Планирование и реализация подходов к выбору ИБ-архитектуры. Проверка эффективности системы обеспечения ИБ

- **Проблематика**
  - **Асимметрия ИБ**
    - Точечные атаки vs Защита всей ИТ-инфраструктуры
    - Конкретная задача vs Облако проектов и задач
    - Фактор неожиданности
    - Вариативность вектора атаки
      - Социальная инженерия
        - Множество инфоповодов
        - Уровень киберграмотности
        - Искуственный интеллект
      - Уязвимости ПО
      - Неправильные конфигурации
  - **Компетенции и ресурсы защитников**
    - Отсутствие понимания технических деталей эксплуатации уязвимостей
    - Незнание или непонимание техник, тактик и процедур атакующих
    - Недостаточные ресурсы на администрирование и настройку СЗИ
    - Отсутствие требуемого обучения и практического опыта
  - **Архитектура ИБ и ИТ**
    - Отсутствие требуемой проработки при внедрении
      - Сложность последующего изменения
        - Масштабирование
        - Обновление
        - Адаптация
      - Сложность администрирования
    - Отсутствие целостного подхода
  - **Комплаенс и ЛНА**
    - Роль комплаенса
    - Стратегия и дорожная карта развития ИБ
  - **Подход к управлению ИБ**
    - Ситуационный
    - Процессный
    - Экосистемы, как набор продуктов
- **Подходы к выбору ИБ-архитектуры**
  - Соответствие ландшафту угроз
    - Модель угроз и нарушителя
      - Бизнес-процессы, бизнес-риски
        - Недопустимые события
      - Активы и конфигурации
    - Гибкость и возможности адаптации
  - Соответствие целям бизнеса
    - Про необходимость и достаточность
    - Обоснованность затрат
      - Человеческие ресурсы и компетенции
      - Коммерческие продукты и решения vs Opensource
      - MSSP, outsource, outstaff и консалтинг
    - Операционная устойчивость
  - Соответствие регуляторным требованиям
    - Организационные меры
    - Встроенные средства защиты ОС, ИС, ПО
    - Компенсационные меры
  - Автоматизация процессов и минимизация человеческих ресурсов
    - Сложность администрирования
    - Сложность масштабирования
    - Сложность эксплуатации и настройки
  - Межкомпонентная интеграция
  - Базовый уровень ИБ
- **Проверка эффективности СОИБ**
  - Про пилотное тестирование продуктов и решений
  - Про пентесты, CPT, bug bounty
  - Про киберполигоны