ИНФОСИСТЕМЫ ДЖЕТ

Защита АСУ ТП: первый шаг в безопасность

Даниил Тамеев

Зам. руководителя направления по работе с ПиТЭК
Центр информационной безопасности

25 сентября 2014 г.

О чем пойдет речь

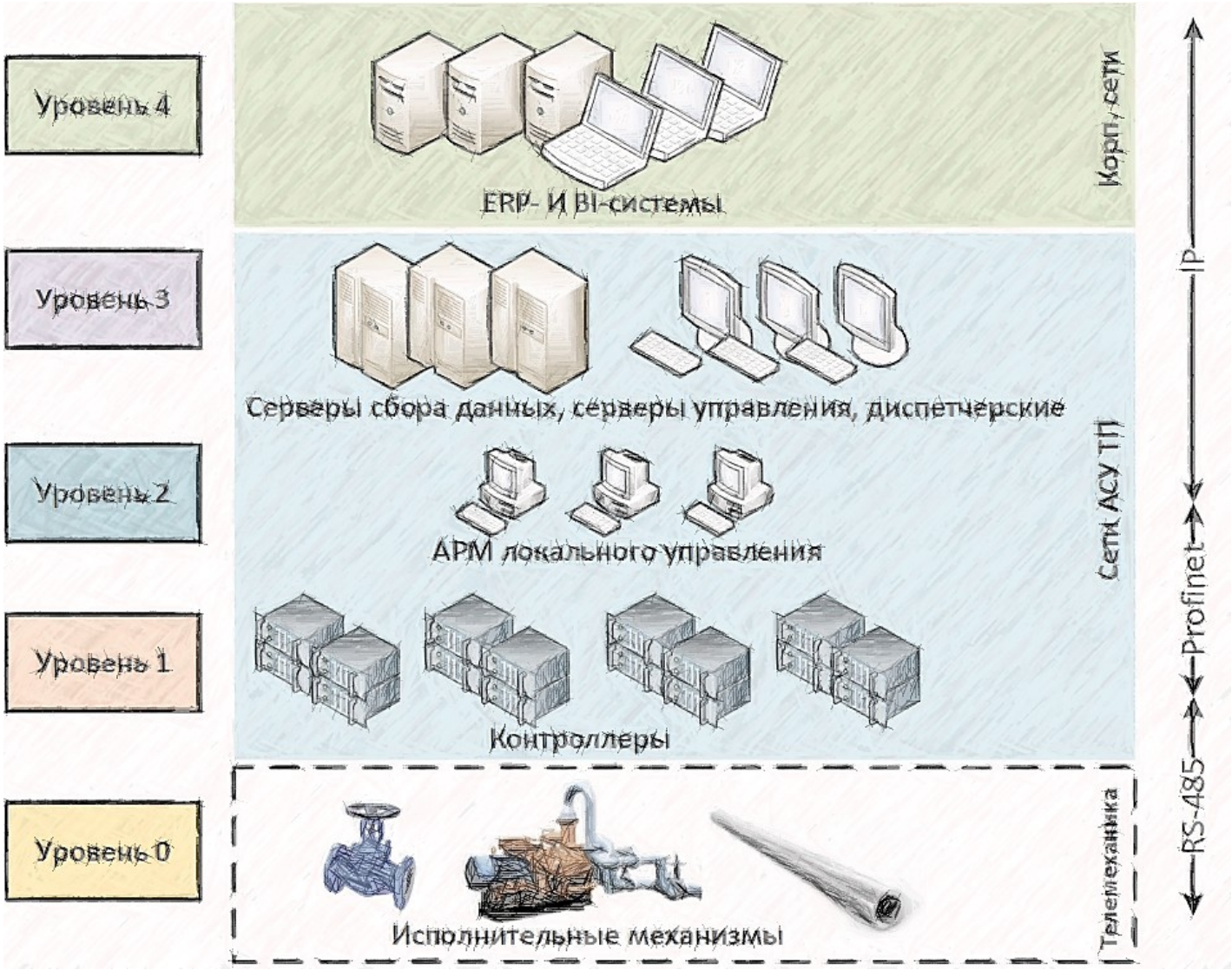
1. Описание подхода
2. Карта пути в светлое будущее
3. Проблематика проектов
4. Результаты

Основы методики

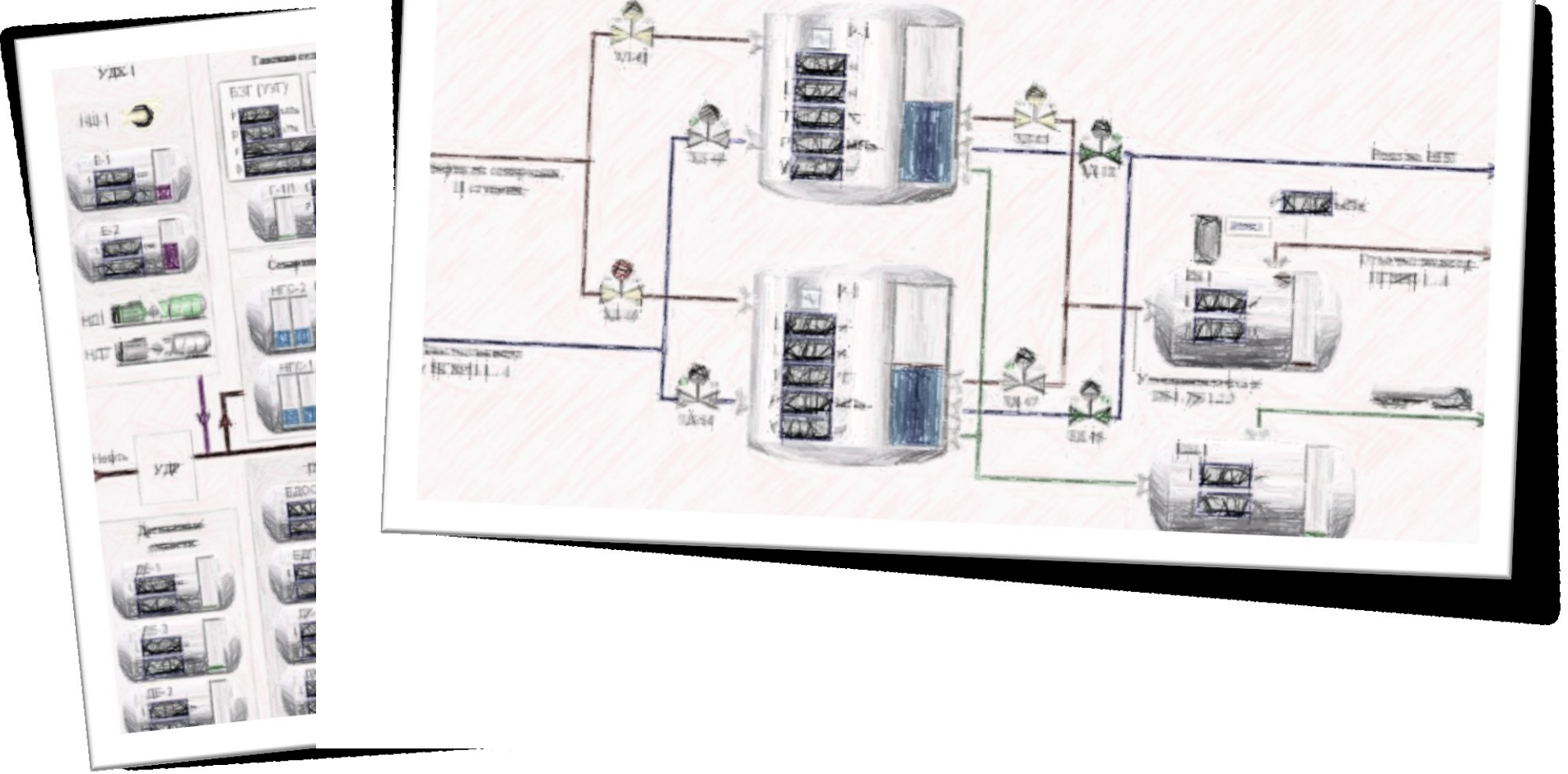
- Международные стандарты
  - ISA-99/IEC-62443
  - NIST SP 800-82
- Законодательные требования
  - Приказ ФСТЭК №31 (2014)
  - Методические документы ФСТЭК (2007)
- Многолетний опыт проектов

Точка отсчета

Шаг №1: Логическая структура



Шаг №2: Физическая архитектура

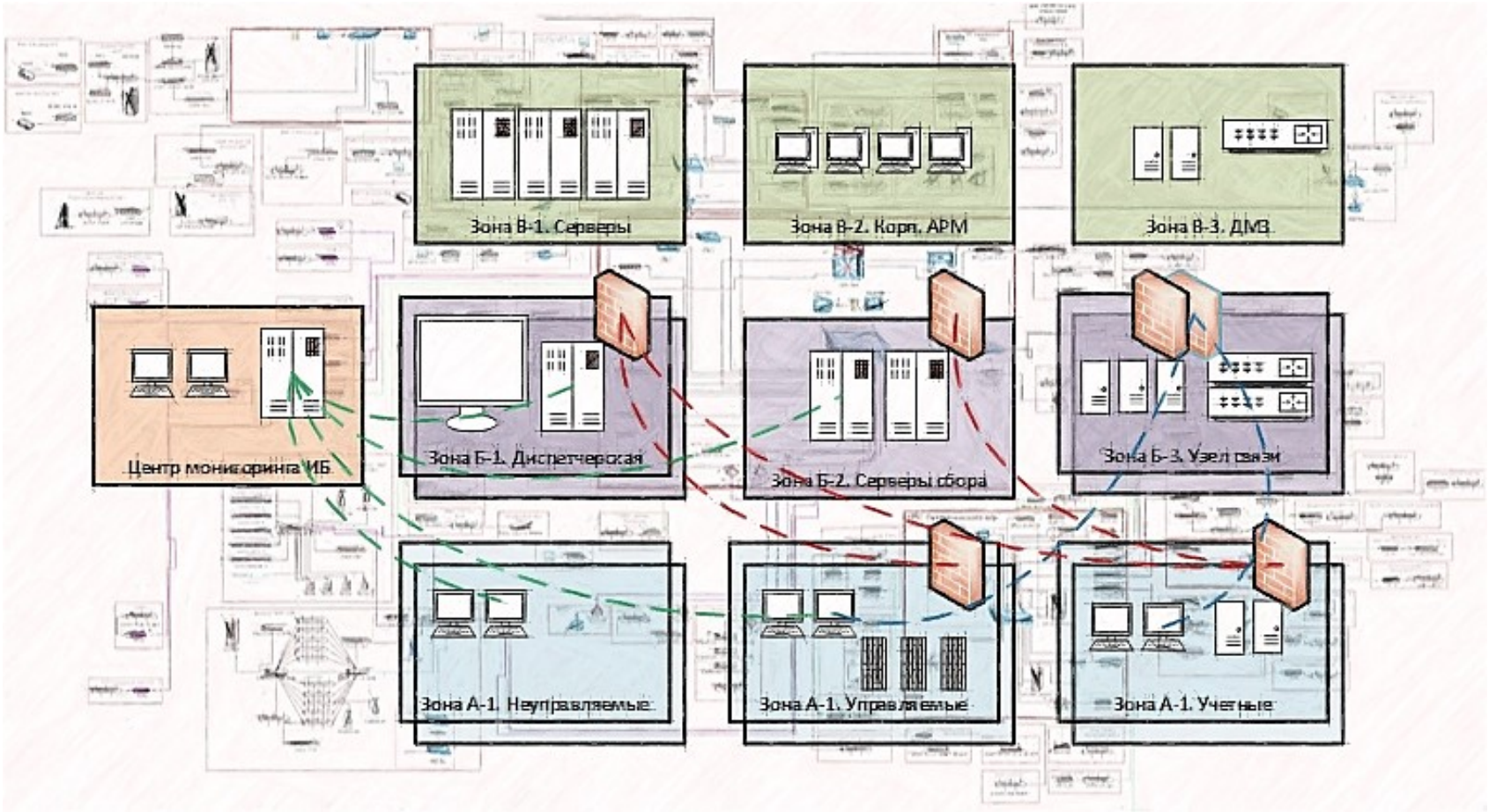


Чаще всего мы видим

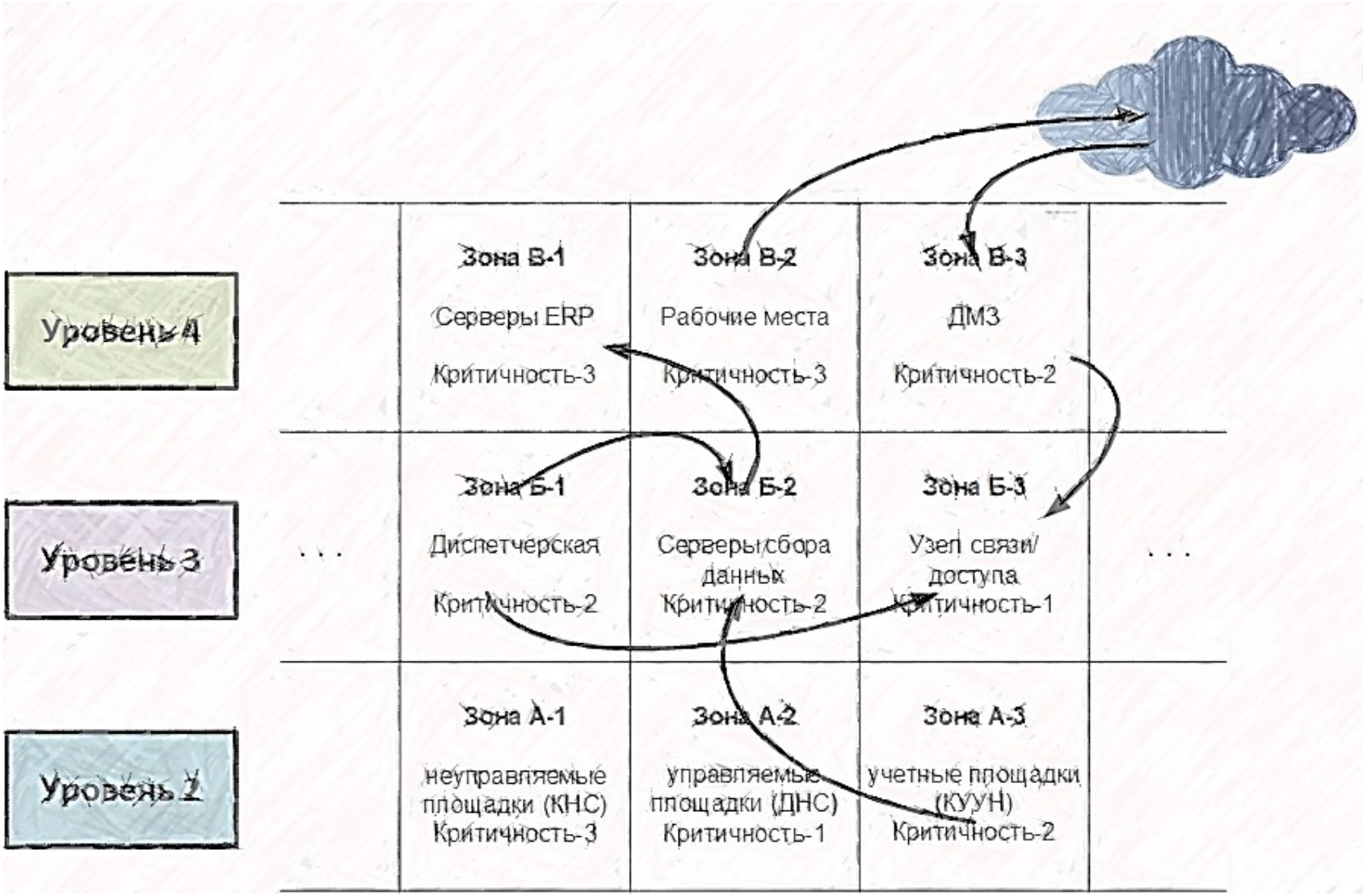
ТОП-5 уязвимых мест

1. **АСУ ТП vs. Безопасность**
   Отсутствие политик, процедур и культуры ИБ при проектирования, разработке и эксплуатации систем.
2. **Сеть**
   Плохо проработанная архитектура и нецелевое использование сети.
3. **Мусор в инфраструктуре**
   Лишнее ПО на АРМах и «железо» на объектах.
4. **Мониторинг**
   Недостаток средств для обнаружения и документирования аномальной активности.
5. **Проблема поддержки и наличие типовых уязвимостей**
   Затрудненная поддержка АСУ ТП и наличие типовых уязвимостей.

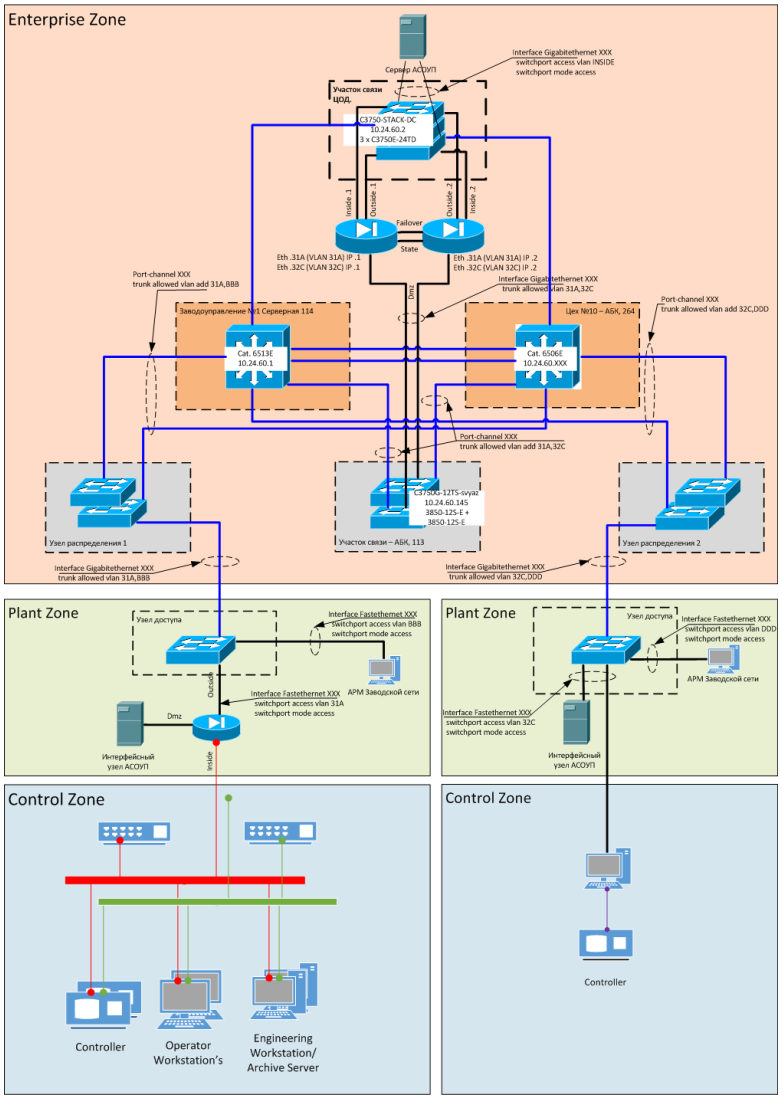
Шаг №3: Модель зонирования

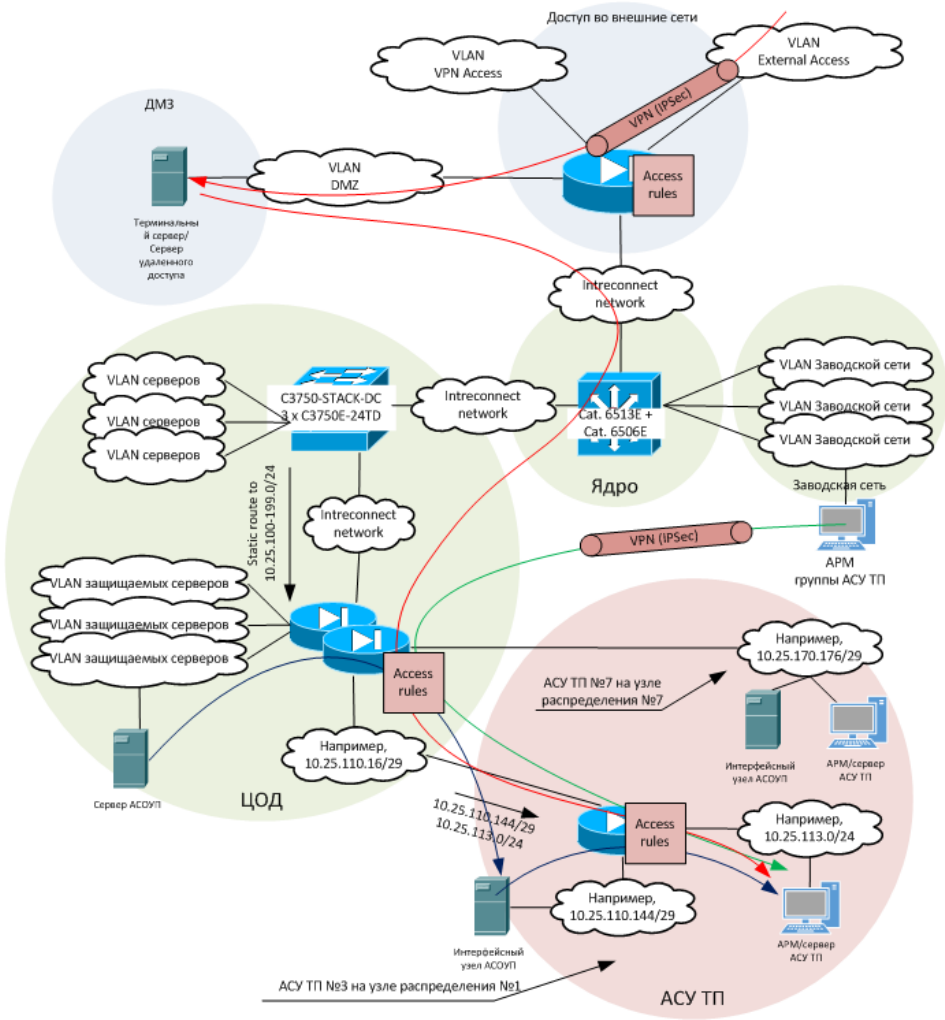


Шаг №4: Метрики и уровни защиты

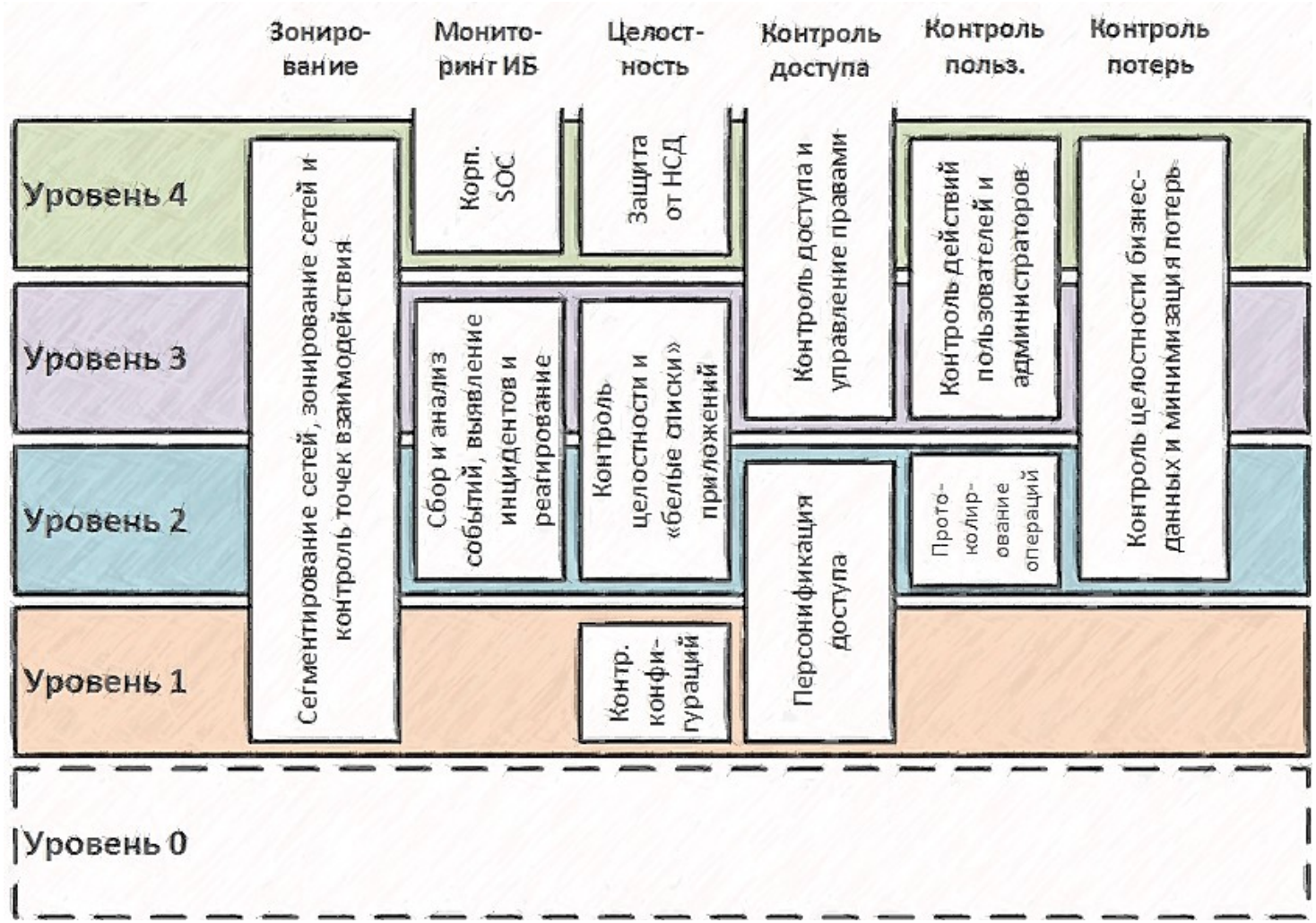


Итоговая схема





Результат



ИНФОСИСТЕМЫ ДЖЕТ

Спасибо за внимание!

Даниил Тамеев
Зам. руководителя направления по работе с ПиТЭК
Центр информационной безопасности
db.tameev@jet.su