Соответствие международным и отраслевым стандартам
Технологические аспекты

Сергей Гордейчик

gordey@ptsecurity.ru

Комплайнс - очень модное слово

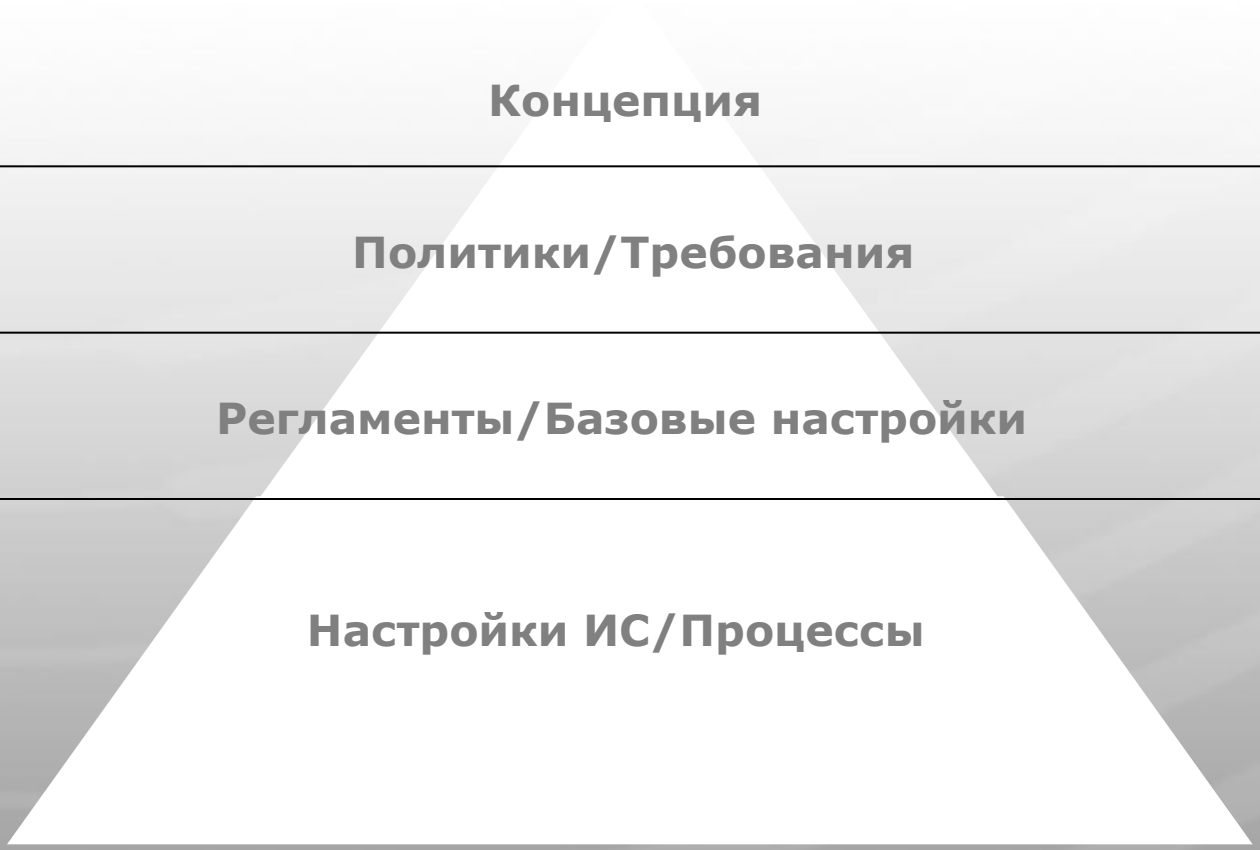
- РД и т.д.
- PCI DSS
- Стандарт ЦБ РФ
- ISO 27001/17799/27002
- SOX 404
- Закон о персональных данных (1Д)

Большинство стандартов носят общий характер

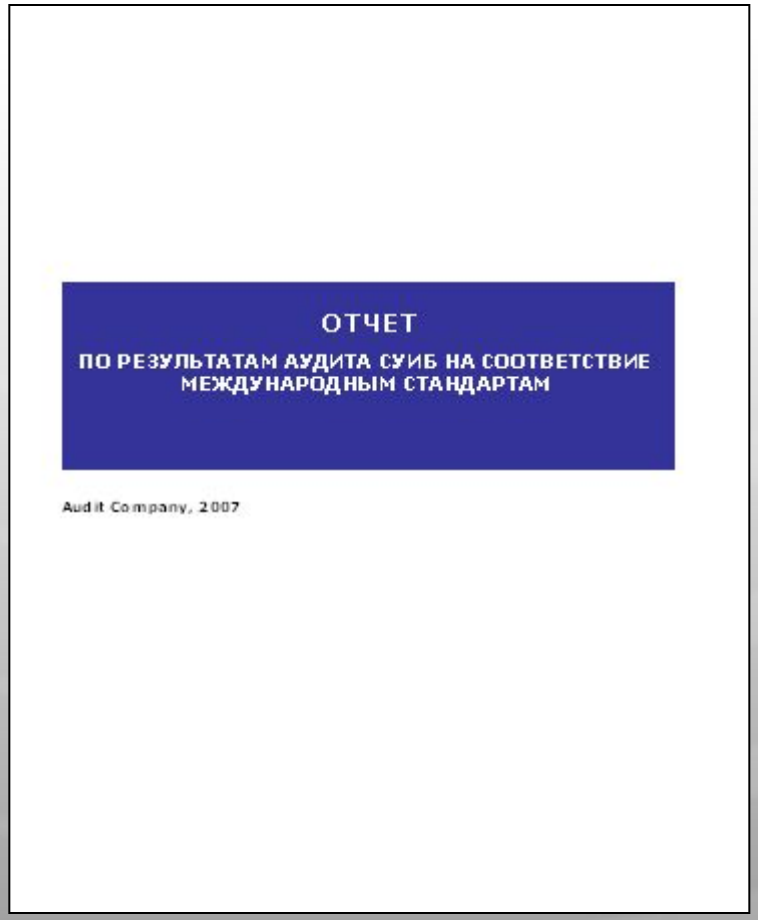
- 27001 – построение процессов
- Стандарт ЦБ РФ – очень близок к 27001
- SOX 404 – всего 4 абзаца

PCI DSS – исключение

Результат…


Концепция
Политики/Требования
Регламенты/Базовые настройки
Настройки ИС/Процессы

Результат...


ОТЧЕТ
ПО РЕЗУЛЬТАТАМ АУДИТА СУИБ НА СООТВЕТСТВИЕ МЕЖДУНАРОДНЫМ СТАНДАРТАМ
Audit Company, 2007

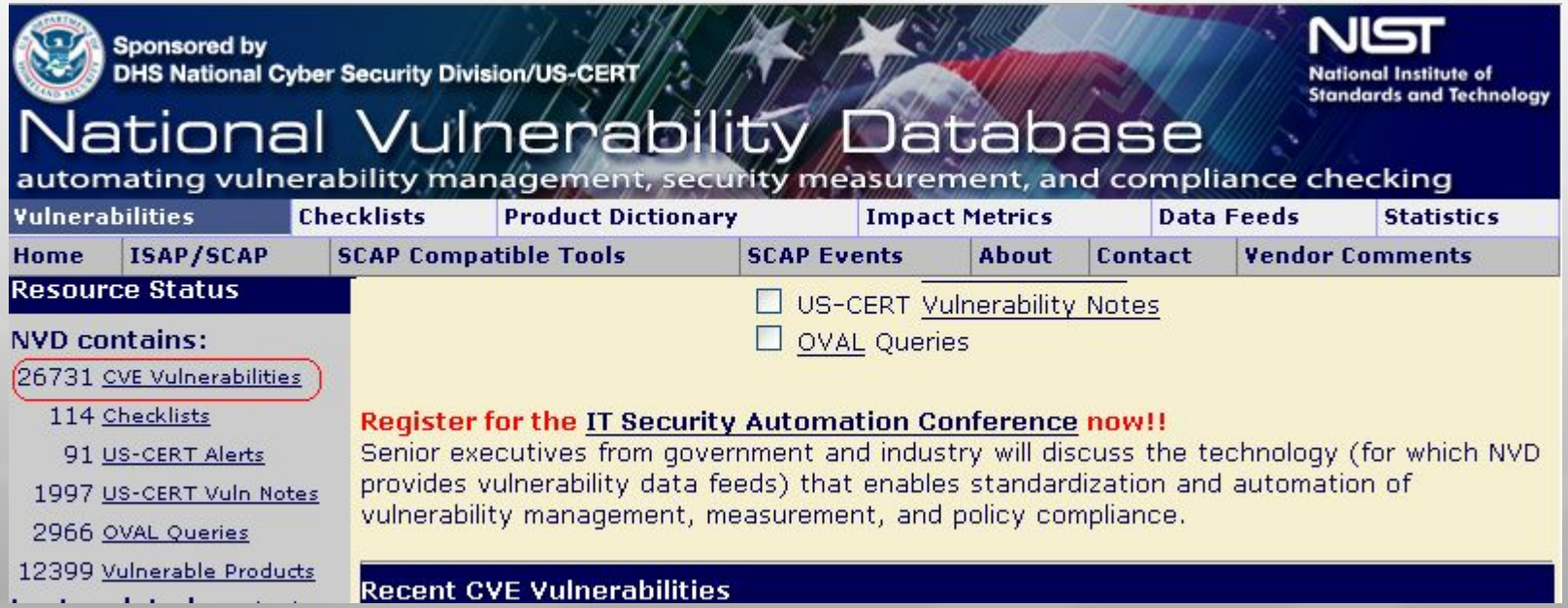

ОТЧЕТ
ПО РЕЗУЛЬТАТАМ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ И ИНСТРУМЕНТАЛЬНОГО КОНТРОЛЯ ЗАЩИЩЕННОСТИ
Audit Company, 2007

Большое количество «рекомендаций», «лучших практик»

- **Производители**
  - Microsoft
  - Cisco
  - Linux
  - Sun
- **Компетентные организации**
  - NIST
  - NSA
  - CIS
  - WASC

Огромное количество уязвимостей

25 сентября 2007 CVE-2007-5079

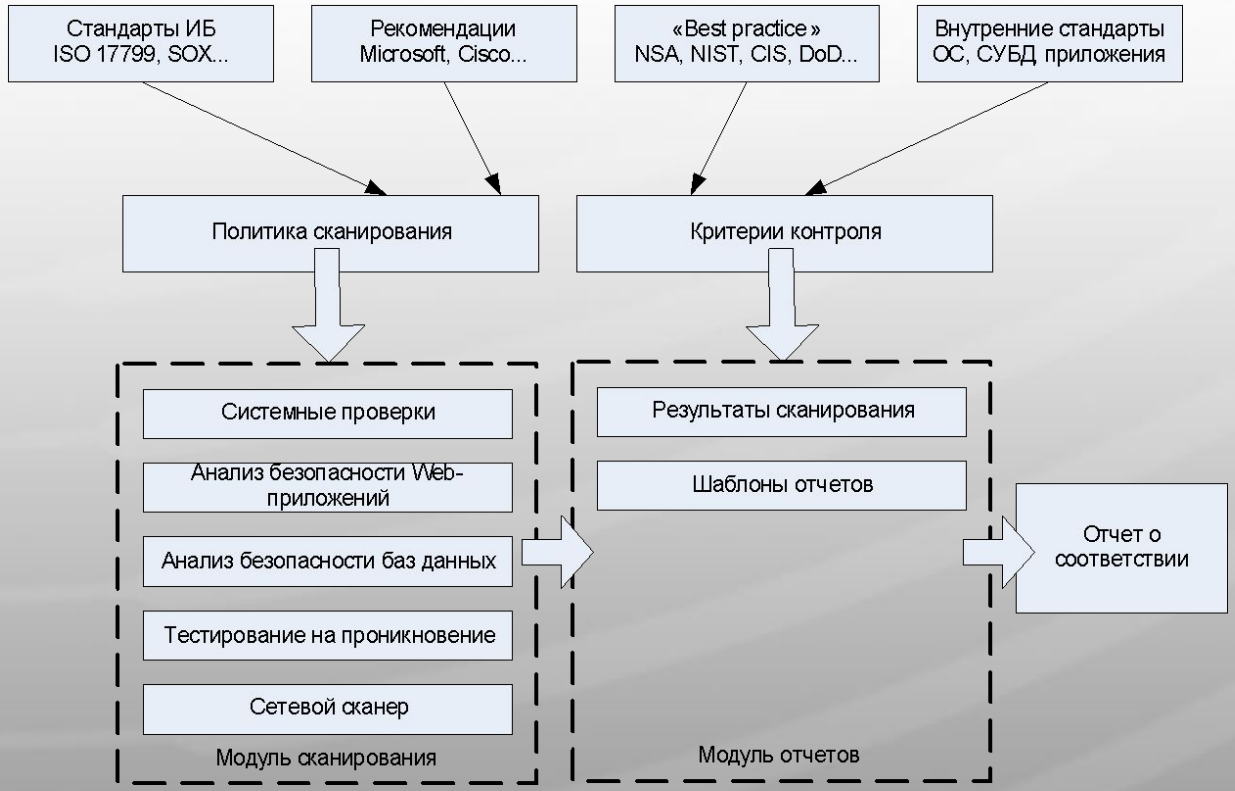


Проверка систем на соответствие техническим требованиям

- **Контроль уязвимостей**
  - Решаемая задача
  - Переход от «хакерских» методик к «мягким» методам аудита
  - Web-приложения – исключение (но мы работаем над этим)
- **Контроль конфигурации**
  - Достаточно сложная задача
    - Различные форматы
    - «настройки по умолчанию»
    - «тихий» ввод новых возможностей
  - Система должна быть адаптируемой
    - Что русскому хорошо…
- **Контроль изменений**
  - Контроль изменений в уязвимостях и конфигурациях

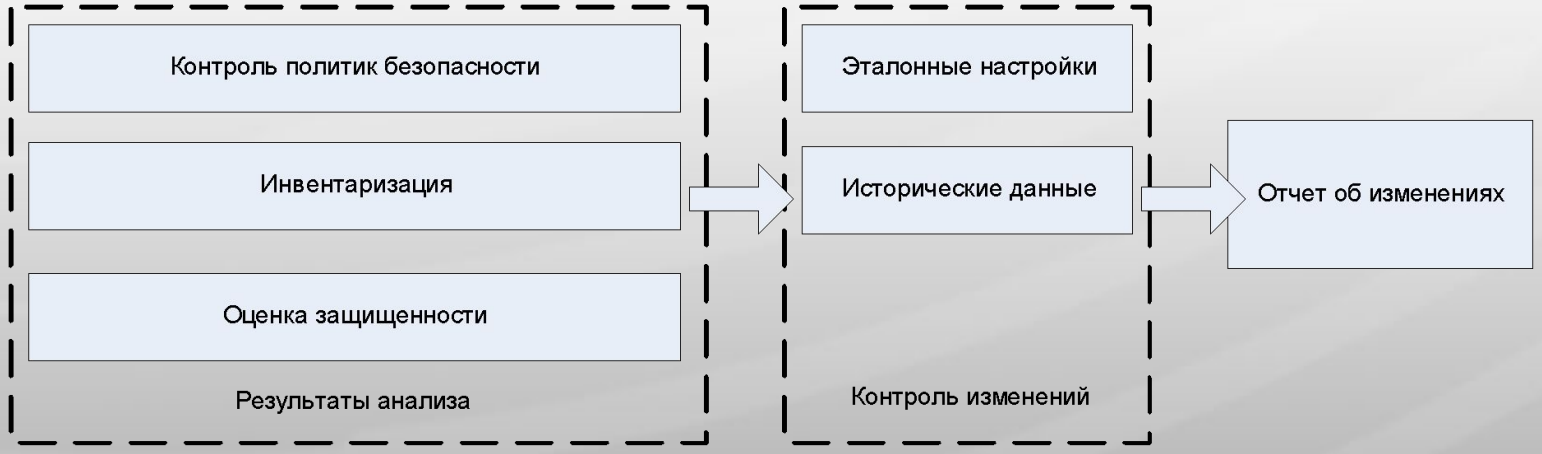
Комплексный подход

Проверка соответсвия



Собственно Compliance

Контроль изменений



Вопросы

Positive Technologies

+7 495 744 01 44

pt@ptsecurity.ru