
# Разработка нормативно-правовой базы по защите АСУТП. Опыт компании ЭЛВИС-ПЛЮС при классификации и оценке защищенности.

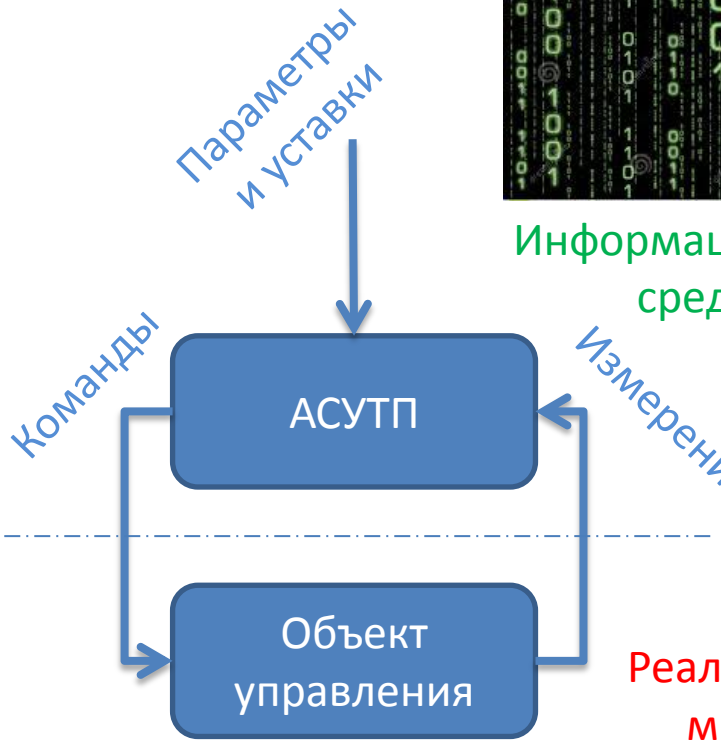
Стефанов Руслан

ЭЛВИС-ПЛЮС

# Главная задача защиты АСУТП КВО

- Недопущение несанкционированного доступа к объектам управления, а именно:
  1. Прямых команд управления
  2. Изменения параметров нормального режима и противоаварийной защиты
  3. Изменения значений измерений

Информационная среда




Реальный мир

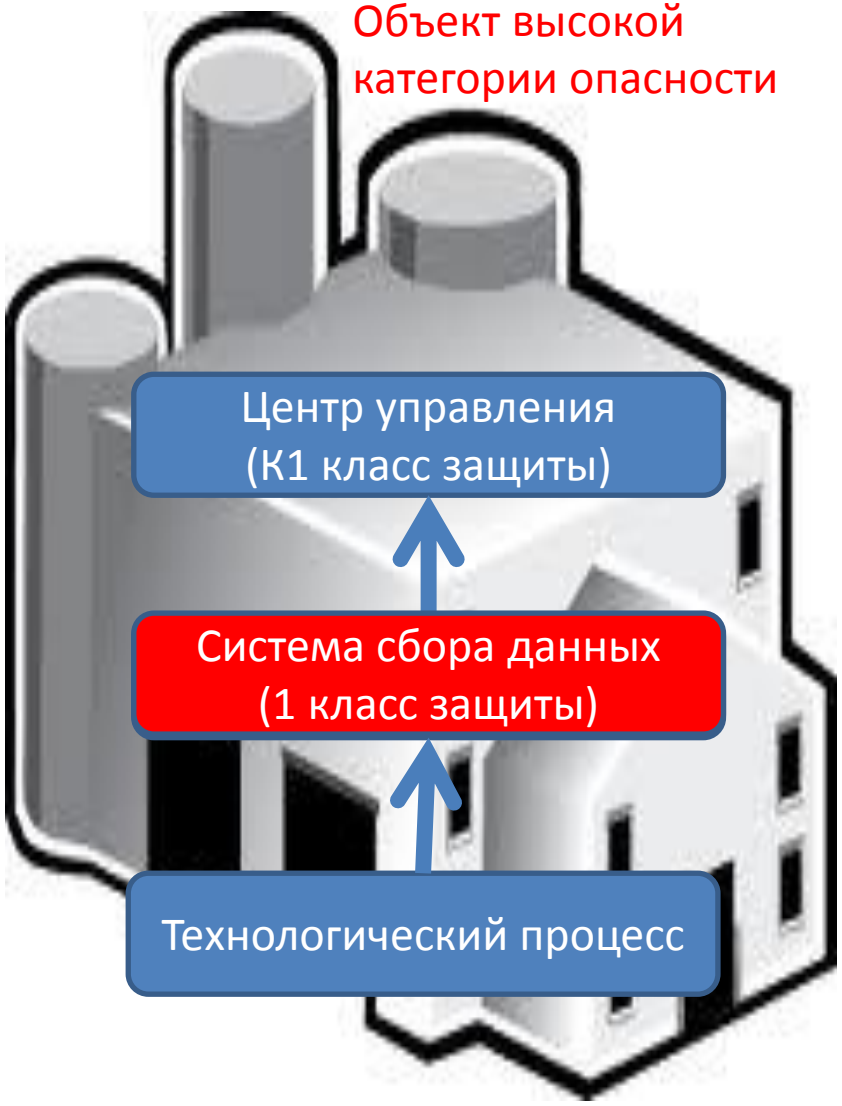
# Подход к классификации

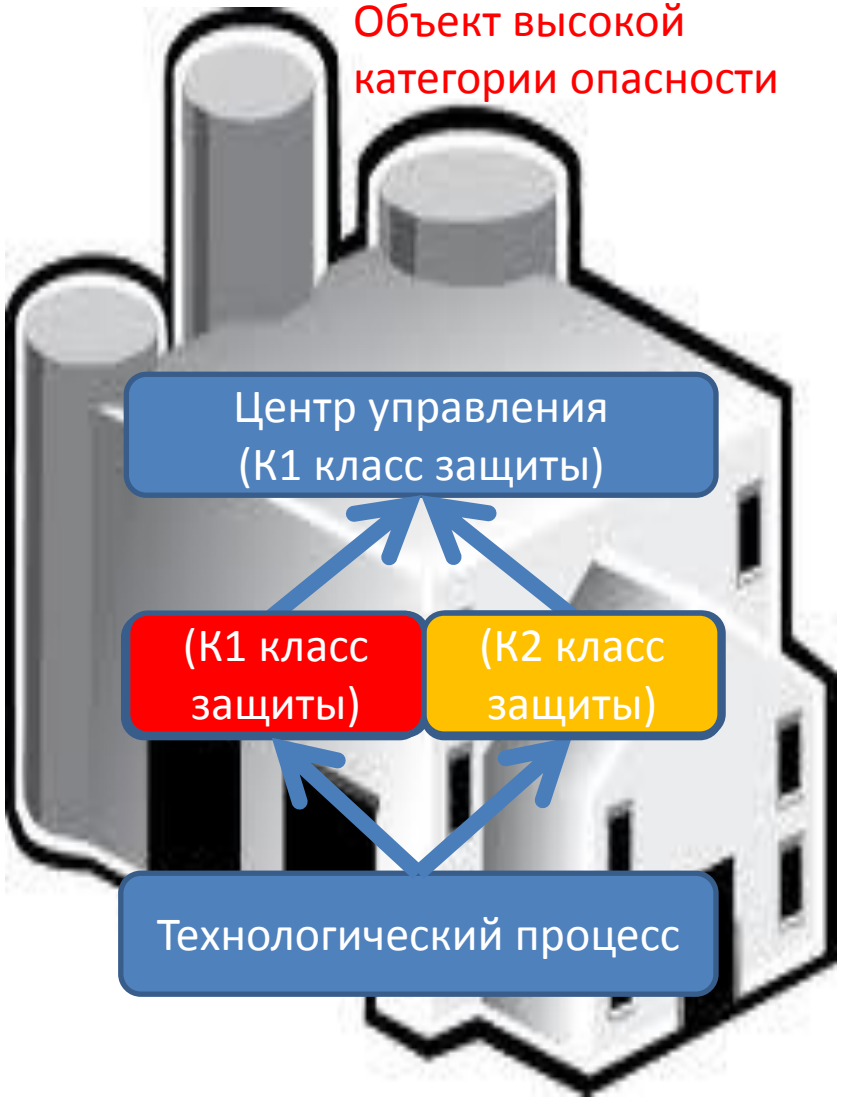
- Правовая и терминологическая база – ожидаемый ФЗ «О защите критической информационной инфраструктуры РФ»
- Классы защищенности систем должны соответствовать категориям опасности объектов и их количества должны совпадать
- Зарубежный опыт IEC 62443 (ISA-99) - ресурсы и мотивация злоумышленника

# Анализ критериев классификации

1. Категория опасности объекта (ФЗ о транспортной безопасности, о безопасности объектов ТЭК, о промышленной безопасности, проект ФЗ о безопасности критической информационной инфраструктуры)
2. Степень связанности системы (информации) с возможным ущербом (уровень значимости, характер влияния, масштаб системы)

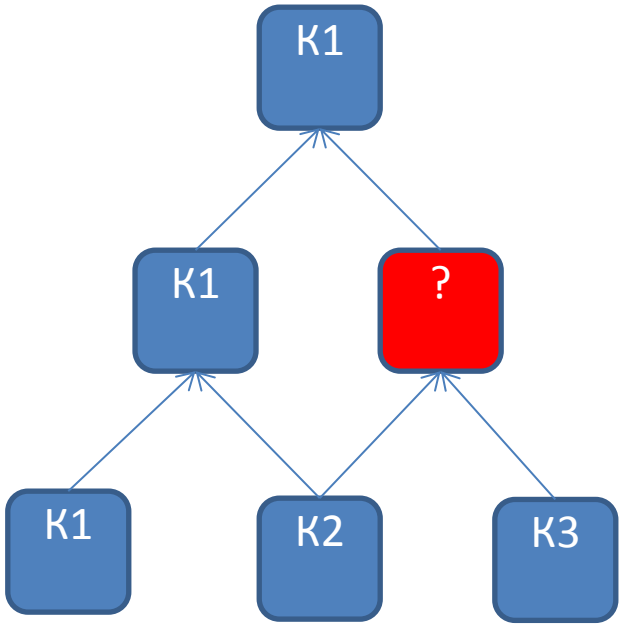
# Анализ критериев классификации



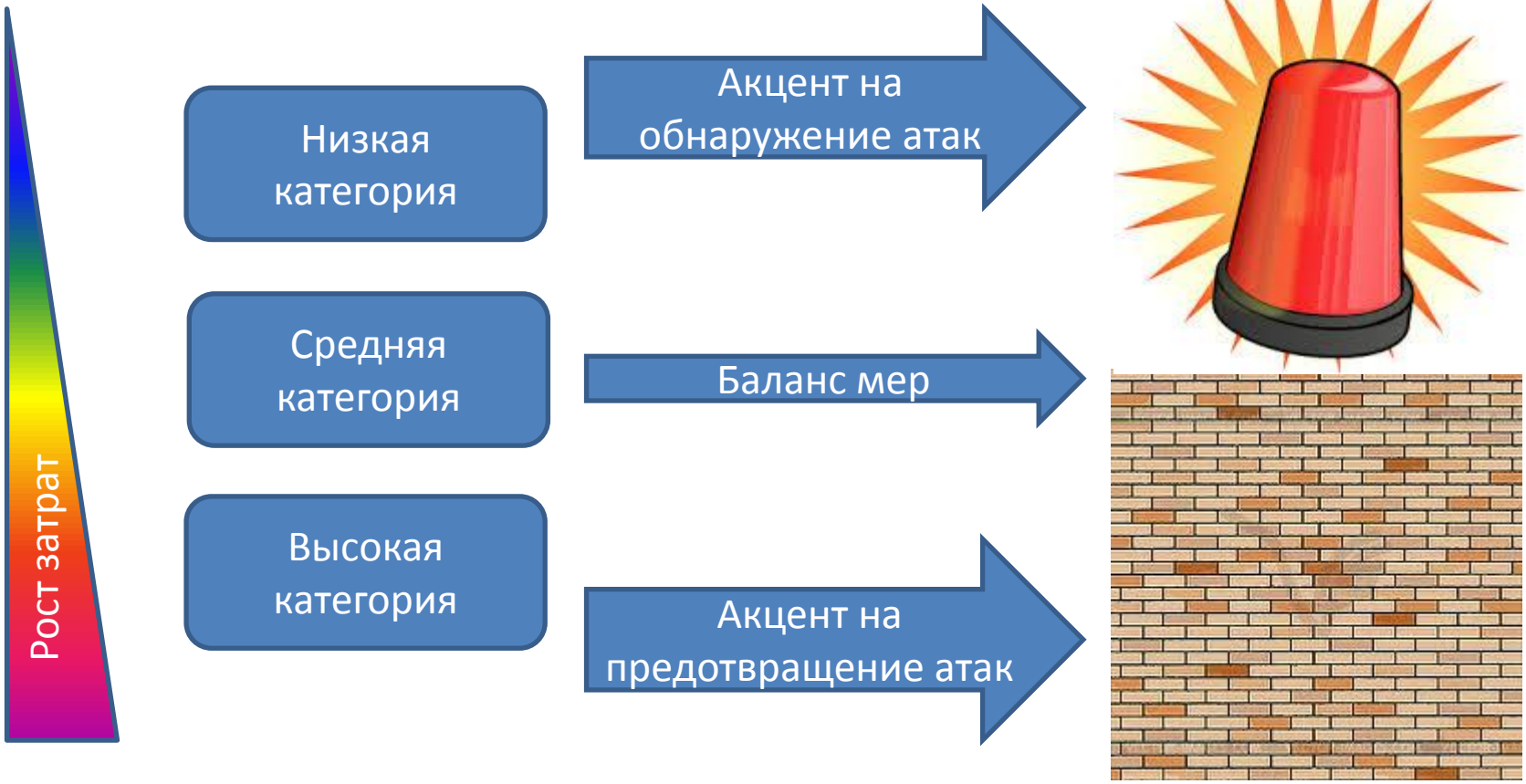



# Анализ критериев классификации (вывод)

Для верной и оптимальной классификации сложных систем необходим анализ зависимости классифицируемой системы от взаимодействующих с ней систем

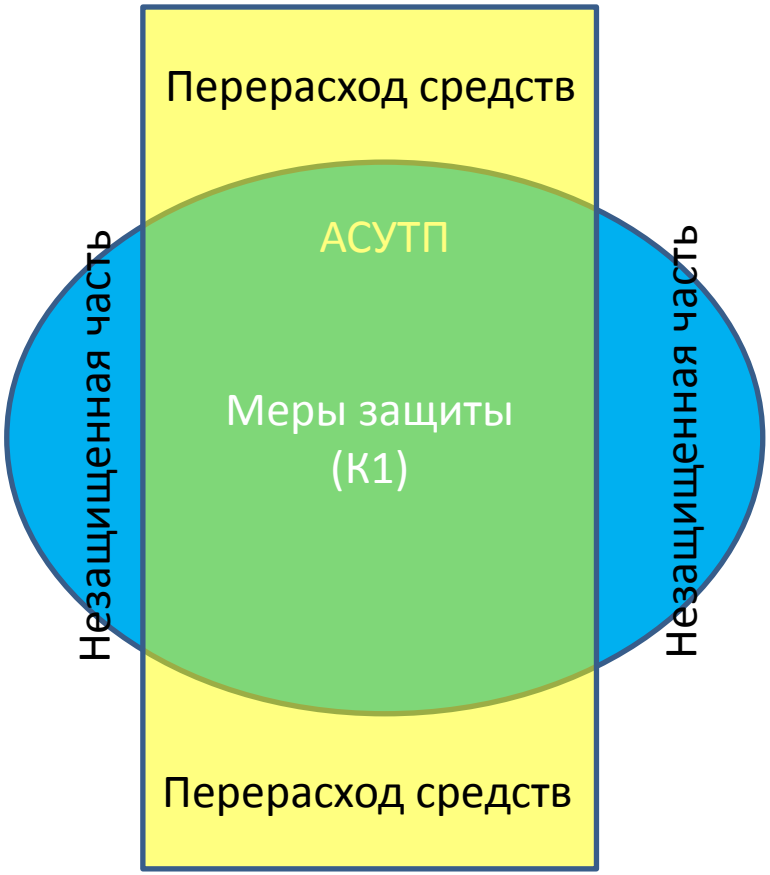


# Подход к мерам защиты

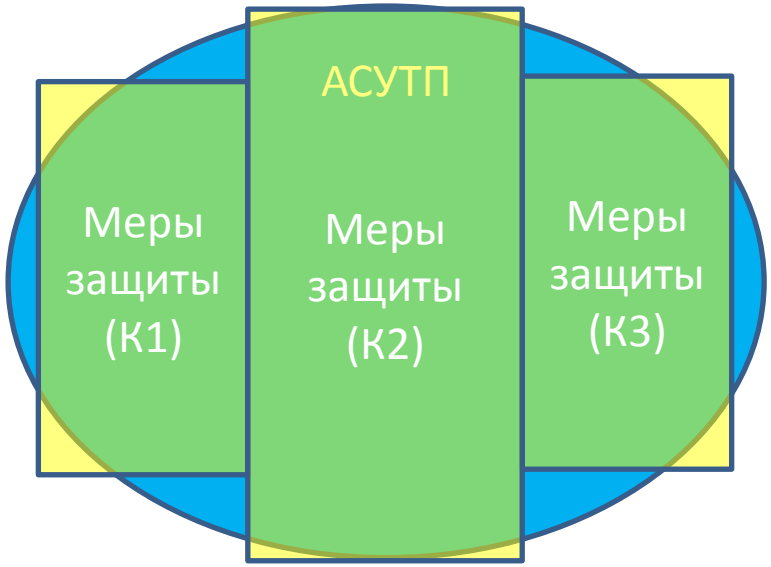


# Подход к оценке защищенности

«Грубая оценка»




«Точная оценка»
по методике ЭЛВИС-ПЛЮС



# Услуги и продукты компании ЭЛВИС-ПЛЮС

- Аудит ИБ АСУТП
  - Методика оценки защищенности
- Формирование требований к защите
- Разработка типовых решений подсистем ИБ АСУТП (системный проект)
- Реализация типовых решений
  - Техно-рабочее проектирование
  - Внедрение
- Техническая поддержка

# Аудит ИБ АСУТП

Дает ответы на вопросы:

- Каким угрозам подвержена система?
- Насколько защищена система?
- Какие мероприятия необходимо выполнить для повышения защищенности?

# Применяемые методы

**Аналитическое исследование**

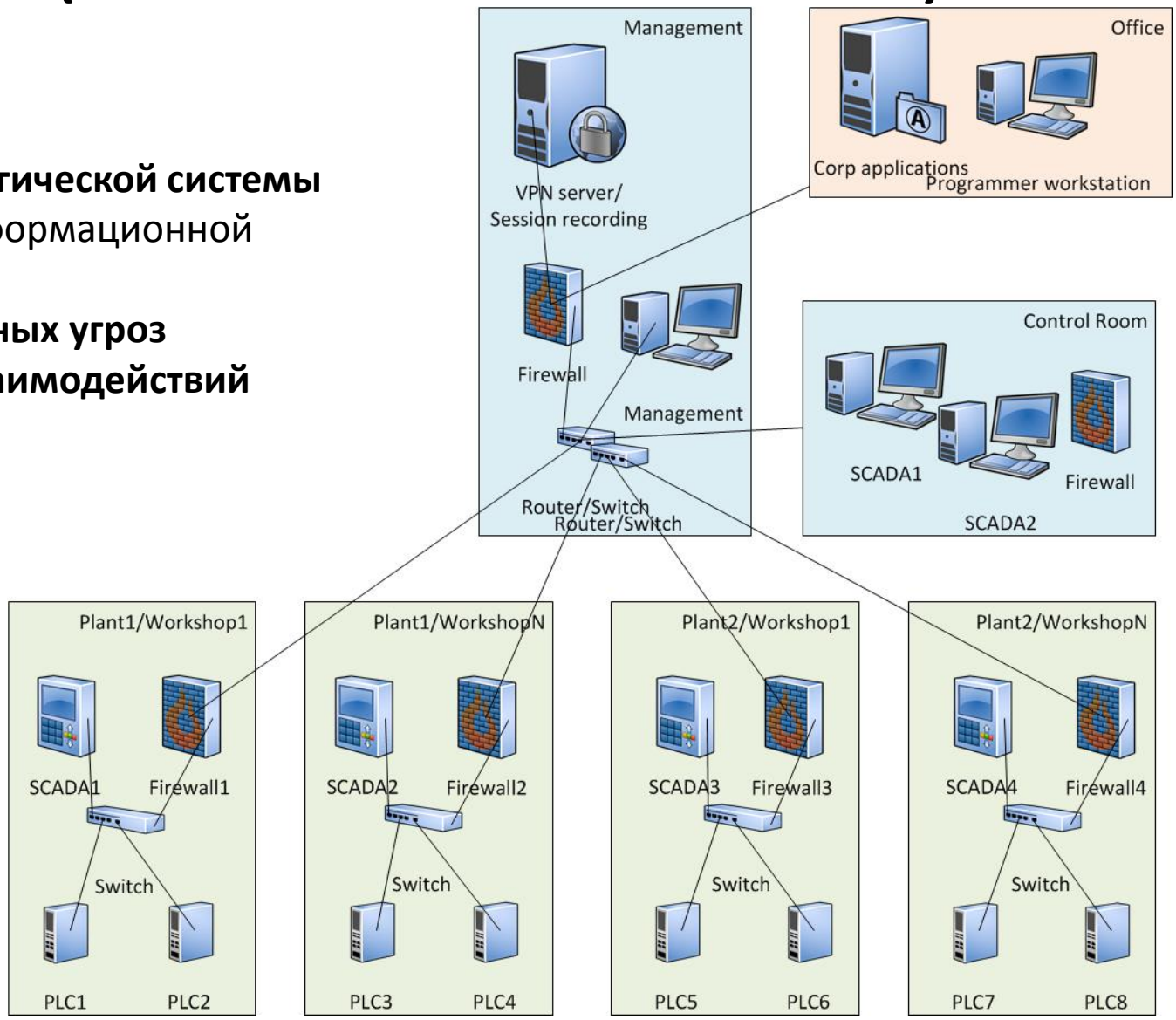
- Опрос
- Изучение эксплуатационной документации
- Изучение организационно-распорядительной документации

**Практическое исследование:**

- Сканирование ресурсов АСУТП
- Проникновение на ресурсы АСУТП
- Проникновение и нарушение работоспособности в тестовой среде

# Отчет (зоны безопасности)

- **Описание технологической системы** с точки зрения информационной безопасности
- **Перечень актуальных угроз**
- **Схемы сетевых взаимодействий**

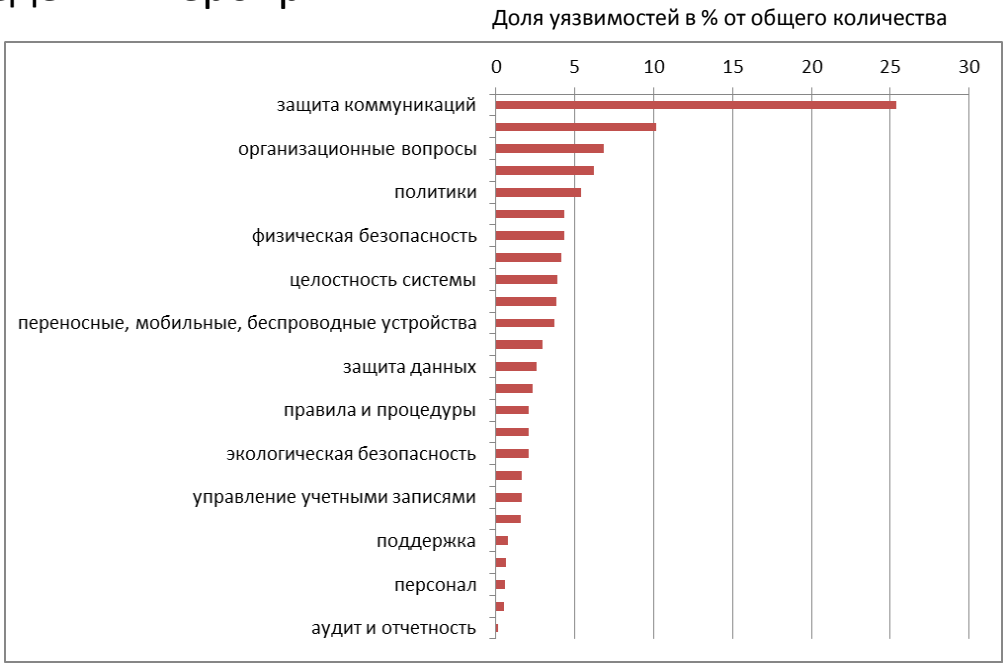


# Отчет (выводы и рекомендации)

- **Приоритетные направления защиты**

- **План мероприятий по нейтрализации актуальных угроз**:
  - Перечень мероприятий
  - Состав организационно-распорядительной документации
  - Состав системы обеспечения информационной безопасности
  - Состав проектной и эксплуатационной документации
  - Предполагаемые сроки проведения мероприятий

- **Стоимостная оценка** проведения мероприятий и закупки технических средств защиты информации



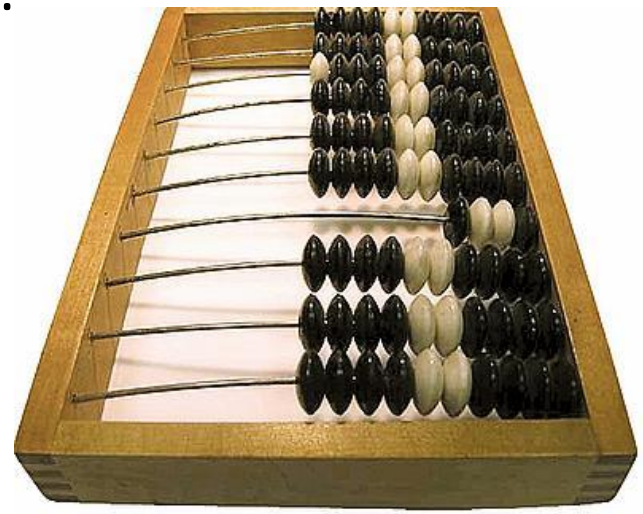
# Системный проект (СОИБ)

- Формируем требования (Common Criteria)
- Определяем подсистемы
- Определяем этапы
- Проектируем решения

# Типовые решения

Системный проект дает ответы на вопросы:

- Почему необходима защита?
- Как защитить систему?
- В какие сроки (этапы)?
- Сколько это будет стоить?



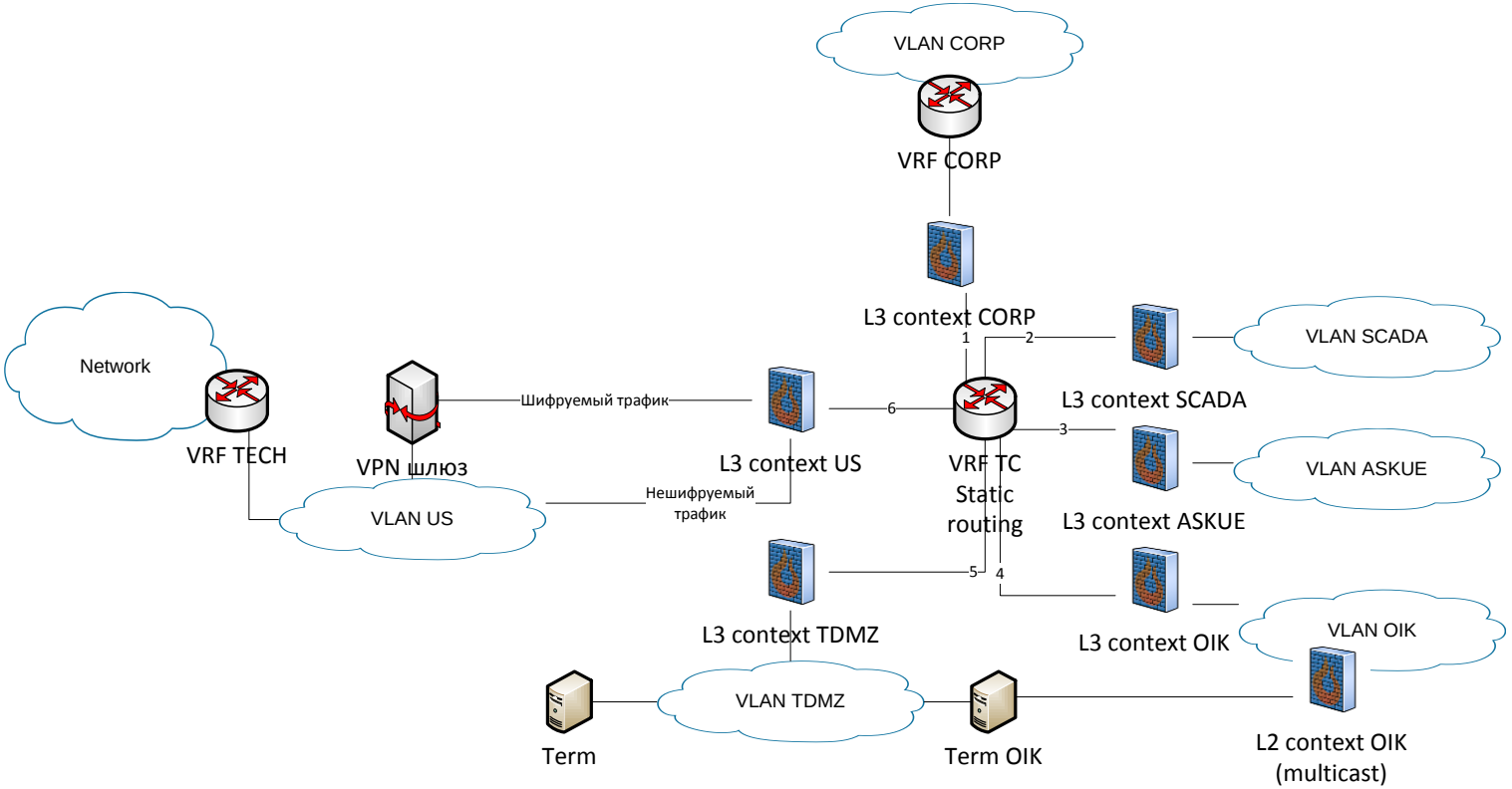
# Обоснование решений

- Рекомендации аудита ИБ
- Модель угроз и модель нарушителя
- Общие критерии по стандарту 15408 включают также формирование требований

# Типовые подсистемы СОИБ

- Защита периметра, межсетевое экранирование, обнаружение и предотвращение вторжений (создание ТДМЗ и сегментирование)
- Защита каналов связи
- Защищенный удаленный доступ
- Антивирусная защита и контроль приложений («белые списки»)
- Терминальный доступ
- Идентификация и усиленная аутентификация
- Управление доступом к инфраструктуре (сетевой, виртуальной)
- Анализ защищенности
- Мониторинг ИБ
- Управление инцидентами ИБ

# Защита периметра и МЭ




| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | x | - | - | - | + | - |
| 2 | - | x | - | - | + | + |
| 3 | - | - | X | - | + | + |
| 4 | - | - | - | x | + | + |
| 5 | + | + | + | + | x | - |
| 6 | - | + | + | + | - | x |

Таблица разрешенных взаимодействий между сегментами

# Специализированные продукты

- МЭ + IPS + VPN – Tofino Eagle (Belden), Phoenix Contact mGuard, Siemens Scalance, Netasq
- Аутентификация – Swivel, IndeedID
- Белые списки – ЛК, McAfee
- Запись экранов – ObserveIT
- Анализ защищенности – MaxPatrol, Nessus
- Дата-диоды – Waterfall, FoxIT

# Заказчики компании ЭЛВИС-ПЛЮС

- ОАО «ФСК ЕЭС»
- ОАО «СО ЕЭС»
- Холдинг МРСК (ОАО «Российские сети»)
- ОАО «АК» «Транснефть»


# Ваши вопросы?

Стефанов Руслан