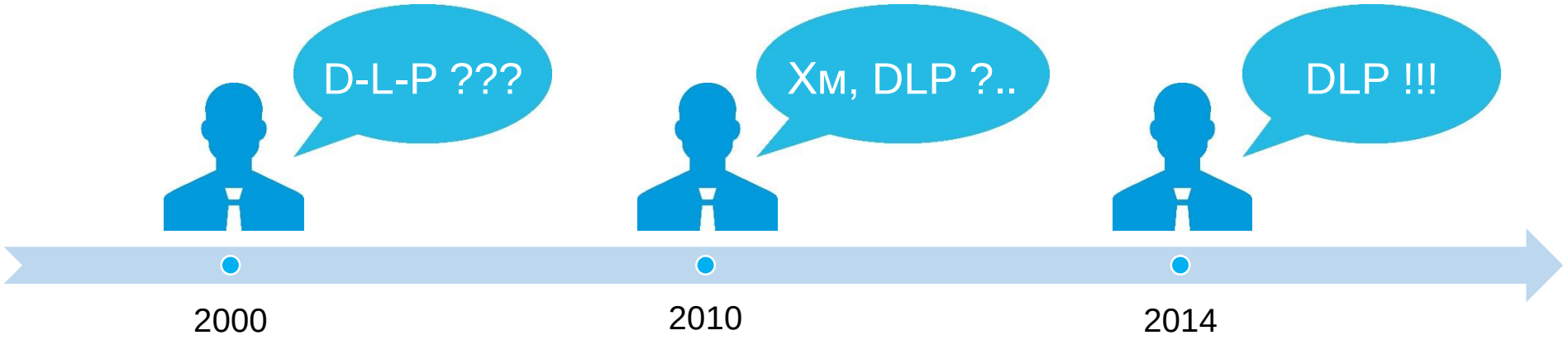
infosecurity RUSSIA
24-26 СЕНТЯБРЯ 2014
Крокус Экспо, Москва

Информзащита
Системный интегратор

Российский рынок DLP-систем

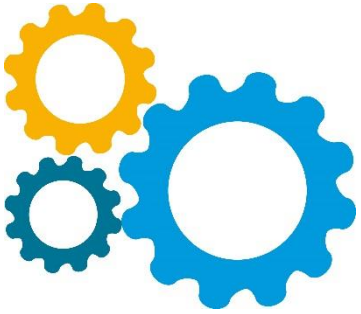


DLP – это…



Инструмент

Процесс



DLP как процесс

1. Классическое внедрение DLP-решения
   - Реализация проекта
   - Результаты внедрения
2. DLP как процесс
   - Что упускается в классической схеме?
   - Жизненный цикл инцидентов
   - Жизненный цикл политик
   - Коммуникации с персоналом
   - Показатели эффективности

1. Классическое внедрение DLP-решения

- Реализация проекта
  - Результаты

Обследование

Выясняются технические детали

- Текущая инфраструктура
- Возможности интеграции со сторонними решениями
- …

Уточняются ожидания

- Типа трафика
- Форматы документов
- Объекты детектирования
- …

Формируется детальное техническое задание на систему

Выполняется сбор и анализ документов, подлежащих защите

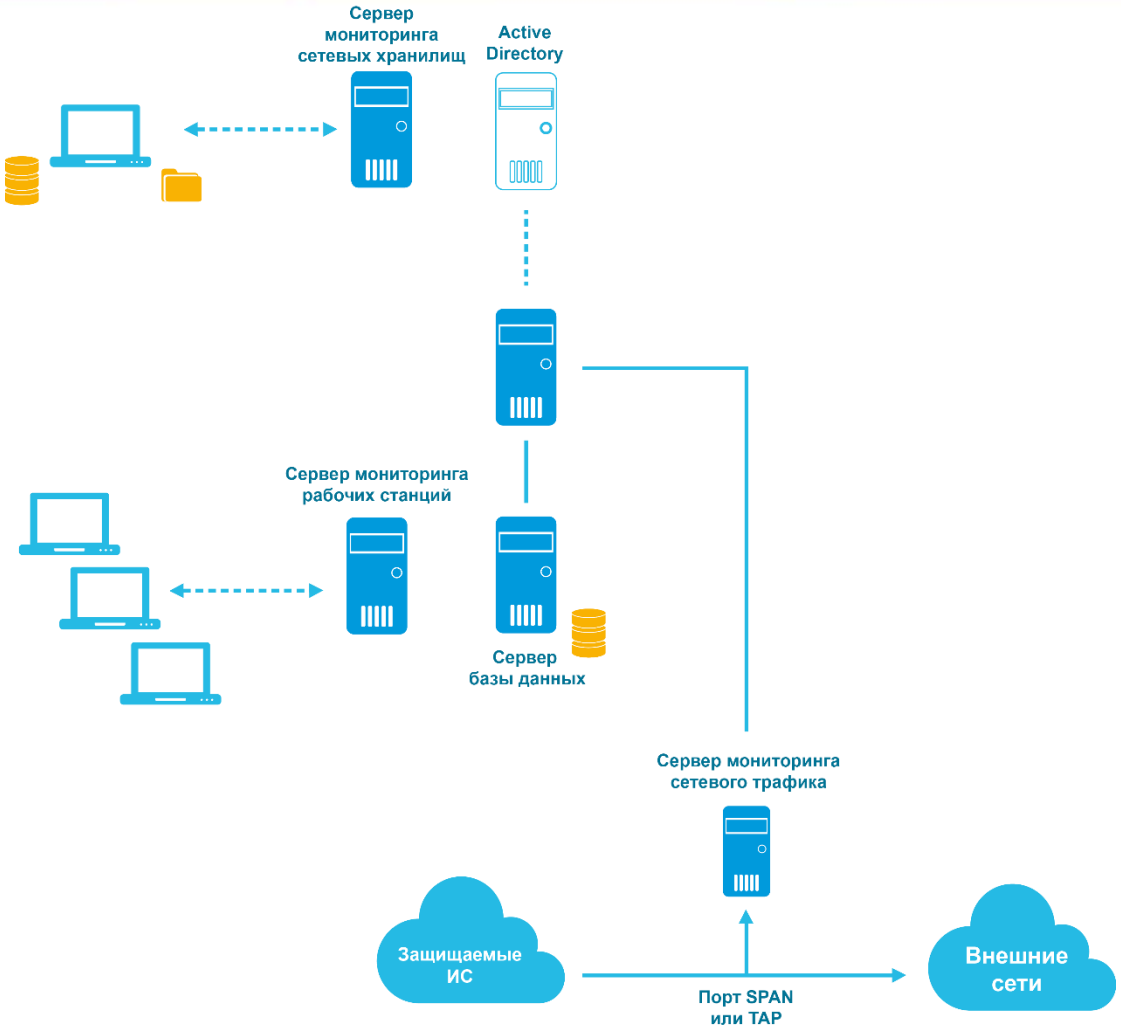
Проектирование

Документы технического проекта

- Пояснительная записка
- Схема структурная комплекса технических средств
- Спецификация
- Программа и методика испытаний
- …

Эксплуатационная документация

- Руководство администратора
- Руководство офицера безопасности
- …



Информзащита
Системный интегратор

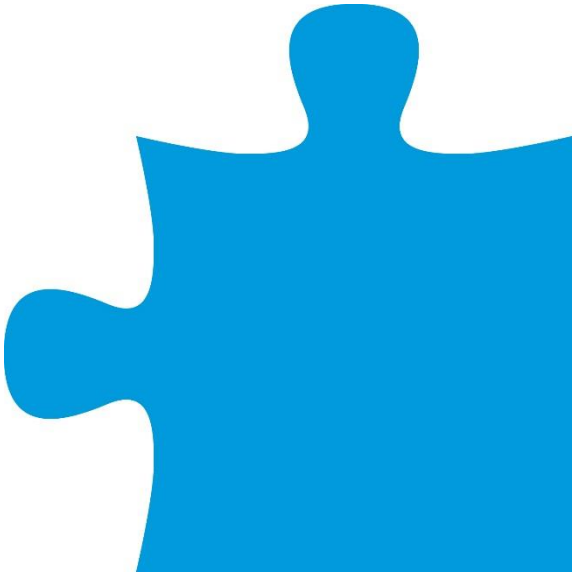
Внедрение

Установка и настройка решения

- Контроль перемещения КИ по сетевым каналам
- Контроль перемещения КИ посредством внешней почтовой переписки
- Контроль над КИ, обрабатываемой на рабочих станциях пользователей
- …

Опытная эксплуатация

- Устранение обнаруженных недостатков
- Приемочные испытания



1. Классическое внедрение DLP-решения

- ✓ Реализация проекта
- ➢ Результаты

Результаты внедрения

DLP как инструмент

- Продукт
- Политики обнаруже-ния КИ
- Документа-ция

Специализированные политики

Наработки интегратора

Стандартный набор вендора

Политики обнаружения КИ

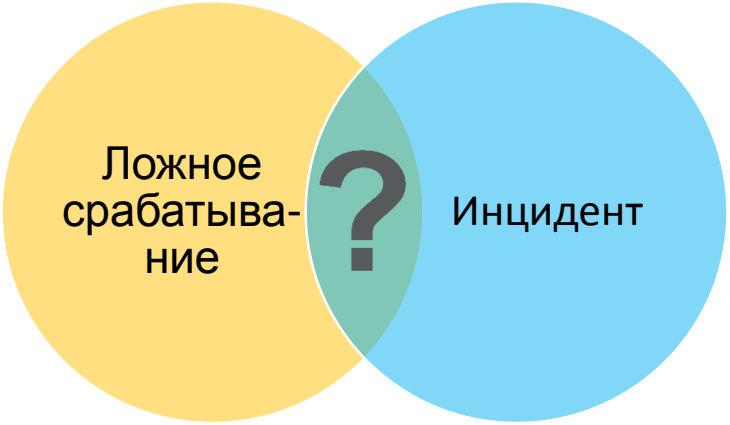
Система внедрена.
Политики актуальны.

Эксплуатация системы

Актуальны ли политики?

Обработка событий

1. Не все события могут быть проанализированы без привлечения владельцев информации



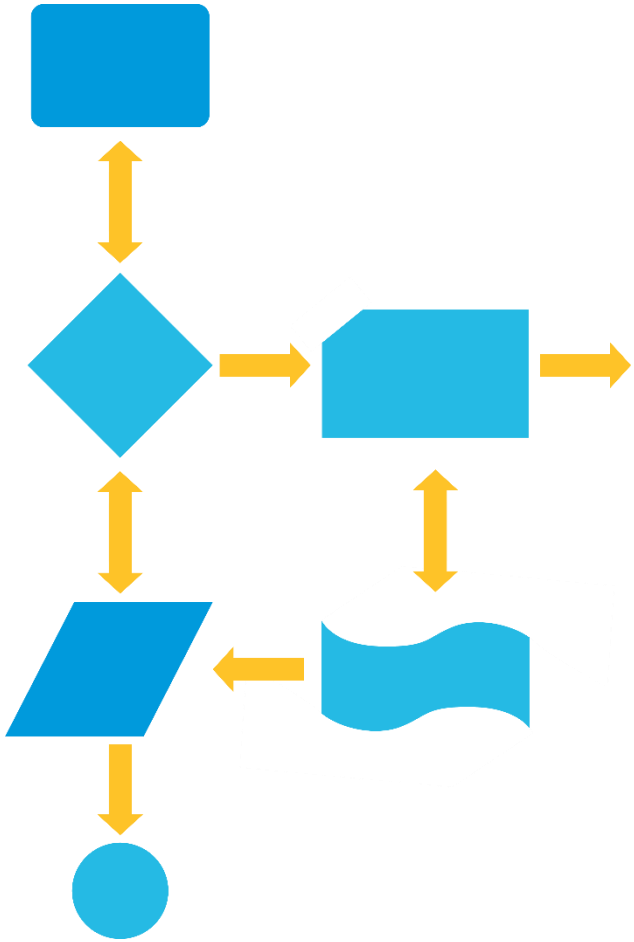
2. Основная часть событий – регулярно повторяющиеся однотипные инциденты

2. DLP как процесс

Что упускается в классической схеме?

Процессный подход = внедрение технологии +

- Жизненный цикл инцидентов
- Жизненный цикл политик
- Коммуникации с персоналом
- Показатели эффективности



Жизненный цикл инцидентов

Как обрабатывать инциденты?

- Стандартизация процесса реагирования на инциденты
- Разработка матрицы статусов инцидентов
- Определение времени реагирования
- Принятие политики архивирования инцидентов

Жизненный цикл политик

Как поддерживать политики в актуальном состоянии?

- Определение владельца для каждой политики
- Установка регулярных встреч с владельцами политик
- Документирование политик
- Ведение сводной информации по всем политикам

Коммуникации с персоналом

Как уменьшить количество типичных инцидентов?

- Уведомления о нарушении политики обработки КИ
- Обучение сотрудников

Показатели эффективности

Как оценить эффективность системы?

- Показатели снижения риска утечки информации
- Оперативные показатели

Вопросы презентации

Информзащита
Системный интегратор

Почему нет эффекта от средств контроля утечек информации?

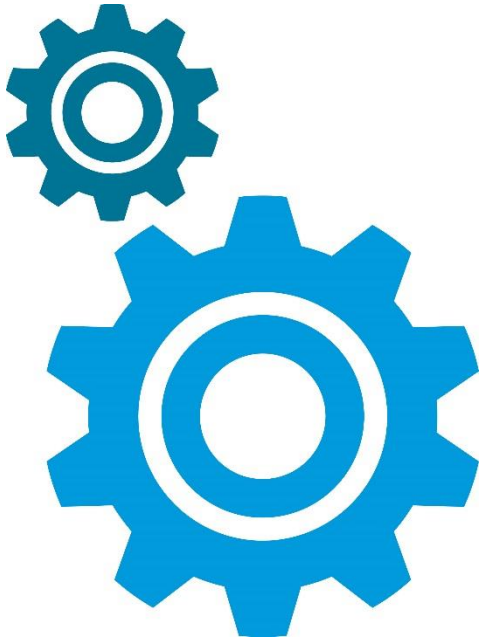
✓ Внедрена DLP-система, выполняющая набор требуемых функций

× Отсутствует выстроенный процесс предотвращения утечек информации

Как изменить ситуацию?

Разработать и ввести в действие процесс предотвращения утечек информации на базе использования имеющегося инструмента

Ориентироваться на разработку процесса при внедрении DLP



Спасибо за внимание!

Артём Пахомов
a.pakhomov@infosec.ru

Информзащита
Системный интегратор