Практика выбора и реализации мер защиты АСУ ТП в соответствии с приказом №31 ФСТЭК России

Стефанов Руслан
руководитель направления защиты АСУ ТП
АО «ЭЛВИС-ПЛЮС»

ЭЛВИС-ПЛЮС

Приказ ФСТЭК №31

Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 14 марта 2014 г. N 31 г. Москва

Вступил в действие 17 августа 2014 года

"Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды"

Зарубежные источники разработки приказа ФСТЭК №31

В основе мер защиты приказов ФСТЭК №17, №21 и №31:

- NIST SP 800-53 rev.3

Если нужно понимание мер защиты в упомянутых приказах обращайтесь к первоисточникам

Для понимания объекта защиты, угроз и мер защиты

- NIST SP 800-82

Для понимания того, что ждет нас в будущем ☺:

- NIST SP 800-53 rev.4

И еще важный стандарт

- IEC-62443 (ранее ISA-99)

Этапы защиты

- Формирование требований – (цель аудита АСУ ТП)
- Разработка системы защиты АСУ ТП
- Внедрение системы защиты АСУ ТП
- Обеспечение защиты в ходе эксплуатации
- Обеспечение защиты при выводе из эксплуатации

Формирование требований

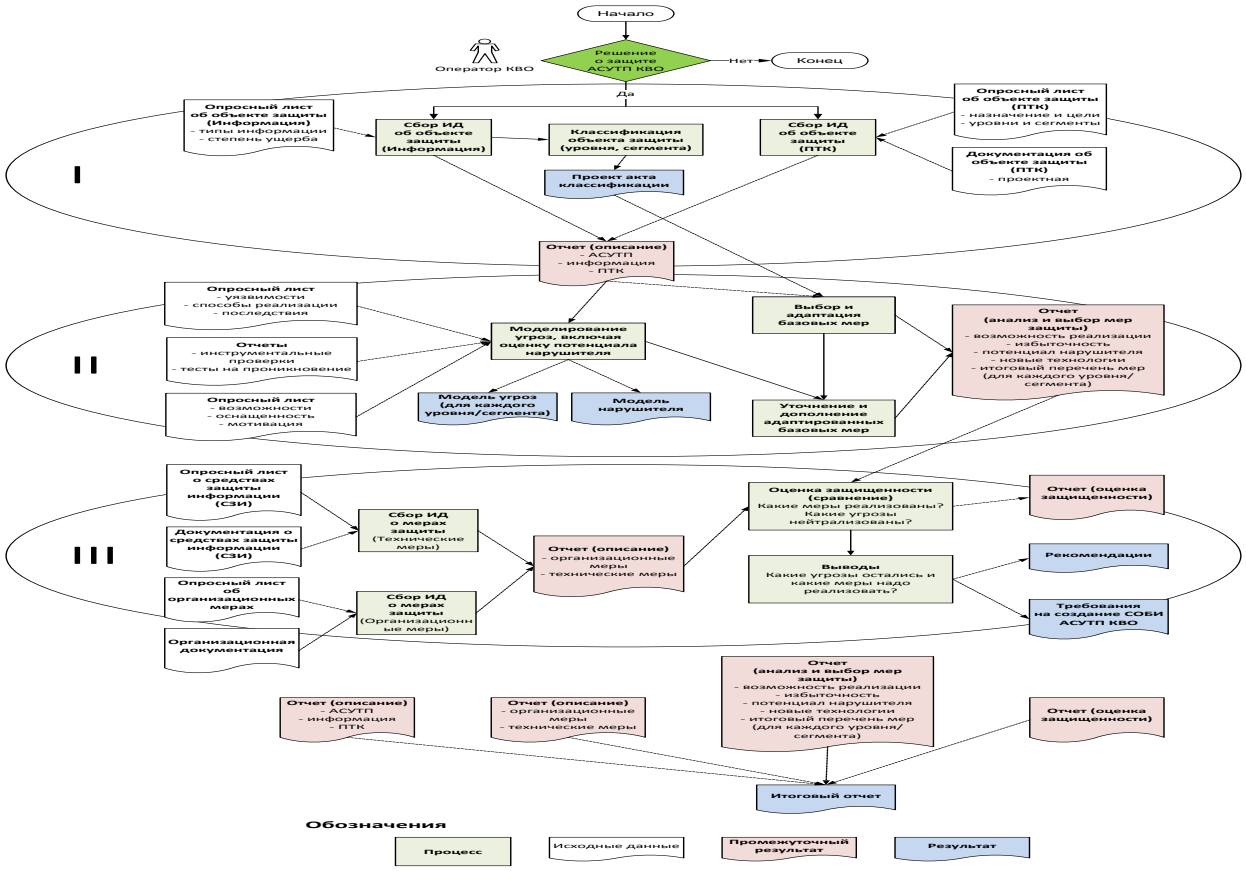
(в рамках аудита)

- *Принятие решения о необходимости защиты информации (отв. Заказчик: формирование бюджета, объявление конкурса на аудит АСУ ТП)*
- **Классификация АСУ ТП по требованиям защиты информации (отв. Заказчик: оформляет акты классификации, мы помогаем: проектами актов классификации и обоснованием)**
- **Определение угроз безопасности информации (отв. Исполнитель: МУ и МН)**
- **Определение требований к системе защиты (отв. Исполнитель: ТЗ)**

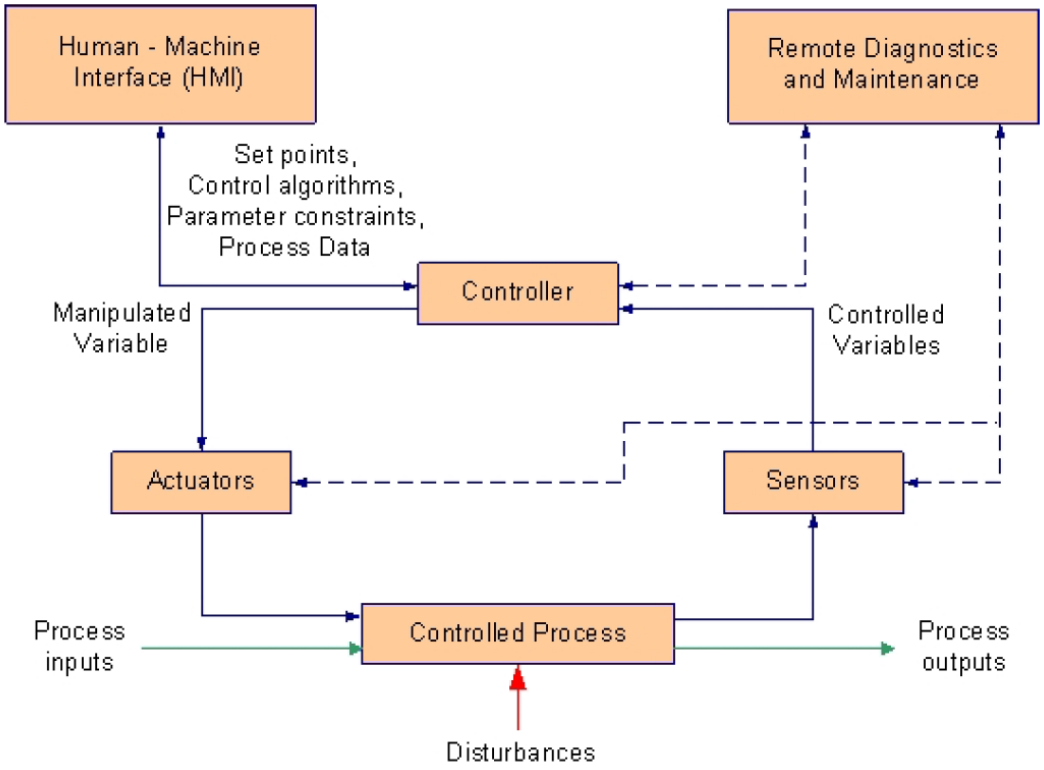
ЭЛВИС-ПЛЮС

Алгоритм аудита АСУ ТП

(статья в Connect №10, 2014)



Процесс управления технологическим процессом (см. теорию управления)



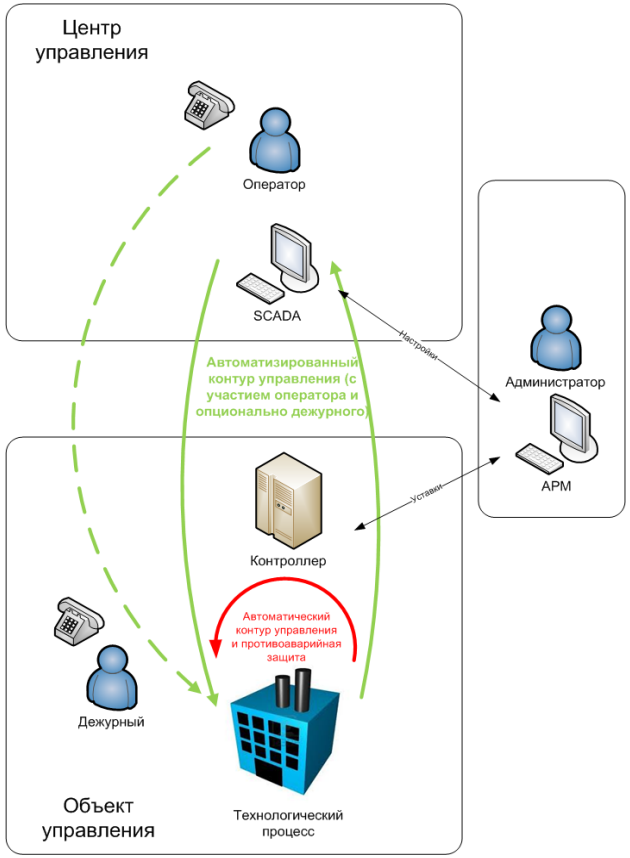
Автоматический и автоматизированный контуры управления

Контуры управления

- Автоматизированный (с участием человека) – секунды, минуты, часы
- Автоматический (без участия человека) – миллисекунды

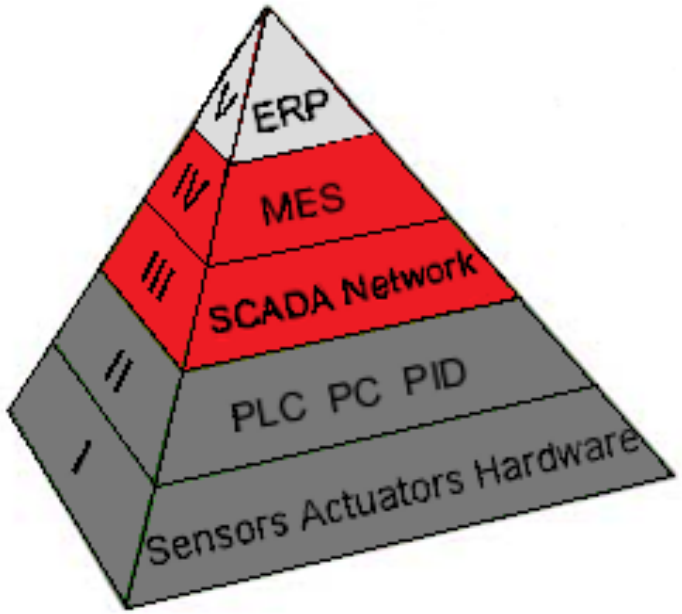
Информационные потоки (внутр и внеш)

- «Снизу-вверх» (измерения, сигнализация)
- «Сверху-вниз» (управление)
- «Административные» (уставки, настройки)
- «Горизонтальные» (между организациями)
- «Вертикальные» (между уровнями)



Иерархия АСУ ТП (приказ ФСТЭК №31)

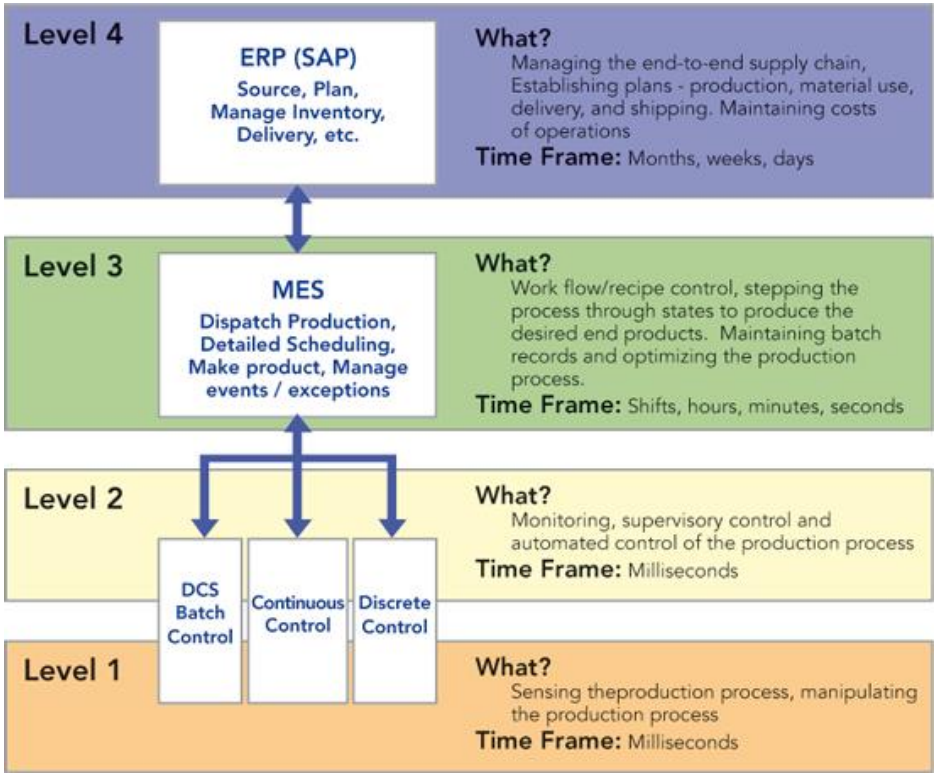
- V – уровень планирования (нет в приказе)
- IV – уровень управления производством (нет в приказе)
- **III – уровень операторского (диспетчерского) управления**
- **II – уровень автоматического управления**
- **I – полевой уровень**



Иерархия АСУ ТП (ISA-95/ISA-88)

(для информации)

Level 4	ERP	Business Planning, Human Resources, Accounting & Finance
Level 3	OM&I	Operations Management & Intelligence
Level 2	SCADA	Monitoring and Supervisory Control
Level 1	Sensors	Sensors and measurements from Operations and Field Devices
Level 0	Operations	



Виды АСУ ТП

АСУ ТП (интересует, как объект защиты - ПТК и информация в нем обрабатываемая)

- SCADA (supervisory control and data acquisition)
- DCS (distributed control system)
- PLC (programmable logic controllers)
- Противоаварийная защита (safety system)

Не совсем АСУ ТП (интересует, как возможные объекты защиты)

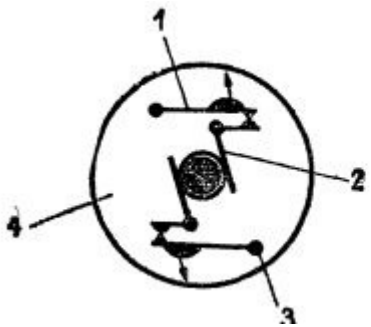
- Системы учета (электроэнергии, нефтепродуктов, ресурсов и материалов технологического процесса)
- Системы верхнего уровня управления предприятием (поддержка принятия решений, управление производством, планирование ресурсов)

Совсем не АСУ ТП (интересуют, как плацдарм для угроз)

- Корпоративные системы и сервисы
- Инженерные системы (например, пожарная сигнализация)

Safety System (противоаварийная защита)

Физическая реализация

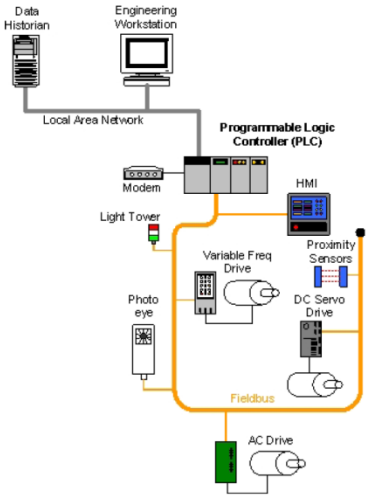


Релейная реализация

Рис. 1 . Эскиз центробежного выключателя:

1 — пружинный контакт; *2* — токосъемник; *3* — точки, соединенные с обмоткой ротора; *4* — диск, вращающийся вместе с ротором

Микропроцессорная реализация



Рекомендация

При разработке ТЗ на Аудит необходимо указывать:

- перечень АСУ ТП
- краткое описание АСУ ТП
- количественный состав компонентов программно-технического комплекса (серверы, АРМ, ПЛК, сетевые устройства)

Перечень и описание компонентов ПТК для каждого уровня/сегмента

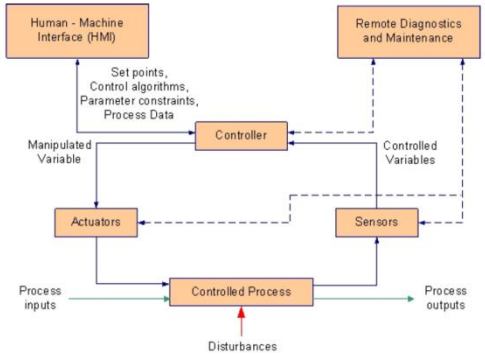
№	Название компонента	Реализуемый функциональный блок	Место монтажа	Краткое описание
Исполнительные устройства				
1	ЭПК	Отдельные компоненты	Кабина локомотива	Электропневматический клапан (ЭПК) – исполнительное устройство, предназначенное для подачи машинисту предупредительного сигнала о необходимости торможения и экстренного торможения поезда. Содержит механические элементы и электрический магнит. Электронные компоненты отсутствуют. Пример внешнего вида представлен на рисунке (см. ПРИЛОЖЕНИЕ А). Более подробное описание содержится в [1], [2], [3].
Измерительные устройства				
4	Носимое устройство ТСКБМ (ТСКБМ-Н)	Контроль бодрствования машиниста	Запястье машиниста	Прибор ТСКБМ-Н – измерительное устройство, предназначенное для получения информации об относительном изменении электрического сопротивления кожи и передачи ее по радиоканалу в цифровом виде на приемник ТСКБМ-П. Представляет собой телеметрический датчик, располагающийся на запястье машиниста, и содержит электроды для измерения сопротивления кожи, электронную схему и элемент электропитания. Детальная информация (элементная база, принципиальная схема) об электронной схеме отсутствует. Пример внешнего вида представлен на рисунке (см. ПРИЛОЖЕНИЕ А). Более подробное описание содержится в [9], [10], [11], [12].

Виды информации

Содержится и обрабатывается в АСУ ТП в рамках технологического процесса (автоматический контур управления):

- Измерительная, сигнализирующая (быстро меняется)
- Управляющая (быстро меняется)

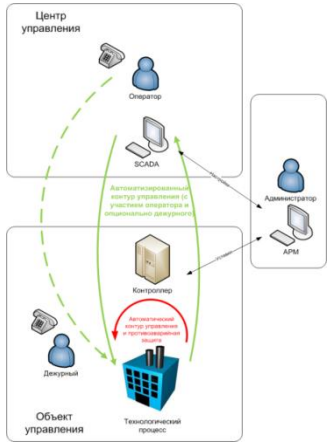
(защита конфиденциальности не актуальна)



Содержится, но не обрабатывается в АСУ ТП в рамках технологического процесса:

- Административная - модели, уставки, настройки (медленно меняется)

(защита конфиденциальности может потребоваться)



Содержится и обрабатывается пользовательская информация в рамках автоматизированного контура управления:

- Вводимая пользователем (входная)
- Отображаемая пользователю (выходная)

Классификация АСУ ТП

(по уровню значимости, степени ущерба)

Исходные данные:

- Паспорт КВО
- Декларация промышленной безопасности
- Технологический регламент
- Учет технологических нарушений

Ориентир оценки ущерба:

Постановление Правительства Российской Федерации от 21 мая 2007 г. N 304 г. Москва

"О классификации чрезвычайных ситуаций природного и техногенного характера"

№	Вид информации	Уровень	Целостность	Доступность	Конфиденциальность
Управляющая (выходная) информация					
1	Команда на открытие вентиля принудительной остановки ЭПК (ЭПВ 266)	1, 2	Средний уровень ущерба	Средний уровень ущерба	Защита не требуется
Измерительная (входная) информация					
3	Состояние выходных ключей (коммутируемых цепей).	2	Средний уровень ущерба	Средний уровень ущерба	Защита не требуется
Параметры (уставки) и вспомогательная информация АСУ					
9	Команды изменения режима работы модуля БС-ДПС	2	Низкий уровень ущерба	Низкий уровень ущерба	Защита не требуется
Вводимая пользователем (входная) информация АСУ					
18	Информация о состоянии бодрствования машиниста	3	Низкий уровень ущерба	Низкий уровень ущерба	Защита не требуется

Моделирование угроз

- Методика ФСТЭК КСИИ (см. Информационное сообщение от 25.07.2014) – сложно применима на практике
  - «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры»
  - «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры»
- ЭЛВИС-ПЛЮС имеет свои наработки
- Опубликован в мае 2015 проект Методики определения УБИ в ИС для ГИС (ФСТЭК)
- Угрозы определяет эксперт (человек)
- Кроме угроз МУ содержит описание АСУ ТП
- Описываются угрозы для каждого уровня АСУ ТП

Угроза доступа к включенным КИПиА (программируемым расходомерам) и ПЛК (пример)

Параметр	Описание
Описание угрозы	Угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по-умолчанию» дискредитируемого объекта защиты или подбора пароля. Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учётные записи «по-умолчанию», предназначенные для первичного входа в систему. Более того, на многих устройствах идентификационная и аутентификационная информация может быть возвращена к заданной «по-умолчанию» после проведения аппаратного сброса параметров системы (функция Reset). Реализация данной угрозы возможна при одном из следующих условий: – наличие у нарушителя сведений о производителе/модели объекта защиты и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по-умолчанию» для объекта защиты; – успешное завершение нарушителем процедуры выявления данной информации в ходе анализа программного кода дискредитируемого объекта защиты.
Источники угрозы	Внутренний нарушитель с низким потенциалом
Объект воздействия	Средства защиты информации, системное программное обеспечение, сетевое ПО, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты
Последствия реализации угрозы	Нарушение целостности Нарушение доступности

Выбор мер защиты (применимые и реализованные меры защиты)

Не все меры применимы к данной АСУ ТП на данном уровне

Внимание на реализованные меры (могут отсутствовать в приказе ФСТЭК №31, но их можно учесть при аудите):

- встроенные в АСУ ТП функции безопасности (информационной и функциональной)
- наложенные на АСУ ТП средства защиты информации
- другие меры физической и функциональной безопасности

Эмпирическое правило определения типа меры:

- Если: В информационной системе…, то: мера – техническая
- Если: Оператором …, то: мера – организационная

Таблица анализа мер защиты

Код меры	Меры защиты информации	Реализация				Адаптированный состав требуемых мер (с учетом класса защищенности)				Уточненный состав требуемых мер (с учетом Модели угроз и иных документов)			
		Меры защиты уровня			Способ реализации	Уровень АСУ ТП			Обоснование применимости	Уровень АСУ ТП			Обоснование дополнительных мер
		1	2	3		1	2	3		1	2	3	
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)													
ИАФ.0	Разработка правил и процедур (политик) идентификации и аутентификации субъектов доступа и объектов доступа	-	-	-		+	+	+		+*	+*	+*	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	-	-	+	ТМ: Средствами ОС MS Windows для АРМ операторов, инженеров и серверов Experion, а также средствами ПО Experion при доступе к консоли	-	-	+	АСУ ТП ЭЛОУ-АВТ-12 уровня 1 и 2 является автоматической и не имеет пользователей, поэтому меры защиты, подразумевающие их наличие, не применимы.	-	-	+	
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	-	-	-	ТМ: Реализована только идентификация устройств (по DNS имени, IP-адресу). Аутентификация устройств отсутствует	+	+	+	Требуется идентификация/аутентификация всех используемых устройств для исключения возможности их подмены	+*	+*	+*	

Итоговый набор мер защиты (пример из опыта)

Пример по одному из аудитов:

- Реализовать организационных мер – 55
- Реализовать технических мер – 12 (ИАФ.2, УПД.3, ЗНИ.5, ЗНИ.7, РСБ.2, РСБ.3, РСБ.4, РСБ.7, АВЗ.1, ОЦЛ.1, ЗИС.11, ЗИС.15)
- Реализовать усиления технических мер – 2 (усиление ЗТС.2 и ЗТС.3)
- Общее количество мер приказа №31 – 167

Статистика

- Доля организационных мер – 33%
- Доля технических мер – 7%

Решения для реализации мер

ИАФ.2, ЗИС.11 – NAC

УПД.3 – МЭ

ЗНИ.5, ЗНИ.7 – контроль сменных носителей

РСБ.2, РСБ.3, РСБ.4, РСБ.7 – SIEM

АВЗ.1 – антивирусная защита

ОЦЛ.1 – контроль целостности ПО

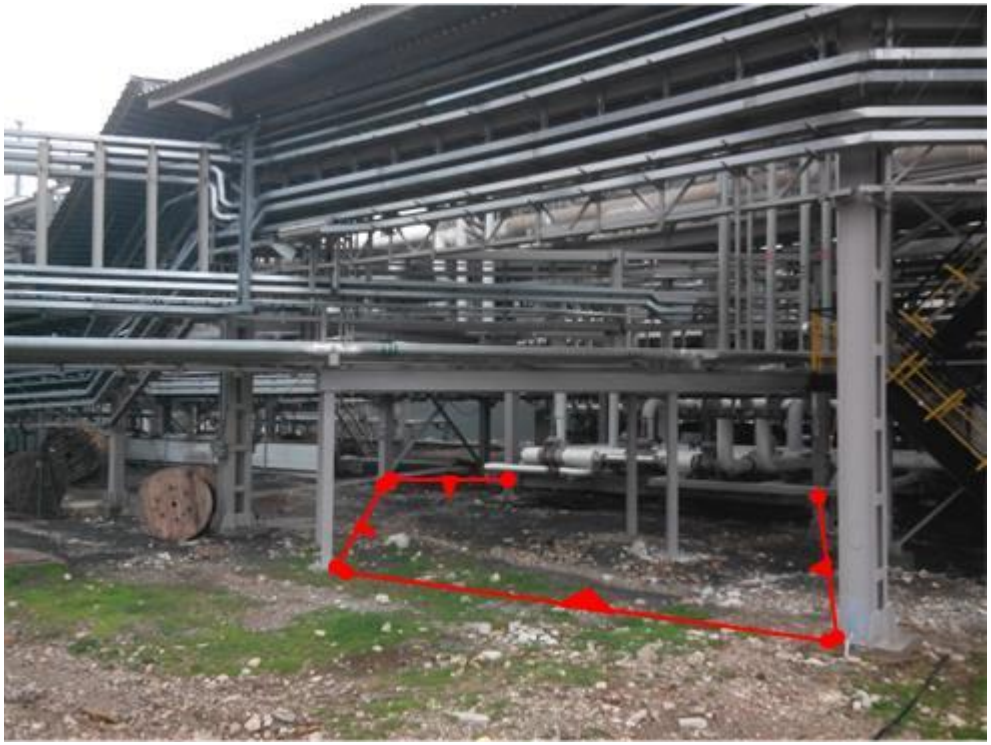
ЗИС.15 – резервное копирование

Усиление ЗТС.2 и ЗТС.3 – видеонаблюдение и контроль доступа

Видеонаблюдение и контроль физического доступа

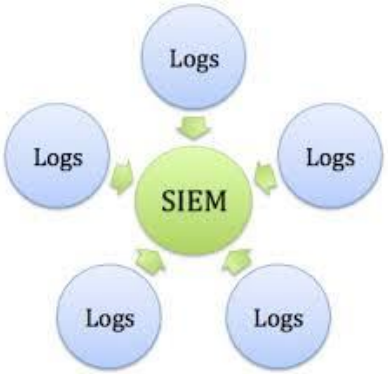
Решение 1: виртуальный периметр расходомера

Проблема: угрозы непосредственного доступа к компонентам (расходомеры, запорная арматура), физический доступ к которым нельзя ограничивать



Регистрация событий безопасности (SIEM КС ИБ)

Решение 2: контроль состояния запорной арматуры (электронная пломбировка)

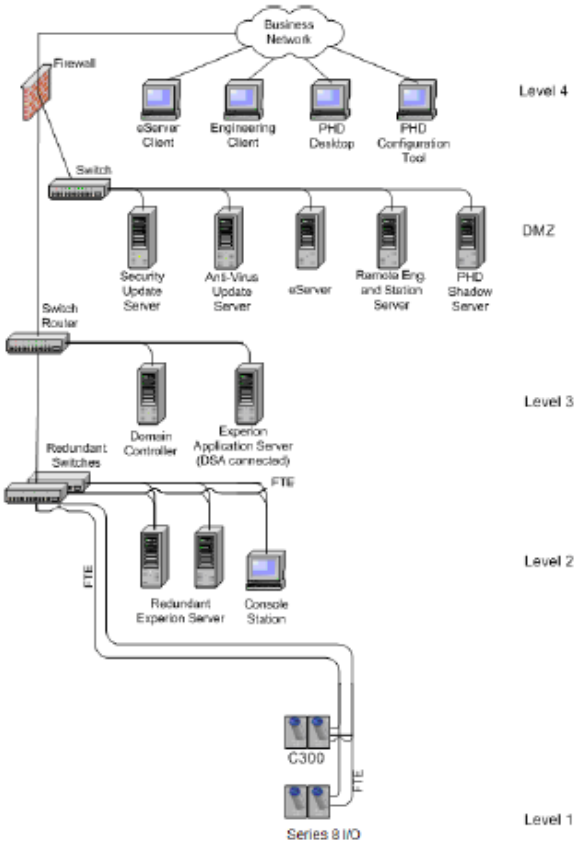


Создание КС ИБ АСУ ТП

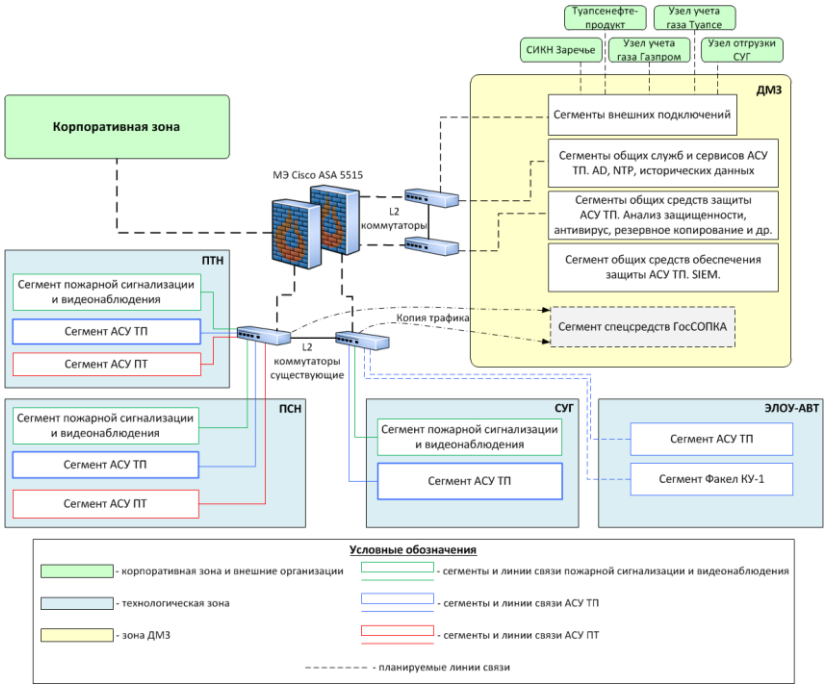
- Разрабатываем проект комплексной системы (в соответствии с рекомендациями производителей и НПА РФ)
  - Виртуальная среда
  - Технологическая ДМЗ
  - Резервное копирование
  - Единый сервер времени
  - Антивирусная защита и другие подсистемы
  - Интеграция с КСБ
  - ГосСОПКА

Целевая архитектура КС ИБ АСУ ТП (пример)

Рекомендации Honeywell



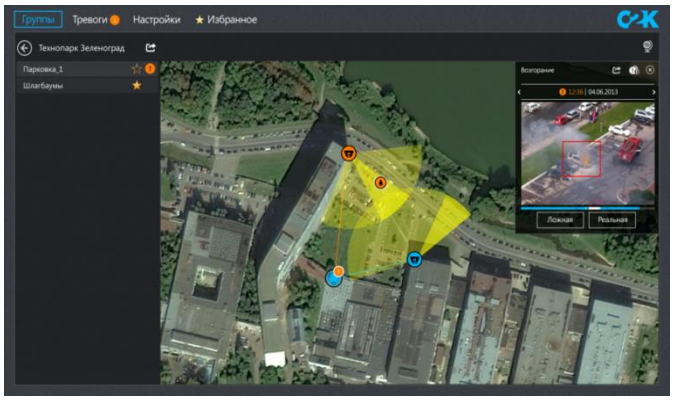
Решение ЭЛВИС-ПЛЮС

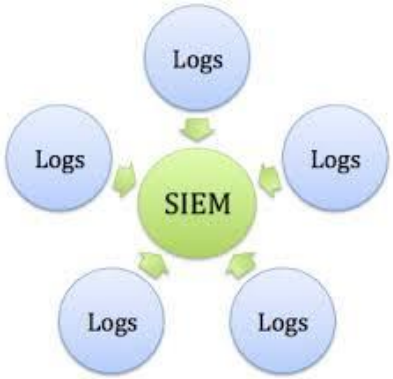


Интеграция КС ИБ с КСБ

Вариант применения:

- Передача событий КСБ (видеоаналитика, сигнализация) в КС ИБ (SIEM) и наоборот



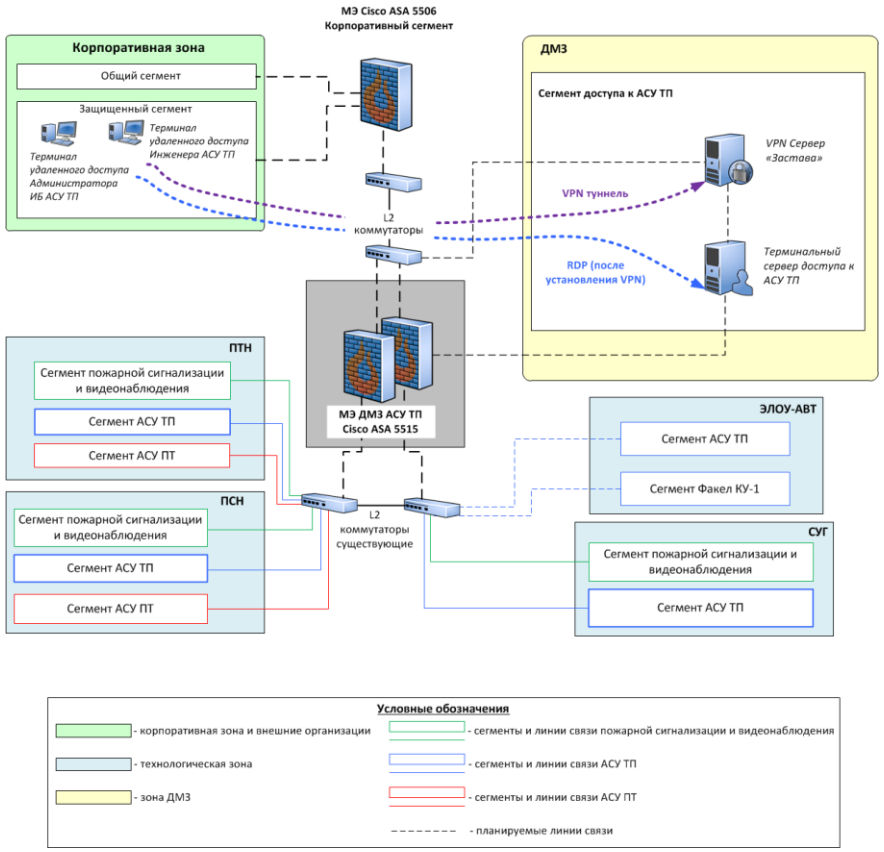


- Открытие/закрытие арматуры
- Нарушение виртуального периметра
- Обнаружение компьютерных атак/инцидентов/подозрительной активности

Защищенный сегмент службы АСУ ТП

Проблема: инженерам АСУ ТП необходимо выполнять свои обязанности по всей территории объекта, протяженность которого может быть большой, что отрицательно влияет на производительность труда

Решение ЭЛВИС-ПЛЮС



Защищенный сегмент метрологической службы

- Выделенное защищенное рабочее место администратора ИБ (тонкий клиент + VPN клиент)
- Выделенное защищенное рабочее место инженера АСУ ТП (тонкий клиент + VPN клиент)
- Возможна аттестация защищенного рабочего места

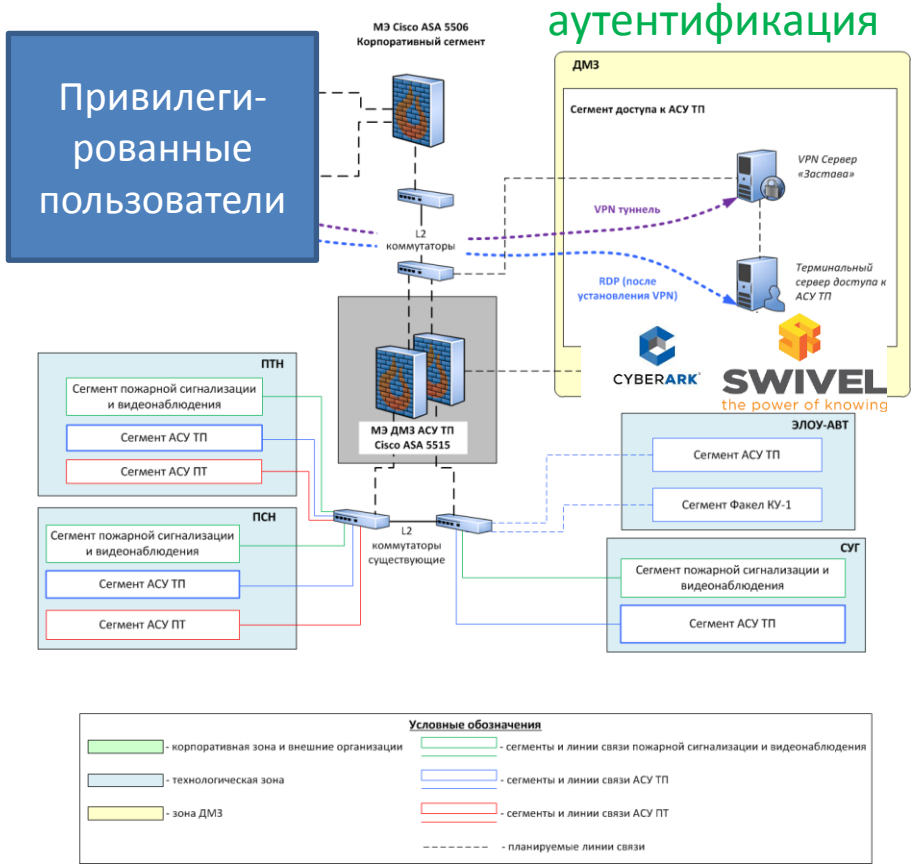
Контроль привилегированных пользователей

Проблема 1: отсутствие контроля действий администраторов и инженеров АСУ ТП со стороны сотрудников служб безопасности

Проблема 2: отсутствие контроля действий субподрядчиков и обслуживающих организаций со стороны сотрудников служб безопасности

Решение ЭЛВИС-ПЛЮС

- Запись сессий
- Двухфакторная аутентификация



Инструментальный анализ защищенности АСУ ТП

- Предоставляем инструменты для анализа защищенности (организация тестовой зоны)
- Проводим работы на сдаваемых в промышленную эксплуатацию объектах или в технологические перерывы совместно с сотрудниками предприятия
- Дальнейшие работы сотрудники предприятия могут проводить самостоятельно
- Оказываем консультационную поддержку

ОРД

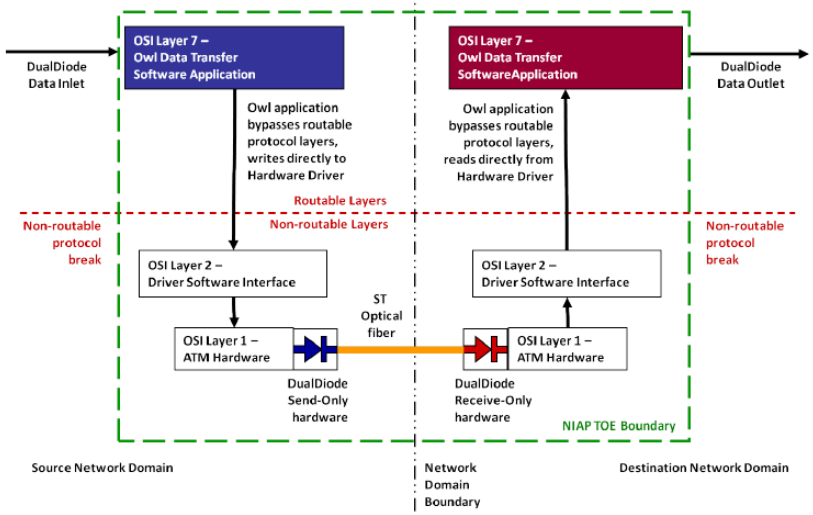
- Политика ИБ АСУ ТП
- Документы для организации системы защиты АСУ ТП в соответствии с (по результатам аудита)

  приказом ФСТЭК России от 14 марта 2014 г. № 31 «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

НИОКР (ОКР)

Темы исследований

- Однонаправленная передача данных (по OPC)
- Защита целостности информации в базах данных (интеграция с SIEM)



Ваши вопросы?

Стефанов Руслан