ЭЛВИС-ПЛЮС

Нужны ли стенды АСУ ТП для обеспечения ИБ?

Изучайте технологии АСУ ТП при помощи стендов!

Стефанов Руслан
Руководитель направления защиты АСУ ТП
ОАО «ЭЛВИС-ПЛЮС»

2013 год

Аудиты нужны

Без аудита процесс обеспечения ИБ немыслим

✓Регулярная оценка уровня защищенности дает начальную точку и определяет вектор движения.

Но самоубийц нет! (проблема аудита)

Ни одно ответственное лицо не разрешит аудит с пен-тестами и инструментальными проверками на действующем объекте АСУ ТП, так как:

✓**Это лицо оценивает риски самого аудита выше рисков, выявляемых этим аудитом (Часто это правда!).**

Показать и убедить

В этом случае цель аудита: показать и при необходимости убедить ответственные лица в том, что их оценки и представления ошибочны и не соответствуют реальному положению вещей…

… либо подтвердить их верность ;)

Изучайте технологии и решения АСУ ТП

Проблема совместимости и обновлений

Действующие АСУ ТП в результате длительной проверки временем выглядят монолитными.

Установка обновлений и внедрение дополнительных решений ИБ вызывает обоснованные опасения.

✓**Необходимы доказательства работоспособности.**

Решение проблем

Невозможно выполнить аудит и предсказать последствия обновлений на действующем объекте, но …

✓можно все это сделать на копии действующего объекта (макете, стенде, модели).

ЭЛВИС-ПЛЮС

National SCADA Test Bed
Idaho National Laboratory (USA)

Цель:	**полномасштабное тестирование АСУТП в реальных условиях**
Статус:	**действует с 1949 года, ведутся ядерные программы, программы DoE, программы кибербезопасности**
Основные характеристики:	**38 кВ ВЛ (61 миля), 7 подстанций и другие сооружения в целом занимают 890 кв.миль в пустыне**

Источник: http://www.inl.gov/research/national-supervisory-control-and-data-acquisition-test-bed/

ЭЛВИС-ПЛЮС

ICS Sandbox (NSERC Canada) и другие…

Цель:	**моделирование атак реального мира на критическую инфраструктуру, обучение персонала правильным действиям в условиях данных атак и тестирование программного обеспечения**
Статус:	**стартовал в 2012 году**
Основные характеристики:	**около 100 устройств, включая серверы, рабочие станции, ПЛК, датчики, симуляторы и ПО SCADA**

Источник: RSA CONFERENCE 2013 (SAN FRANCISCO)
http://www.darkreading.com/vulnerability/scada-sandbox-tests-real-world-impact-of/240149728

ЭЛВИС-ПЛЮС

Лаборатории и стенды в России

Все российские компетентные органы (ФСБ, ФСТЭК, Минобороны) следят за работами по моделированию угроз ИБ АСУ ТП с использованием наглядных стендов и макетов, как за рубежом, так и в России.

Многие компании, производители и системные-интеграторы, а также научные и учебные заведения в России заинтересованы и/или проводят работы по созданию стендов для решения своих бизнес-задач.

Основной целью проводимых работ в данной области является понимание и демонстрация возможностей повторения описанных за рубежом атак на компоненты АСУ ТП различных производителей, применяемых в России.

Так они выглядят

SCADA Lab

INL

Training center

Power lines & substation Simulation

ЭЛВИС-ПЛЮС

Цели стендов

Какие же цели достигаются в направлении обеспечения ИБ?

✓ Для государства

Повышение обеспокоенности и осведомленности общества проблемами ИБ АСУ ТП (кибербезопасности)

✓ Для производителей решений АСУ ТП

Определение уровня защищенности их решений

✓ Для компаний операторов АСУ ТП

Выявление и определение угроз

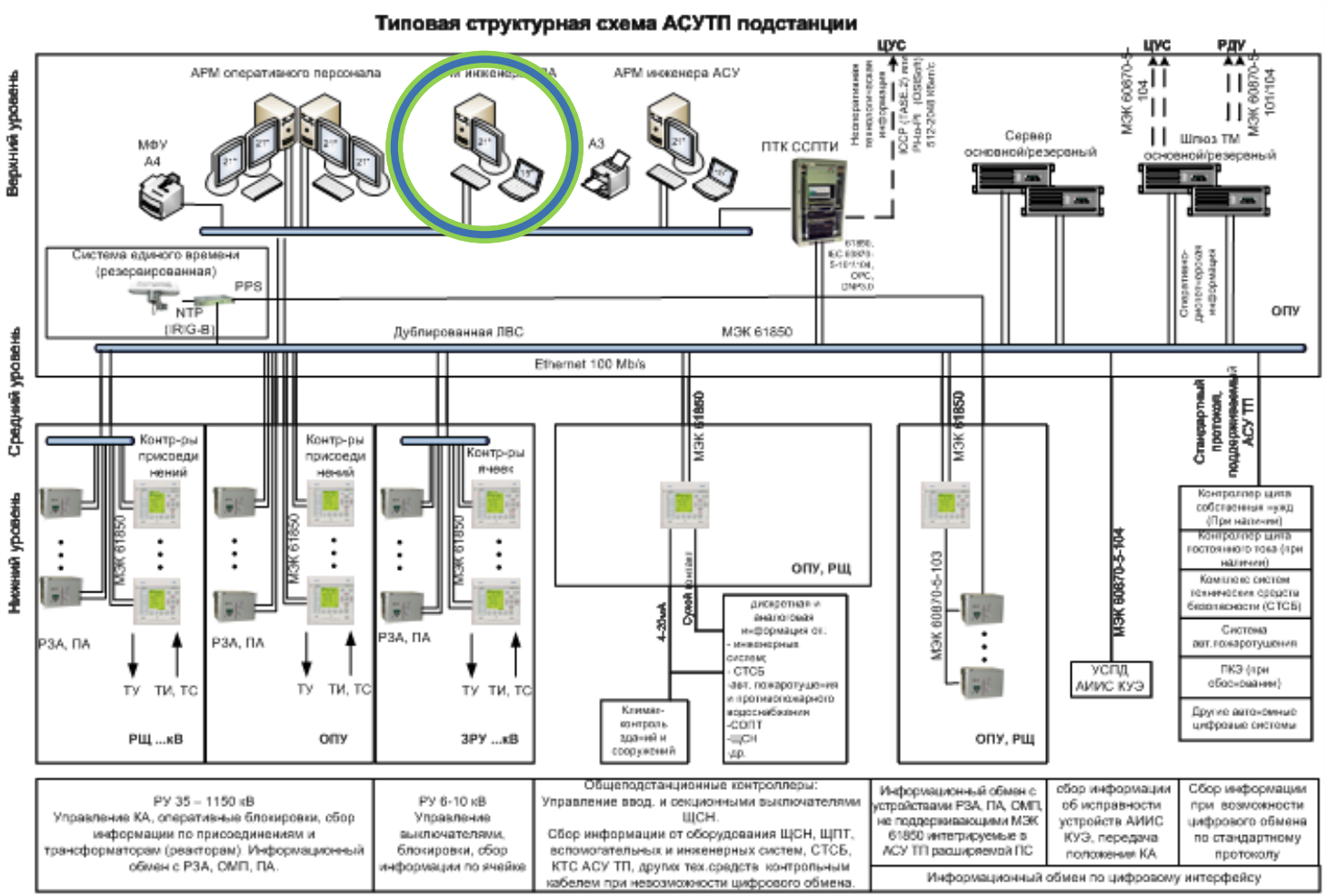
Повышение квалификации персонала в области ИБ

✓ Для компаний и исследователей ИБ

Поддержка разработки защищенных решении

Повышение компетенции и опыта исследователей

Архитектура стенда (минимальный вариант)



ЭЛВИС-ПЛЮС

Минимальный вариант. Плюсы и минусы.

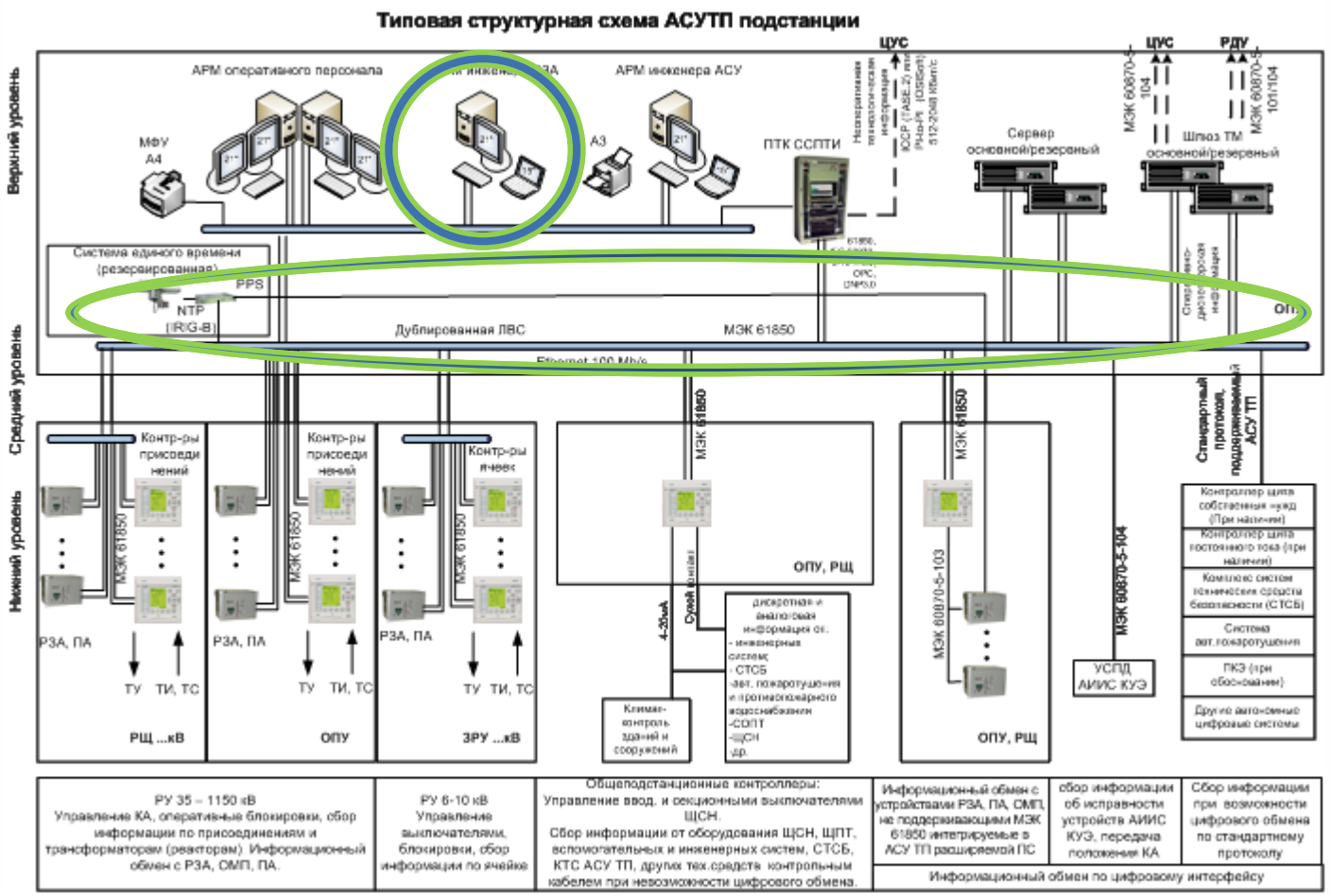
+	−
Реализовать макет может один человек в кратчайшие сроки Вероятность найти уязвимости в ПО высока Не требуются специальные знания в области АСУ ТП	Это не цельная система

Представляет интерес для исследователей и небольших производителей решений ИБ

Проблемы, которые надо решить

- **Собственно копирование**
  - ✓ **P2V (Physical to Virtual, VMWare Converter)**
    - Необходим административный пароль цели
    - Необходим сетевой (Ethernet) или физический доступ (USB)
    - Требуется временная установка агента
    - Необходимы вычислительные ресурсы цели
    - Длительная процедура для больших дисков
  - ✓ **Клонирование диска (Acronis TrueImage)**
    - Требуется перезагрузка
- **Восстановление в виртуальной среде**
  - Конфигурация ВМ, BIOS и прочее.
  - Защита ПО от копирования (лицензии и прочее)

Архитектура стенда (промежуточный вариант)



ЭЛВИС-ПЛЮС

Промежуточный вариант. Плюсы и минусы.

+	–
Небольшие затраты и сроки на реализацию	Это не цельная система
Позволяет моделировать сетевые угрозы (MITM, fuzzing)	Требуются некоторые знания в области АСУ ТП

Представляет интерес для исследователей и небольших производителей решений ИБ

ЭЛВИС-ПЛЮС

Проблемы, которые надо решить

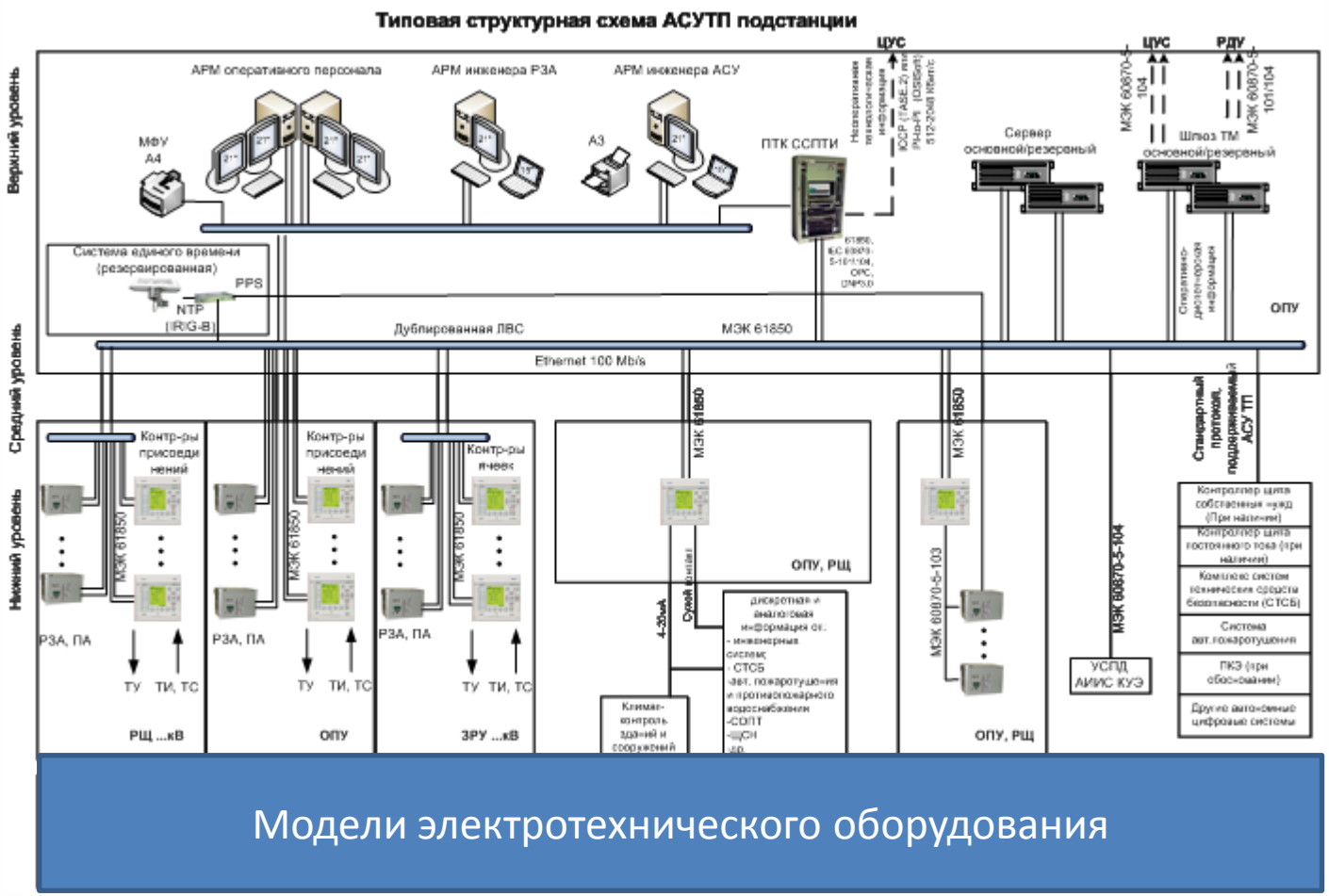
Имитация трафика

- ✓ **Откуда взять трафик похожий на реальный**
  - **Перехват снифферером на реальной системе**
  - **Моделирование**

Интеграция имитаторов с продуктами АСУ ТП

- **Знание паролей (сброс)**
- **Настройка параметров**

Архитектура стенда (максимальный вариант)



Модели электротехнического оборудования

ЭЛВИС-ПЛЮС

Максимальный вариант. Плюсы и минусы.

+	−
Максимально реалистичное моделирование	Дорогостоящее решение
Тестирование нештатных режимов	Требуется знание моделируемых физических процессов
Нулевой риск повреждения реального оборудования (физических устройств)	

Представляет интерес для крупных исследований в рамках государственных программ

ЭЛВИС-ПЛЮС

Проблемы, которые надо решить

- Интеграция моделей в единое и синхронное целое
- Разработка недостающих моделей
- Разработка программных адаптеров для цифровой и дискретной передачи сигналов
- Генерация сигналов в аналоговой форме

ЭЛВИС-ПЛЮС

Опыт компании ЭЛВИС-ПЛЮС

В рамках аудитов ЭЛВИС-ПЛЮС выполнял копирование и исследование (сканирование) отдельных программных компонент технологических систем.

ЭЛВИС-ПЛЮС провел исследования с привлечением ИСП РАН для оценки возможностей создания подобных стендов.

В настоящее время в ЭЛВИС-ПЛЮС подготовлено ТЗ на разработку максимального варианта стенда для исследования вопросов защиты АСУ ТП.

ЭЛВИС-ПЛЮС

Макетирование компонентов стенда

Пакет CERTI
Библиотека общей памяти ФГУП ГосНИИАС
Пакеты Labview, Matlab, SciCos Simulink
Языки программирования C, C++, Python, Perl, Ruby
Библиотека libpcap
Протокол ModbusTCP, IEC 60870-50104

Макетирование инфраструктуры стенда (сервер, АРМ, ПЛК, сетевые устройства)

Макетирование подключения моделей к инфраструктуре

Макетирование моделей технологического оборудования (электротехнического и др.)

Макетирование анализаторов сетевого трафика с целью определения корректности трафика

Макетирование имитаторов сетевой нагрузки с целью имитации встречной стороны клиент-серверного взаимодействия

Какие же выгоды?

Развитие исследований ИБ АСУ ТП

Создание проверенных решений ИБ АСУ ТП

Повышение квалификации специалистов ИБ АСУ ТП

Что еще?

Ваши вопросы?

Стефанов Руслан