ИНФОСИСТЕМЫ ДЖЕТ

# Эффективны ли современные бюджеты на ИБ? За 80% денег только 20% безопасности?

Ляпунов Игорь
Директор Центра информационной безопасности

28 сентября 2010 г.

# О чем речь

- **Пять вопросов про ЭТО:**
  - А есть ли безопасность?
  - Кто виноват?!
  - На что мы тратим наши бюджеты?
  - Как перестать быть слепыми?
  - Кто? Как? Куда?

# А есть ли безопасность?

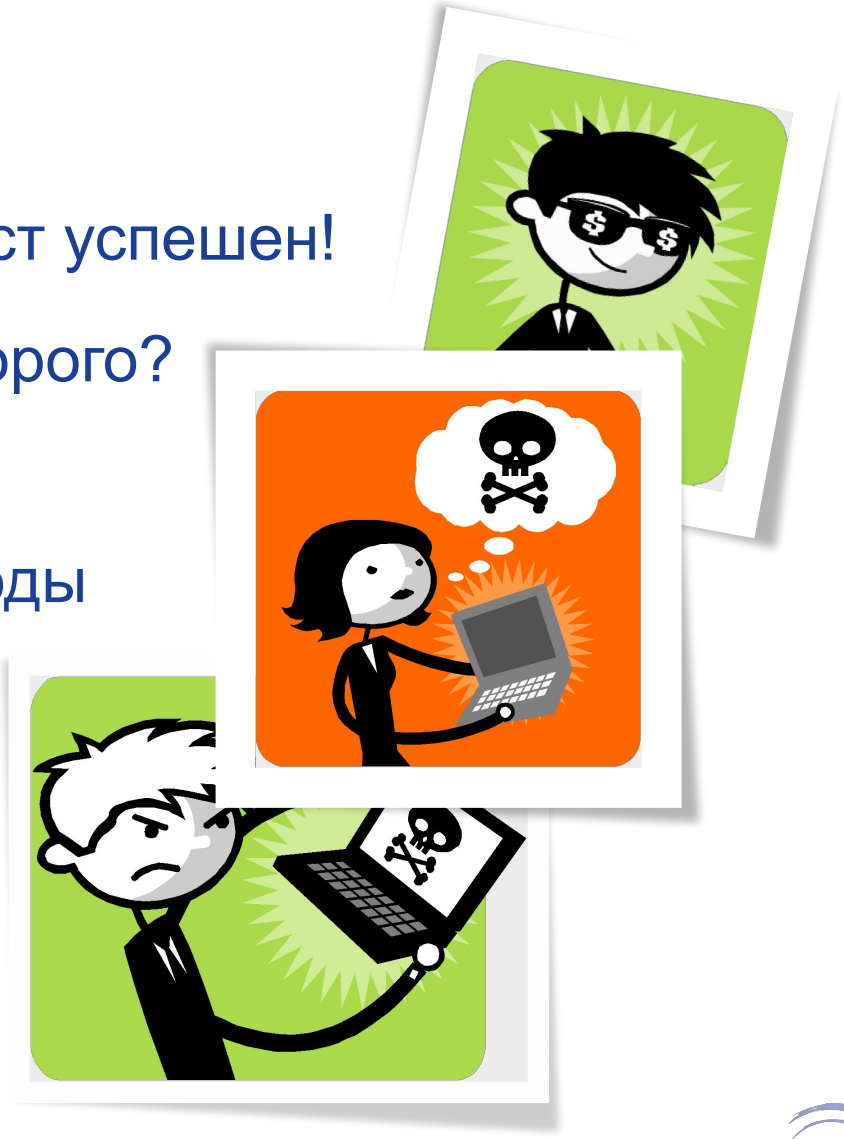
**Безопасности.NET**

- Наш каждый первый пен-тест успешен!
- Может быть это сложно и дорого?

# А есть ли безопасность?

**Безопасности.NET**

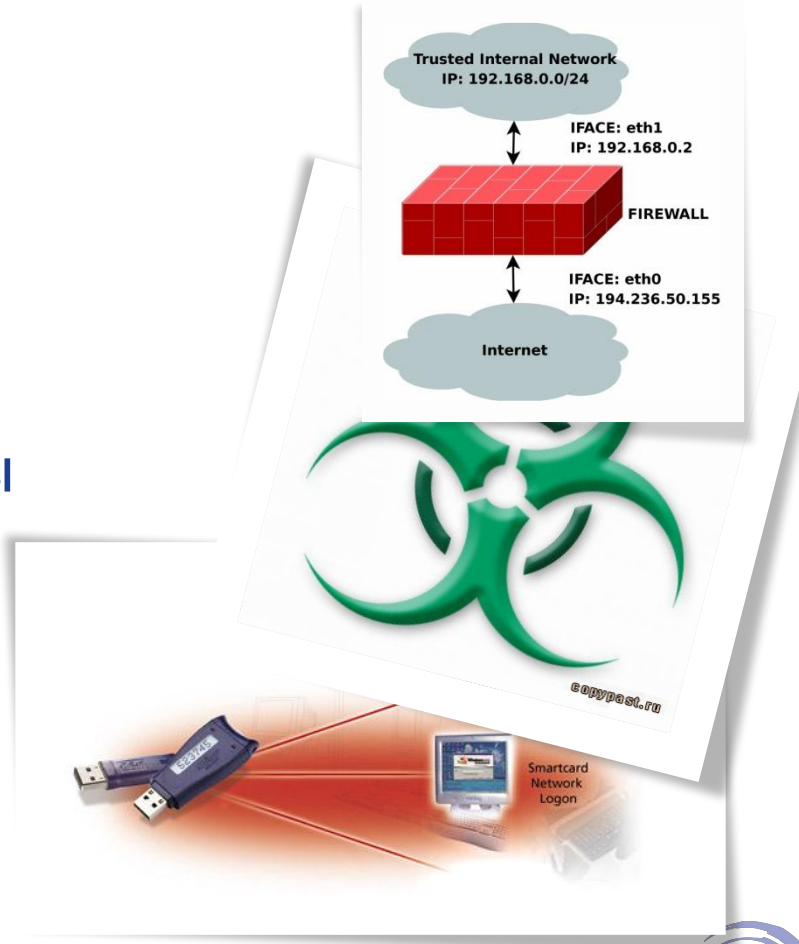
- Наш каждый первый пен-тест успешен!
- Может быть это сложно и дорого?
- Нет! Это «пионерские» методы
- И размер бюджета на ИБ не имеет никакого значения ☹



# В чем причины успешности?

- **У вас нет межсетевых экранов, антивирусов, систем обнаружения атак?**

- **Все гораздо проще:**
  - Непропатченные ОС
  - Необновленные антивирусы
  - Кривые настройки экранов



# Почему? Кто виноват?

- **Когда мне страшно, я зажмуриваюсь!**
  - Мы не смотрим на реально происходящие процессы в ИС
  - Мы не смотрим на состояние ресурсов и средств защиты
  - Мы не анализируем причины инцидентов

# Экспресс-тест!

- **Ответьте для себя на три вопроса:**

  **#1.** Какие проекты по ИБ вы реализовали за два года?

  **#2.** Что было драйвером проектов по ИБ?

  **#3.** Как оценивается успешность службы ИБ?

# Экспресс-тест!

- **Правильные ответы:**

  **#1.** Инраструктура ИБ и compliace

  **#2.** Нормативные требования и соображения «гигены»

  **#3.** Никак или «по понятиям»

# Как повысить защищенность?

## Выше забор?

# Как повысить защищенность?

## Или больше собака?


# Безопасность не должна быть слепой

**«Прозрение» это:**

- Мониторинг событий и инцидентов
- Управление уязвимостями и обновлениями
- Анализ конфигураций средств защиты

# Заметки на полях

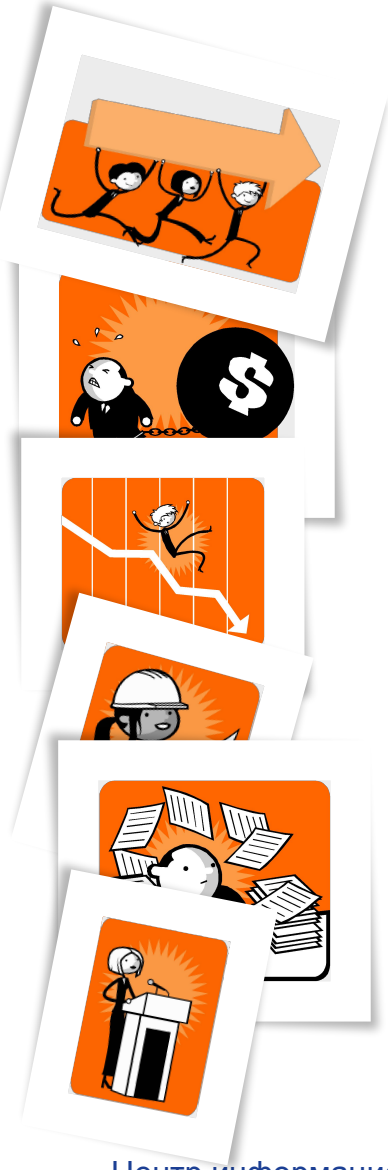
Не важны вопросы «как» и «чем» мониторить ИБ
важно ответить
на вопрос «кто»!

Очень важно стать службе ИБ прозрачнее и перестать быть черным ящиком для окружающих

На основе систем мониторинга можно построить измеримые KPI службы ИБ

Маленький, но аккуратный безопасник, гораздо важнее большой, но бессмысленной системы ИБ ☺

# Резюме



- **Активные средства безопасности стоят уже в «три ряда»**
- **Инвестировать нужно в управляемость системы ИБ, в ее прозрачность**

Есть еще моменты, которыми также не занимаются, но это уже совсем другая история…

ИНФОСИСТЕМЫ ДЖЕТ

## Контакты:

Ляпунов Игорь
Директор Центра информационной безопасности

Москва: (495) 411-7601
liapunov@jet.msk.su