Практические замечания к процессу построения и эксплуатации системы обеспечения информационной безопасности

- Беспорядок или хаос?
- Управление процессом/Цикл Деминга (PDCA)
  - Немногие доходят до Check и Act
  - Ландшафт угроз постоянно меняется. Меняются, усовершенствуются тактики и инструменты злоумышленников.
    - Нужно проверять наличие актуальных уязвимостей в инфраструктуре и оперативно исправлять их, либо применять компенсационные меры
      - Доступность и время работы ИТ-сервисов, особенно с доступом из-за информационного контура компании
      - Не забываем про тестовую инфраструктуру
      - Библиотека эталонного программного обеспечения
      - Управление конфигурациями
      - Плановый патчинг
      - Виртуальный патчинг
      - Альтернативные методы доступа к ИС
        - Тонкие клиенты с RO ОС+ терминальные фермы для сокращения трудоемкости патчинга
        - Загрузка с внешних доверенных носителей информации с RO ОС
    - Нужно приводить СЗИ в соответствие, для возможности обнаружения актуальных угроз
      - Перенастройка СЗИ для детектирования актуальных угроз
      - Регулярное обновление и проверка установки сигнатурных баз, пакетов экспертизы
      - Не забываем про ИТ
    - Нужно обучать работников ИБ-гигиене и порядку действий при возникновении угрозы информационной безопасности
      - Рассылка информационных бюллетеней об актуальных угрозах
      - Проведение обучения посредством небольших обучающих видео
      - Очное обучение
      - Регулярные проверки знаний, для точечной корректировки
    - Внутренние злоумышленники
      - Непривилегированные пользователи
        - Много. Сложно контролировать.
      - Привелигированные пользователи
        - Высокие компетенции и привилегии в ИС. Сложно контролировать.
  - Проверки соответствия
    - Сканеры уязвимостей
    - Внешние проверки
      - Аудит
      - Пентесты
- Откуда людей взять?
  - Разгрузить ИБ-шников от части бумажной работы и других непрофильных функций
  - Посмотреть в сторону ИТ-шников
- Что если у меня еще ничего нет в части СОИБ или моя компания из сегмента SMB?
  - Начните с малого, не усложняйте
    - Фокусная группа для определения угроз, рисков, целей и т.п.
    - Базовые средства СОИБ
    - Настройка имеющихся в ПО, на железе функций обеспечения ИБ
      - Учетные данные по-умолчанию
      - Доступ в/из Интернета
      - Встроенные средства обеспечения ИБ
  - Open source