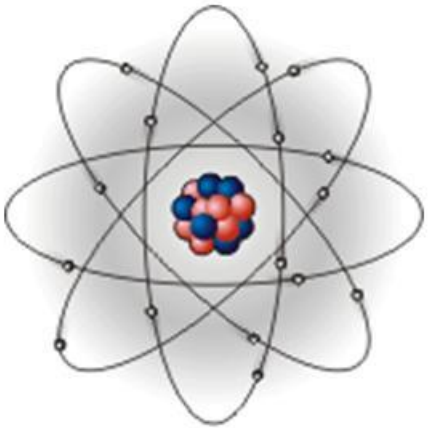
Кибербезопасность АСУ ТП АЭС

infosecurity RUSSIA
20–22 Сентября 2016
КРОКУС ЭКСПО, МОСКВА

Подольный Вадим Павлович

Группа «Киербезопасность АСУ ТП»

КБ АСУ ТП АЭС. Статистика (на конец 2015 г.)



Атомная энергетика доступна в **30** странах мира;
Суммарно работающих энергоблоков - **450**;
Общая мощность энергоблоков - **387 Гвт**;
Доля атомной энергетики в мире = до **11%;**
Доля атомной энергетики в России = **17% (177 млрд кВт·ч);**
Средняя мощность реактора = **850 МВт**;
Сооружается энергоблоков — **60** (20 Китай);
Общая мощность сооружаемых энергоблоков **59** Гвт;
Средняя мощность новых реактора = **1100 МВт**;
Необходимое количество урана в год — около **80 000 тонн;**
1 кг закиси урана U3O8 = примерно **90$ за кг = 7,2$ млрд в год**;
Стоимость сооружения АЭС = от **1.5-3.0 млрд за ЭБ** без инфраструктуры (+50%);
Затраты на АСУ ТП = порядка **10% от стоимости АЭС** без инфраструктуры (с оговоркой, что оборудование включает компоненты АСУ + НИОКР);
Защита АСУ ТП обойдется в **10% от затрат на АСУ ТП** = **15-30 Млн на ЭБ**.
Оценка до **2050** г. построят АЭС мощностью до **1000 Гвт (рост в 3 раза);**
До 2050 г. объем рынка КБ АСУ ТП АЭС составит до 30$ Млрд ~ 1$ Млрд в год.

КБ АСУ ТП АЭС. Статистка. ТОП 10 стран с АЭ (+ Япония)

	АЭС	ЭБ	ЭБ. Выкл.	ЭБ Стр.	Мощ-ь,МВт текущая	млрд кВт·ч/год (2015)	% выработки
США	62	100	32/1	4	100 350	797	20
Франция	19	58	12	1	63 130	416	77
Япония	*17*	*48/43*	*10/6*	*2*	*40 290*	*4*	*30/0*
Китай	11	36	0	20	31 402	170	3
Россия	10	40	5	7	24 654	195	19
Южная Корея	6	25	0	3	20 717	157	31
Канада	5	19	6	0	13 500	98	17
Украина	4	15	4	2	13 107	82	57
Германия	8	9	28	0	10 799	86	14
Швеция	3	10	3	0	9 651	62	42
Великобритания	8	15	30	0	8 818	58	17

КБ АСУ ТП АЭС. Объект защиты. Базовые показатели (РФ)

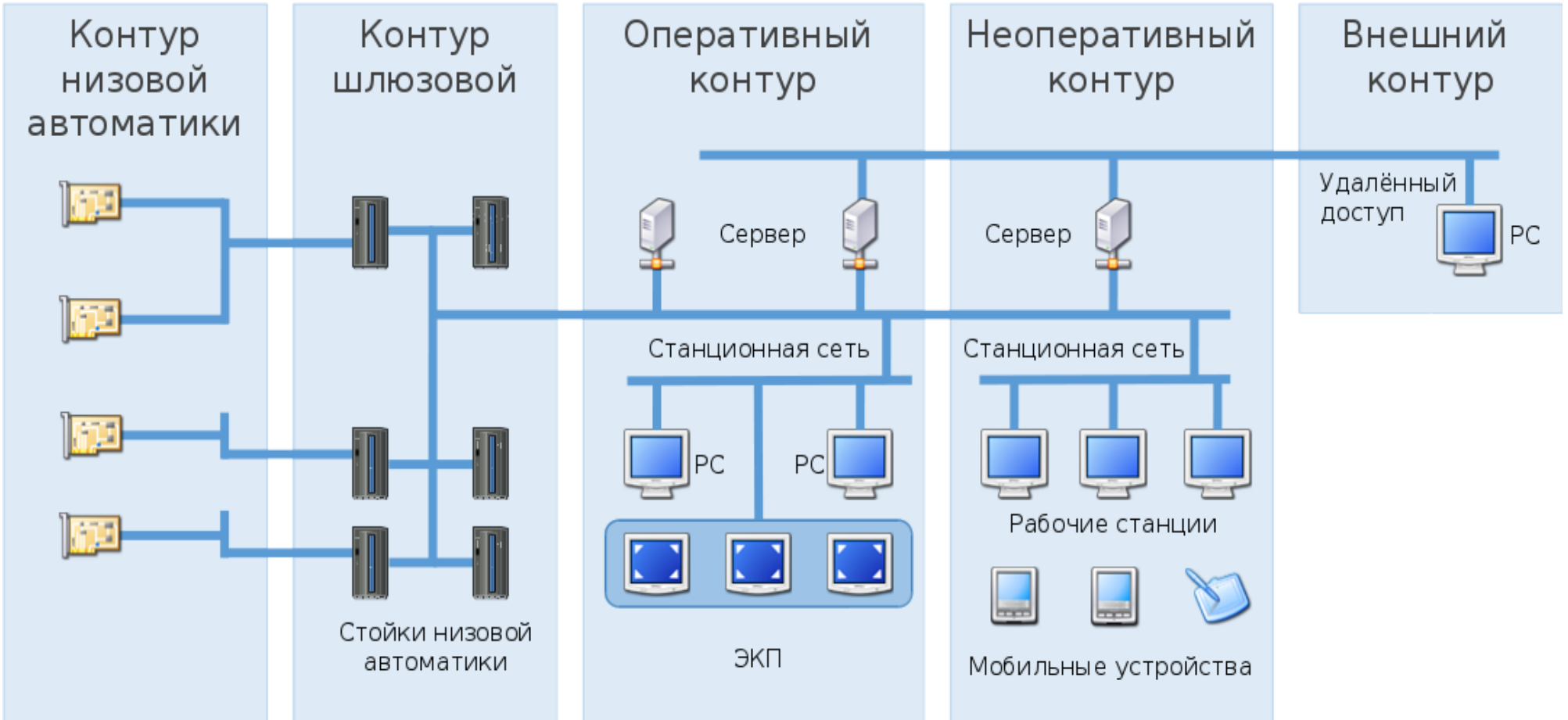
СУБЪЕКТЫ

Персонал — более тысячи человек на энергоблок (1 человек / МВт);
Смена операторов — 3 человека (НСБ, ВИУР, ВИУТ);
Смена обслуживания подсистем — 2 человека на подсистему

ОБЪЕКТЫ

Подсистемы — десятки подсистем АСУ ТП;
Оборудование — сотни поставщиков оборудования;
Источники данных — сотни различного типа контроллеров;
Источники сигналов — десятки тысяч источников сигналов (оборудования);
Динамика изменений — до 200К изменений параметров в секунду (ПРВ);
Надежность доставки — 10E+6 (возможна потеря/ошибка 1 из 10E+6 изменений);

КБ АСУ ТП АЭС. Схема контуров изоляции



КБ АСУ ТП АЭС. Задача обеспечения КБ.

Задача обеспечения кибербезопасности - обеспечение непрерывности, безопасности и эффективности технологических и производственных процессов

КБ АСУ ТП АЭС. КБ АСУ ТП

Кибербезопасность (КБ) являет собой набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты ресурсов КВО и потребителей.

КБ подразумевает достижение и сохранение свойств безопасности у ресурсов КВО или потребителей, направленных против соответствующих киберугроз.

Основными задачами обеспечения КБ считаются: доступность, целостность, включающая достоверность, а также конфиденциальность.

Выделяются следующие типы угроз КБ АСУ ТП:

- Техногенные
  - Не корректные обновления ПО;
  - Замена аппаратного обеспечения;
- Антропогенные
  - Внутренний нарушитель (преднамеренный);
  - Человеческий фактор (непреднамеренный);
- НСД, НДВ
  - Непреднамеренные ошибки в ПО приводящие к НСД;
  - Преднамеренные НДВ в ПО приводящие к НСД и прочим инцидентам;

КБ АСУ ТП АЭС. Методы обеспечения КБ в ЖЦ АСУ ТП

Методы обеспечения КБ различны и применяются:

- при проектировании (Secure By Design);
- при разработки компонентов и подсистем;
- при сопряжении подсистем в систему в целом;
- при подготовке к вводу в эксплуатацию;
- при эксплуатации;
- при планово-предупредительных ремонтах;
- при модернизации;
- при выводе из эксплуатации;

Методы обеспечения КБ позволяют:

- исключить внешнего нарушителя как возможного;
- повысить доверие к аппаратным средствам без наличия РКД и схем;
- обеспечить доверие к аппаратным средствам при наличии РКД и схем;
- повысить доверие к программным компонентам без исходного кода;
- обеспечить доверие к программным компонентам при наличии исходного кода;
- обеспечить доверие к системе в целом состоящей из недоверенных компонентов;

КБ АСУ ТП АЭС. Что делать с КБ

Вариант 1
Стадия проектирования

Проектирование с учетом КБ

Вариант 2
Уже построена

Аудит КБ АСУ ТП

Обеспечение КБ АСУ ТП при проектировании и разработке

Процедура обеспечения КБ непрерывно интегрирована в процесс создания компонентов и АСУ ТП в целом.

Методы обеспечения КБ при проектировании и разработке:

- исследования на НСД, НДВ;
- статический анализ исходного кода;
  исследования на наличие опасных конструкций исходного кода;
- динамический анализ программных компонентов
  маппинг;
  брутфорсинг;
  фаззинг;
  DoS, DDoS;
- сопряжение с интеграционным тестированием;
- сопряжение с нагрузочным тестированием;
- реверс инжиниринг;

Методы обеспечения КБ в период эксплуатации

Необходимые компоненты КБ:

- интеллектуальная система разграничения доступа (СРД);
- подсистема сопряжения СРД со СКУД;
- подсистема сопряжения СРД с биометрическими сенсорами;
- подсистема обеспечения доверия к источникам изменений (контроллерам);
- подсистема обеспечения доверия к серверам, шлюзовым устройствам;
- подсистема обеспечения доверия к РС и терминальным устройствам;
- подсистема обеспечения доверия к сетевому и коммутационному оборудованию;
- подсистема обеспечения доверия трафика;
- подсистема однонаправленной (в т.ч. широковещательной) передачи данных;

Методы обеспечения КБ в период эксплуатации

Необходимые компоненты КБ:

- подсистема зеркалирования трафика;
- промышленная СОПКА (IIDS, IIPS);
- подсистема обнаружения аномалий на базе сигнатурного анализа;
- подсистема обнаружения аномалий на базе статистического анализа;
- подсистема обнаружения аномалий на базе искусственного интеллекта;
- подсистема обнаружения аномалий на базе симулятора (физический принцип);
-
- подсистема отвлечения внимания нарушителя (Honey Pot);

Системы управления КБ:

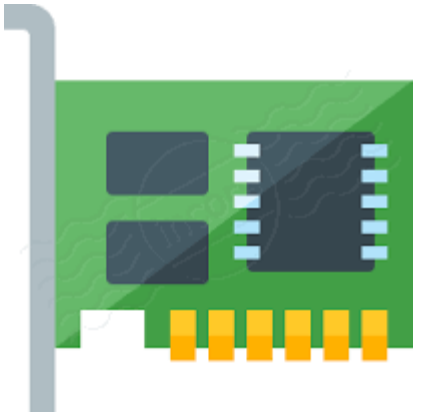
- промышленный мониторинг событий КБ (ISIEM);
- **подсистема сопряжения ISIEM со SCADA;**

Основой безопасности АСУ ТП служат
- базовые защищенные информационные технологии (БЗИТ)

- Доверенные базовые средства ввода/вывода (БСВВ, BIOS) на СВТ;
- Доверенный гипервизор нулевого домена;
- Доверенные ОС с компонентами обеспечения режима РВ;
- Доверенные СУБД;
- Доверенный транспорт данных;
- Доверенное ядро программной платформы АСУ ТП (универсальная промышленная защищенная интеграционная шина);
- Доверенная программная платформа АСУ ТП;
- Доверенные программные проектные модули АСУ ТП;

Аппаратные и программный модули доверенной загрузки (МДЗ)

- МДЗ для серверов;
- МДЗ для рабочих станций;
- МДЗ для терминальных клиентов;
- МДЗ для сетевого оборудования;
- МДЗ для контроллеров и встраиваемых устройств;



План аудита КБ АСУ ТП

- Инвентаризация аппаратного обеспечения (АО), контроллеры, прошивки, версии;
- Инвентаризация СВТ, серверы, РС, ОС, драйверы, ПО, прошивки, версии;
- Сертификаты, документация на АО, соответствие реально установленному АО;
- Порты ввода/вывода АО, не подключено ли что нибудь лишнее;
- План сети. Инвентаризация сетевого оборудования, прошивки;
- Инвентаризация программного обеспечения (ПО), версии;
- Схема работы ПО. Схема деления ПО. РКД, ЭД, ПД. Доля иностранного ПО;
- Учет изменений ПО и АО, сопряжение в систему учета ТОиР;
- Соответствуют ли документация и сертификаты реально установленным версиям;
- Исследование объекта в целом, сканнирование, фаззинг, пентесты;
- Ввод в действие системы мониторинга событий ИБ и сбор информации о системе;
- Модель угроз, модель нарушителя, модель защиты;
- План обеспечения КБ АСУ ТП, план аттестации объекта и подрядчиков;
- План обучения персонала;

Повышение КБ путем импортозамещения может быть обеспечено путем:

- Снижения зависимости от импорта компонентов АСУ;
- Повышения технологической независимости отрасли;
- Унификации программно технических средств;
- Межотраслевого взаимодействия и применения опыта;

Это обеспечит:

- Снижение издержек на проектирование и эксплуатацию;
- Поддержку отечественных производителей компонентов АСУ ТП;
- Технологический задел для возможности экспорта наработок;
- Формирование новых рабочих мест;
- Поддержку системы образования в ВУЗ;





Спасибо за внимание!

Вадим Подольный
vadim.podolniy@gmail.com
+7 916 530 46 56

Группа Кибербезопасность АСУ ТП в Facebook