Стратегия защиты информации в АСУТП

Докладчик:
Шамсутдинов Марат Масгутович
Эксперт
Информационная безопасность и техническая защита

КОД ИБ УФА
08.02.2018

Стратегия защиты информации в АСУТП

ЦЕЛИ

- Беспрерывная и безаварийная работа АСУТП
- Достоверность информации в АСУТП
- Соответствие требованиям федерального законодательства

ЗАДАЧИ

- Создание системы управления ИБ АСУТП, как части общей СУИБ Предприятия
- Учет, классификация, определение угроз безопасности и системы защиты каждой АСУТП
- Обеспечение безопасности периметра сети АСУТП и разграничение зон ответственности обслуживающего персонала.

Руководящие документы

1	Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"
2	Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"
3	"Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации" (утв. Президентом РФ 03.02.2012 N 803)
4	Приказ ФСТЭК России от 14.03.2014 N 31 (ред. от 23.03.2017) "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"
5	Документы ФСТЭК России в области КСИИ (см. слайд 4)
6	Стандарт ISA/IEC 62443 Industrial Automation and Control Systems Security
7	Рекомендации NIST SP 800-82 «Guide to Industrial Control Systems Security»

Руководящие документы.
Документы ФСТЭК России в области КСИИ

5.1	«Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007)
5.2	«Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007)
5.3	«Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007)
5.4	«Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007)
5.5	«Положение о реестре ключевых систем информационной инфраструктуры» (утв. приказом ФСТЭК России от 04.03.2009 года №74)

**Указанные на слайде документы ФСТЭК России имеют гриф ДСП.*

***Не путать с КИИ!*

Стратегия защиты информации в АСУТП

Автоматизированная система управления производственными и технологическими процессами

– это комплекс аппаратных и программных средств, информационных систем и информационно-телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса.

Требования к обеспечению защиты информации в АСУТП, утвержденные приказом ФСТЭК России от 14 марта 2014 г. №31

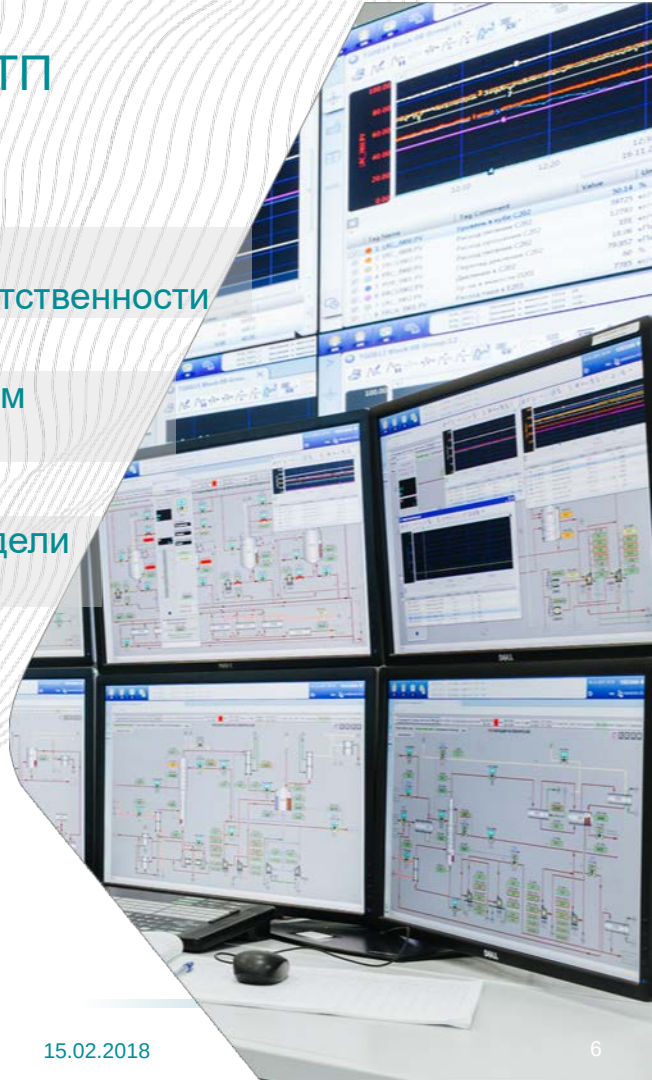
Ст.3 Действие настоящих требований распространяется на автоматизированные системы управления, обеспечивающие контроль и управление технологическим и (или) производственным оборудованием (исполнительными устройствами) **и реализованными на нем технологическими и (или) производственными процессами** (в том числе системы диспетчерского управления, системы сбора (передачи) данных, системы, построенные на основе программируемых логических контроллеров, распределенные системы управления, системы управления станками с числовым программным управлением).

Организационные меры защиты информации в АСУТП

1. Назначить ответственное лицо/подразделение за обеспечение информационной безопасности в АСУТП. Разделить зоны ответственности

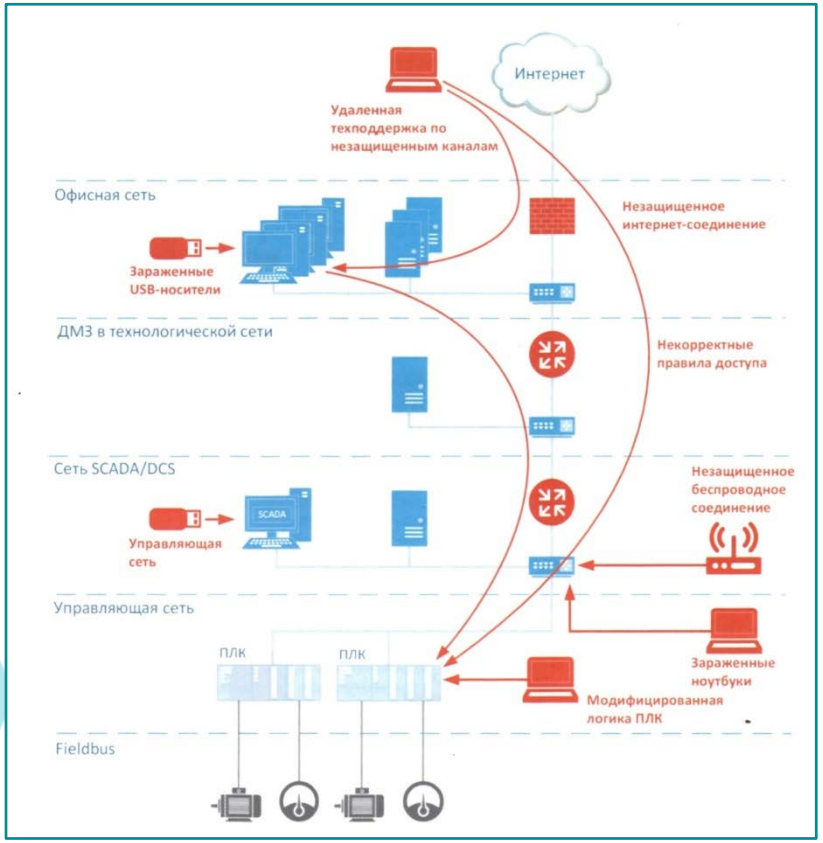
2. Инвентаризация АСУТП. Создание и поддержание в актуальном состоянии перечня АСУТП. Классификация АСУТП;

3. Определение угроз безопасности информации, разработка модели угроз безопасности;



**В части организационных мер необходимо руководствоваться требованиями методических и распорядительных документов ФСТЭК России.*

Технические меры. Ландшафт угроз



См. подробнее

Спецраздел журнала InformationSecurity № 2, май 2017

http://www.itsec.ru/imag/insec-2-2017/

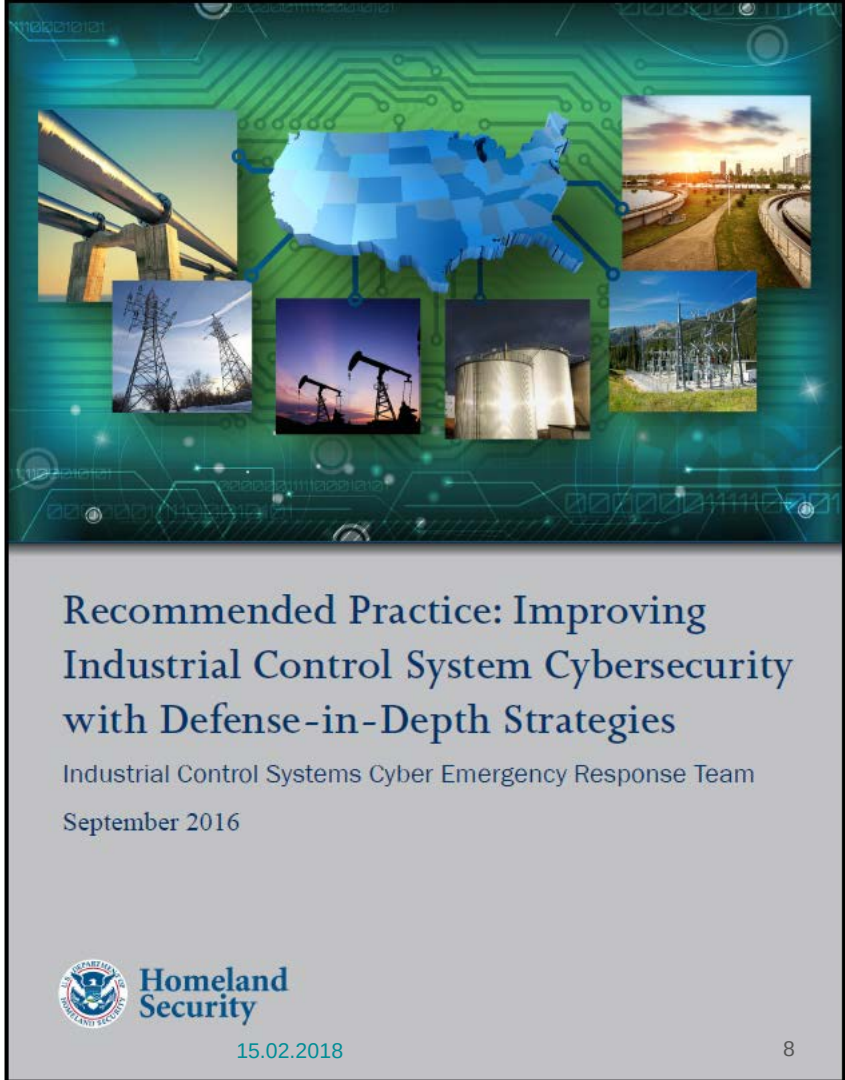
Технические меры. Defense-In-Depth

Стратегия защиты в глубину.

(*см. https://ics-cert.us-cert.gov/Recommended-Practices*)

Технические элементы стратегии:

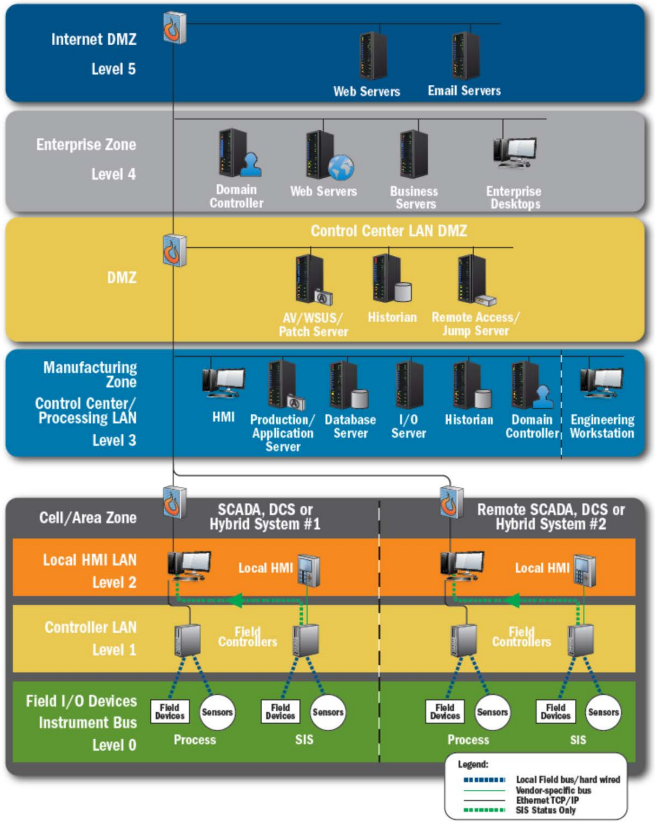
1. Физическая безопасность элементов АСУТП;
2. Безопасная архитектура технологической сети;
3. Защита периметра технологической сети;
4. Защита хостов, АРМов;
5. Мониторинг состояния и событий безопасности.

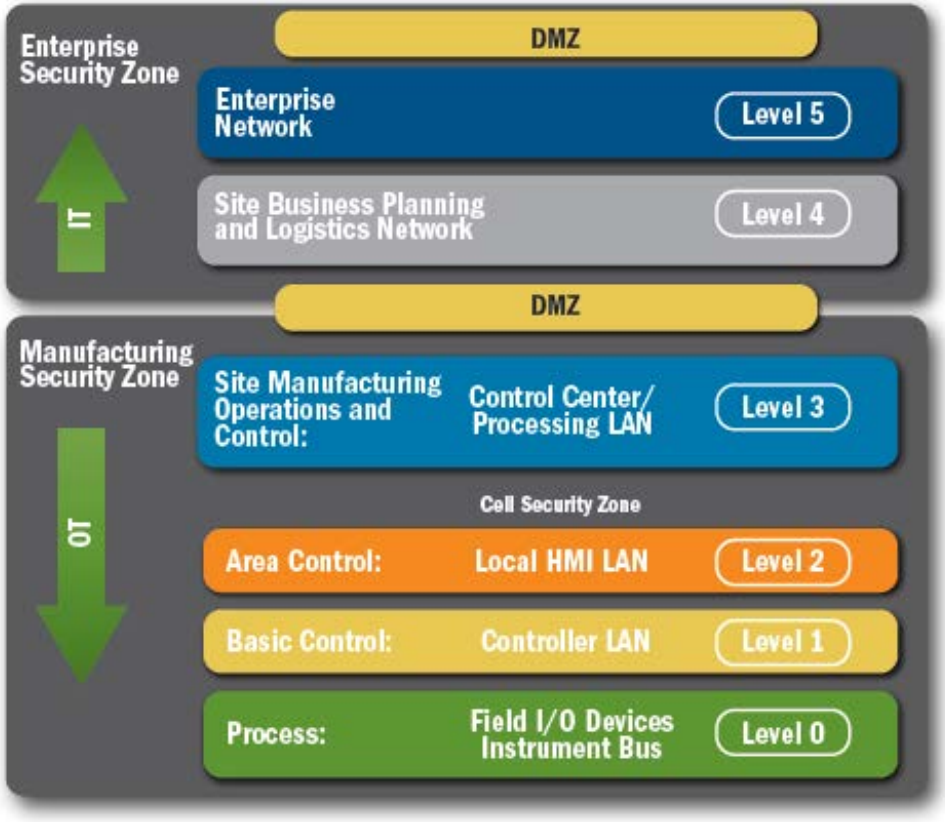


Физическая безопасность элементов АСУТП.

1	Контроль доступа на объекты и к элементам АСУТП
2	Контроль доступа в контроллерные комнаты АСУ и в серверные помещения
3	Многофакторная аутентификация для физического доступа (карта + пин-код)
4	Мониторинг объектов с использованием систем видеонаблюдения и сигнализации
5	Настройка сигнализации на элементах АСУТП на различные события, такие как: отключение питания, перезагрузка устройства, переподключение кабелей, потеря связи, подключение съемных носителей
6	Постоянное сопровождение посетителей и внешнего обслуживающего персонала

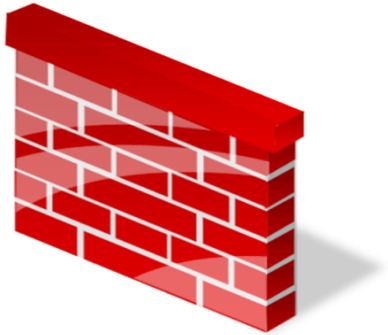
Архитектура технологической сети



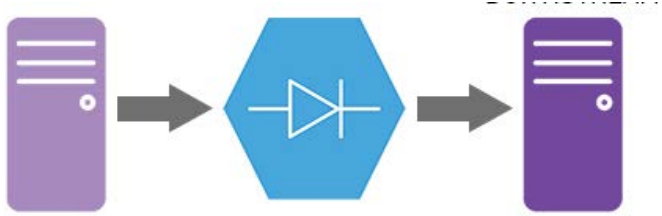


Защита периметра технологической сети

Firewall



Data Diode



Контроль аутентификации и доступа

Bring-Your-Own-Device

Защита хостов, АРМов

Применяем правила защиты АРМов в АСУТП, аналогичные правилам в ИТ, но с некоторыми особенностями:

- Ориентация на использование белых списков. На АРМ все приложения, функции и порты, которые не нужны для конкретной задачи АРМ, должны быть удалены или выключены
- Антивирусное ПО устанавливать только после тестирования на совместимость. Ориентация работы АВ в первую очередь на контроль изменений АРМ
- Максимальное ограничение прав пользователей
- Установка системных обновлений. Постоянно, но обязательно после тестирования

***ПЛК и другие подобные устройства не поддерживают большинство защитных механизмов из ИТ и их защита должна обеспечиваться на уровне сети.**

Мониторинг состояния сети и событий безопасности

Мониторинг состояния сети и событий безопасности обеспечивается тремя основными системами:

- Системы обнаружения и предотвращения вторжений (IDS/IPS)
- Журналы безопасности (Логи)
- Системы класса SIEM

СПАСИБО ЗА ВНИМАНИЕ

E-mail: ShamsutdinovMM@polief.sibur.ru

Благовещенская площадка СИБУРа - АО «ПОЛИЭФ»
Тел: +7 (347) 279-75-24, (34766) 2-12-21
E-mail: inbox@polief.sibur.ru
www.sibur.ru/polief