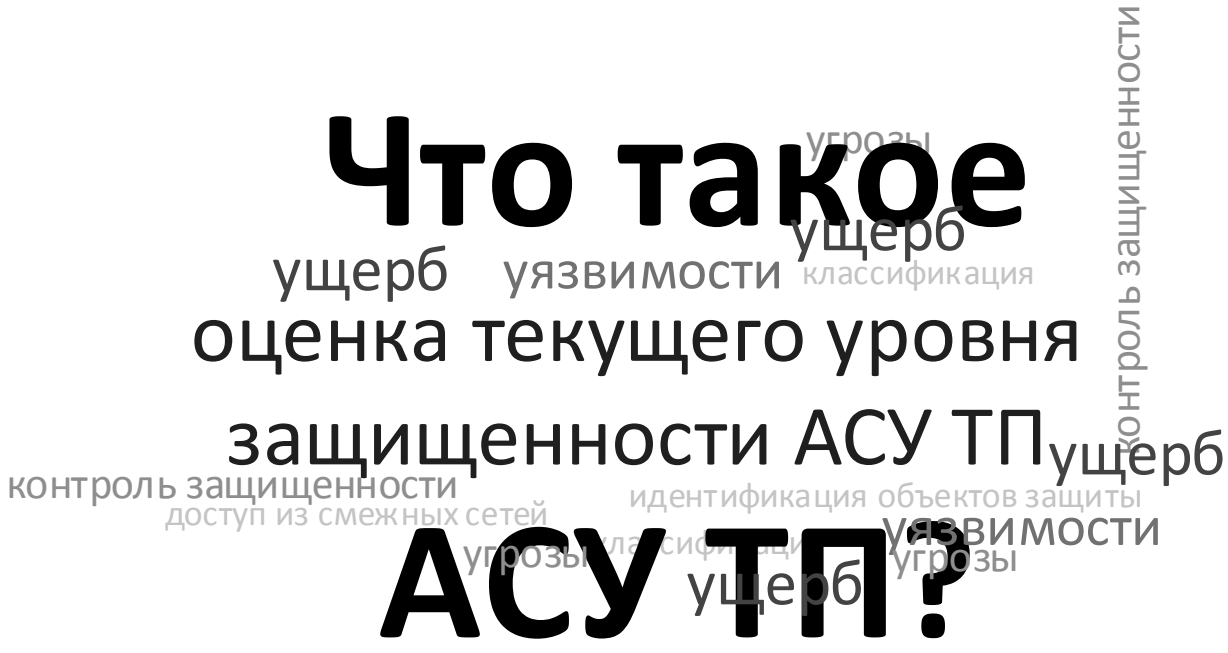
Практика проведения аудитов информационной безопасности систем автоматизации и управления

Николай Домуховский
Главный инженер ДСИ
ООО «УЦСБ»

Зачем заказывают аудит ИБ АСУ ТП?

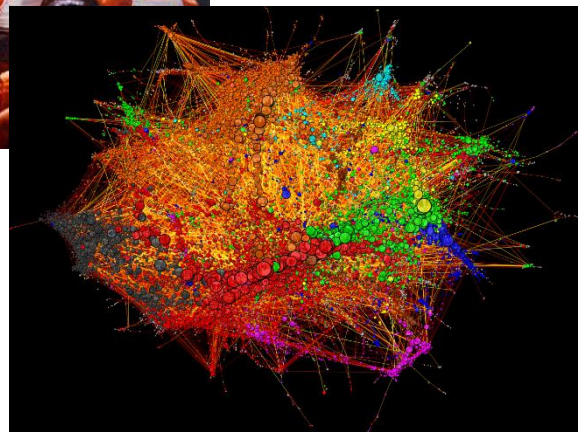


Основные этапы аудита

Сбор данных

Моделирование угроз

Тестирование на проникновение



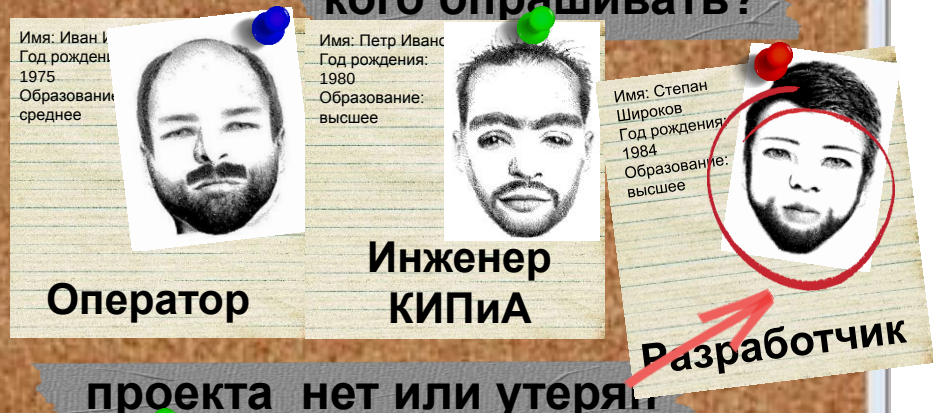
Представление результатов

Сбор данных

задачи

Интервьюирование

кого опрашивать?



Анализ документации

журнал ТО

Проект

ЭД

проекта нет или утерян

- Технологический регламент
- Инструкции персонала
- Осмотр и документирование

Инструментальное обследование

Программа обследования

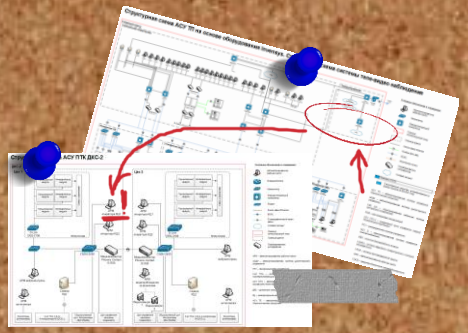
нельзя использовать стороннее ПО

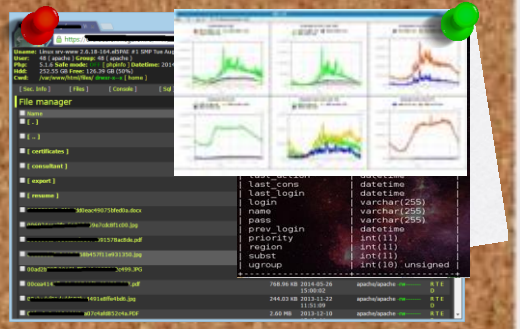
- Встроенные средства системного и прикладного ПО

Тестирование на проникновение

задачи

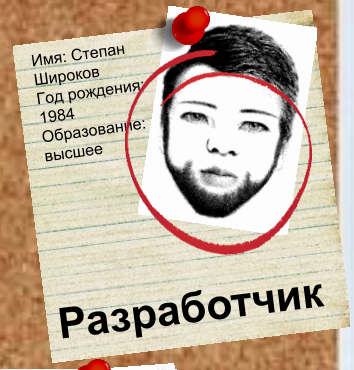
1. Разработка Программы и выбор инструментов





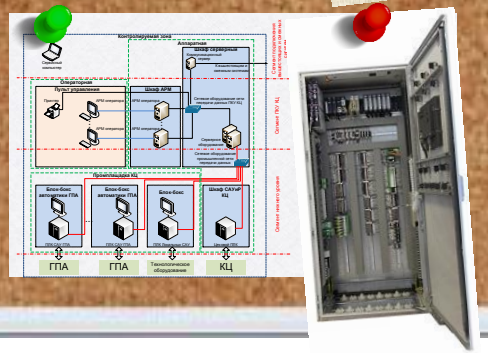
2. Проникновение в защищаемый сегмент

только **до границы** сегмента АСУ ТП



3. Демонстрация атак

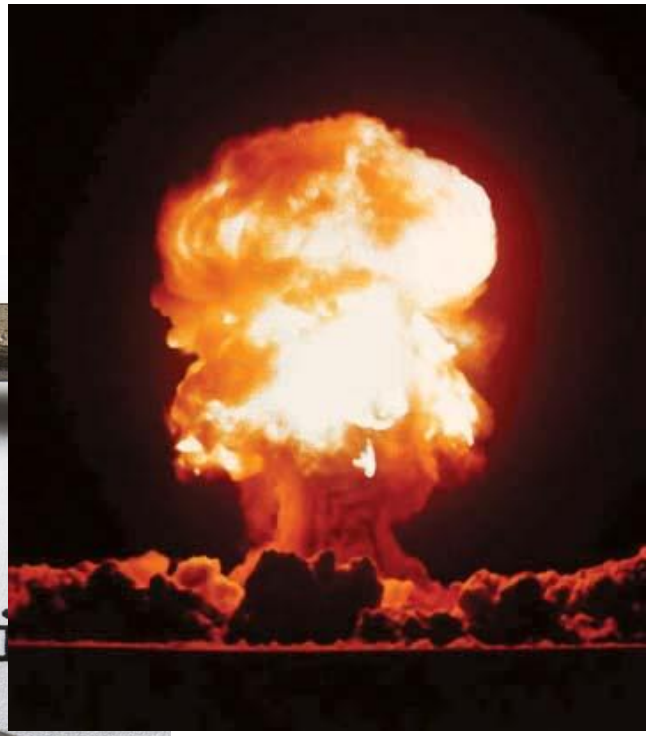
на стенде разработчика

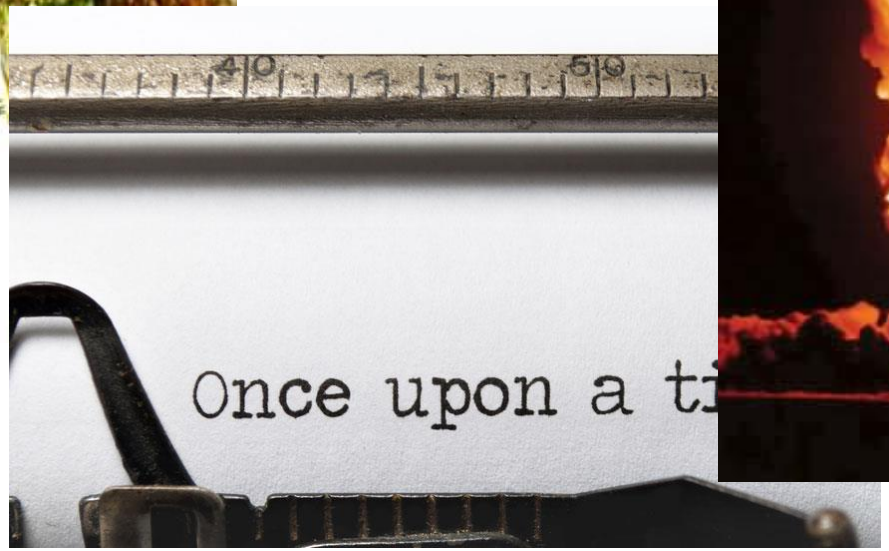


Моделирование угроз

Модель нарушителя

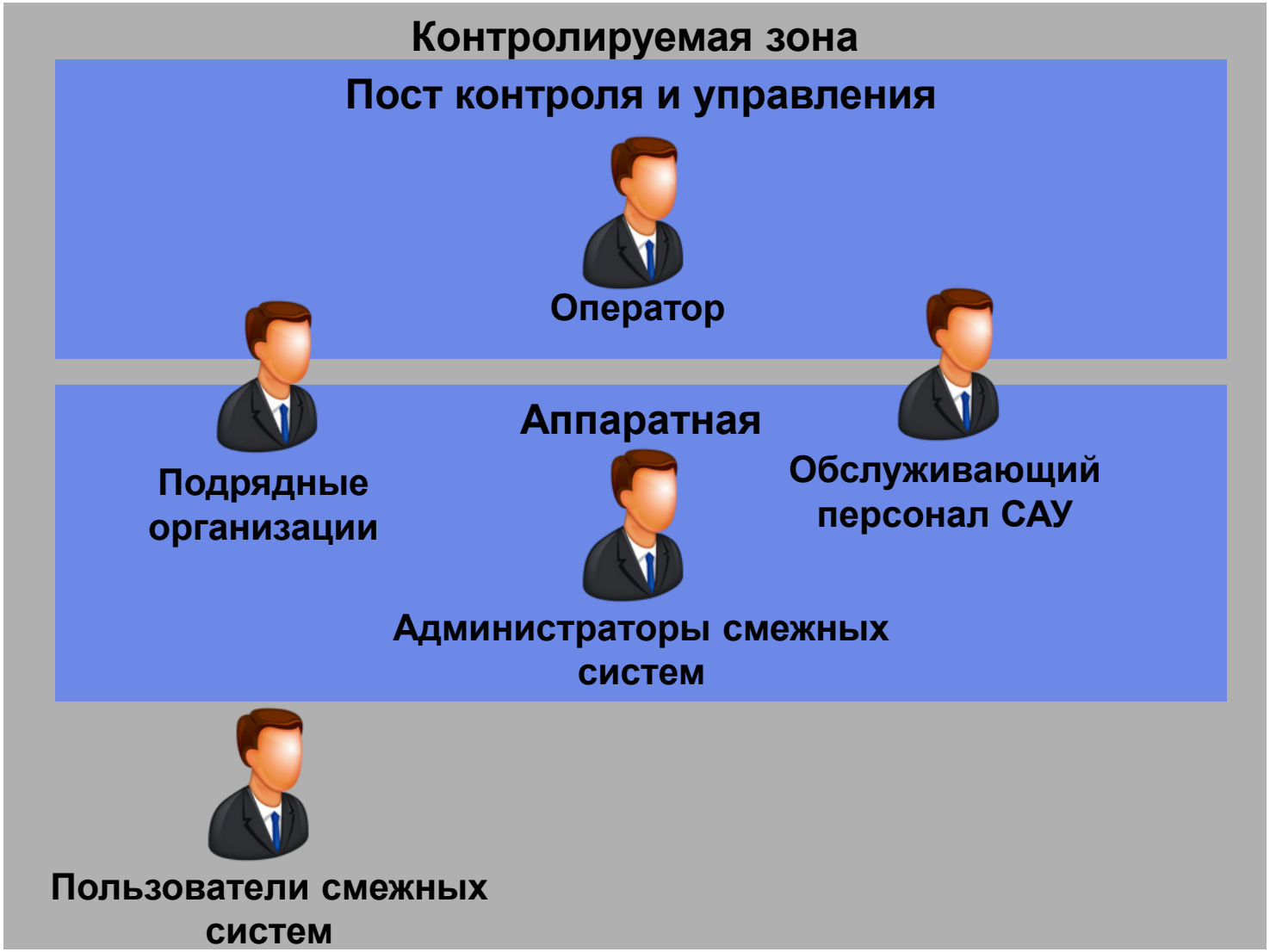
Оценка ущерба





Сценарии реализации

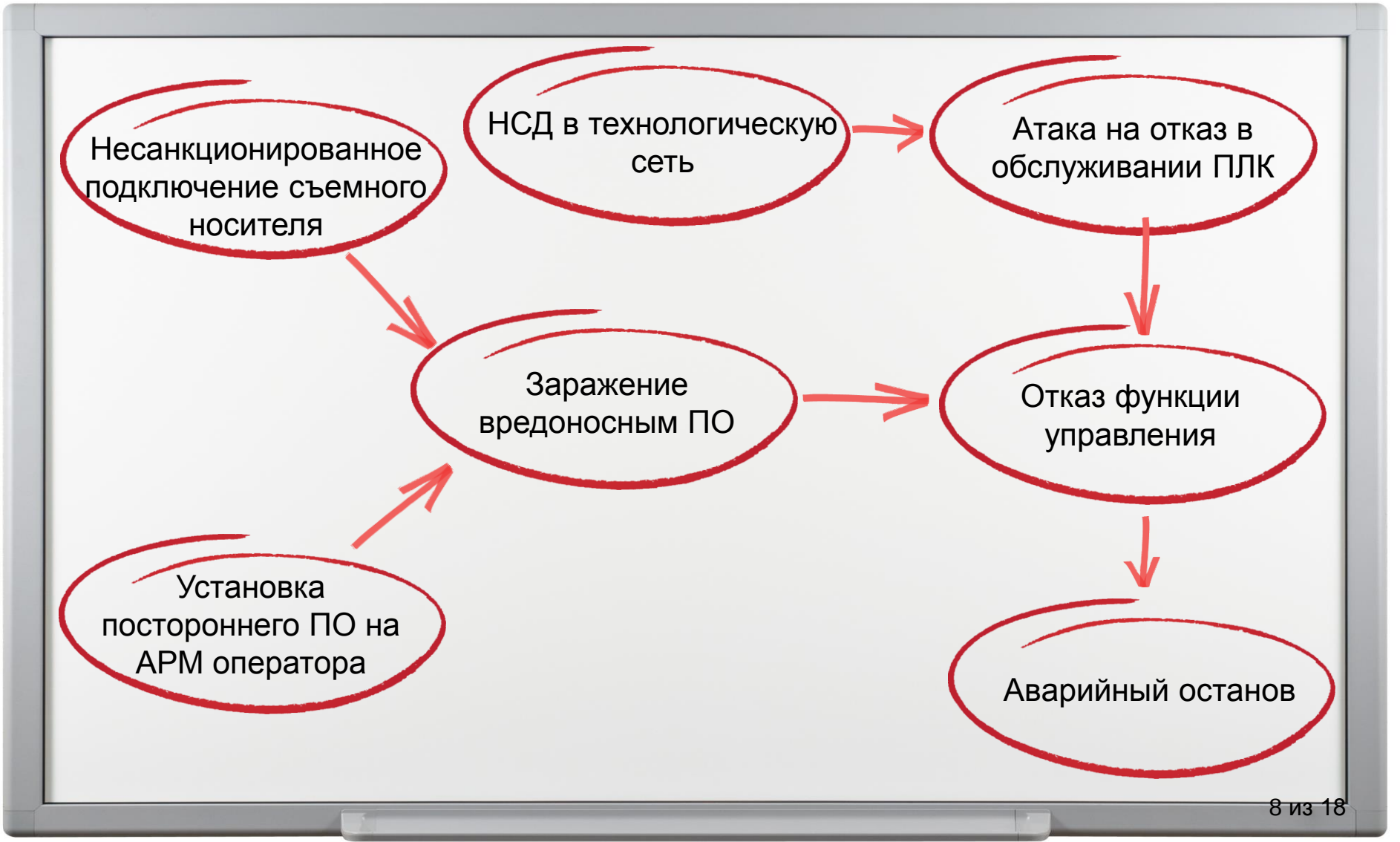
Модель нарушителя



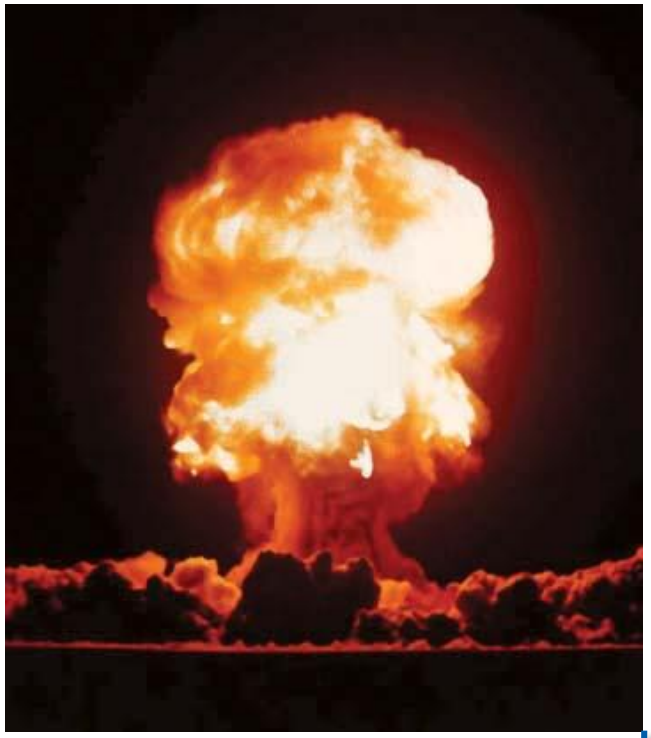
Сервисные организации

Преступные элементы

Сценарии реализации



Оценка ущерба



ИБ

ПБ

Представление результатов

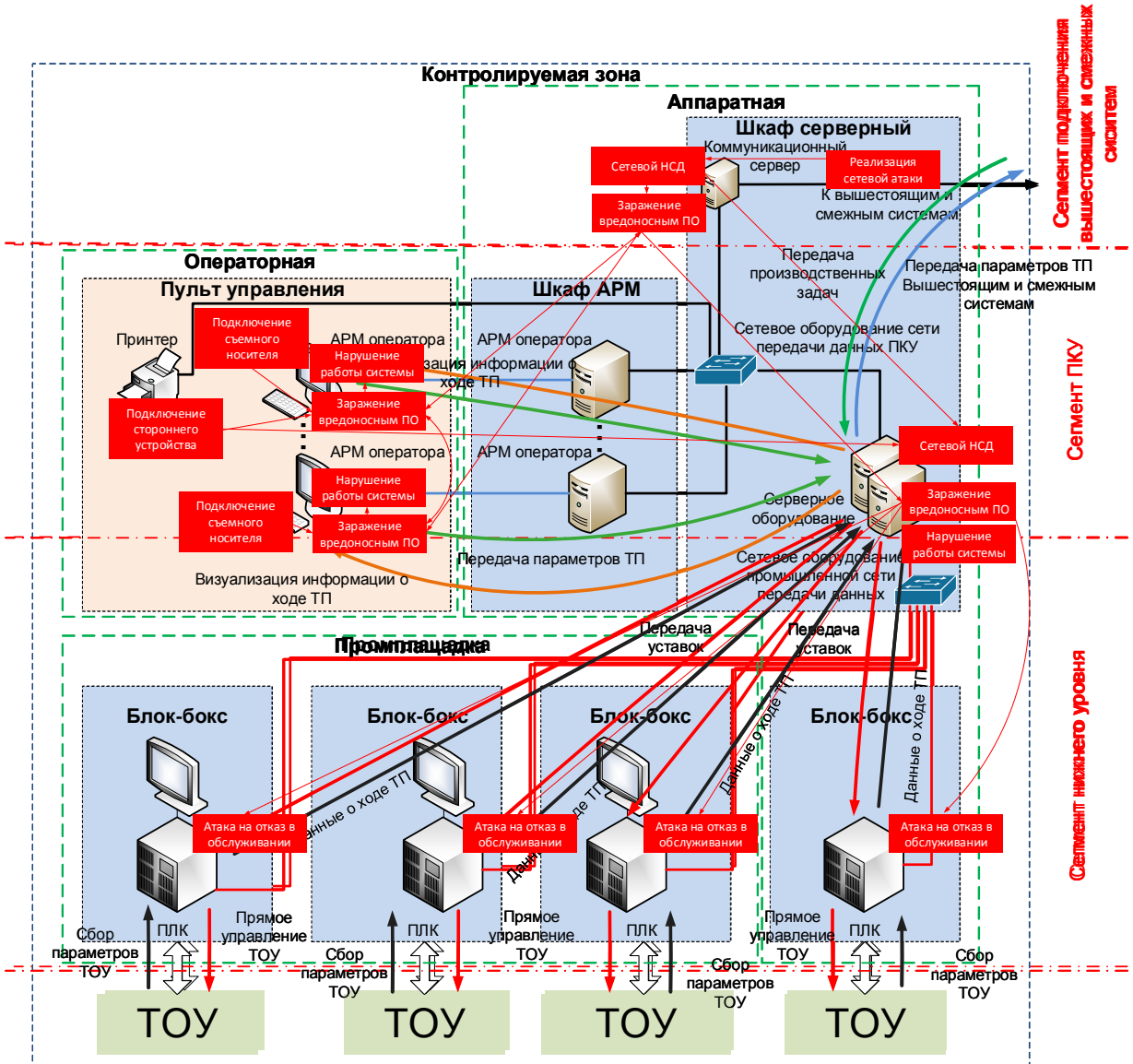


Схема структурная

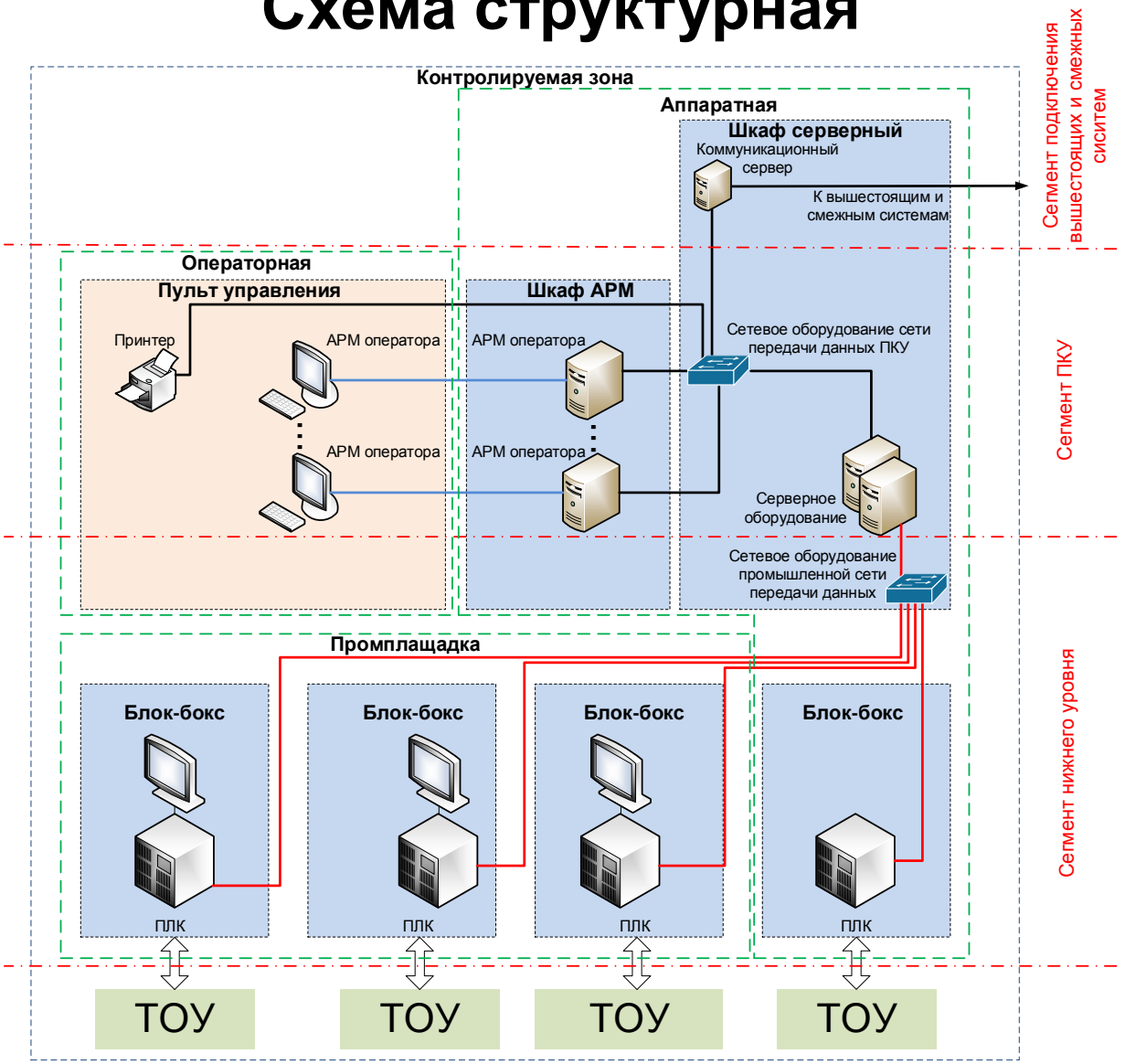
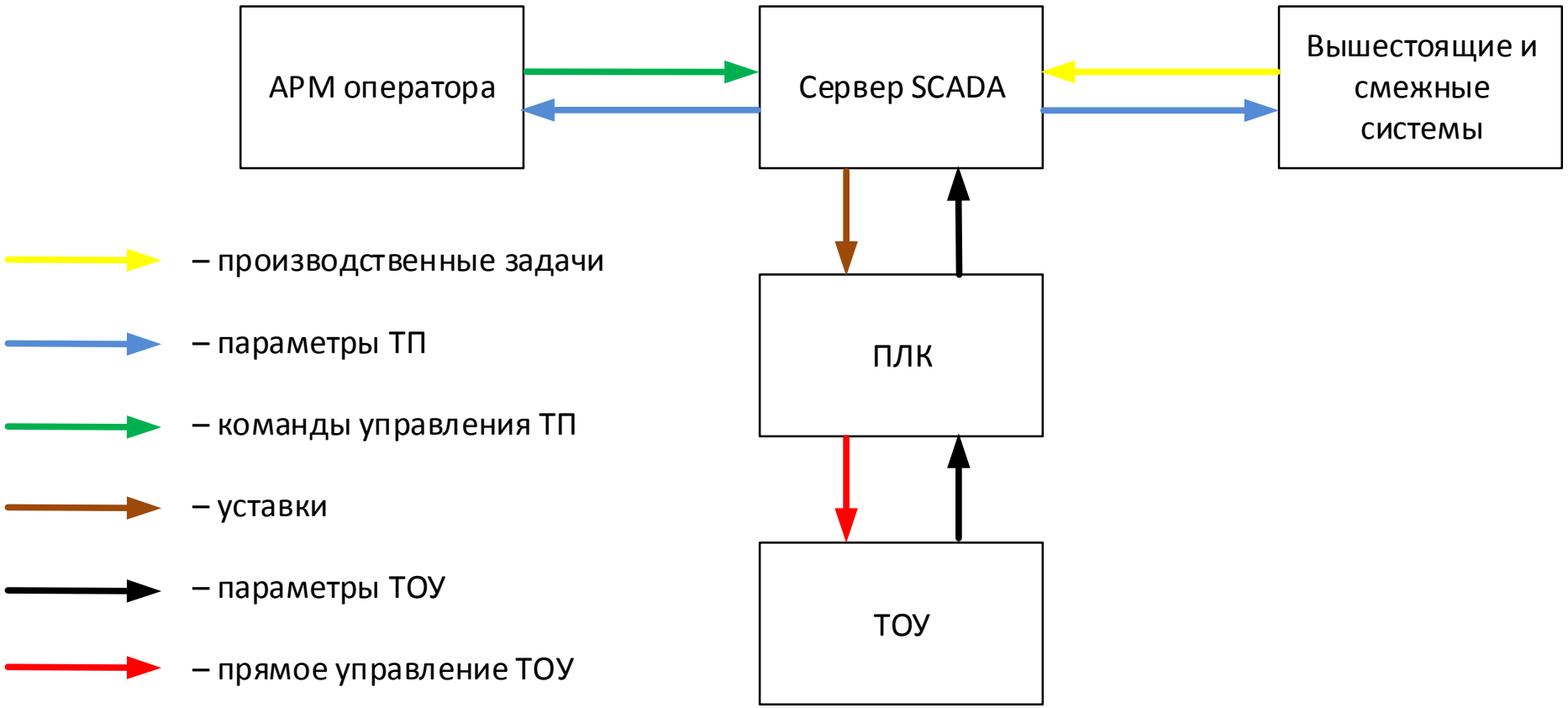
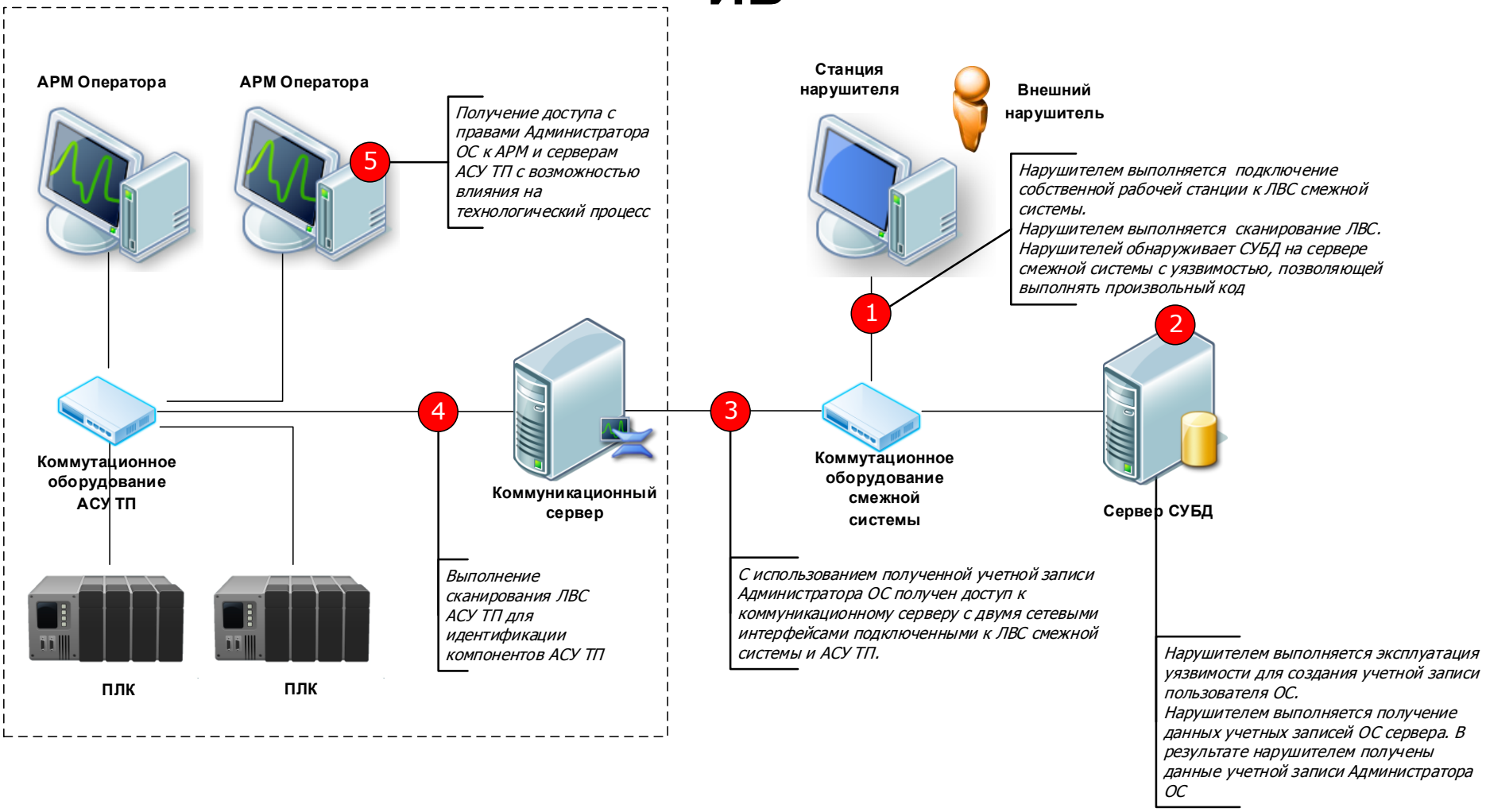


Схема функциональная



Визуализация сценариев реализации угроз ИБ

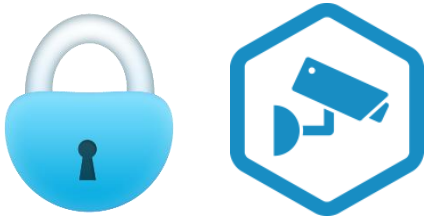


Результаты аудитов действующих АСУ ТП

1. В предприятиях металлургической отрасли и ТЭК
2. На более 30 производственных объектах
3. Включавших более 150 АСУ ТП

Организационные мероприятия

Технические меры защиты



Физическая безопасность

Технические меры защиты

Сетевая безопасность	• Обеспечивается для **88%** объектов • Для **17%** АСУ ТП есть удаленный доступ из корп. сети
Встроенные механизмы защиты	• HMI – аутентификация, режим киоска, ограничения доступа к меню • Системное ПО – по умолчанию • ПЛК – отключены
Антивирусная защита	• Применяется в **25%** АСУ ТП • Обновляется в **11%** АСУ ТП
Обновления	• Своевременные для **8%** АСУ ТП

Организационные мероприятия

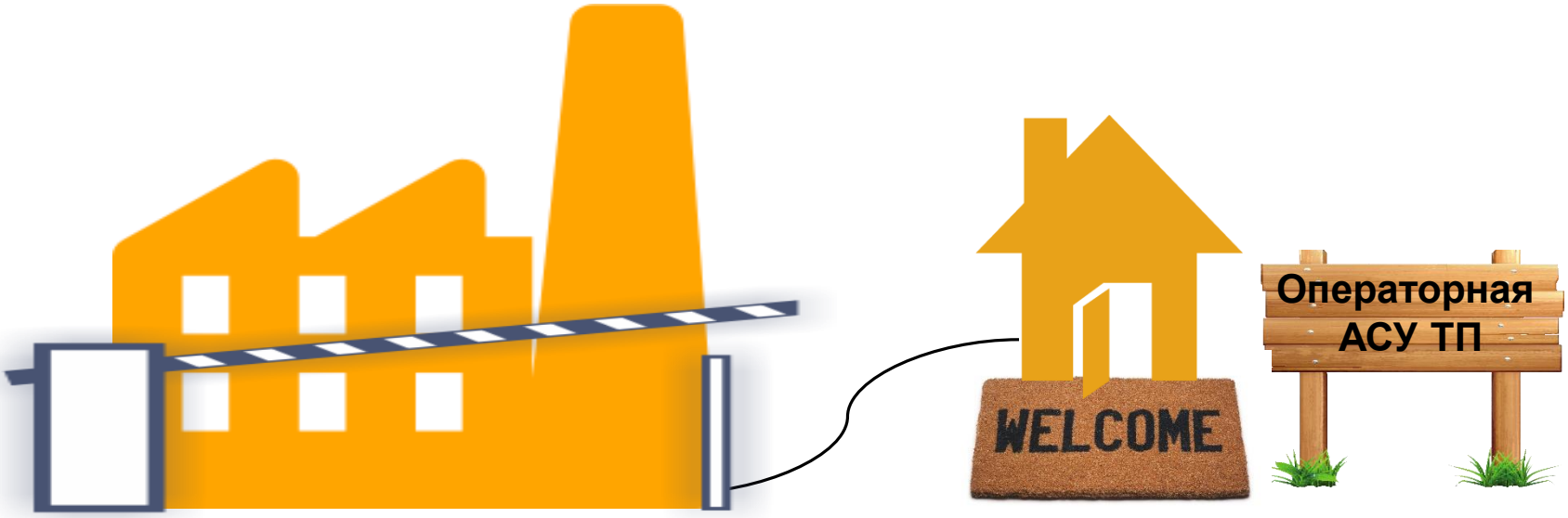
Организационно-распорядительная документация	• Присутствует у **100%** предприятий
Специалисты ИБ на производственных объектах	• Присутствуют на **15%** объектов
Контроль выполнения требований ИБ подрядчиками	• Не осуществляется

Физическая безопасность

Применяется комплекс мер физ. безопасности по причине:

- Требований законодательства
- Внутренних требований
- Рисков хищения продукции

Но бывает и так:



Благодарю за внимание!

Николай Домуховский

ООО «УЦСБ»
620100, Екатеринбург, ул. Ткачей, д.6
Тел.: +7 (343) 379-98-34
Факс: +7 (343) 382-05-63
info@ussc.ru
www.USSC.ru