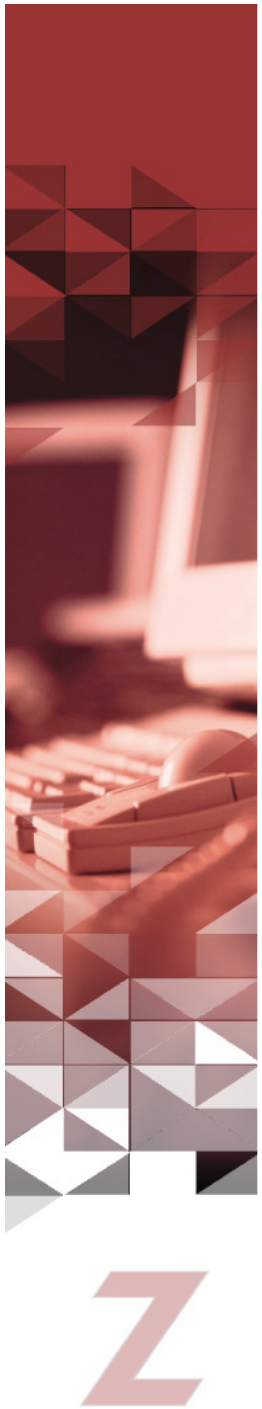
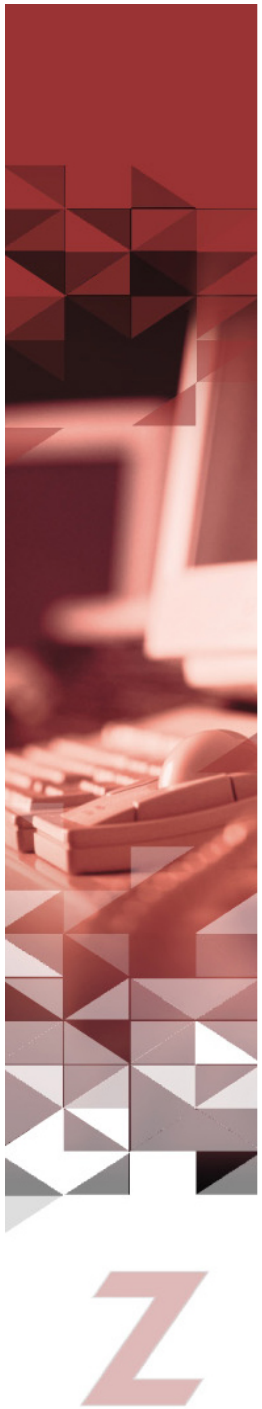


SECURIT

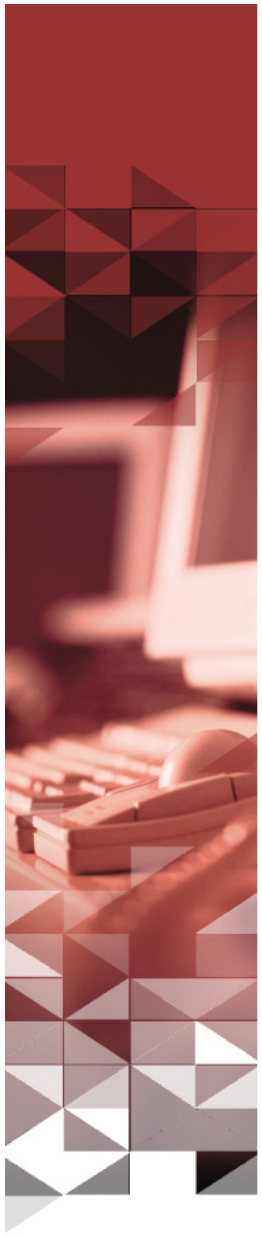
Практика выбора IPC для защиты от внутренних угроз

Александр Белявский
Компания SecurIT



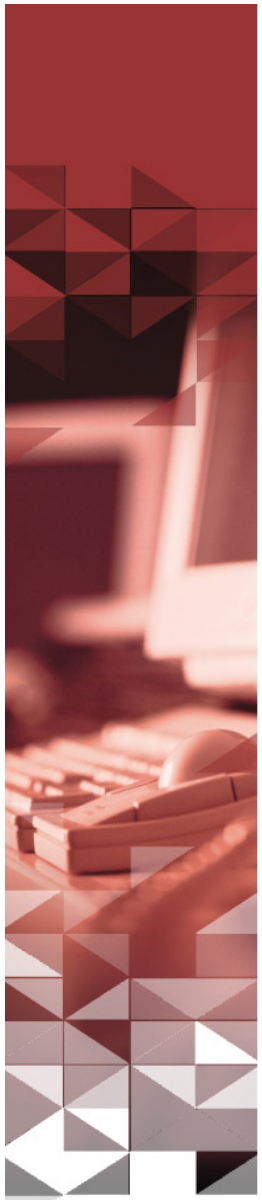
Почему внутренние угрозы?

- Хакеры являются причиной только 1% утечек данных
- Инсайдеры находятся на 1 месте по количеству инцидентов
- 79% IT-директоров сообщили хотя бы об одном инциденте за последний год
- Изнутри сети получить доступ к конфиденциальной информации гораздо проще
- Open Security Foundation: только за первое полугодие 2009 года в мире произошло 250 утечек



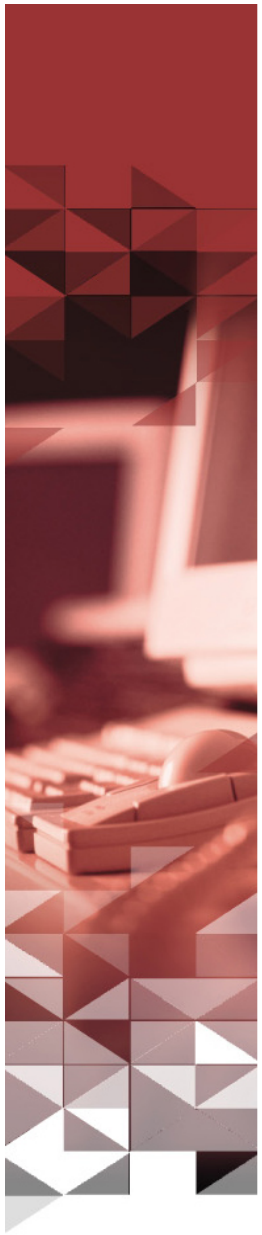
Почему внутренние угрозы?

- 152-ФЗ «О защите персональных данных»
- 781-ое постановление Правительства РФ
- Гражданская ответственность
- Административная ответственность (ст. 13.11 КоАП РФ)
- Уголовная ответственность (ст. 137 УК РФ – злоупотребления и незаконные действия с данными о частной жизни)



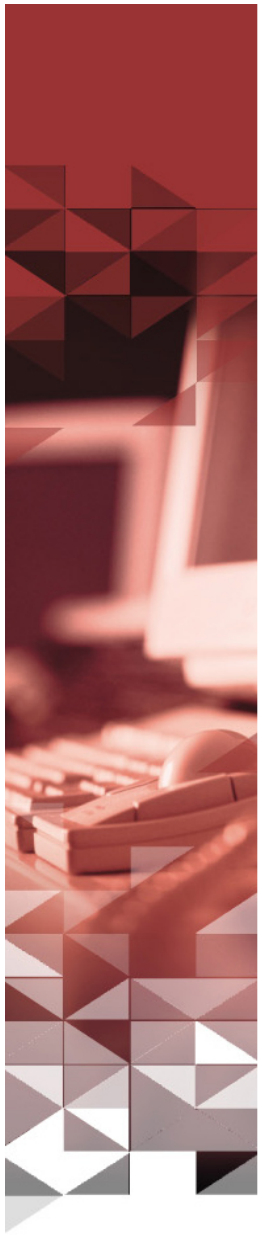
DLP: традиционный подход

- Контроль наиболее очевидных каналов утечки:
  - Периферийные устройства (USB-диски и т.д.)
  - Принтеры
  - Электронная почта
  - Веб-трафик и IM
  - Социальные сети
- Контентный анализ
- Архивирование для обеспечения возможности расследования инцидентов



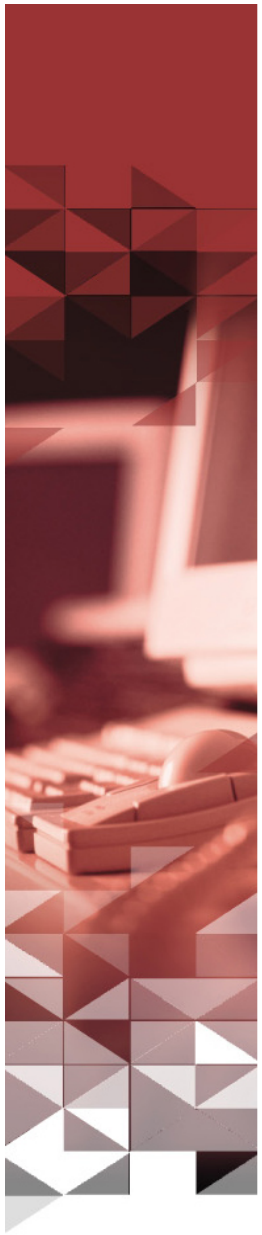
DLP != защита от внутренних угроз

- Физический доступ к носителям
  - Магнитные ленты
  - Жесткие диски и хранилища
  - Ноутбуки
- Аутентификация и идентификация



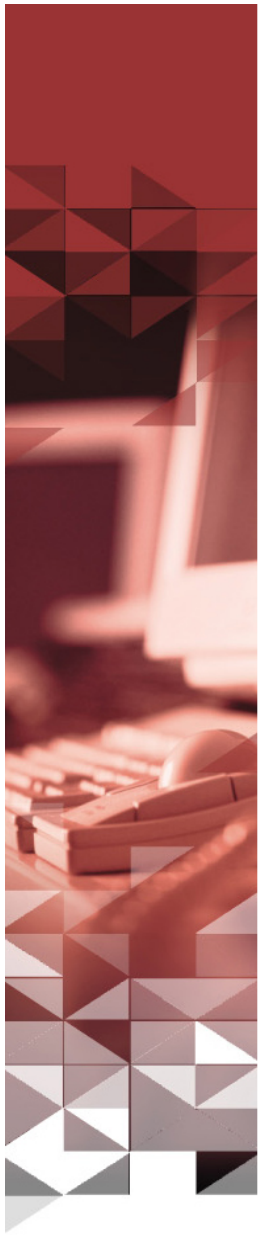
Ключевые аспекты выбора IPC

- Существенные отличия решений по возможностям
- Финансовая целесообразность
- Трудоемкость внедрения
- Архитектура IPC-решений
- Известность производителя
- Наличие сертификата



Возможности IPC

- Перечень контролируемых каналов передачи информации
- Архивирование всех входящих и исходящих данных
- Шифрование данных при хранении и обработке
- Система менеджмента и отчетности
- Проблема блокировки рабочих станций
- Детектирование конфиденциальной информации



Технологии детектирования утечек

- ✓ Метод сигнатур
- ✓ Регулярные выражения

- ❖ Цифровые отпечатки
- ❖ Технология меток
- ❖ Лингвистика анализ с использованием морфологии и стемминга
- ❖ Метод Байеса

Реальное детектирование или “гомеопатия”?

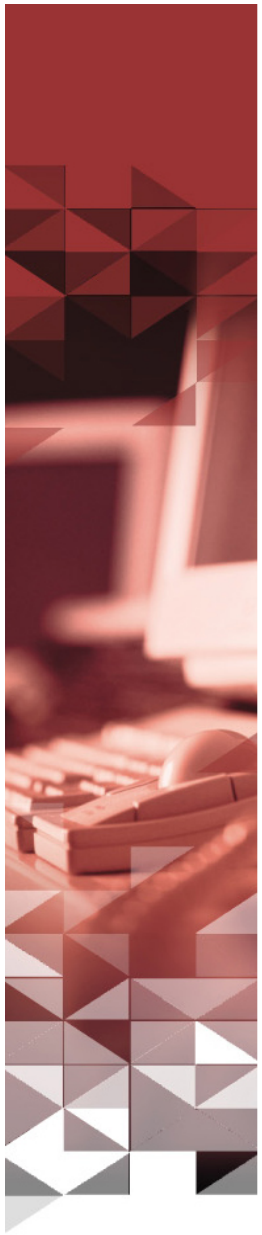
Вопрос 1: **Каков механизм работы технологии детектирования?**

Вопрос 2: **Можно ли каким-либо образом оценить или проверить результат работы технологии детектирования?**

Миф или реальная технология???

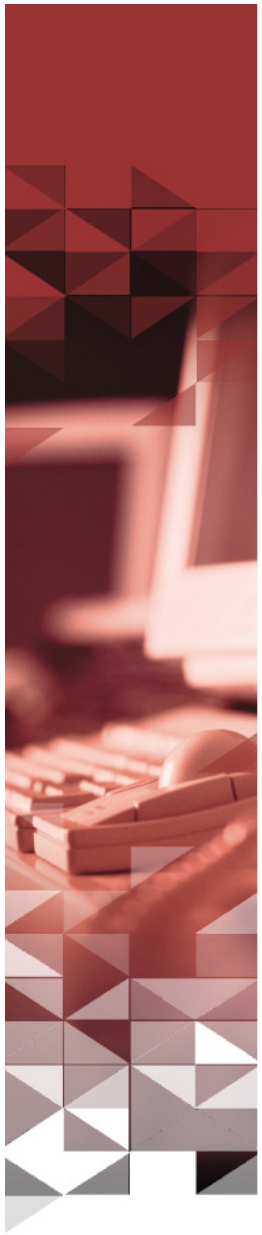
Гибридный анализ:

- **Детектор на базе регулярных выражений**
- **Защита статистических данных на базе цифровых отпечатков**
- **Защиты новых и динамических данных на базе контекстного и контентного**



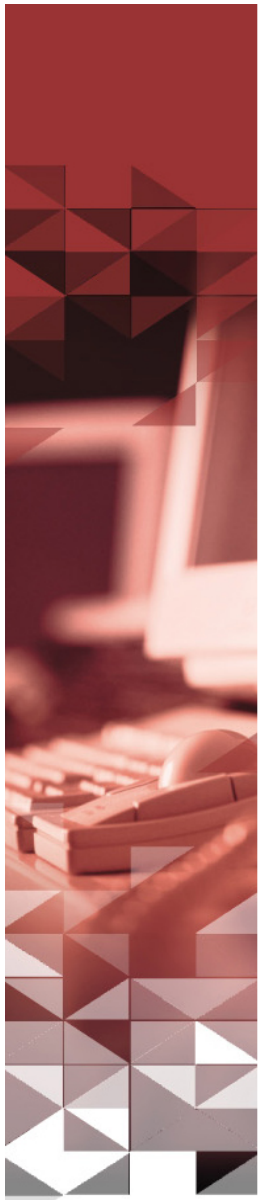
Этапы взаимодействия с подрядчиками

- Оценка заявленных возможностей и способов их реализации
- Написание политик внутреннего контроля
- Реализация «пилотного» проекта
- Полноценное внедрение
- Дальнейшее сопровождение



IPC: прогнозы

- Исследование IDC:
- По мнению 81% опрошенных, IPC – это важная часть в общей стратегии ИБ
- 64% респондентов собираются внедрять новые IPC технологии
- Рынок средств IPC будет расти на 33% в год и в 2011 достигнет суммы в $3 млрд.



Линейка IPC продуктов

- Zserver Suite – защита магнитных лент, жестких дисков и хранилищ
- Zdisk – защита данных на ноутбуках
- Zlock – контроль внешних устройств и принтеров
- Zgate – контроль электронной почты и интернет-трафика
- Zlogin – защищенный вход в сеть с использованием электронных ключей и смарткарт
- Централизованное управление из единой консоли

Вопросы

http://www.securit.ru